Cisco live!

January 29 – February 2, 2018 · Barcelona

BRKCRS-2810

Software Defined Access

Under The Hood

Shawn Wargo

Principal Engineer - Technical Marketing

Cisco live!

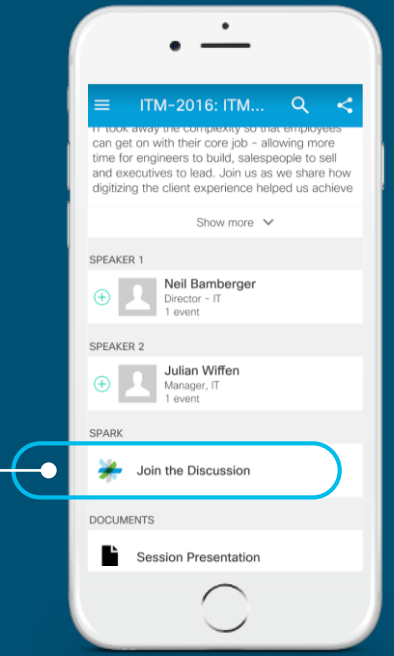
Cisco Spark

Questions?

Use Cisco Spark to communicate with the speaker after the session

How

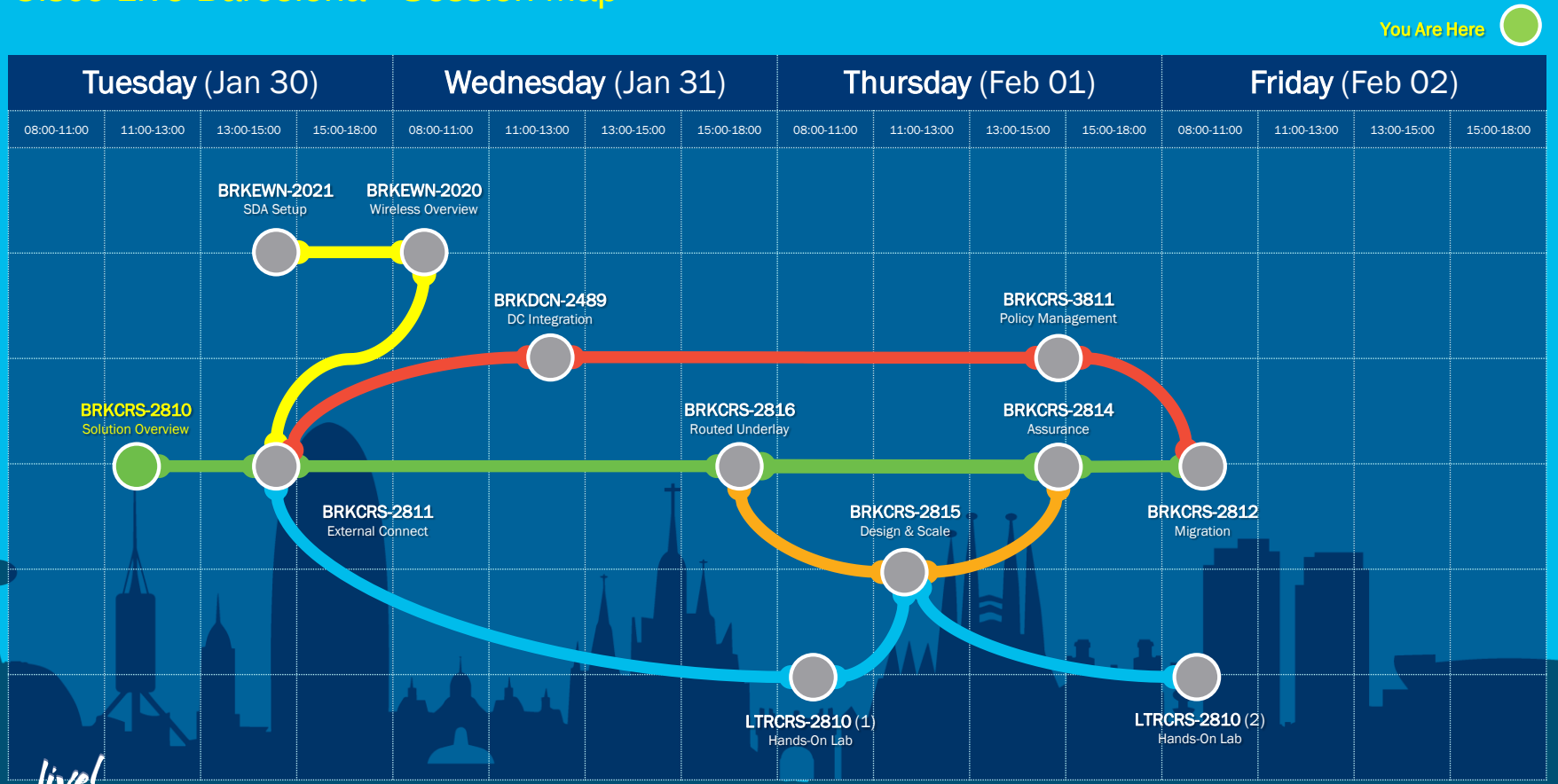
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space



cs.co/ciscolivebot#BRKCRS-2810

Software Defined Access

Cisco Live Barcelona - Session Map



Session Agenda

1. **Key Benefits**
   Why do you care?
2. **Key Concepts**
   What is SD-Access?
3. **Fabric Fundamentals**
   How does it work?
4. **Controller Fundamentals**
   How does it work?
5. **Take Away**
   Where to get started?

Key Benefits

Why do you care?

New Requirements for the Digital Age

Insights & Actions

Automation & Assurance

Security & Compliance

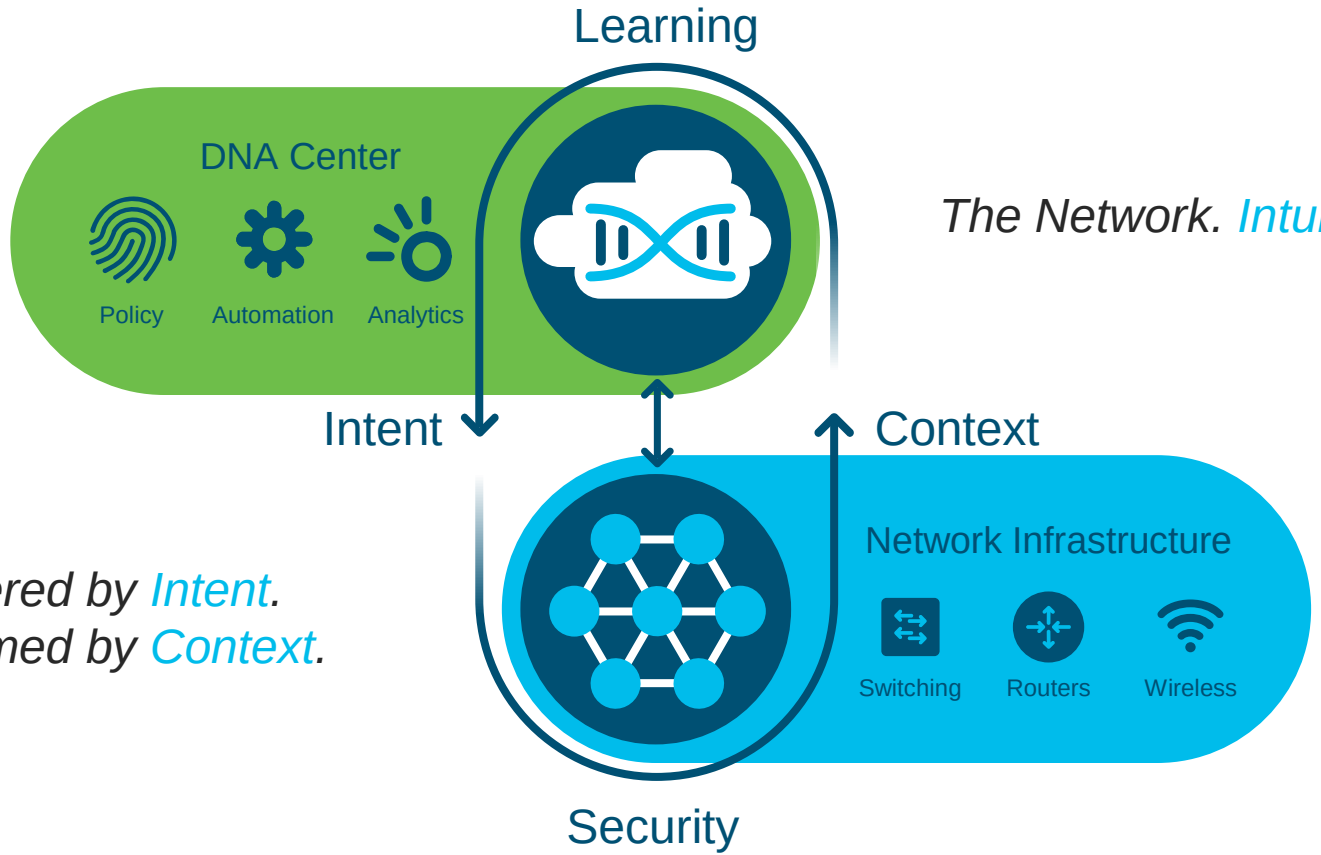
Innovate FASTER

REDUCE
Cost & Complexity

LOWER Risk

Cisco Digital Network Architecture (DNA)

Cisco's Intent-based Networking

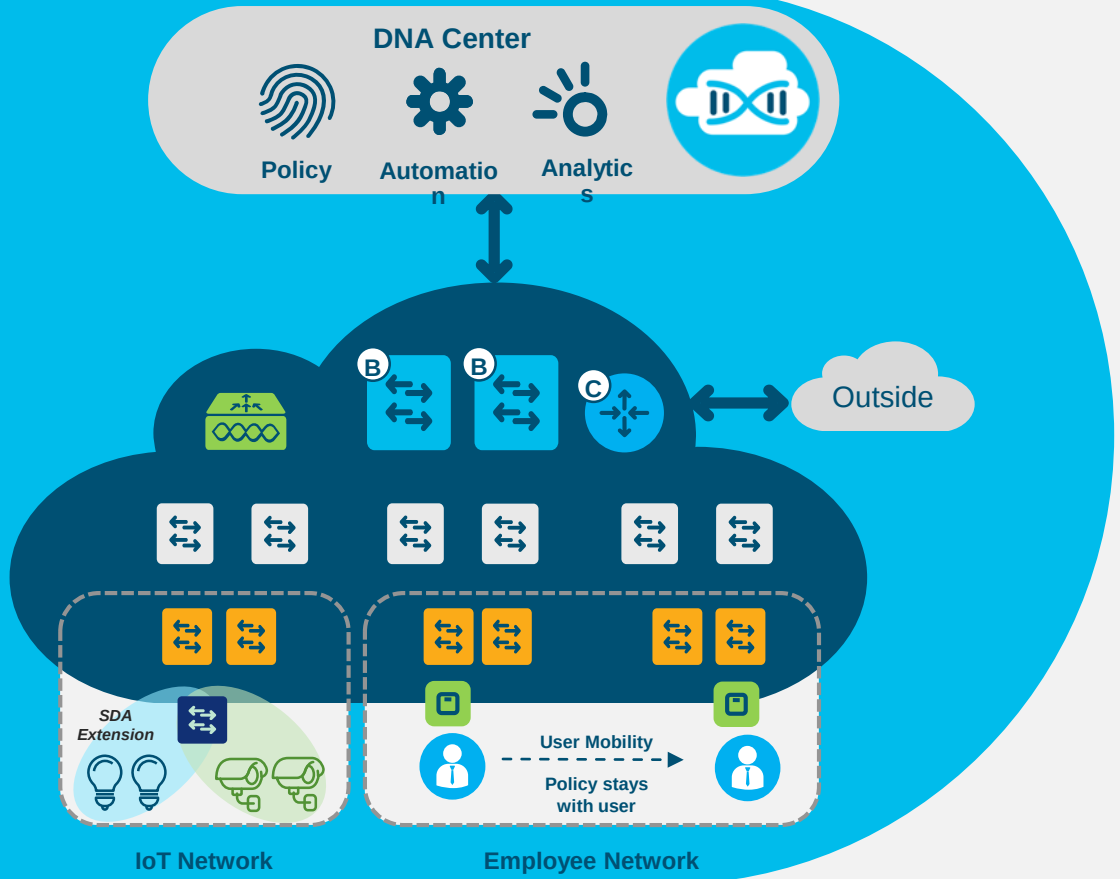


The Network. Intuitive.

Powered by Intent.
Informed by Context.

Software Defined Access

Networking at the speed of Software!



Identity-Based Policy & Segmentation

Decoupled security policy from VLAN and IP Address

Automated Network Fabric

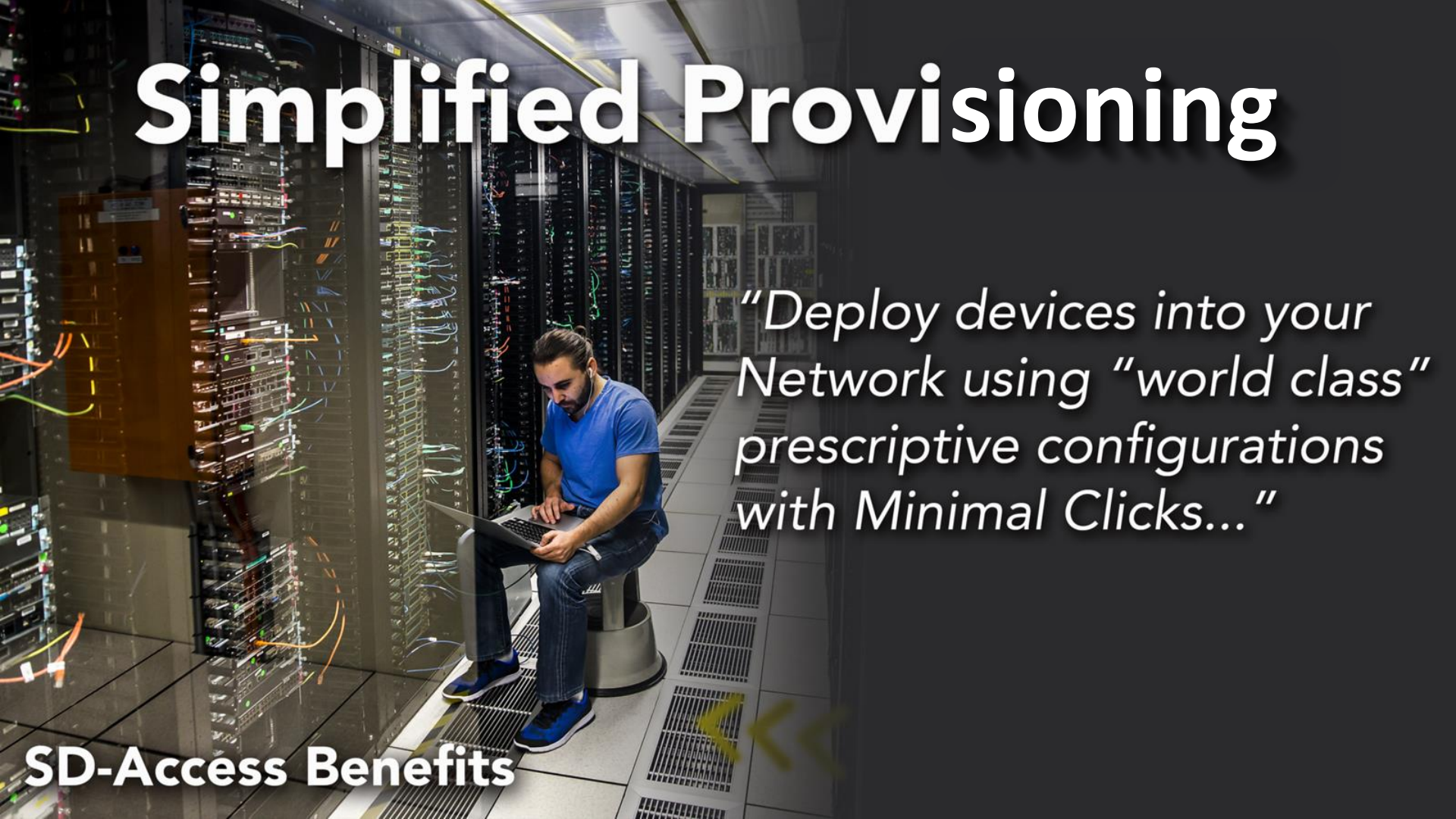
Single Fabric for Wired & Wireless with workflow Automation

Insights & Telemetry

Analytics and Insights into User and Application behavior

Streamlined Design

"Create site hierarchy, build out wireless heat maps and formulate reusable network profiles for your device provisioning... "

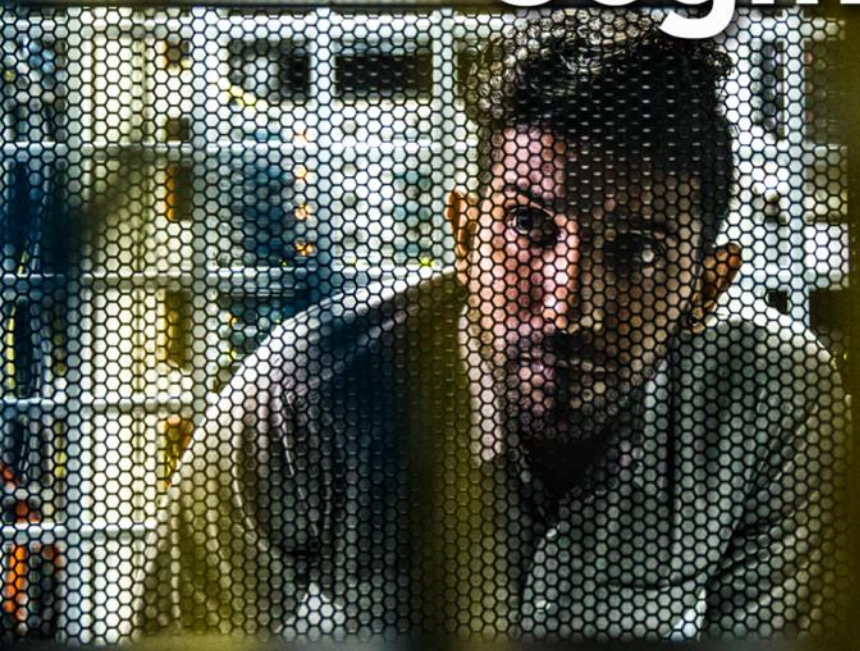


Simplified Provisioning

"Deploy devices into your Network using "world class" prescriptive configurations with Minimal Clicks..."

SD-Access Benefits

Segmentation



"Virtual Networks and Micro-Segmentation made simple to more effectively secure boundaries between user and device groups..."


Policy Enforcement
"Assigned policy follows users and devices irrespective of location or place in network..."
SD-Access Benefits

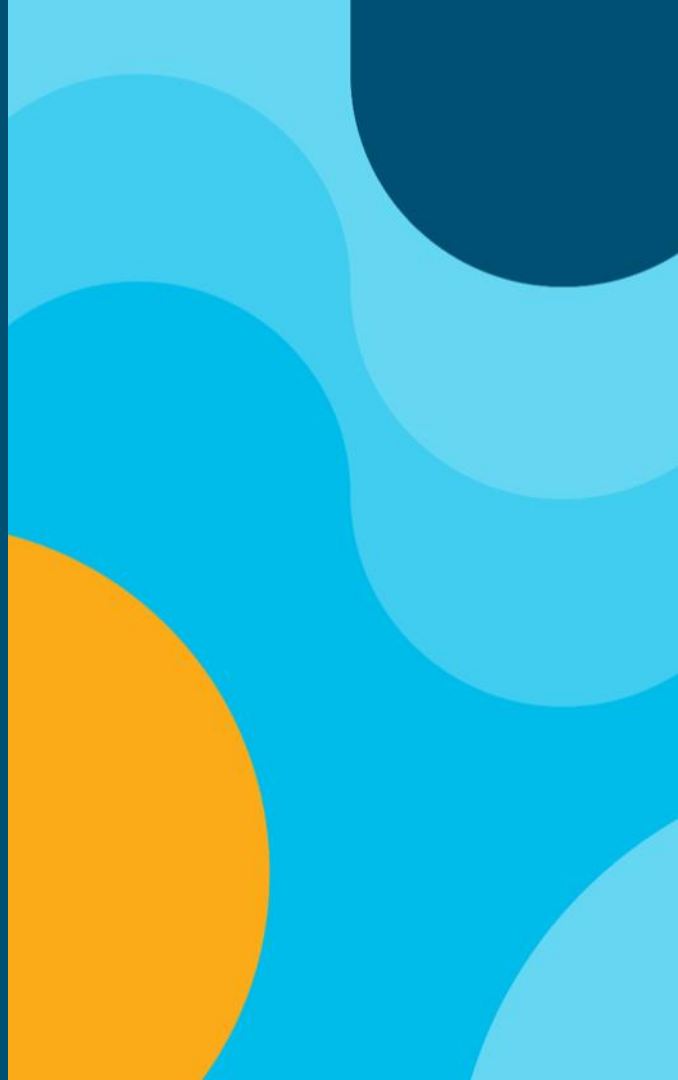
Insights & Telemetry

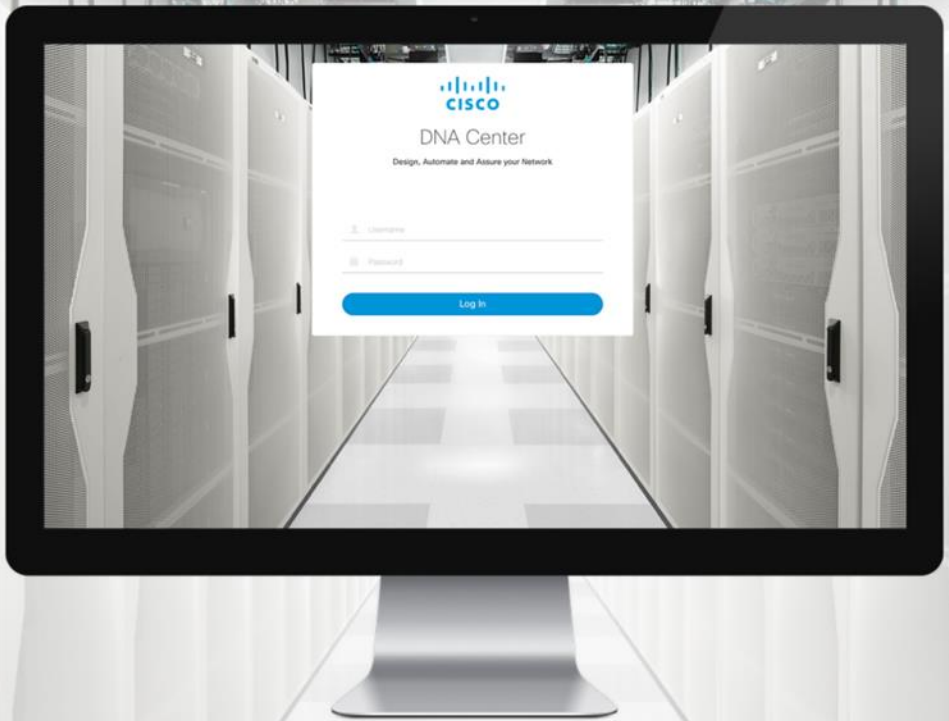
"Proactive issue identification and resolution through analytics and insights into User and Application behavior..."

SD-Access Benefits

Key Concepts

What is Software Defined Access?

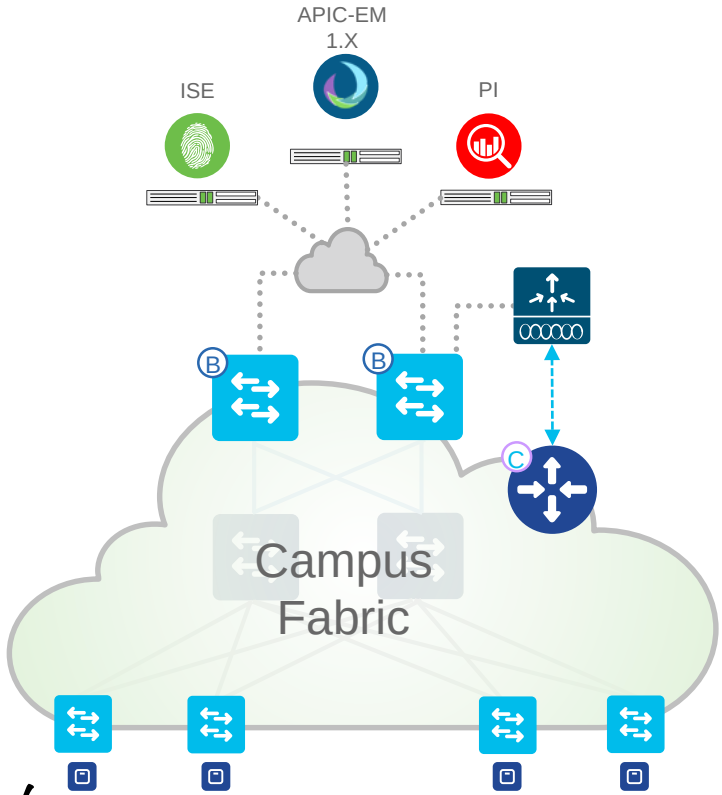




What is SD-Access?

What is SD-Access?

Campus Fabric + DNA Center (Automation & Assurance)



- **Campus Fabric**

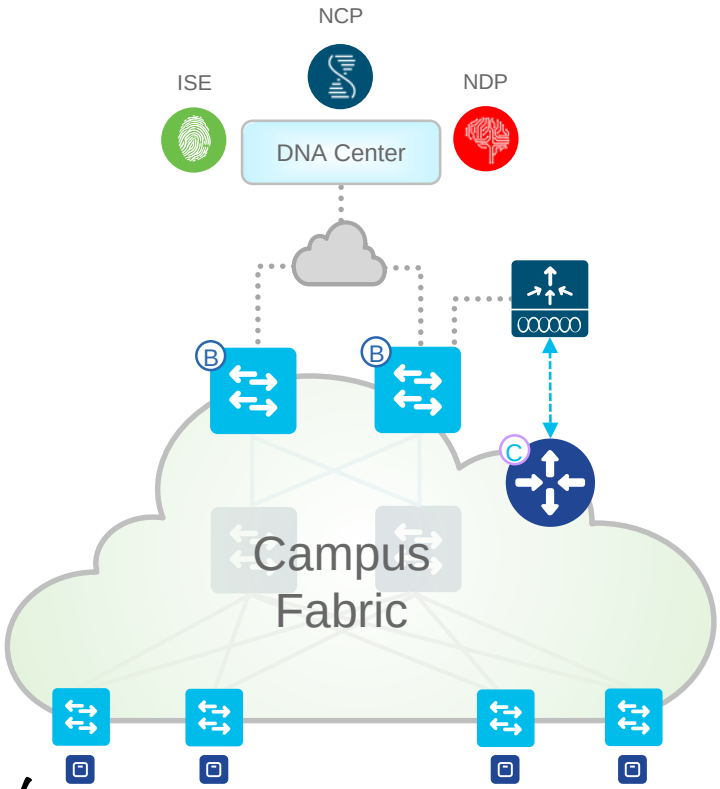
  CLI or API approach to build a LISP + VXLAN + CTS Fabric overlay for your enterprise Campus networks

  CLI provides backwards compatibility but management is box-by-box. API provides device automation via NETCONF/YANG

  Separated management systems

What is SD-Access?

Campus Fabric + DNA Center (Automation & Assurance)



- **SD-Access**

  GUI approach provides automation & assurance of all Fabric configuration, management and group-based policy

  DNA Center integrates multiple systems, to orchestrate your LAN, Wireless LAN and WAN access

- **Campus Fabric**

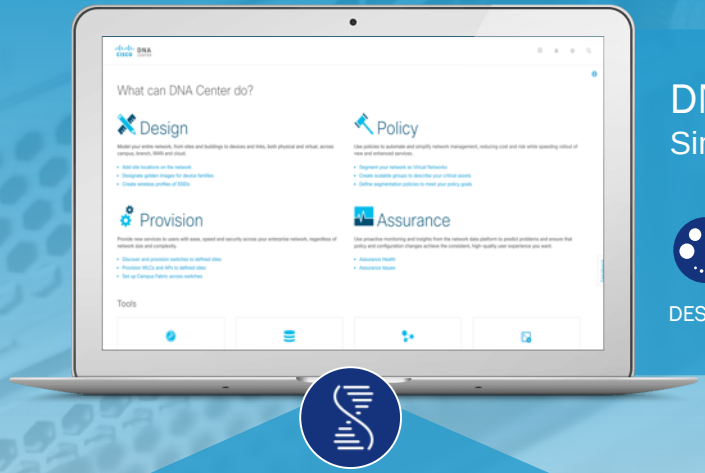
  CLI or API approach to build a LISP + VXLAN + CTS Fabric overlay for your enterprise Campus networks

  CLI provides backwards compatibility but management is box-by-box. API provides device automation via NETCONF/YANG

  Separated management systems

DNA Solution

Cisco Enterprise Portfolio



DNA Center

Simple Workflows

DESIGN — PROVISION — POLICY — ASSURANCE

DNA Center

Identity Services Engine — Network Control Platform — Network Data Platform

Routers

Switches

Wireless Controllers

Wireless APs

Roles & Terminology

What is Software Defined Access?

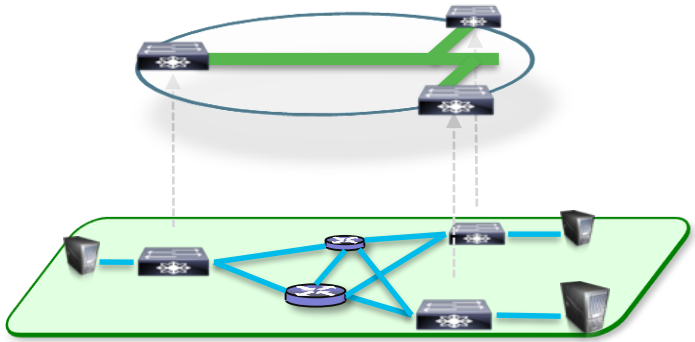
1. High-Level View
2. Roles & Platforms
3. Fabric Constructs

A **Fabric** is an **Overlay**

An ***Overlay network*** is a ***logical topology*** used to *virtually connect* devices, built ***over*** an arbitrary physical *Underlay* topology.

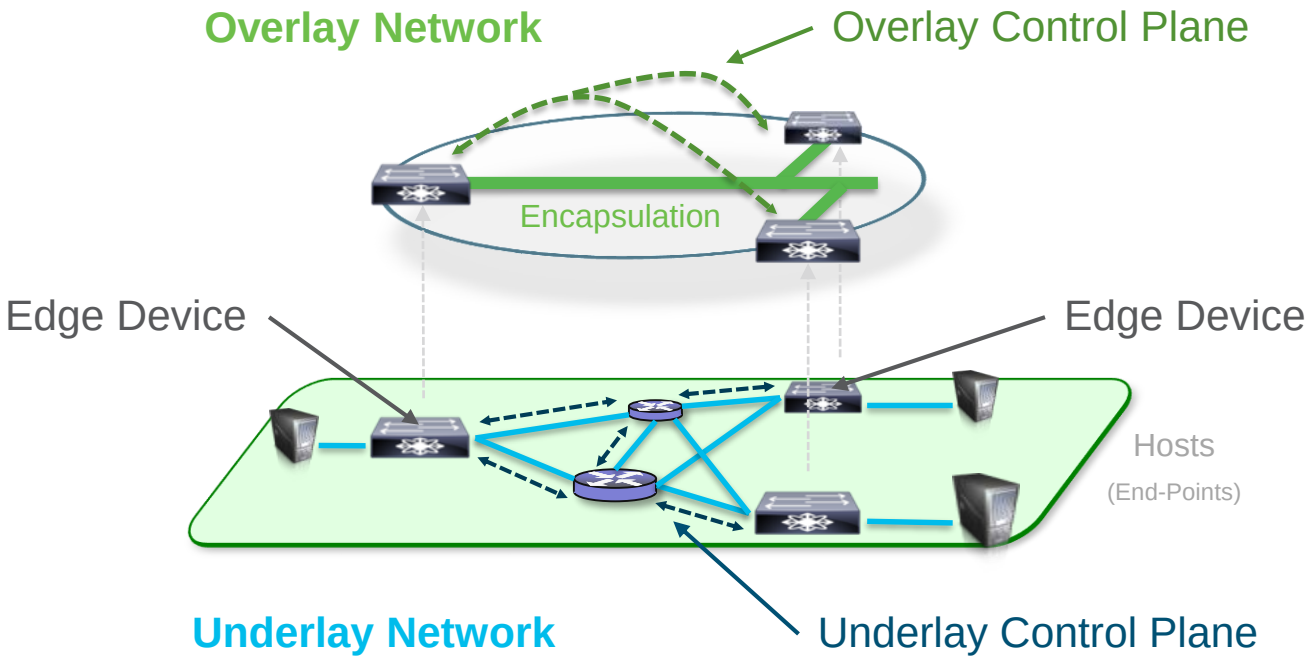
An ***Overlay network*** often uses ***alternate forwarding attributes*** to provide ***additional services***, not provided by the *Underlay*.

Examples of Network Overlays	
• GRE, mGRE	• LISP
• MPLS, VPLS	• OTV
• IPSec, DMVPN	• DFA
• CAPWAP	• ACI



SD-Access

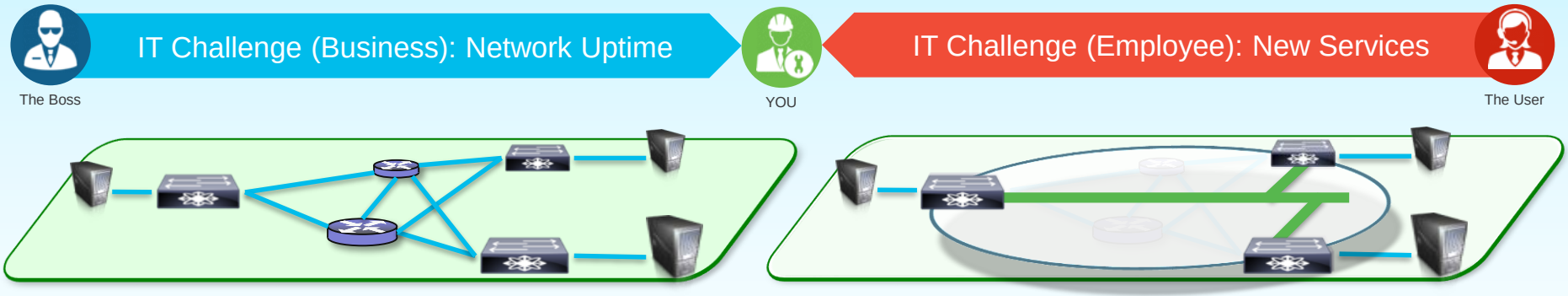
Fabric Terminology



SD-Access

Why Overlays?

Separate the "Forwarding Plane" from the "Services Plane"



Simple Transport Forwarding

- Redundant Devices and Paths
- Keep It Simple and Manageable
- Optimize Packet Handling
- Maximize Network Reliability (HA)

Flexible Virtual Services

- Mobility - Map Endpoints to Edges
- Services - Deliver using Overlay
- Scalability - Reduce Protocol State
- Flexible and Programmable

SD-Access

Fabric Underlay – Manual vs. Automated

Manual Underlay

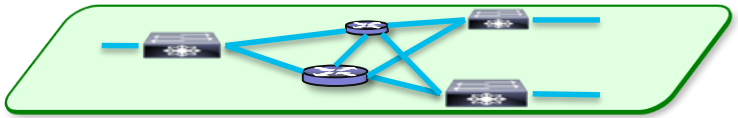
You can reuse your existing IP network as the Fabric Underlay!

- **Key Requirements**
  - IP reach from Edge to Edge/Border/CP
  - Can be L2 or L3 – We recommend L3
  - Can be any IGP – We recommend ISIS
- **Key Considerations**
  - MTU (Fabric Header adds 50B)
  - Latency (RTT of =/< 100ms)

Automated Underlay

Fully automated prescriptive IP network Underlay Provisioning!

- **Key Requirements**
  - Leverages standard PNP for Bootstrap
  - Assumes New / Erased Configuration
  - Uses a Global “Underlay” Address Pool
- **Key Considerations**
  - Seed Device pre-setup is required
  - 100% Prescriptive (No Custom)



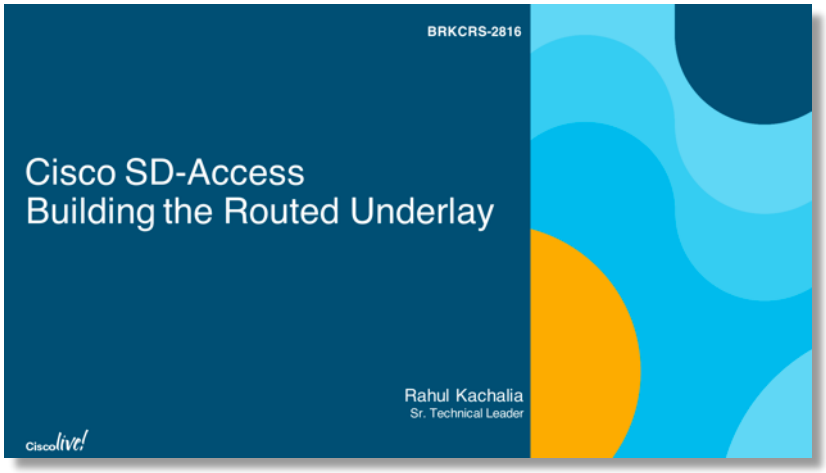
Would you like to know more?

Routed Underlay

Check out the following session:

BRKCRS-2816

SD-Access - Building the Routed Underlay



This session covers:

- More details about Fabric Underlay
- How to automate Underlay setup
- Underlay best practices and tips

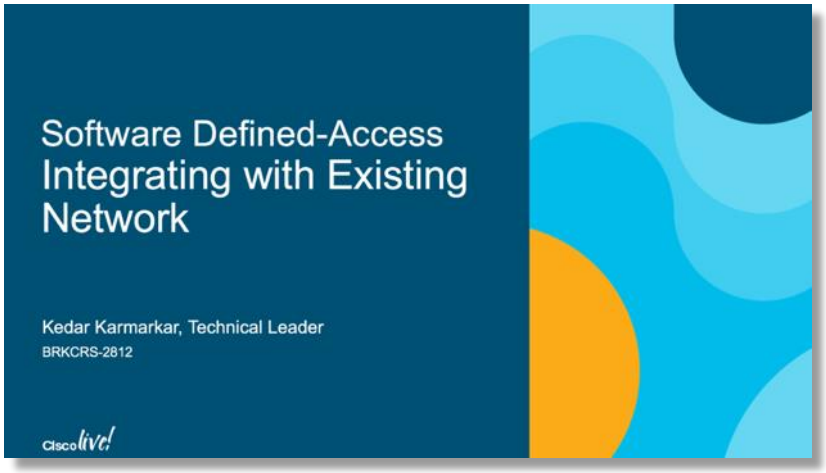
Would you like to know more?

Routed Underlay

Check out the following session:

BRKCRS-2812

SD-Access - Integrating with Existing Network

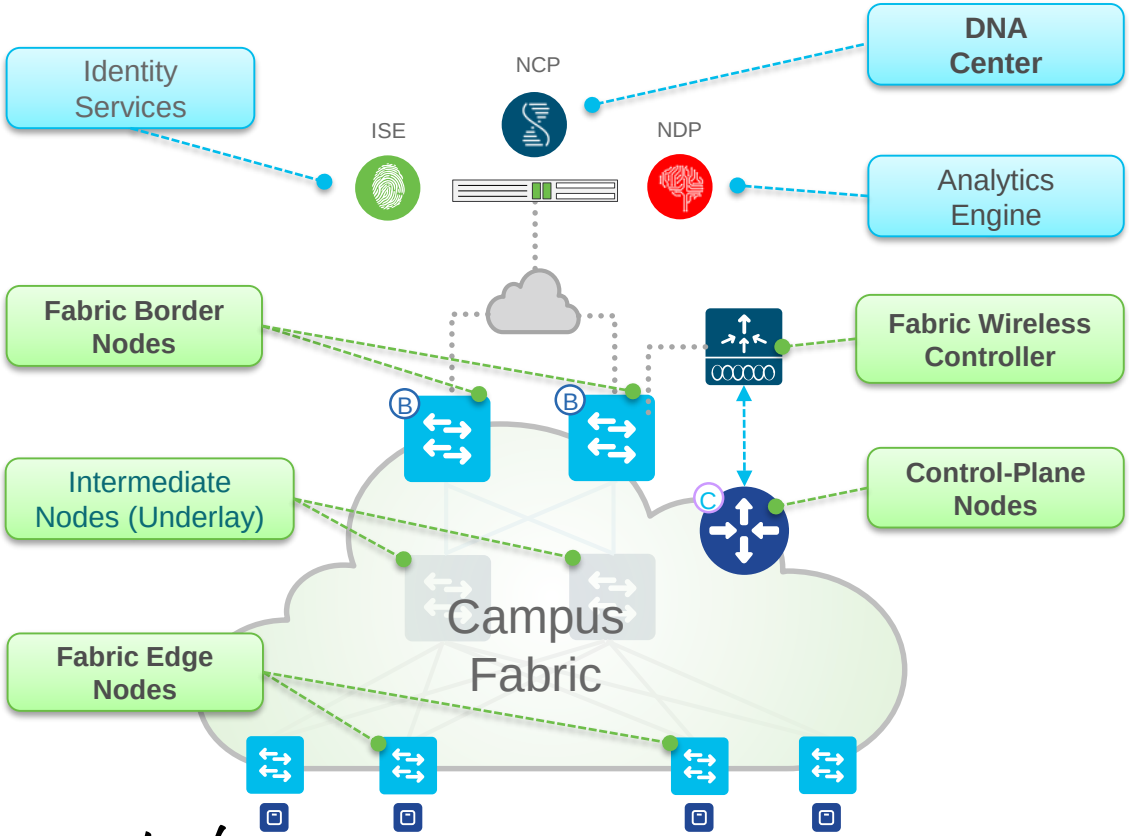


This session covers:

- More details about Fabric Underlay & Overlay
- How to migrate legacy networks to SD-Access
- Various SD-Access design approaches

SD-Access

Fabric Roles & Terminology



- **DNA Center** – Enterprise SDN Controller provides GUI management and abstraction via Apps that share context
- **Identity Services** – NAC & ID Systems (e.g. ISE) for dynamic Endpoint to Group mapping and Policy definition
- **Analytics Engine** – Data Collectors (e.g. NDP) analyze Endpoint to App flows and monitor fabric status
- **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 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 APs and Wireless Endpoints to the SDA Fabric

Roles & Terminology

What is Software Defined Access?

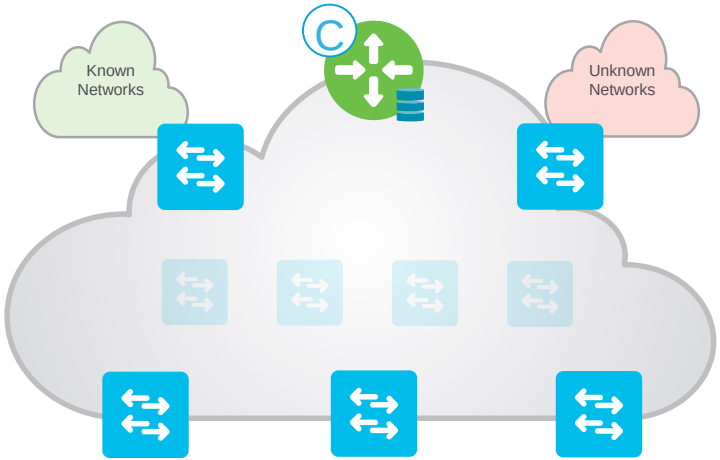
1. High-Level View
2. Roles & Platforms
3. Fabric Constructs

SD-Access Fabric

Control-Plane Nodes – A Closer Look

Control-Plane Node runs a Host Tracking Database to map location information

- A simple Host Database that maps Endpoint IDs to a current Location, along with other attributes
- Host Database supports multiple types of Endpoint ID lookup types (IPv4, IPv6 or MAC)
- Receives Endpoint ID map registrations from Edge and/or Border Nodes for “known” IP prefixes
- Resolves lookup requests from Edge and/or Border Nodes, to locate destination Endpoint IDs



SD-Access Platforms

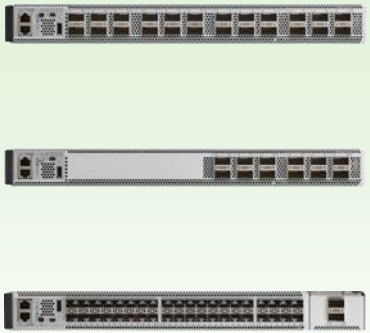
Control-Plane Nodes

Catalyst 3K

- Catalyst 3850
- 1/10G SFP
- 10/40G NM Cards
- IOS-XE 16.6.2+

Catalyst 9K

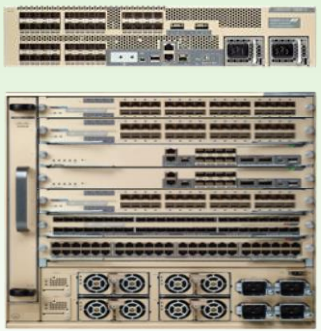
NEW



- Catalyst 9500
- 10/40G SFP/QSFP
- 10/40G NM Cards
- IOS-XE 16.6.2+

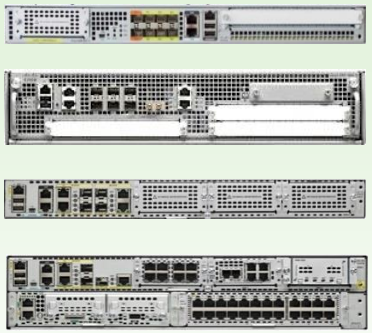
Catalyst 6K*

* Wired Only



- Catalyst 6800
- Sup2T/6T
- 6840/6880-X
- IOS 15.4.1SY4+

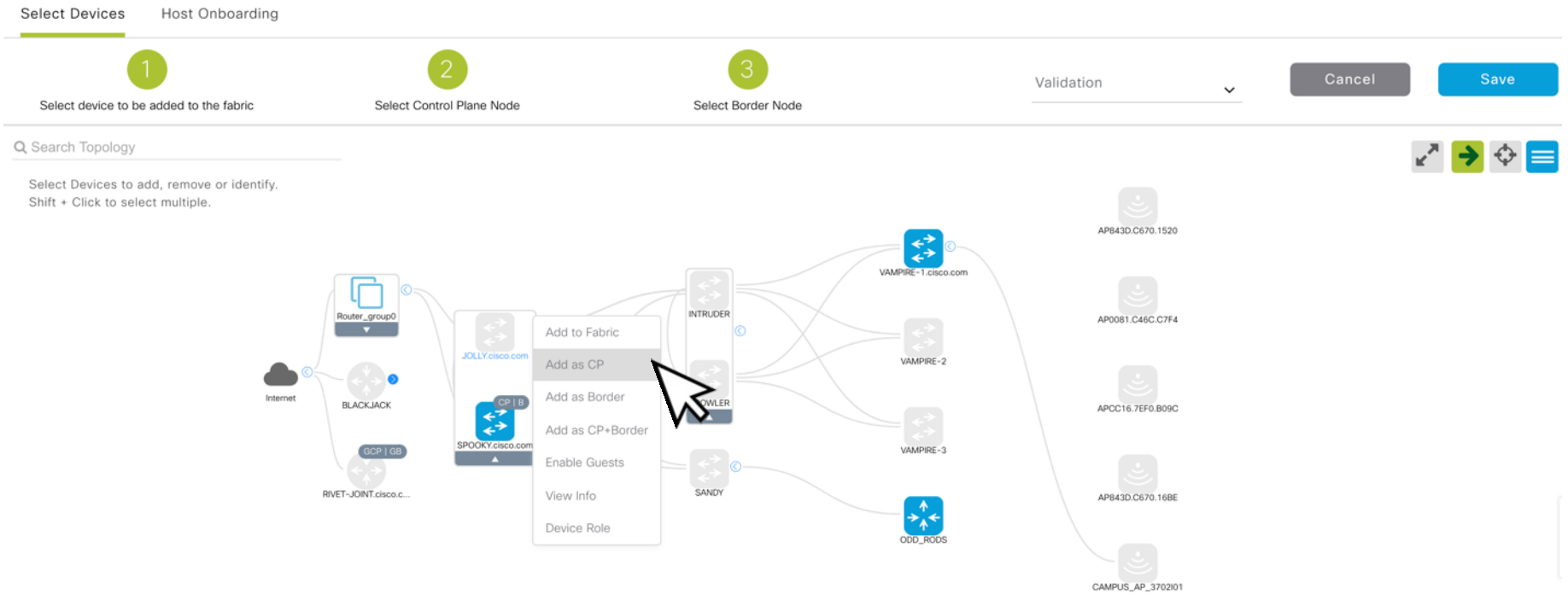
ASR1K, ISR4K & CSRv



- CSRv
- ASR 1000-X/HX
- ISR 4300/4400
- IOS-XE 16.6.2+

SD-Access @ DNA Center

Control-Plane Nodes

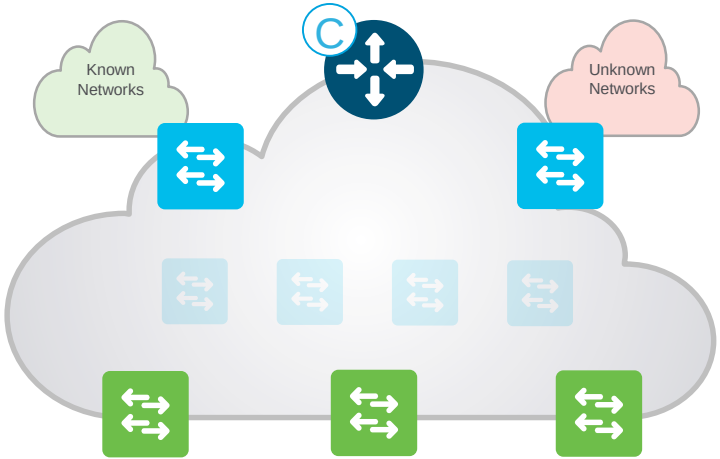


SD-Access Fabric

Edge Nodes – A Closer Look

Edge Node provides first-hop services for Users / Devices connected to a Fabric

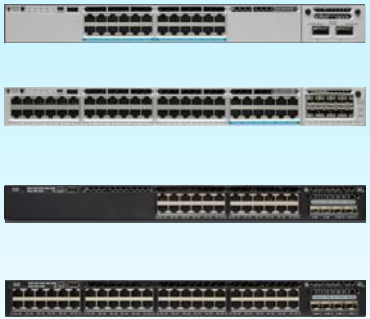
- Responsible for Identifying and Authenticating Endpoints (e.g. Static, 802.1X, Active Directory)
- Register specific Endpoint ID info (e.g. /32 or /128) with the Control-Plane Node(s)
- Provide an Anycast L3 Gateway for the connected Endpoints (same IP address on all Edge nodes)
- Performs encapsulation / de-encapsulation of data traffic to and from all connected Endpoints



SD-Access Platforms

Edge Nodes

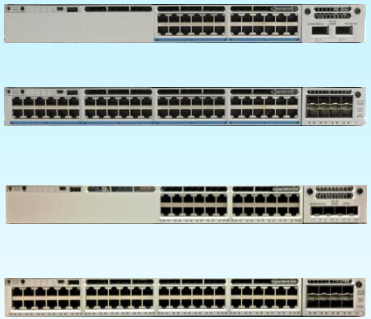
Catalyst 3K



- Catalyst 3650/3850
- 1/MGIG RJ45
- 10/40G NM Cards
- IOS-XE 16.6.3+

Catalyst 9K

NEW



- Catalyst 9300
- 1/MGIG RJ45
- 10/40/mG NM Cards
- IOS-XE 16.6.3+

Catalyst 4K

- Catalyst 4500
- Sup8E/9E (Uplink)
- 4700 Cards
- IOS-XE 3.10.1+

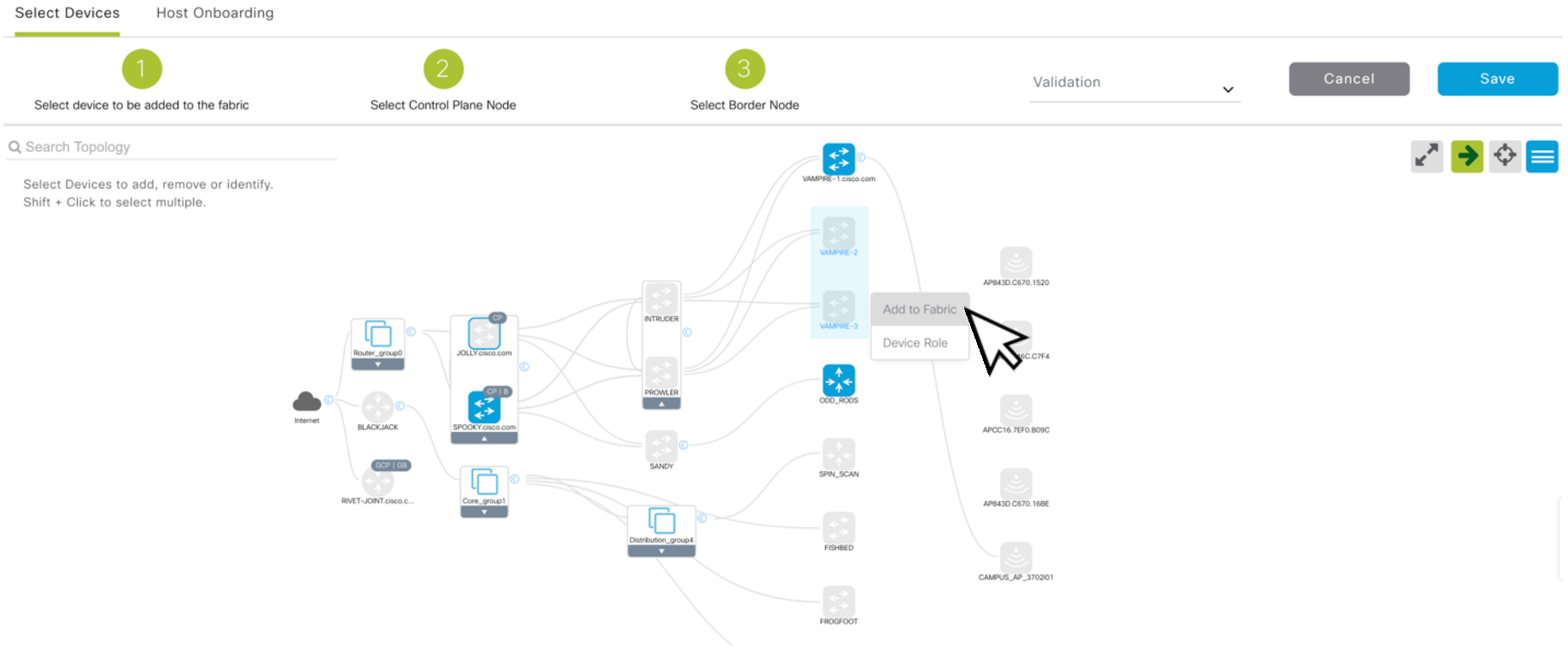
Catalyst 9400

NEW

- Catalyst 9400
- Sup1E
- 9400 Cards
- IOS-XE 16.6.3+

SD-Access @ DNA Center

Edge Nodes



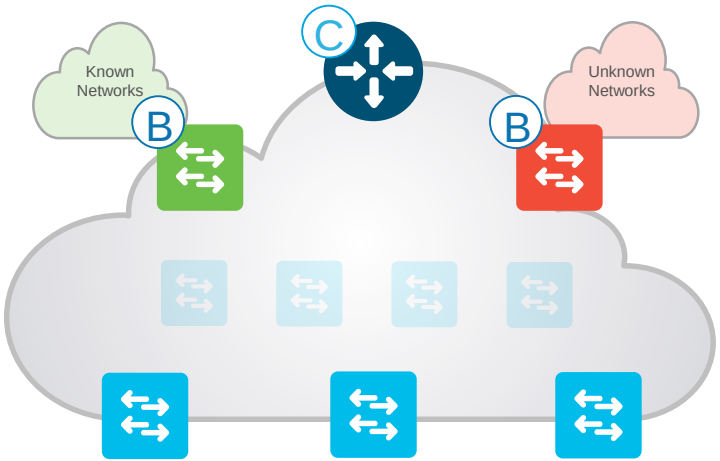
SD-Access Fabric

Border Nodes

Border Node is an Entry / Exit point for data traffic going In / Out of a Fabric

There are **2 Types** of **Border Node**!

- **Internal Border**
  - Used for “Known” Routes inside your company
- **External Border (Default)**
  - Used for “Unknown” Routes outside your company

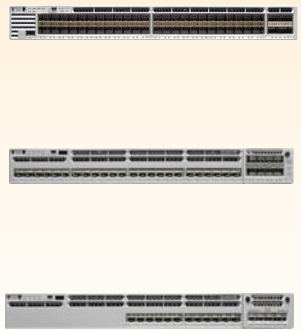


SD-Access Platforms

Border Nodes

* External Border Only

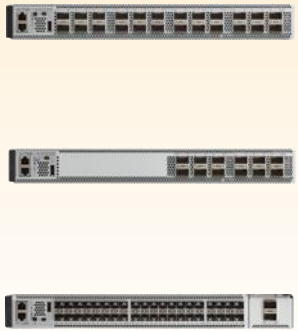
Catalyst 3K



- Catalyst 3850
- 1/10G SFP+
- 10/40G NM Cards
- IOS-XE 16.6.3+

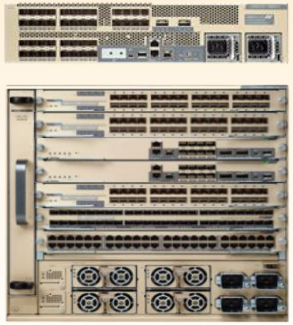
Catalyst 9K

NEW



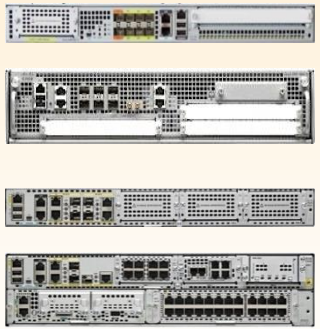
- Catalyst 9500
- 10/40G SFP/QSFP
- 10/40G NM Cards
- IOS-XE 16.6.3+

Catalyst 6K



- Catalyst 6800
- Sup2T/6T
- 6840/6880-X
- IOS 15.4.1SY4+

ASR1K & ISR4K



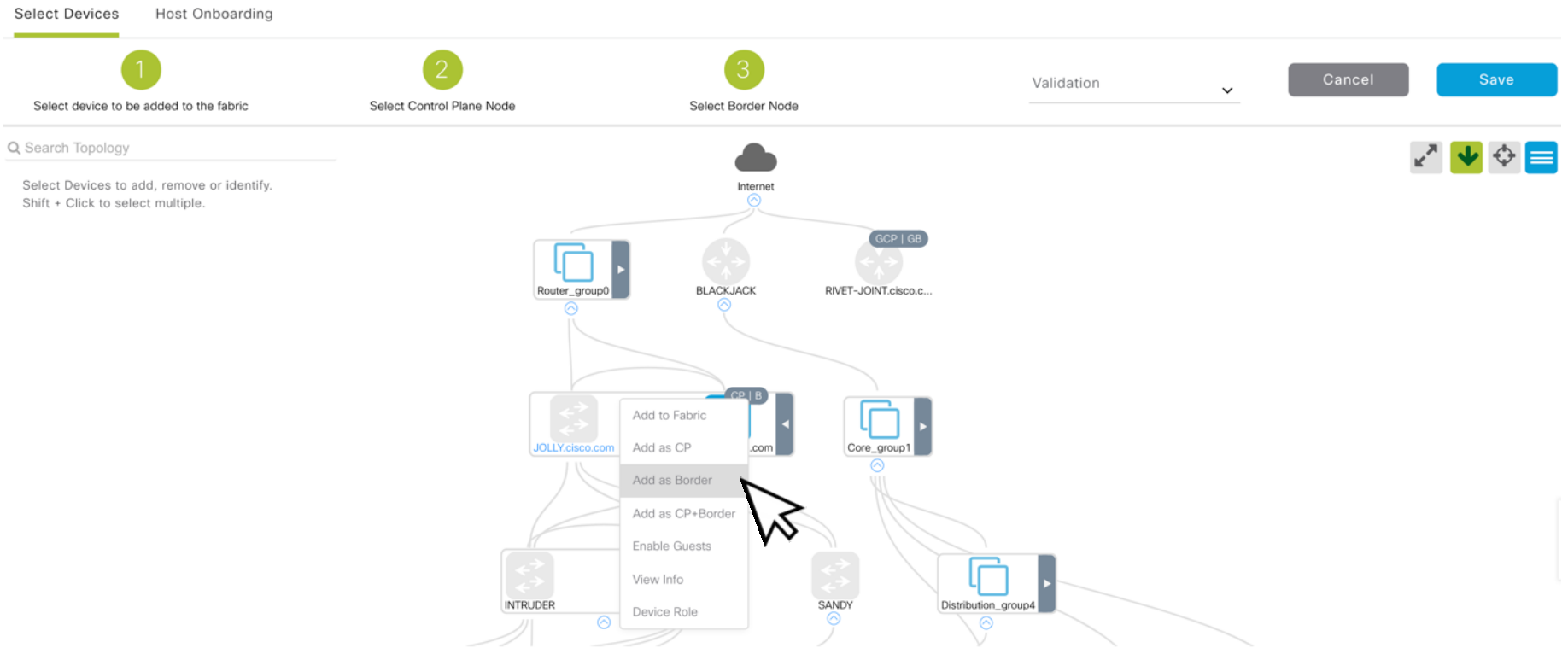
- ASR 1000-X/HX
- ISR 4430/4450
- 1/10G/40G
- IOS-XE 16.6.3+

Nexus 7K*

- Nexus 7700
- Sup2E
- M3 Cards
- NXOS 8.2.1+

SD-Access @ DNA Center

Border Nodes

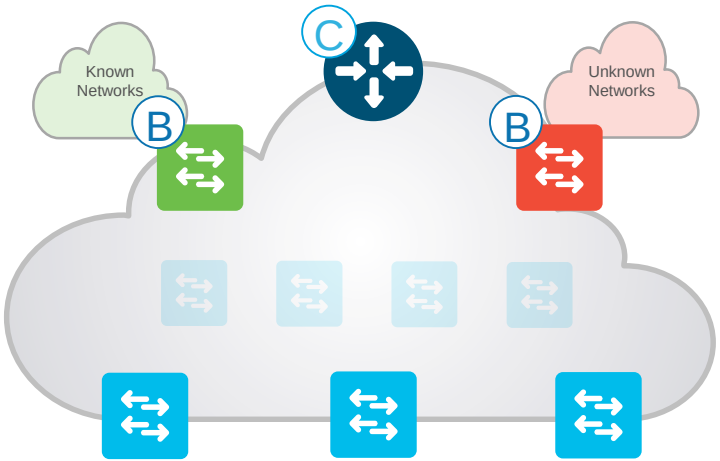


SD-Access Fabric

Border Nodes - Internal

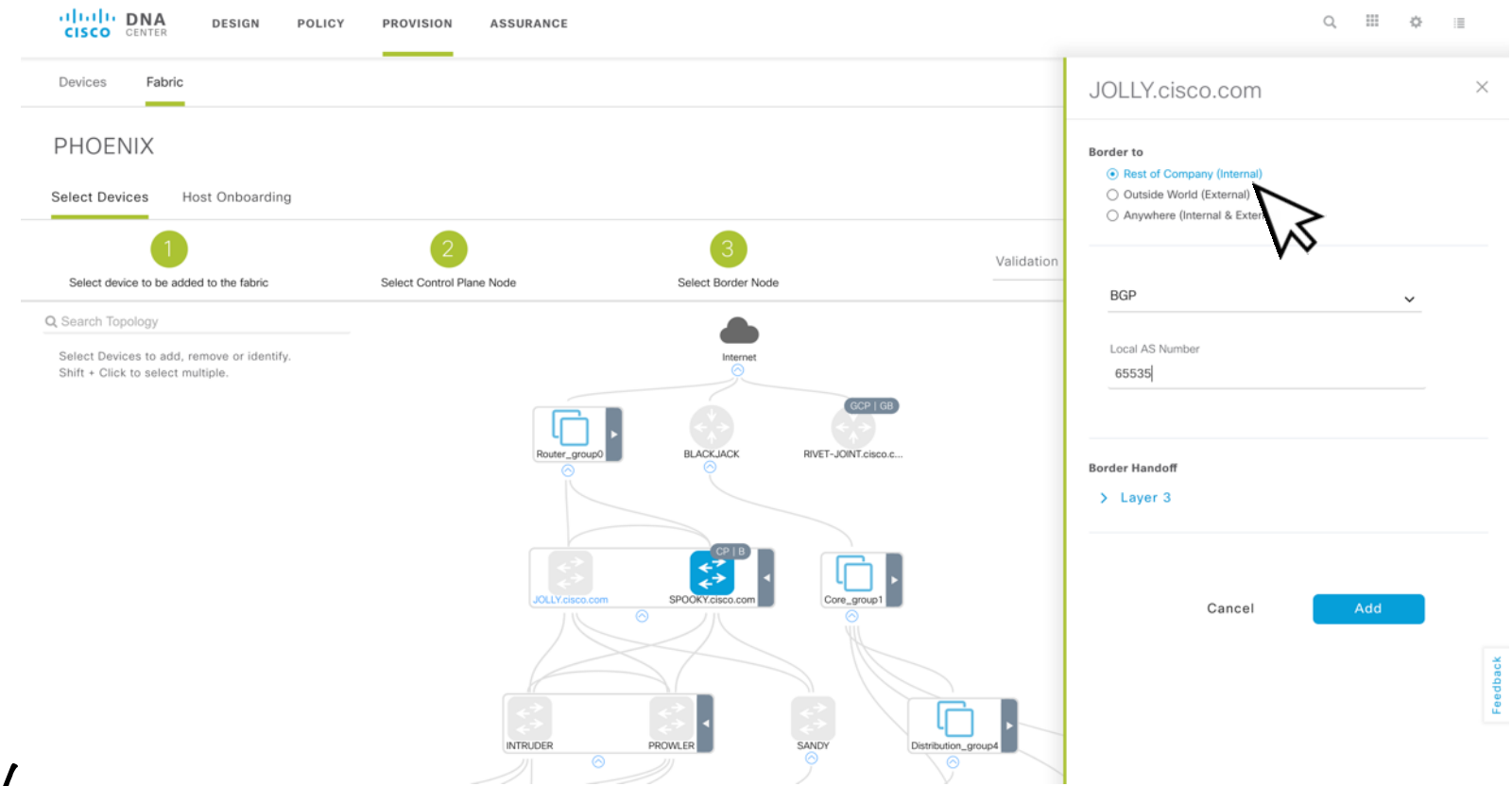
Internal Border advertises Endpoints to outside, and known Subnets to inside

- Connects to any “known” IP subnets available from the outside network (e.g. DC, WLC, FW, etc.)
- Exports all internal IP Pools to outside (as aggregate), using a traditional IP routing protocol(s).
- Imports and registers (known) IP subnets from outside, into the Control-Plane Map System
- Hand-off requires mapping the context (VRF & SGT) from one domain to another.



SD-Access @ DNA Center

Internal Borders

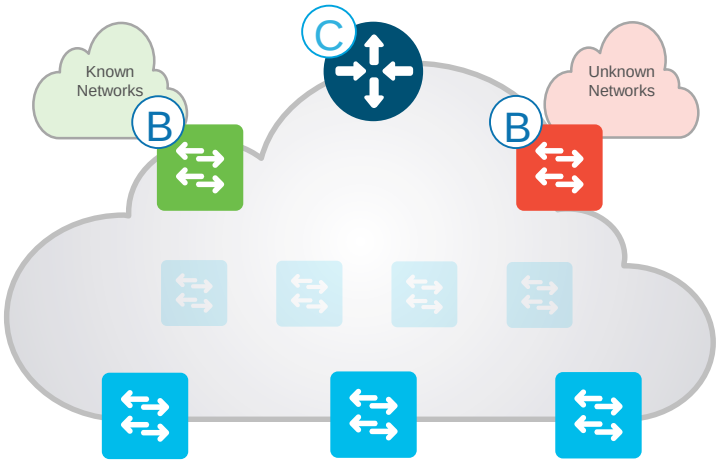


SD-Access Fabric

Border Nodes - External

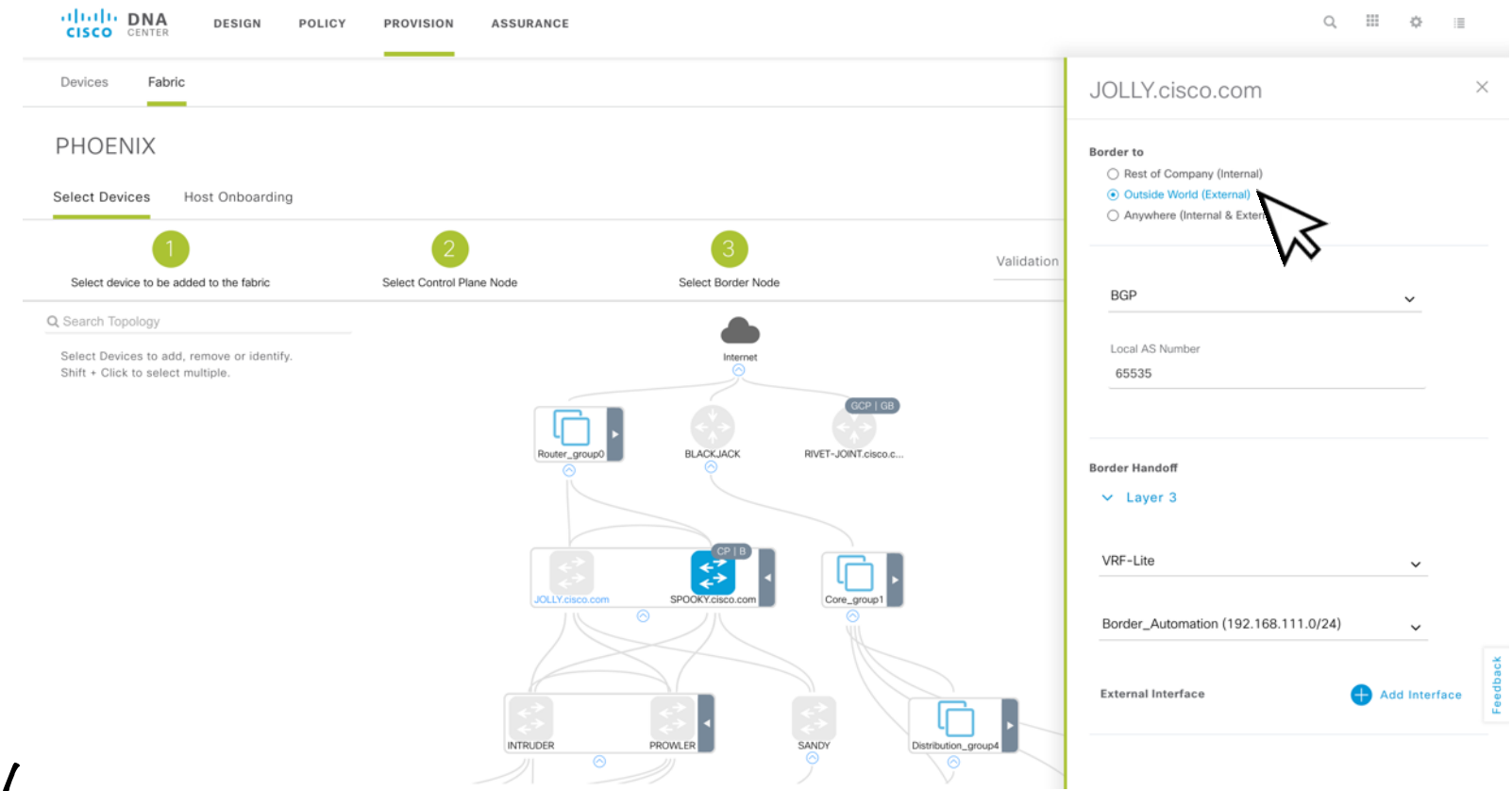
External Border is a “Gateway of Last Resort” for any unknown destinations

- Connects to any “unknown” IP subnets, outside of the network (e.g. Internet, Public Cloud)
- Exports all internal IP Pools outside (as aggregate) into traditional IP routing protocol(s).
- Does NOT import unknown routes. It is a “Default” Exit, if no entry is available in Control-Plane.
- Hand-off requires mapping the context (VRF & SGT) from one domain to another.



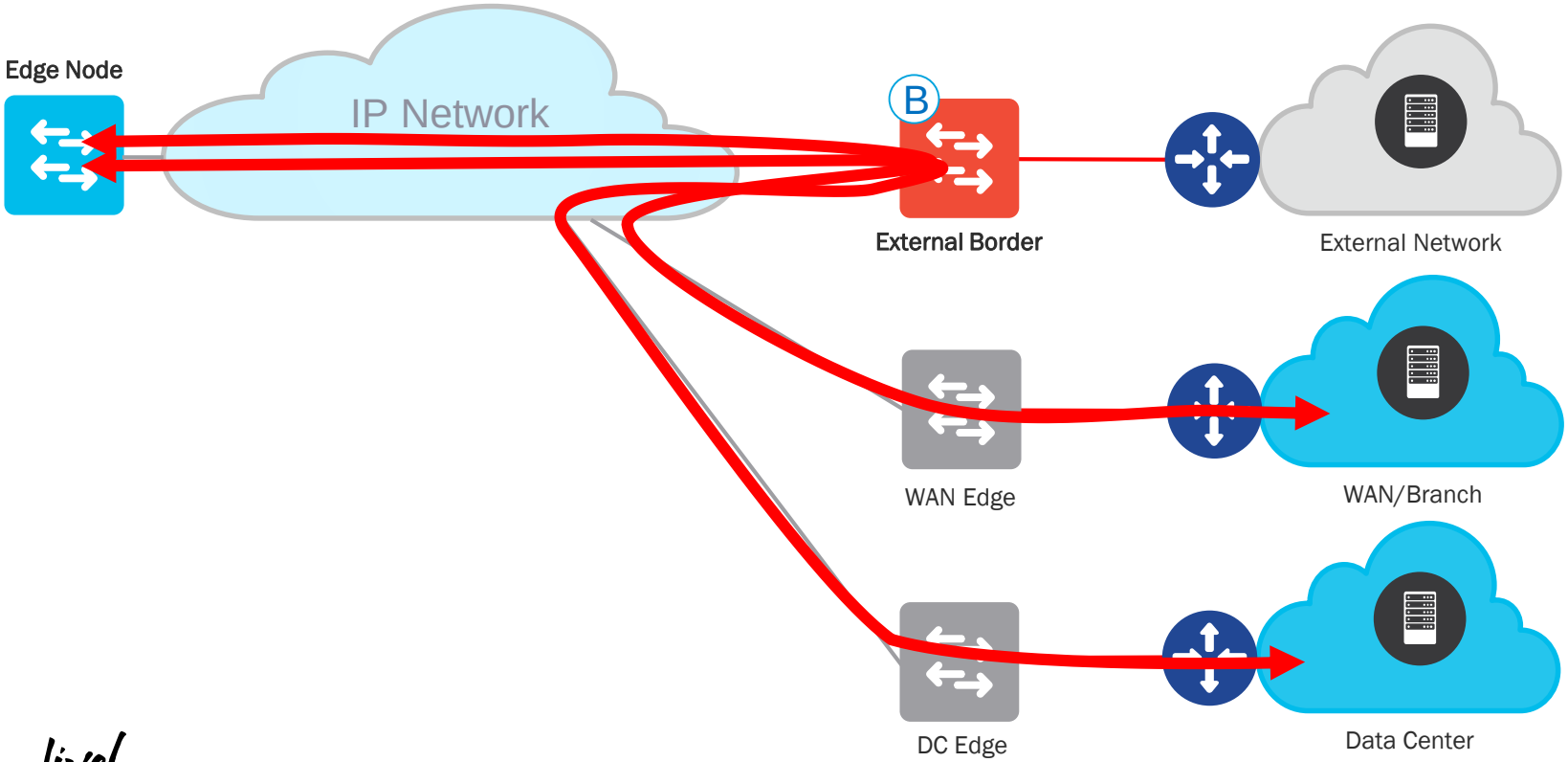
SD-Access @ DNA Center

External Borders



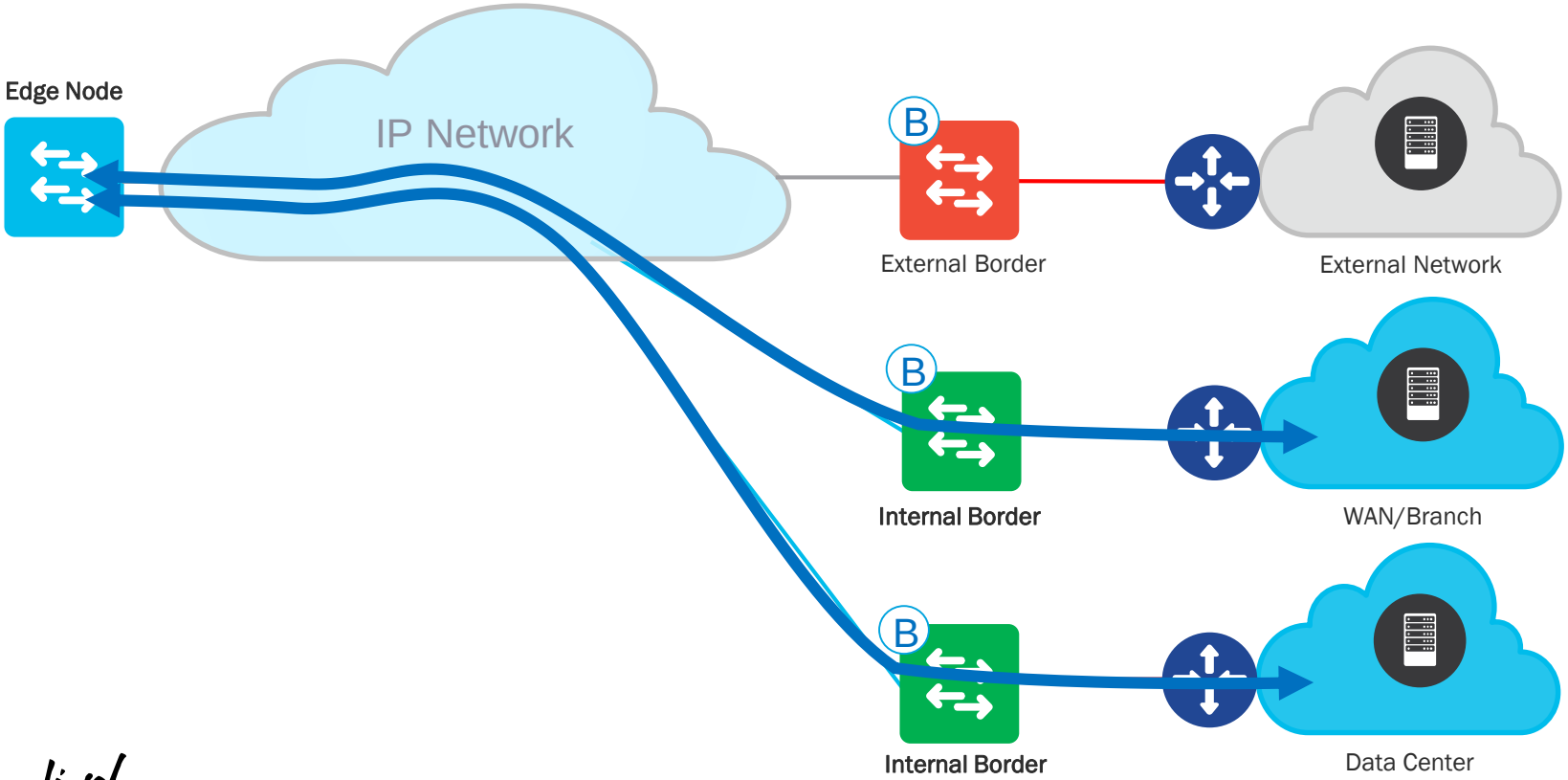
SD-Access - Border Deployment

Why? Internal Traffic with External Borders



SD-Access - Border Deployment

Why? Internal Traffic with Internal Borders



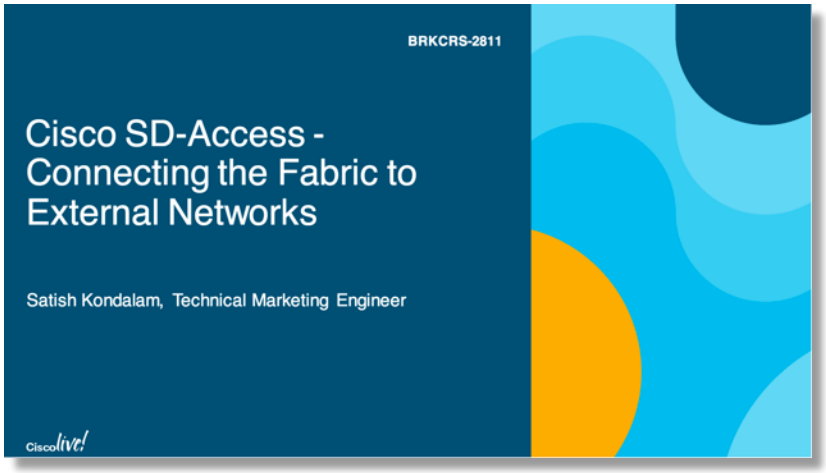
Would you like to know more?

External Connectivity

Check out the following session:

BRKCRS-2811

SD-Access - Connecting to External Networks



This session covers:

- More details about Fabric Border Nodes
- How Borders communicate to outside networks
- Various Fabric Border design approaches

Would you like to know more?

External Connectivity

Check out the following session:

BRKCRS-2815

SD-Access - Deploy a Fabric in Large Enterprise

This session covers:

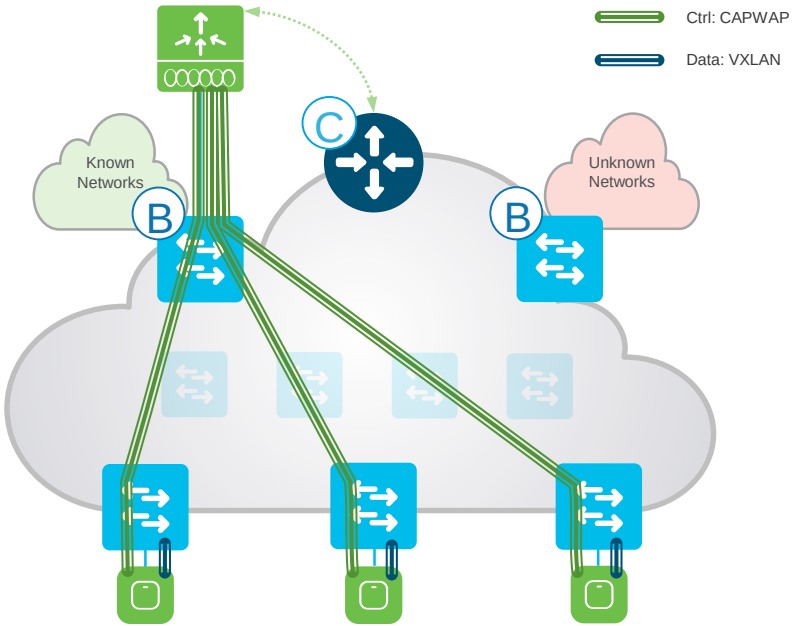
- More details about Fabric Border Nodes
- How multiple Fabrics communicate
- Various Multi-Site design approaches

SD-Access Fabric

Fabric Enabled Wireless – A Closer Look

Fabric Enabled WLC is integrated into Fabric for SDA Wireless clients

- Connects to Fabric via Border (Underlay)
- Fabric Enabled APs connect to the WLC (CAPWAP) using a dedicated Host Pool (Overlay)
- Fabric Enabled APs connect to the Edge via VXLAN
- Wireless Clients (SSIDs) use regular Host Pools for data traffic and policy (same as Wired)
- Fabric Enabled WLC registers Clients with the Control-Plane (as located on local Edge + AP)



SD-Access Platforms

Fabric Wireless

* Some caveats with Wave1 APs.

3504 WLC

NEW

- AIR-CT3504
- 150 APs
- 1G/mGig RJ45
- AireOS 8.5.1+

5500 WLC

- AIR-CT5520
- 1500 APs
- 1G/10G SFP+
- AireOS 8.5.1+

8500 WLC

- AIR-CT8540
- 5000 APs
- 1G/10G SFP+
- AireOS 8.5.1+

Wave 2 APs

NEW

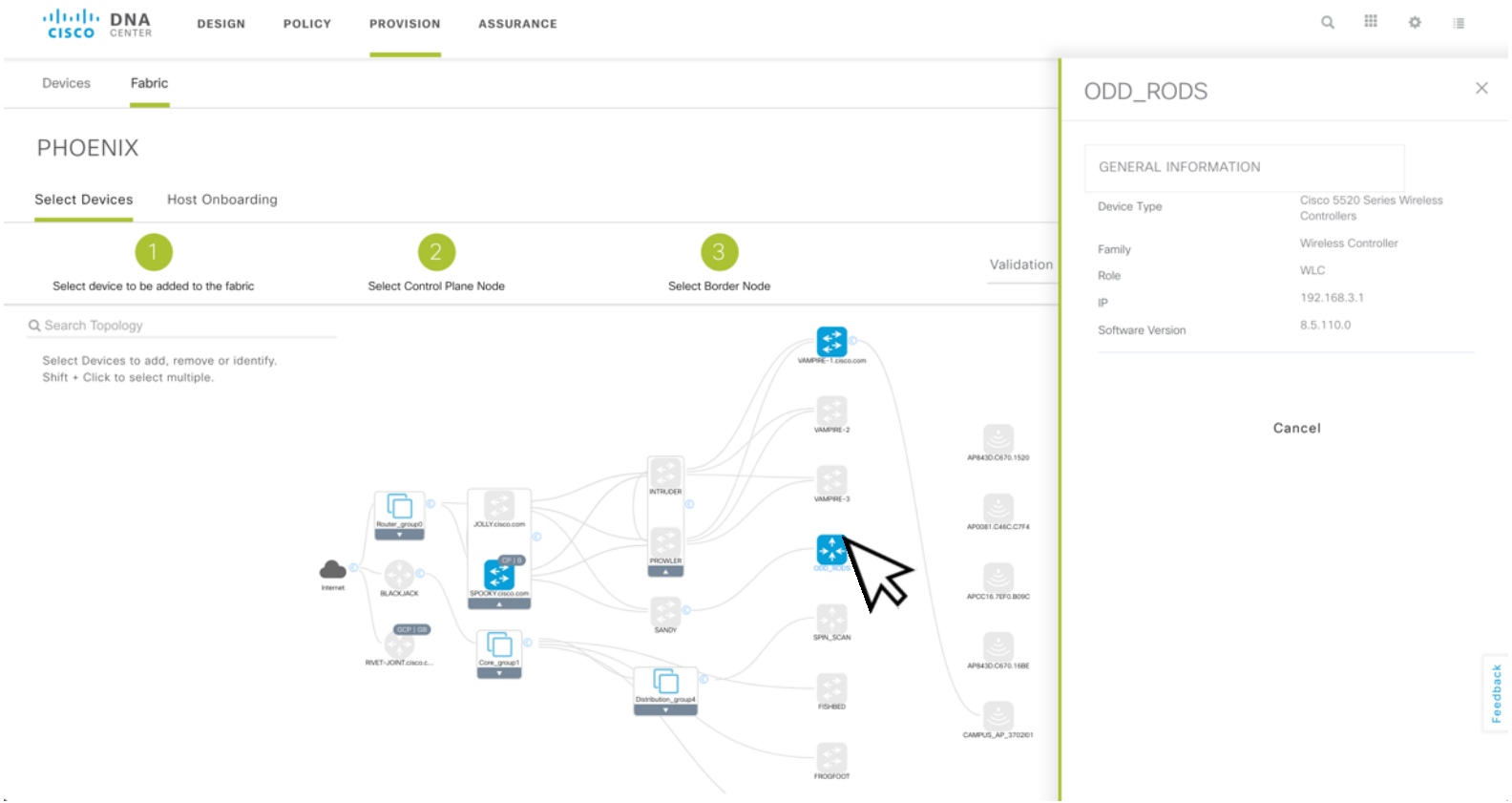
- 1800/2800/3800
- 11ac Wave2 APs
- 1G/mGIG RJ45
- AireOS 8.5.1+

Wave 1 APs*

- 1700/2700/3700
- 11ac Wave1 APs
- 1G RJ45
- AireOS 8.5.1+

SD-Access @ DNA Center

Fabric Wireless



Would you like to know more?

Fabric Wireless

Check out the following session:

BRKEWN-2020

SD-Access - Wireless Integration

This session covers:

- More details about Fabric Wireless
- How Fabric WLC and APs communicate
- Various Fabric Wireless approaches

Would you like to know more?

Fabric Wireless

Check out the following session:

BRKEWN-2021

SD-Access - How to setup Wireless

This session covers:

- More details about Fabric Wireless
- SD-Access Fabric Wireless Setup (LIVE)
- Fabric Wireless best practices and tips

Roles & Terminology

What is Software Defined Access?

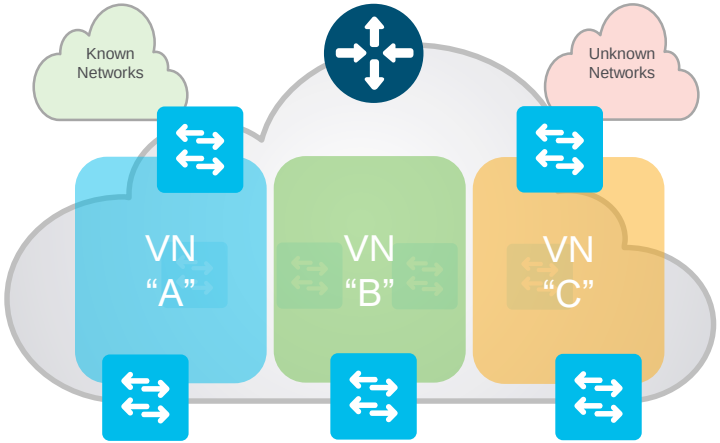
1. High-Level View
2. Roles & Platforms
3. Fabric Constructs

SD-Access Fabric

Virtual Network– A Closer Look

Virtual Network maintains a separate Routing & Switching table for each instance

- Control-Plane uses Instance ID to maintain separate VRF topologies (“Default” VRF is Instance ID “4098”)
- Nodes add VNID to the Fabric encapsulation
- Endpoint ID prefixes (Host Pools) are routed and advertised within a Virtual Network
- Uses standard “vrf definition” configuration, along with RD & RT for remote advertisement (Border Node)

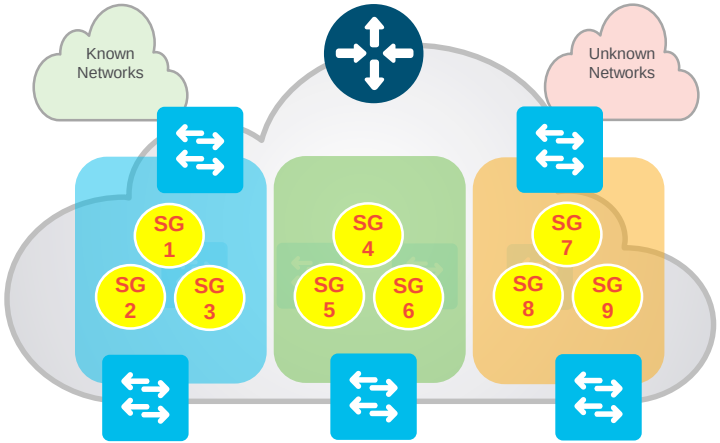


SD-Access Fabric

Scalable Groups – A Closer Look

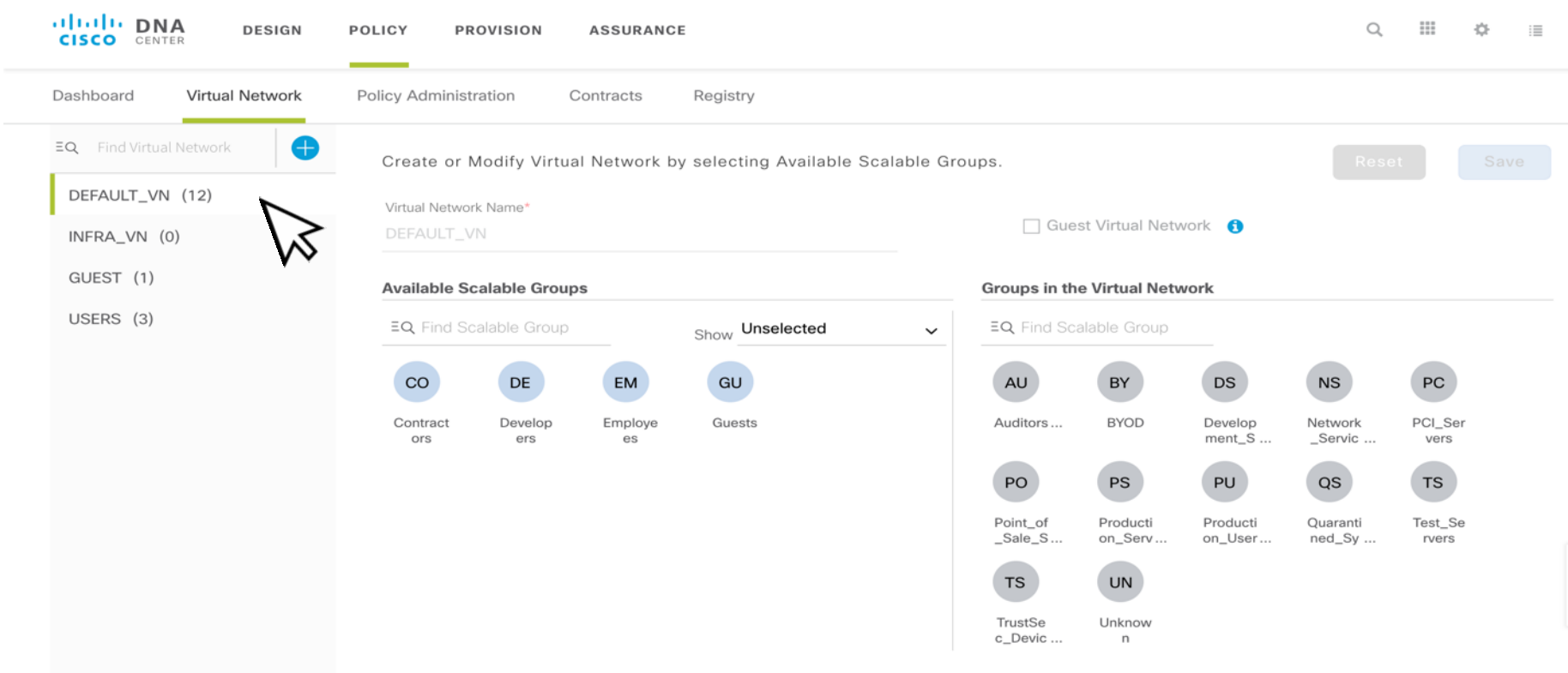
Scalable Group is a logical policy object to “group” Users and/or Devices

- Nodes use “Scalable Groups” to ID and assign a unique Scalable Group Tag (SGT) to Endpoints
- Nodes add SGT to the Fabric encapsulation
- SGTs are used to manage address-independent “Group-Based Policies”
- Edge or Border Nodes use SGT to enforce local Scalable Group ACLs (SGACLs)



SD-Access @ DNA Center

Virtual Networks and Scalable Groups

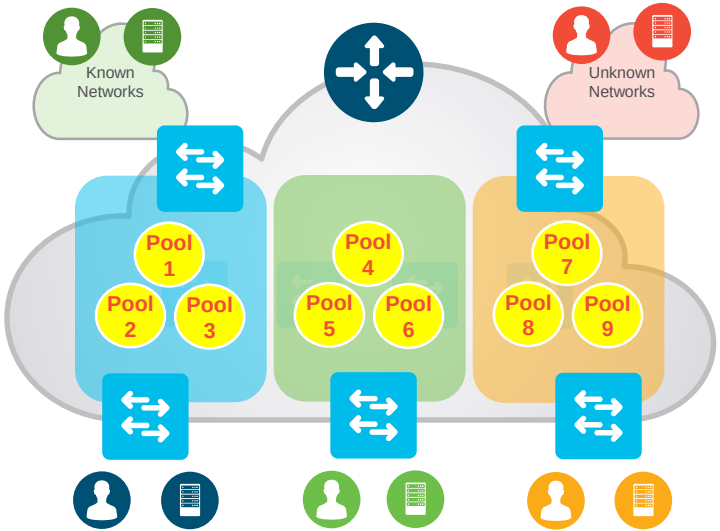


SD-Access Fabric

Host Pools – A Closer Look

Host Pool provides basic IP functions necessary for attached Endpoints

- Edge Nodes use a Switch Virtual Interface (SVI), with IP Address /Mask, etc. per Host Pool
- Fabric uses Dynamic EID mapping to advertise each Host Pool (per Instance ID)
- Fabric Dynamic EID allows Host-specific (/32, /128, MAC) advertisement and mobility
- Host Pools can be assigned Dynamically (via Host Authentication) and/or Statically (per port)

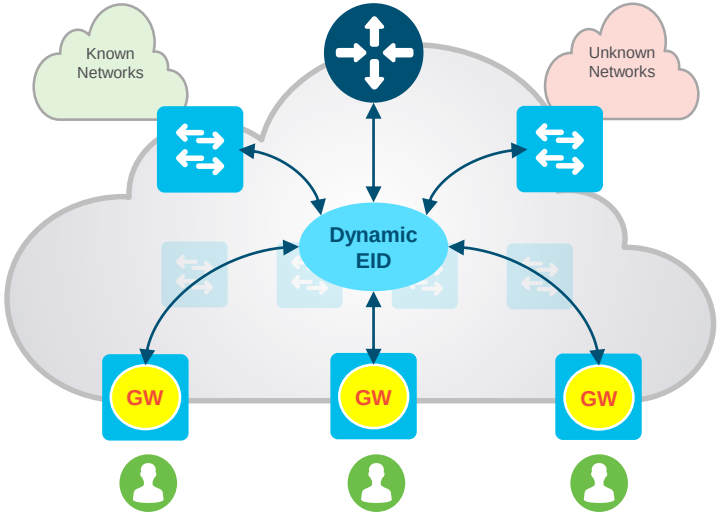


SD-Access Fabric

Layer 3 Overlay – A Closer Look

Stretched Subnets allow an IP subnet to be "stretched" via the Overlay

- Host IP based traffic arrives on the local Fabric Edge SVI, and is then transferred by Fabric
- Fabric Dynamic EID mapping allows Host-specific (/32, /128, MAC) advertisement and mobility
- Host 1 connected to Edge A can now use the same IP subnet to communicate with Host 2 on Edge B
- No longer need a VLAN to connect Host 1 and 2 ☺

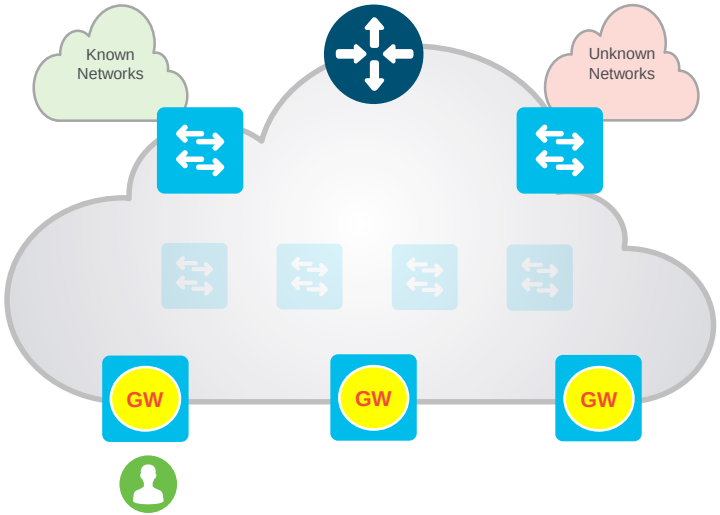


SD-Access Fabric

Anycast Gateway– A Closer Look

Anycast GW provides a single L3 Default Gateway for IP capable endpoints

- Similar principle and behavior as HSRP / VRRP with a shared “Virtual” IP and MAC address
- The same Switch Virtual Interface (SVI) is present on EVERY Edge, with the same Virtual IP and MAC
- Control-Plane with Fabric Dynamic EID mapping creates a Host (Endpoint) to Edge relationship
- When a Host moves from Edge 1 to Edge 2, it does not need to change it’s Default Gateway ☺

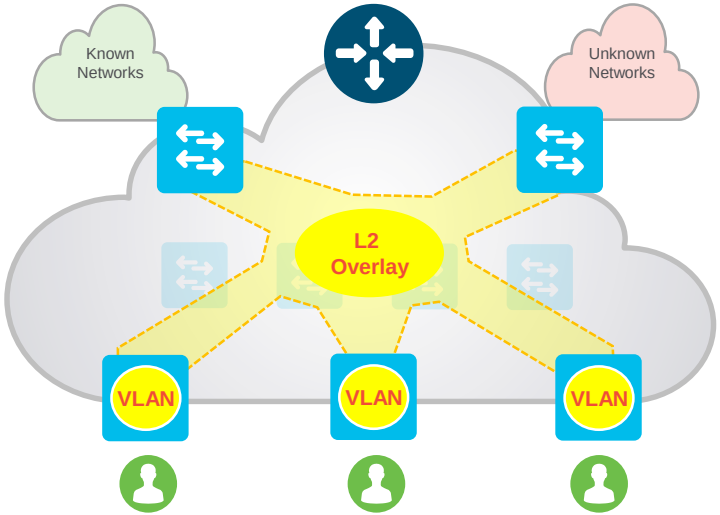


SD-Access Fabric

Layer 2 Overlay – A Closer Look

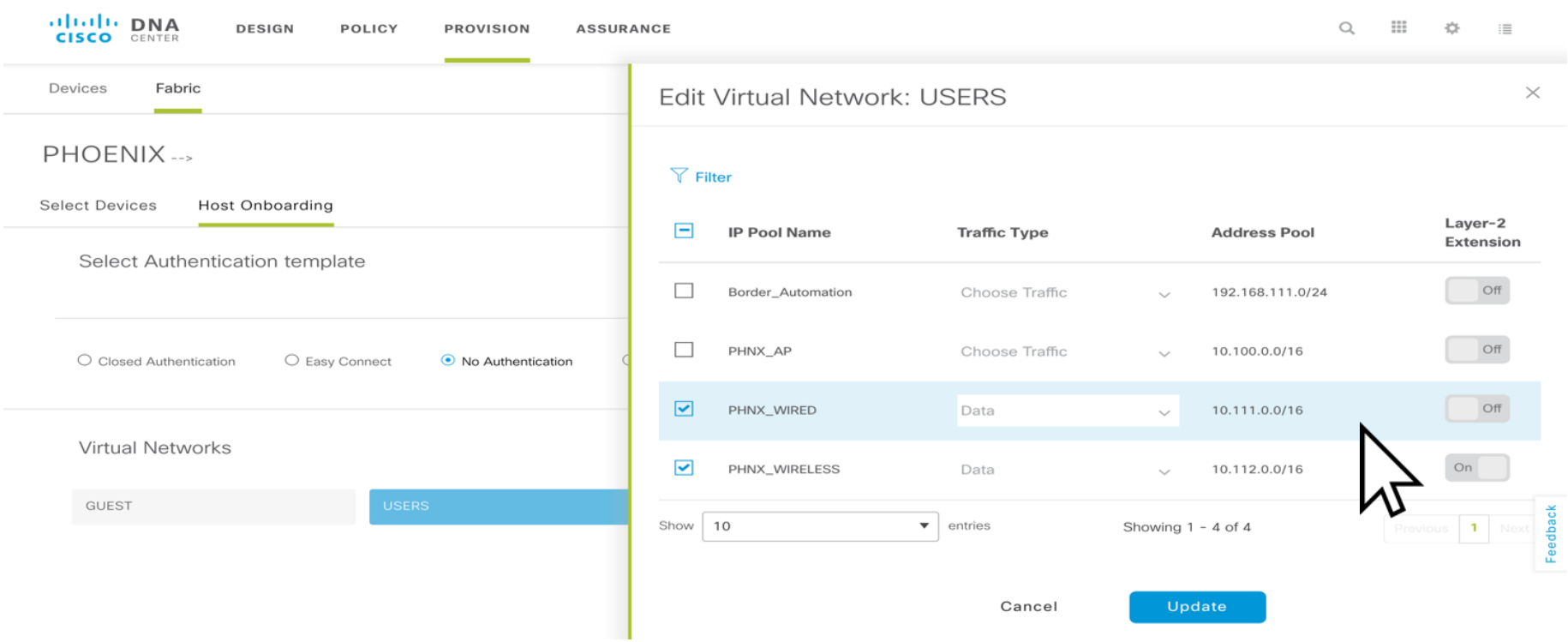
Layer 2 Extension allows Non-IP endpoints to use Broadcast & L2 Multicast

- Similar principle and behavior as Virtual Private LAN Services (VPLS) P2MP Overlay
- Uses a pre-built Multicast Underlay to setup a P2MP tunnel between all Fabric Nodes.
- L2 Broadcast and Multicast traffic will be distributed to all connected Fabric Nodes.
- Can be enabled for specific Host Pools that require L2 services (use Stretched Subnets for L3)



SD-Access @ DNA Center

Host Pools & Layer-2 Extension



Fabric Fundamentals

What is Campus Fabric?

1. Control-Plane
2. Data-Plane
3. Policy-Plane

SD-Access

Campus Fabric - Key Components

1. **Control-Plane** based on **LISP**
2. **Data-Plane** based on **VXLAN**
3. **Policy-Plane** based on **CTS**

Key Differences

- L2 + L3 Overlay -vs- L2 or L3 Only
- Host Mobility with Anycast Gateway
- Adds VRF + SGT into Data-Plane
- Virtual Tunnel Endpoints (Automatic)
- NO Topology Limitations (Basic IP)

SD-Access Fabric

Key Components – Control Plane

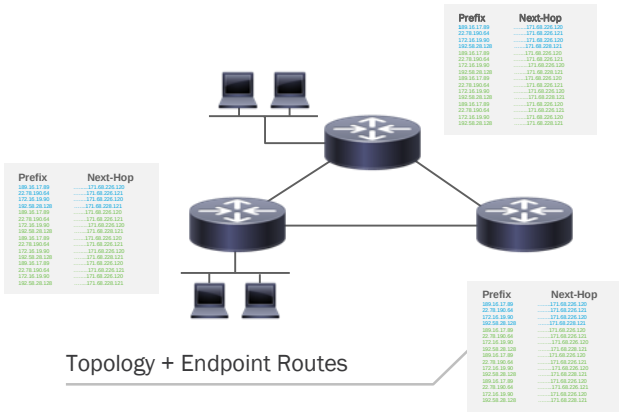
Host Mobility

1. Control-Plane based on LISP

Routing Protocols = **Big Tables** & **More CPU** with Local L3 Gateway

BEFORE

IP Address = Location + Identity

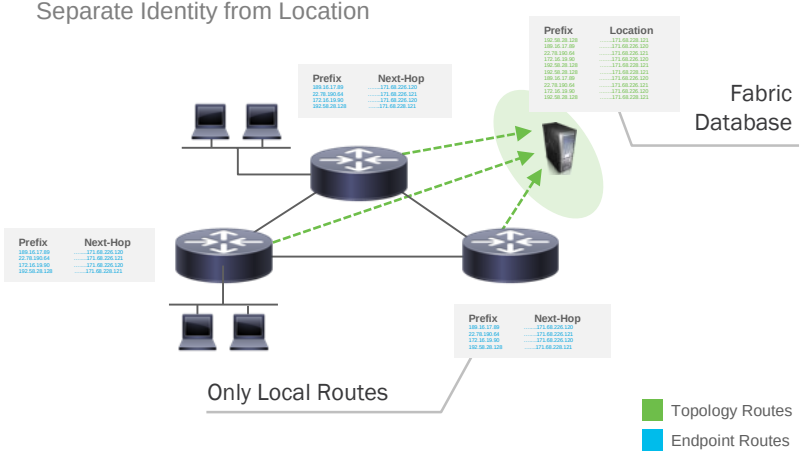


Endpoint Routes are Consolidated to LISP DB

Fabric DB + Cache = **Small Tables** & **Less CPU** with Anycast L3 Gateway

AFTER

Separate Identity from Location



Fabric Operation

Control-Plane Roles & Responsibilities

Fabric Control Plane

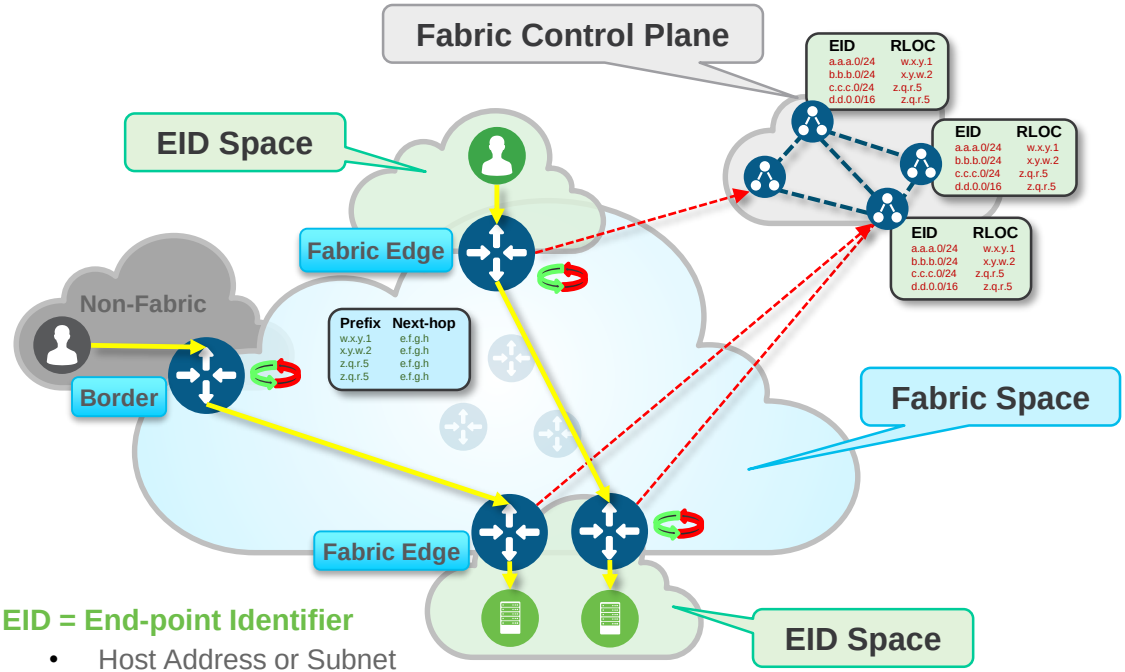
- EID to Location Mappings
- Can be distributed across multiple nodes

Fabric Edge Node

- Edge Encap / Decap
- Ingress / Egress to EID

Fabric Border Node

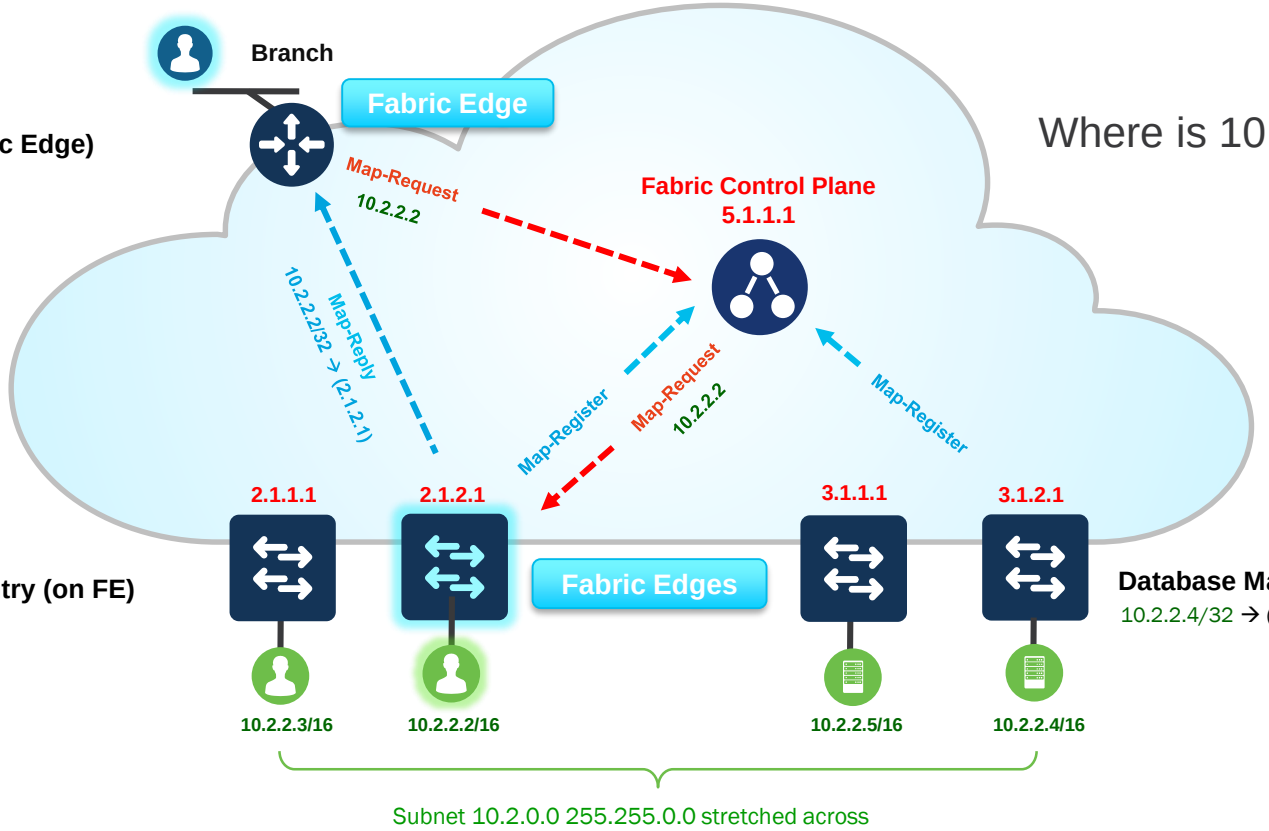
- Connects between Fabric and non-Fabric domains
- Proxy Encap / Decap



- **EID = End-point Identifier**
  - Host Address or Subnet
- **RLOC = Routing Locator**
  - Local Router Address

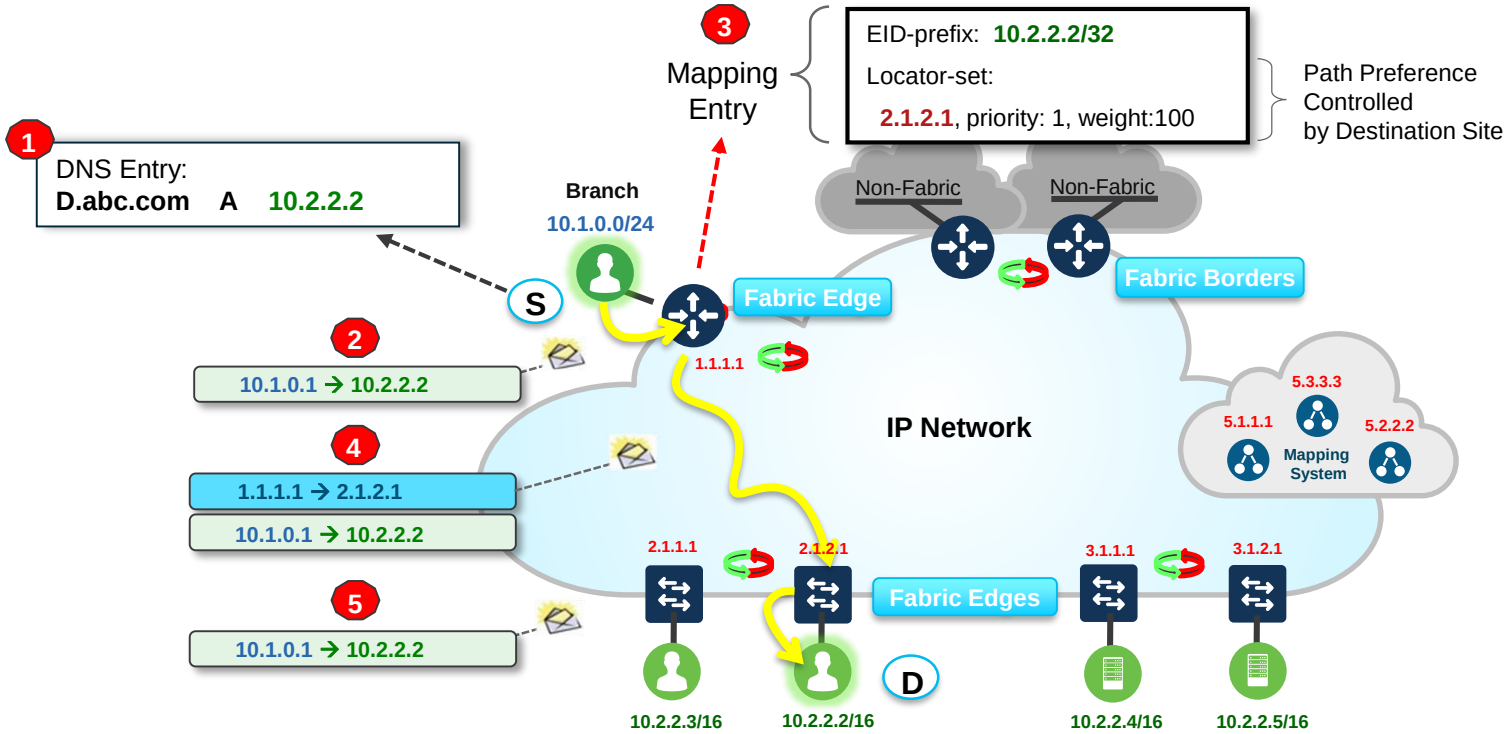
Fabric Operation

Control Plane Register & Resolution



Fabric Operation

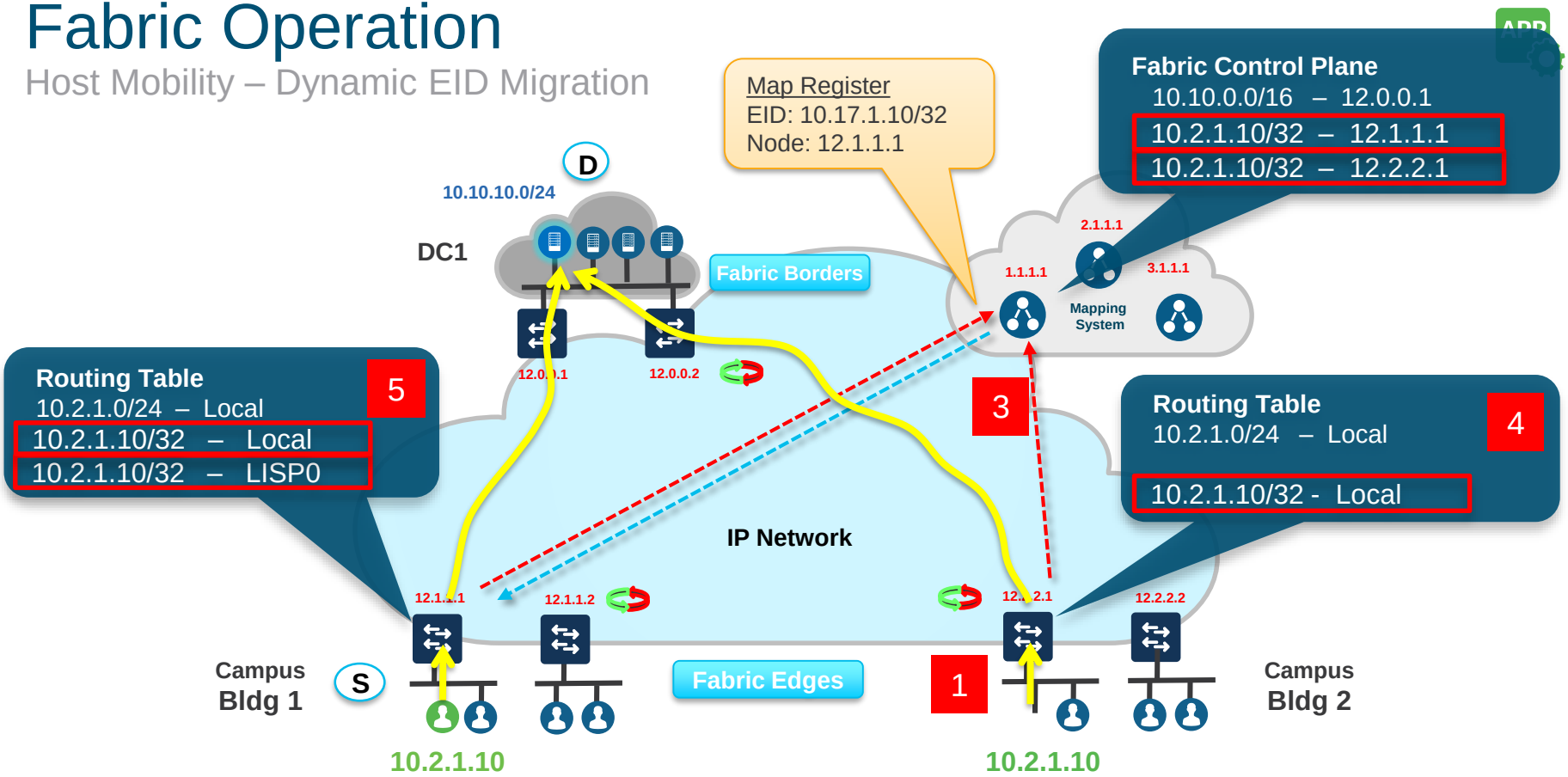
Fabric Internal Forwarding (Edge to Edge)



Subnet 10.2.0.0 255.255.0.0 stretched across

Fabric Operation

Host Mobility – Dynamic EID Migration



Subnet 10.2.0.0 255.255.0.0 stretched across

SD-Access Fabric

Unique Control-Plane Extensions compared to LISP

Capability	Traditional LISP	SD-Access Fabric
Layer 2 Extension	Not Supported	Fabric Control Plane extended to support MAC to IP binding, and Layer 2 Overlays
Virtual Networks	Layer-3 (aka VRF) based VN only	Both Layer-3 (VRF) and Layer-2 VN support (using VXLAN)
Fast Roaming	Fast roaming not supported	Fabric Control Plane extended to support fast roaming in =/< 50ms
Wireless Extensions	Not Supported	Fabric Control Plane supports wireless extensions for: • AP Onboarding • Wireless Guest • VXLAN functionality on AP

Fabric Fundamentals

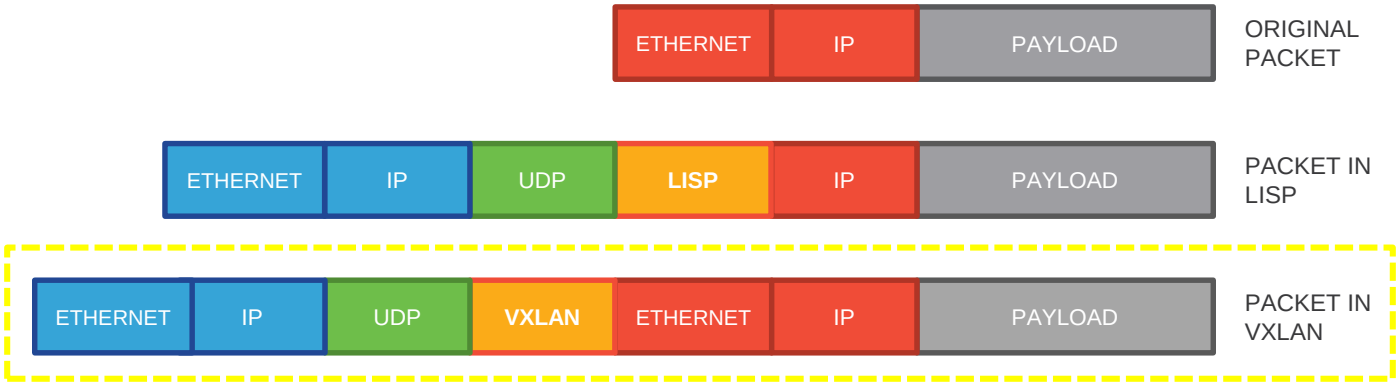
What is Campus Fabric?

1. Control-Plane
2. Data-Plane
3. Policy-Plane

SD-Access Fabric

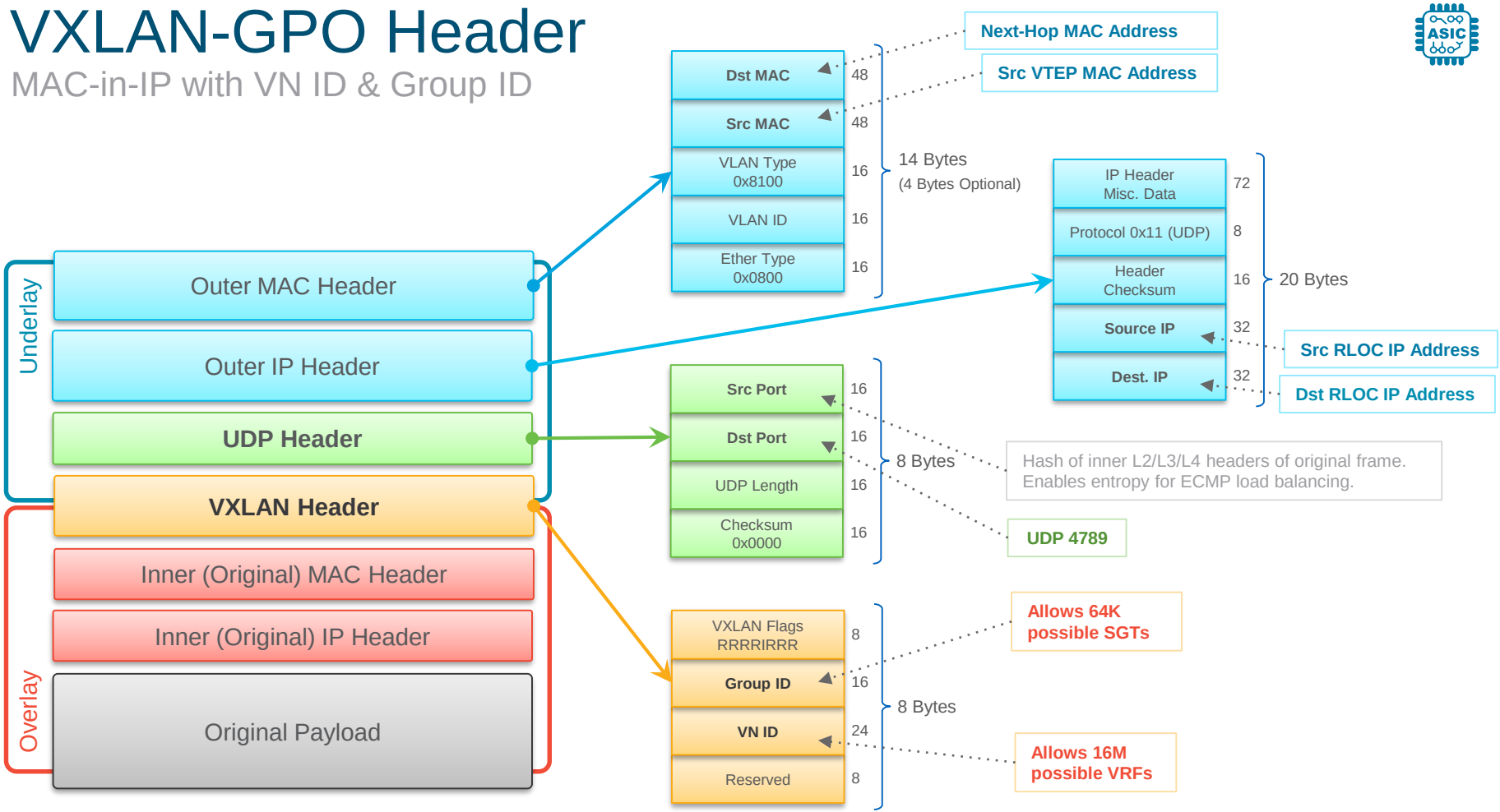
Key Components – VXLAN

1. **Control-Plane** based on **LISP**
2. **Data-Plane** based on **VXLAN**



VXLAN-GPO Header

MAC-in-IP with VN ID & Group ID



Data-Plane Overview

Fabric Header Encapsulation

Fabric Data-Plane provides the following:

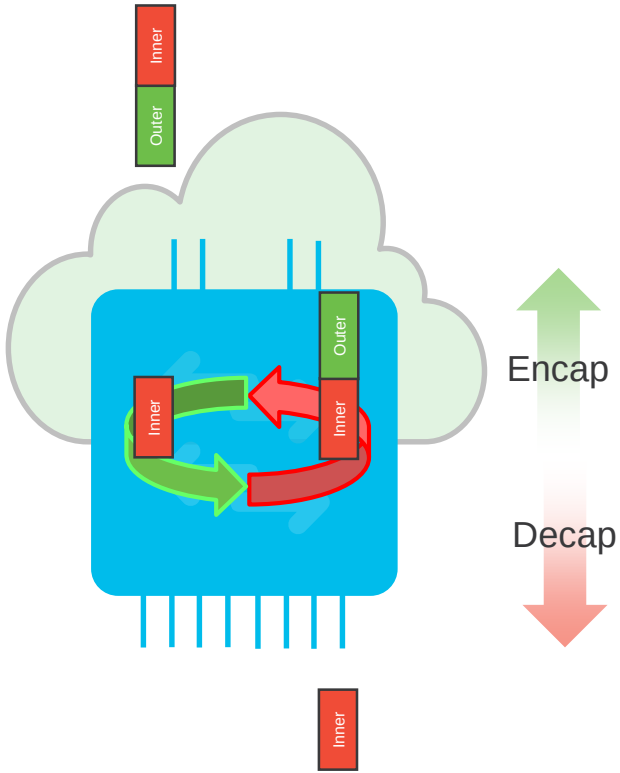
- Underlay address advertisement & mapping
- Automatic tunnel setup (Virtual Tunnel End-Points)
- **Frame encapsulation between Fabric Nodes**

Support for VXLAN header format

- Support for Layer 2 and Layer 3 Segmentation using VNI (VXLAN Network Identifier)
- VXLAN header carries MAC payload (MAC in IP)
- Support for Group Tags for Policy

Triggers Control Plane events

- Registration of Endpoints (Hosts)
- ARP or NDP Learning on L3 Gateways
- Map-Reply or Cache on Fabric Nodes



SD-Access Fabric

Unique Data-Plane Extensions compared to LISP

Capability	LISP Header	VXLAN Header
SGT Tag	No place to carry SGT	VXLAN-GPO uses Reserved field to carry SGT
Layer 3 Extension (VRF)	Yes	Yes, by mapping VRF->VNI
Layer 2 Extension	Not Supported	Fabric supports Layer 2 extension by mapping VLAN ->VNI
Wireless	Not Supported	AP to Fabric Edge uses VXLAN Fabric Edge to Edge/Border uses VXLAN for both Wired and Wireless (same)

Fabric Fundamentals

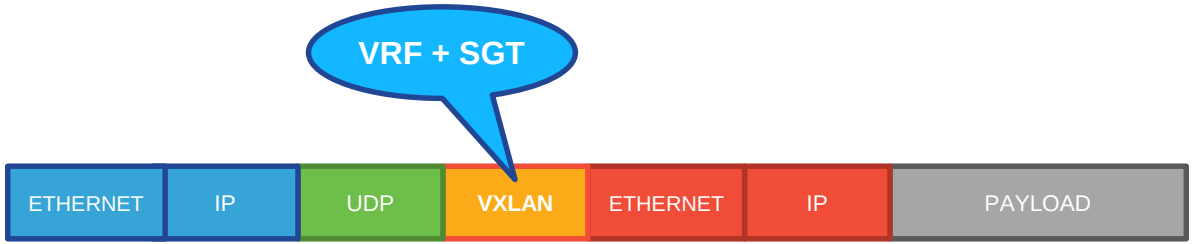
What is Campus Fabric?

1. Control-Plane
2. Data-Plane
3. Policy-Plane

SD-Access Fabric

Key Components – Group Based Policy

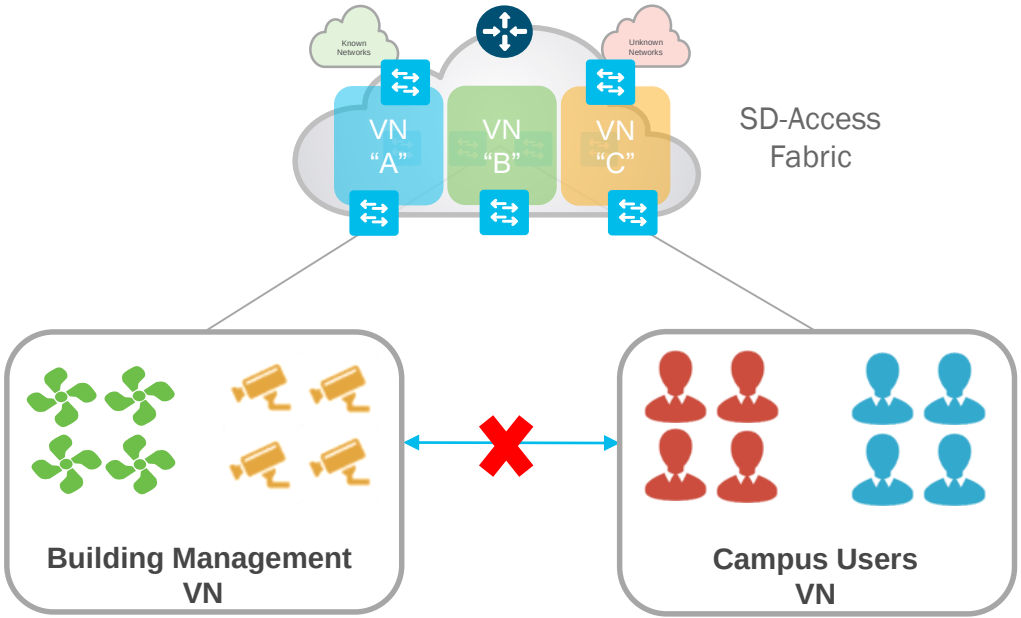
1. **Control-Plane** based on **LISP**
2. **Data-Plane** based on **VXLAN**
3. **Policy-Plane** based on **CTS**



Virtual Routing & Forwarding
Scalable Group Tagging

SD-Access Policy

Two Level Hierarchy - Macro Level

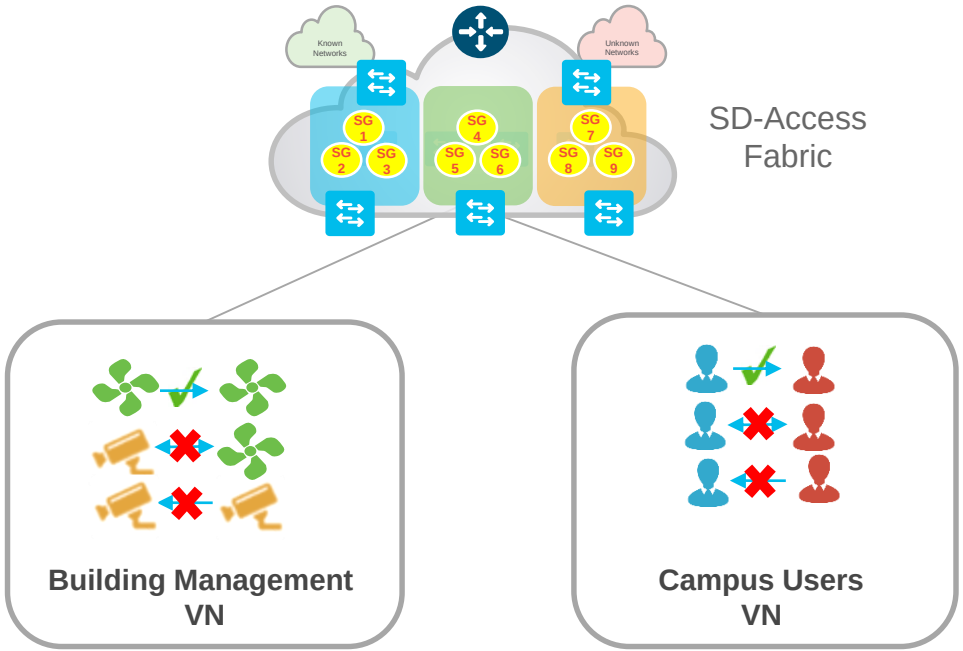


Virtual Network (VN)

First level Segmentation ensures **zero communication** between forwarding domains. Ability to consolidate multiple networks into one management plane.

SD-Access Policy

Two Level Hierarchy - Micro Level



Scalable Group (SG)

Second level Segmentation ensures **role based access control** between two groups within a Virtual Network. Provides the ability to segment the network into either line of businesses or functional blocks.

SD-Access Policy

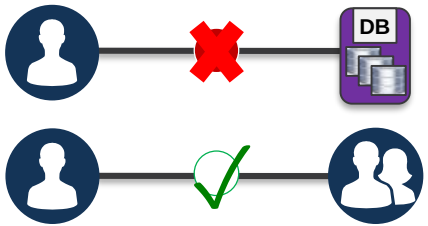
Policy Types

Access Control Policy

↓

Who can access What?

Rules for Inter-Group Access:
Permit / Deny Group to Group



Application Policy

↓

How to treat Traffic?

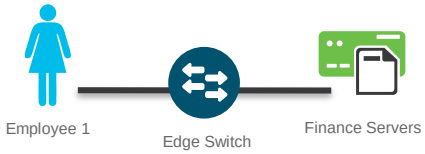
QoS for Applications
Application Compression
Application Caching

Traffic Copy Policy

↓

Need to Mirror Traffic?

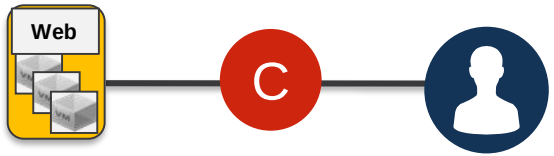
Configures ERSPAN for specific endpoints and traffic (source and destination SGT)



SD-Access Policy

Policy Contracts

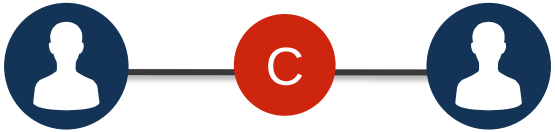
1. App to User Contracts



App to User Contracts

provider → ← consumer

2. User to User Contracts



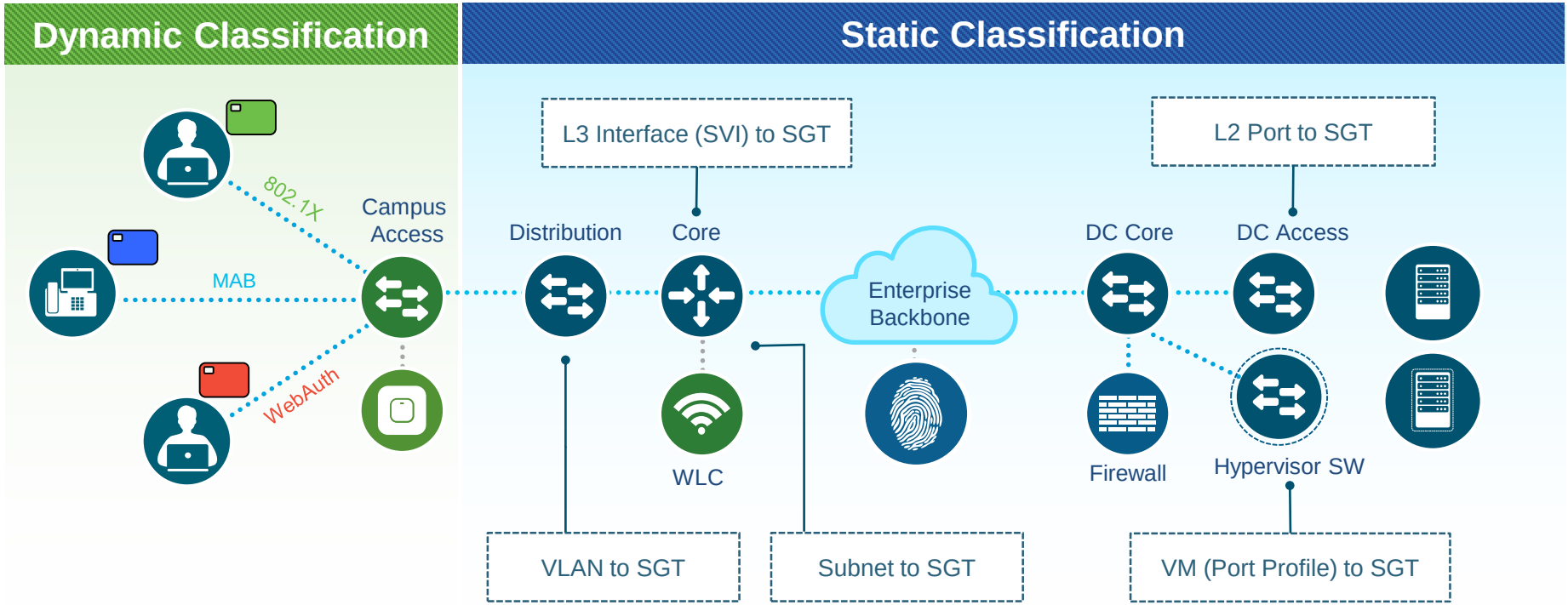
User to User Contracts

consumer → ← provider

Authored and Enforced in Campus/Branch

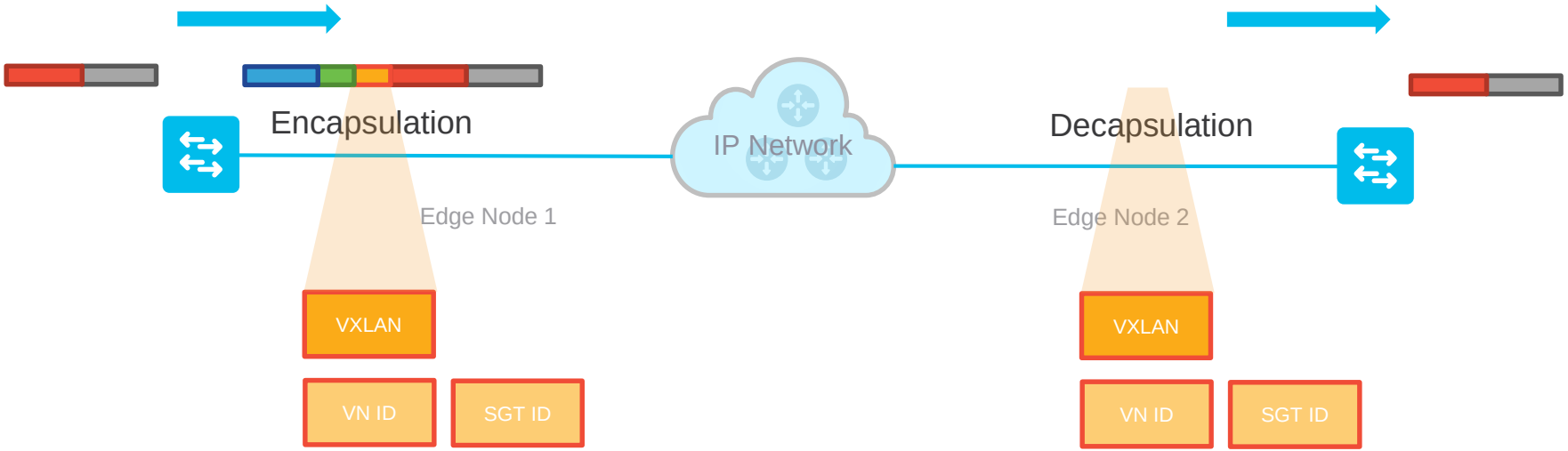
Group Assignment

Two ways to assign SGT



Group Propagation

VN & SGT in VXLAN-GPO Encapsulation



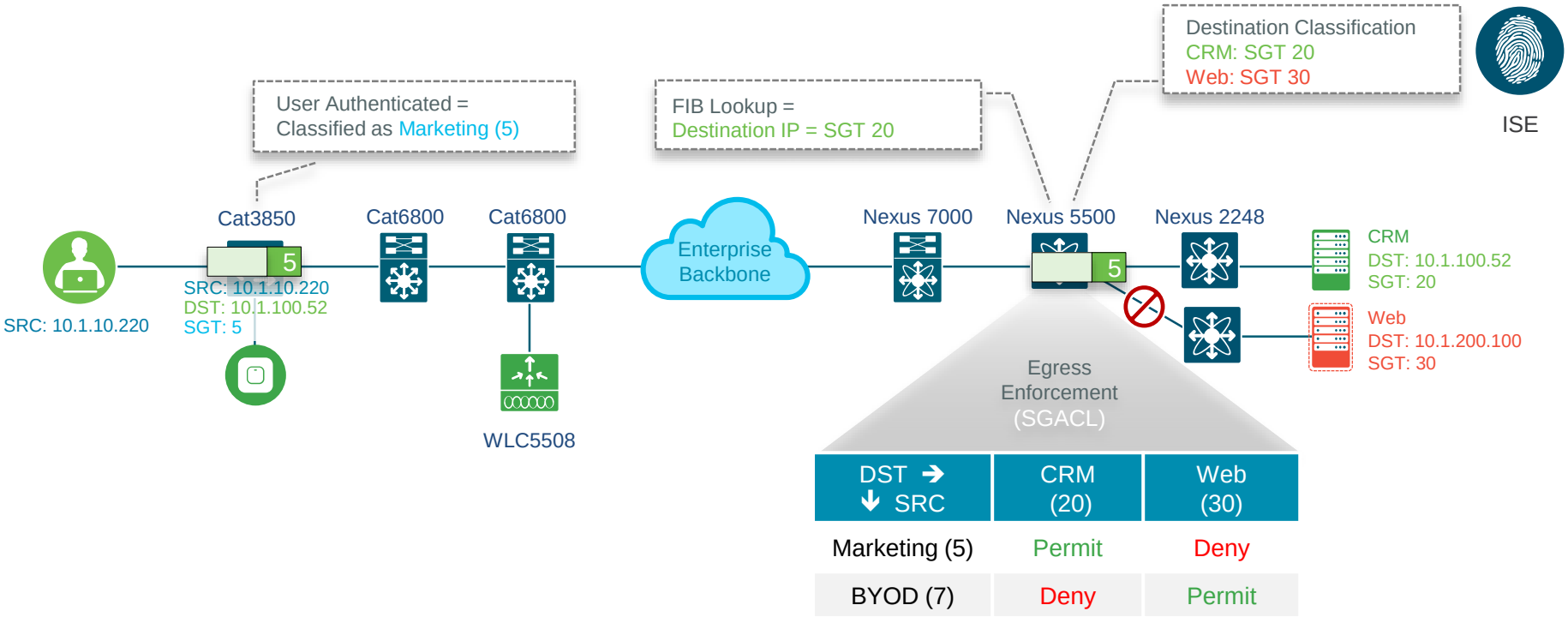
Classification
Static or Dynamic VN and SGT assignments

Propagation
Carry VN and Group context across the network

Enforcement
Group Based Policies
ACLs, Firewall Rules

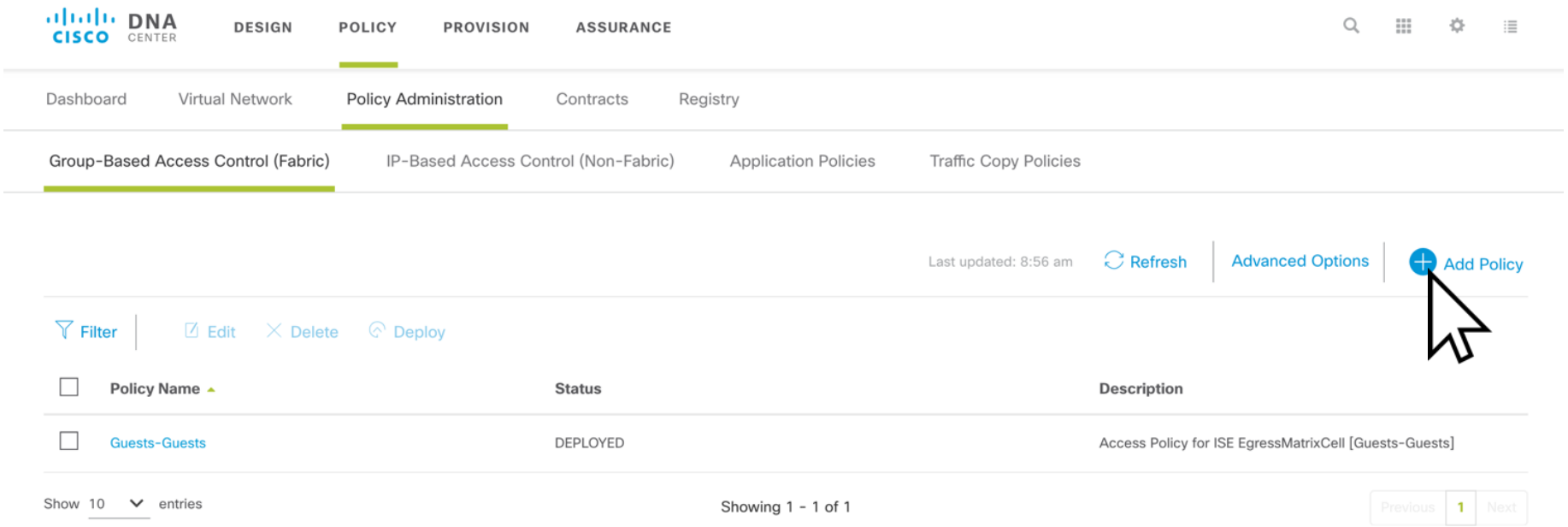
Policy Enforcement

Ingress Classification with Egress Enforcement



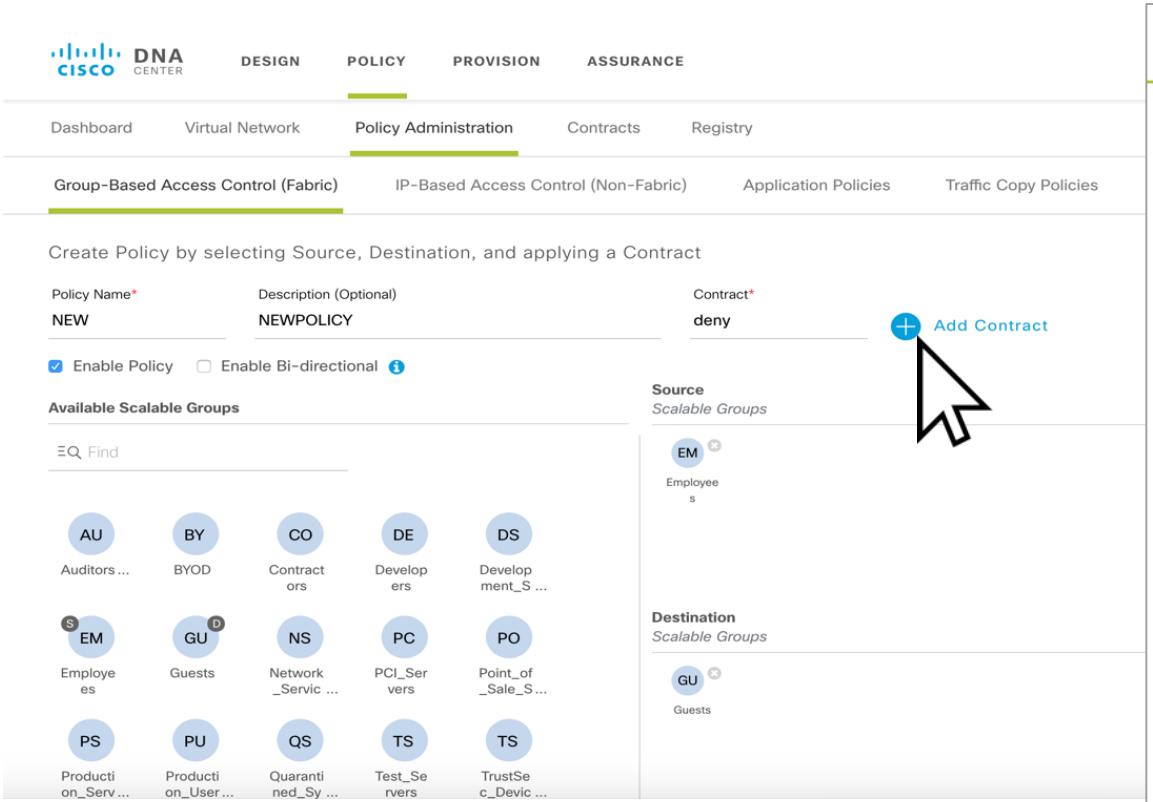
SD-Access @ DNA Center

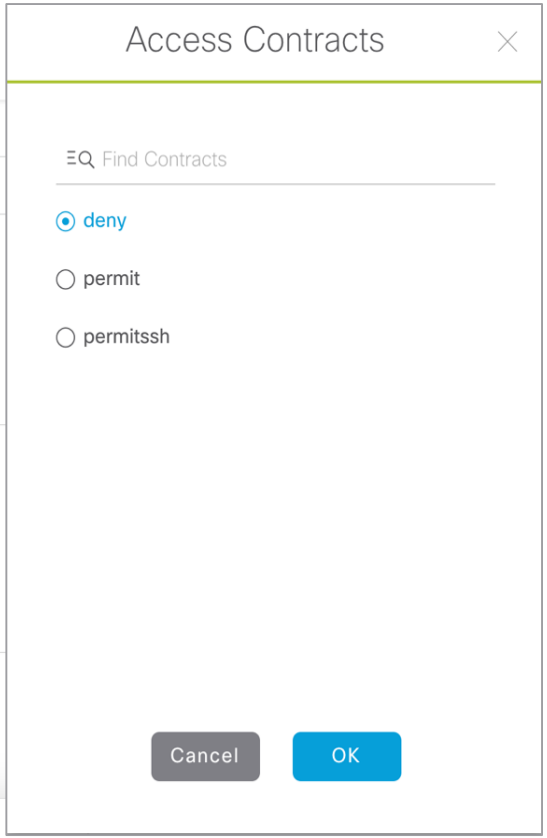
Group-Based Access Control Policy



SD-Access @ DNA Center

Group-Based Access Control Policy





SD-Access Fabric

Unique Data-Plane Extensions compared to LISP

Capability	Traditional CTS	SD-Access Policy
SGT Propagation	Enabled hop-by-hop, or by separate Security-Group Exchange Protocol (SXP) sessions	Carried with the data traffic inside VXLAN-GPO (overlay) end-to-end
VN Integration	Not Supported	VN + SGT-aware Firewalls
Access Control Policy	Yes	Yes
QoS (App) Policy	Not Supported	App based QoS policy, to optimize application traffic priority
Traffic Copy Policy	Not Supported	SRC/DST based Copy policy (using ERSPAN) to capture data traffic

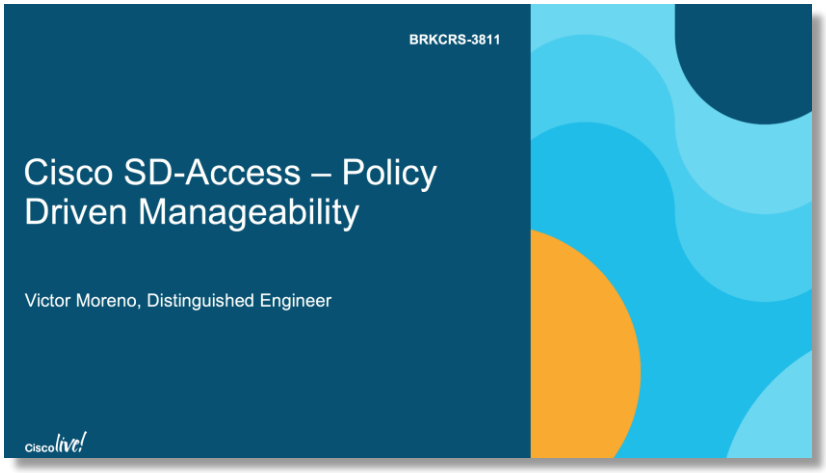
Would you like to know more?

Fabric Wireless

Check out the following session:

BRKCRS-3811

SD-Access - Policy Driven Manageability



This session covers:

- More details about Group-Based Policy
- How VNs and SGTs are related
- Various Fabric Policy design approaches

Controller Fundamentals

What is DNA Center?

1. DNAC Architecture
2. DNAC User Interface
3. DNAC Workflows

SD-Access

DNA Center Appliance

DNA Center Platform

DN1-HW-APL

DNAC 1.1 Scale: Per Node

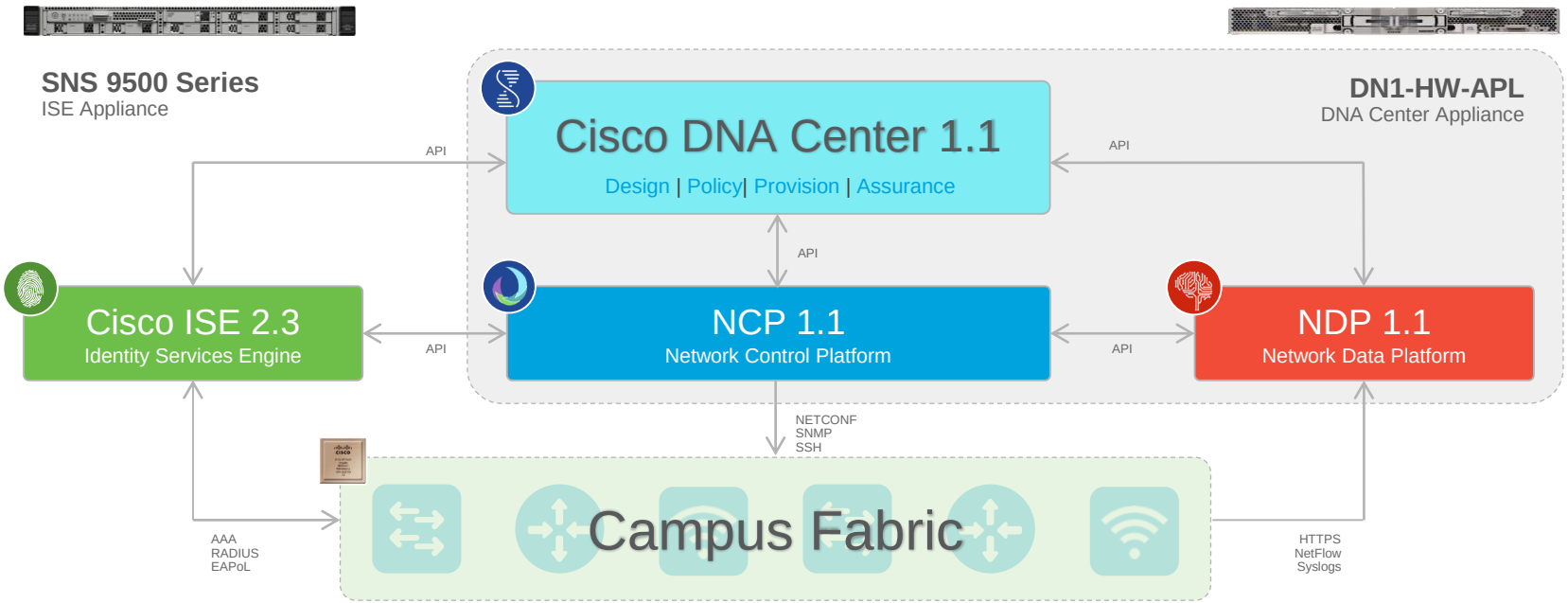
- 5,000 Nodes (1K Devices + 4K APs)
- 25,000 Clients (Concurrent Hosts)

- **Fully Integrated Automation & Assurance**
  - Centralized Deployment - Cloud Tethered
  - Built-In Telemetry Collectors (FNF, SNMP, Syslog, etc)
  - Built-In Contextual Connectors (ISE/PxGrid, IPAM, etc)
  - Multi-Node High Availability (3 Node, Automation)
  - RBAC, Backup & Restore, Scheduler, APIs
- **1RU Server (Small form factor)**
  - UCS 220 M4: 64-bit x86
  - vCPU: 44 core (2.2GHz)
  - RAM: 256GB DDR4
  - Control Disks: 2 x 480GB SSD RAID1
  - System Disks: 6 x 1.9TB SSD M-RAID
  - Network: 2 x 10GE SFP+
  - Power: 2 x 770W AC PSU

Single Appliance for DNAC (Automation + Assurance)

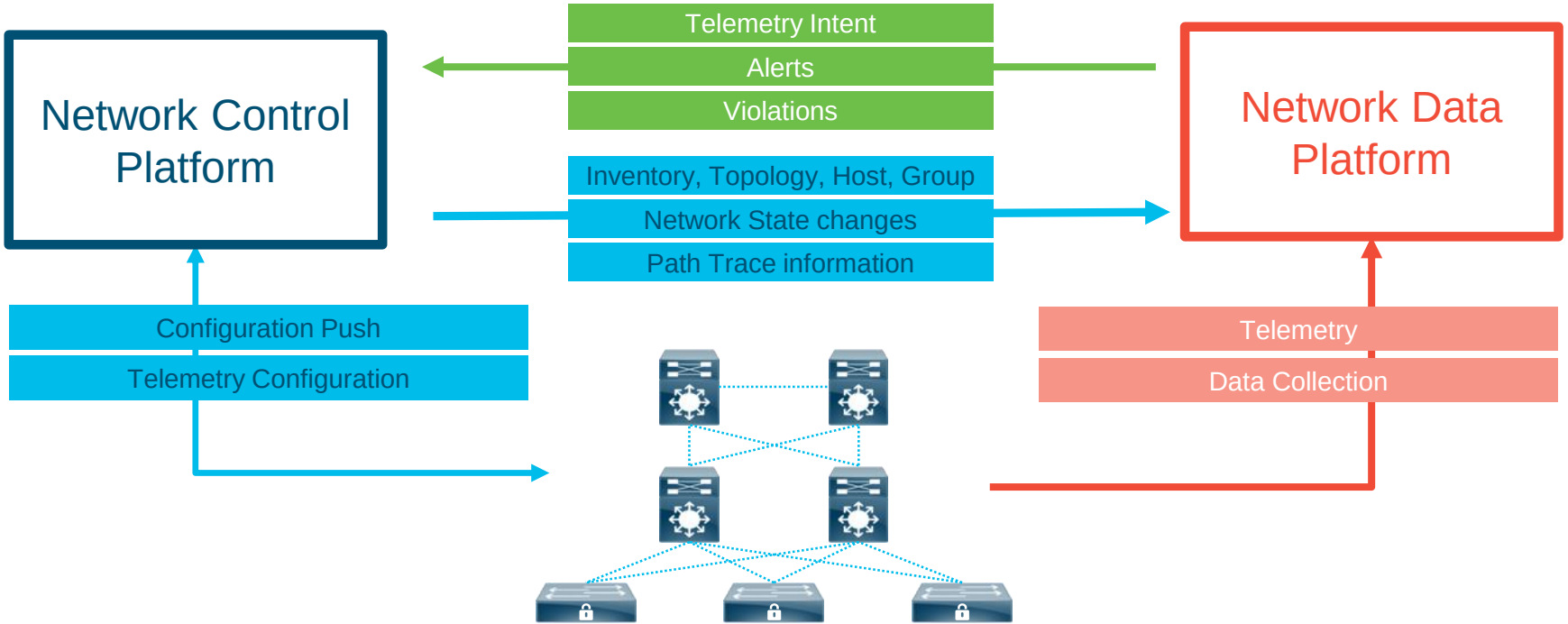
SD-Access

DNA Center – Service Components



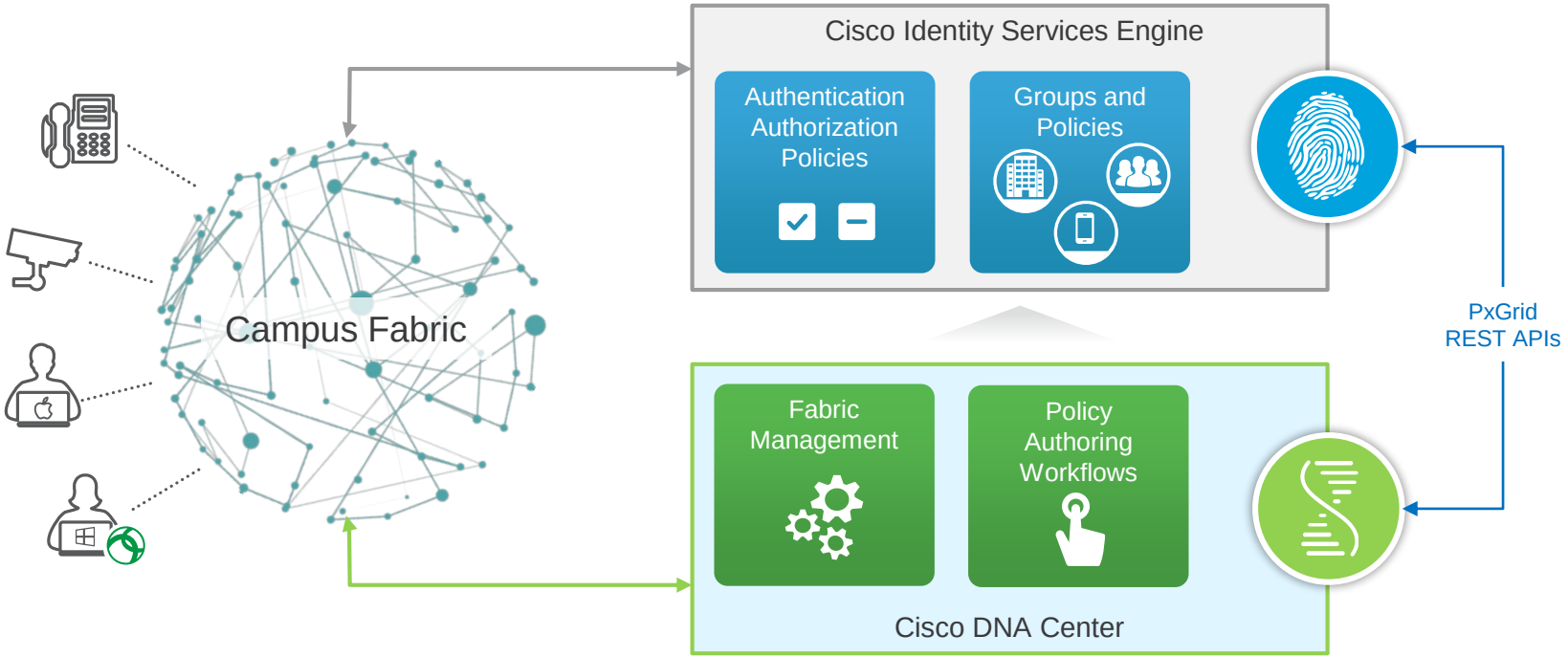
DNA Center Interaction

Automated Provisioning and Telemetry Enrichment



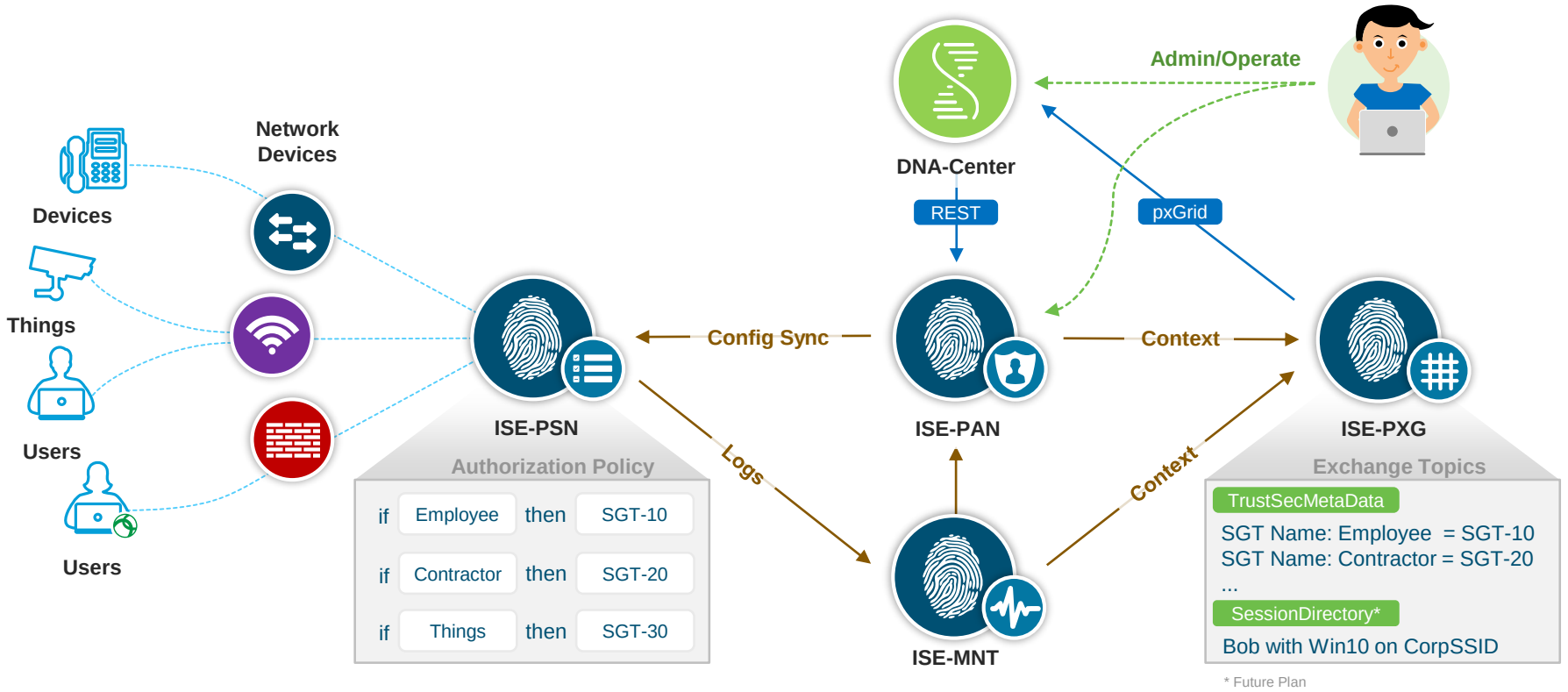
DNA Center and ISE integration

Identity and Policy Automation



DNA Center and ISE integration

ISE node roles in SD-Access



Controller Fundamentals

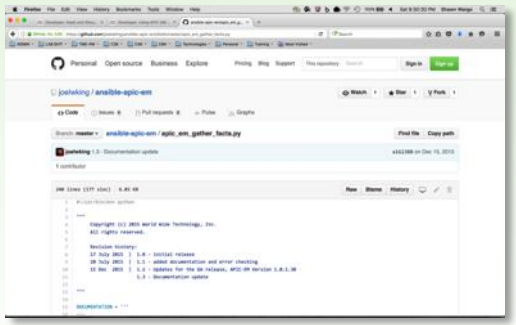
What is DNA Center?

1. DNAC Architecture
2. DNAC User Interface
3. DNAC Workflows

SD-Access

Campus Fabric + DNA Center (Automation & Assurance)

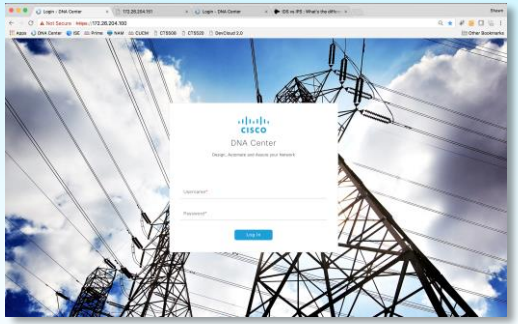
Campus Fabric



- SmartCLI Macros
- Simple User Inputs
- Customized Workflows
- Box-by-Box Management

- Programmable APIs
- NETCONF / YANG
- Automated Workflows
- Box-by-Box Management

SD Access

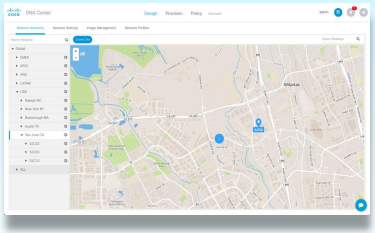


- DNA Center GUI
- Cross-App REST APIs
- Automated Workflows
- Centralized Management

DNA Center

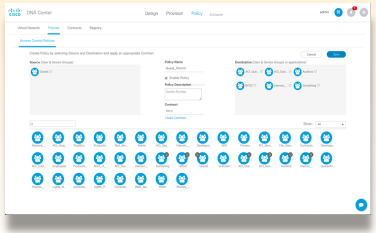
4 Step Workflow

Design



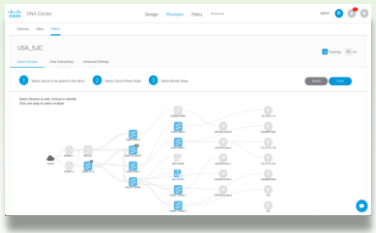
- Global Settings
- Site Profiles
- DDI, SWIM, PNP
- User Access

Policy



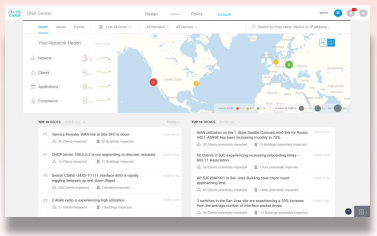
- Virtual Networks
- ISE, AAA, Radius
- Endpoint Groups
- Group Policies

Provision



- Fabric Domains
- CP, Border, Edge
- FEW, OTT WLAN
- External Connect

Assurance

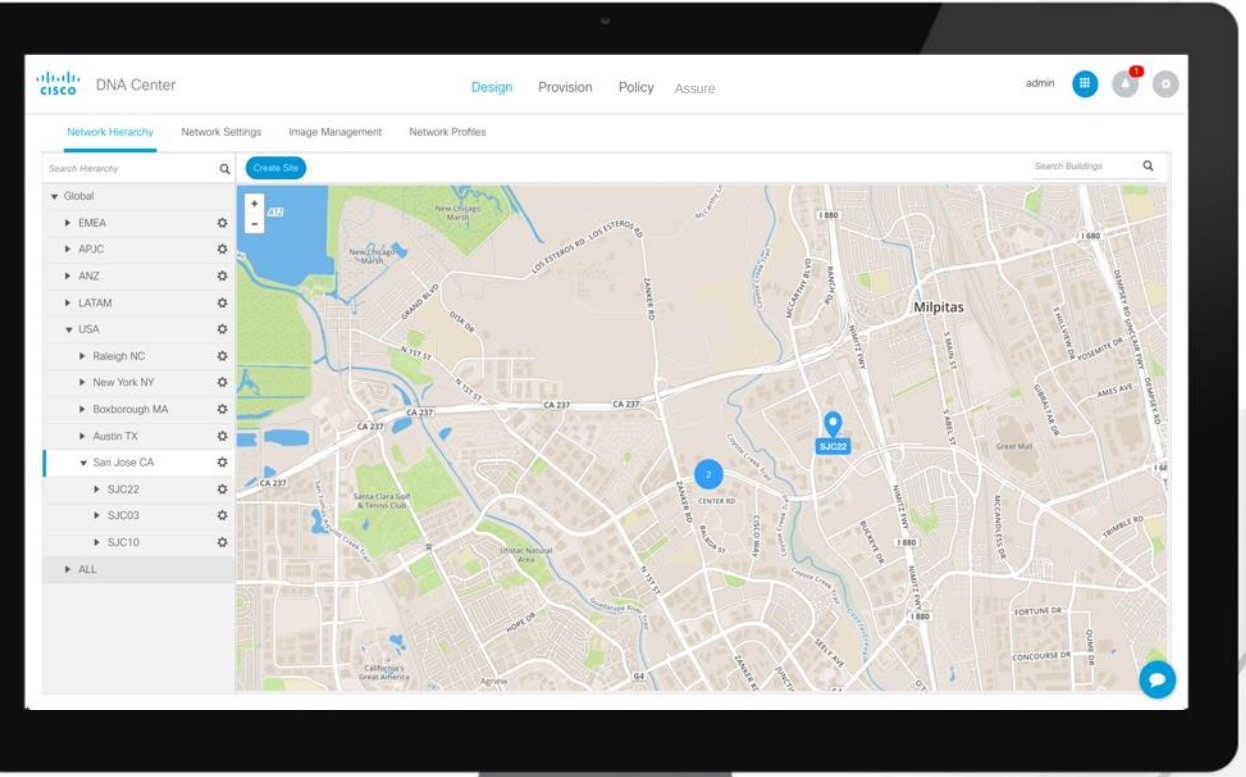


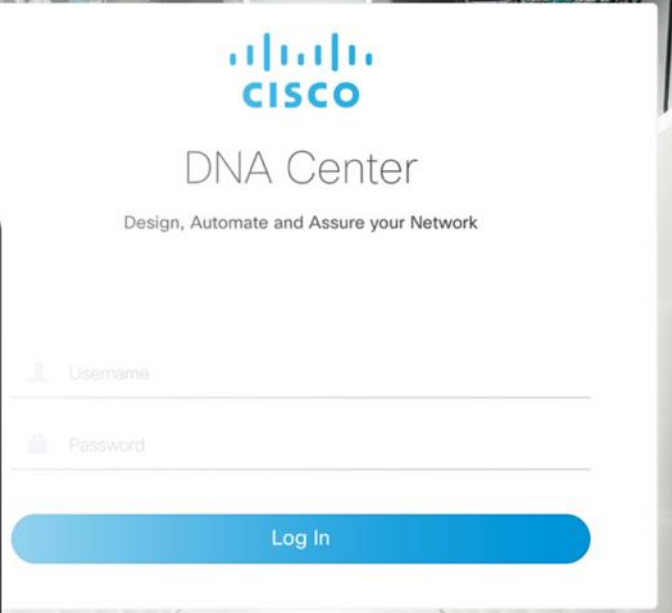
- Health Dashboard
- 360º Views
- FD, Node, Client
- Path Traces

Planning & Preparation

Installation & Integration

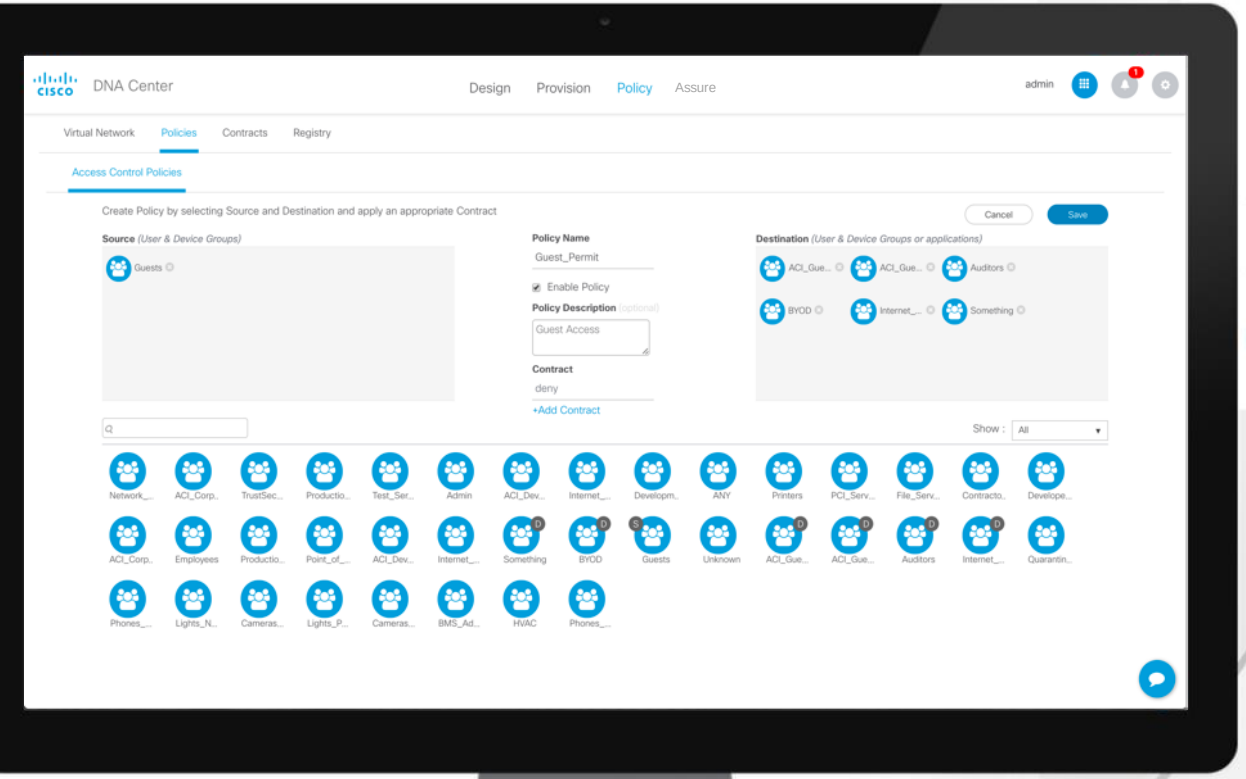
SDA - Design

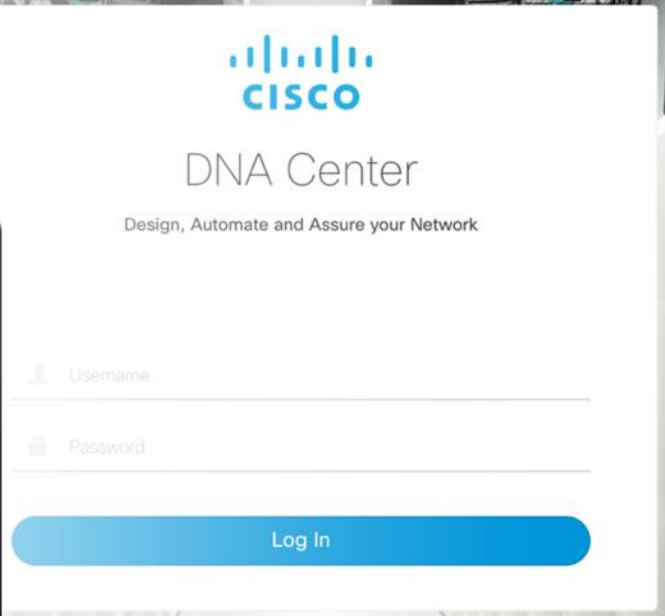




Network Hierarchy
Network Settings
Image Management
Network Profiles

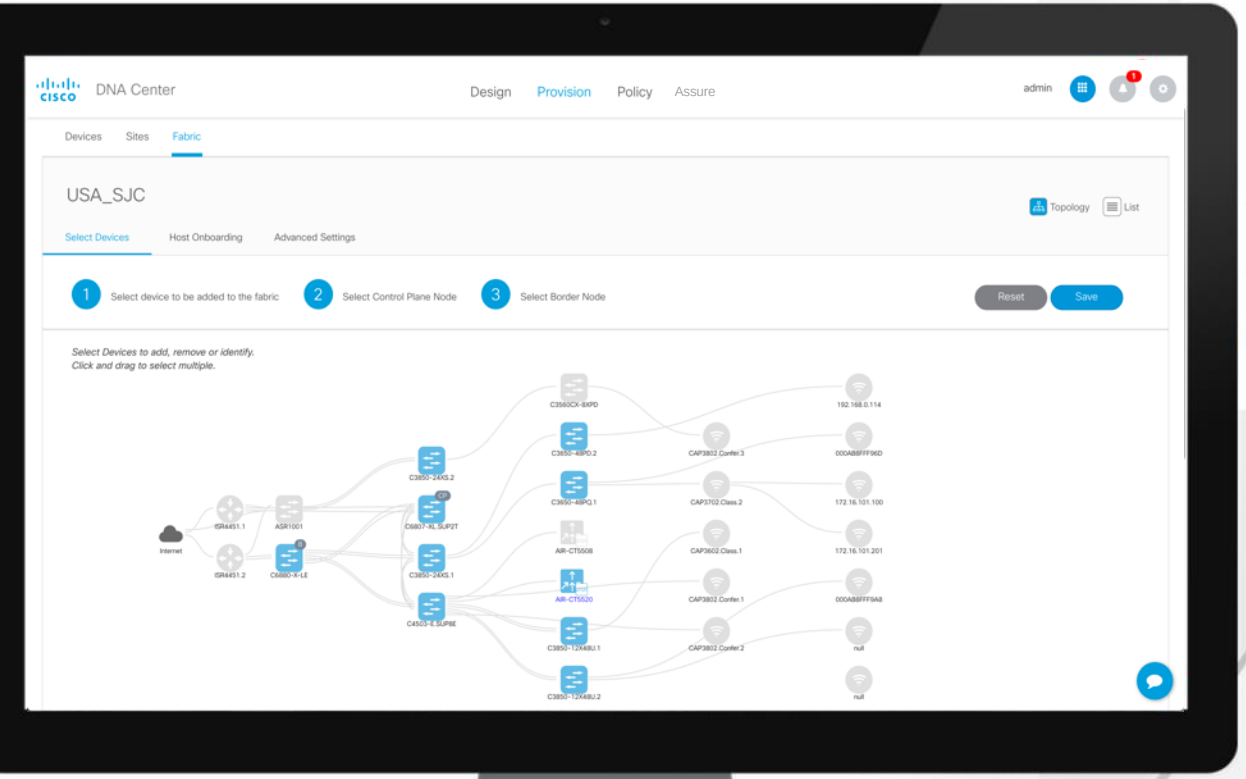
SDA - Policy

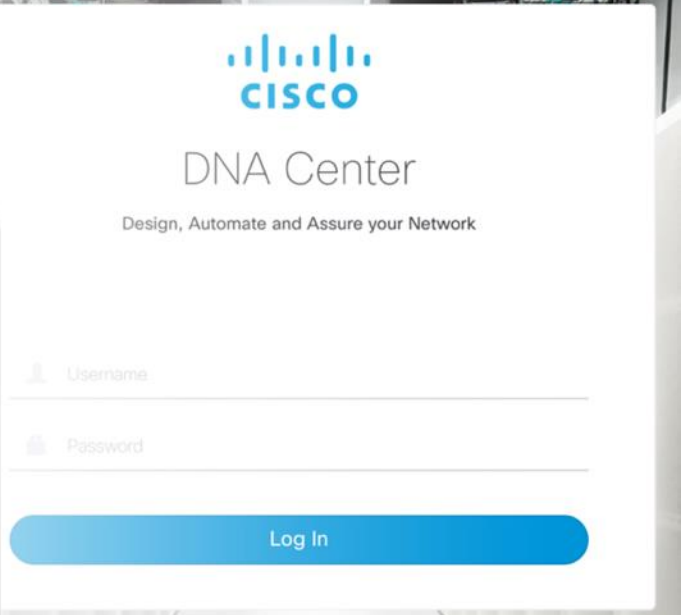




Virtual Networks
Access Control
Application Priority
Application Registry

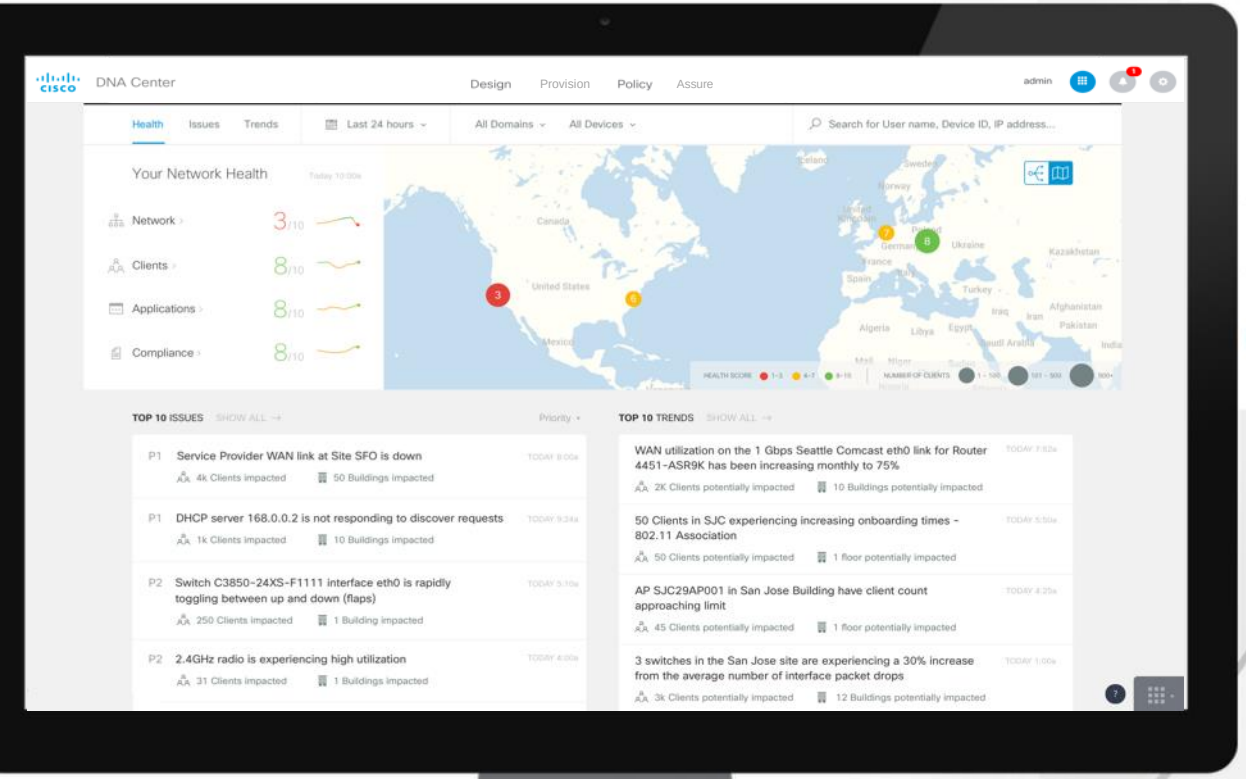
SDA - Provision

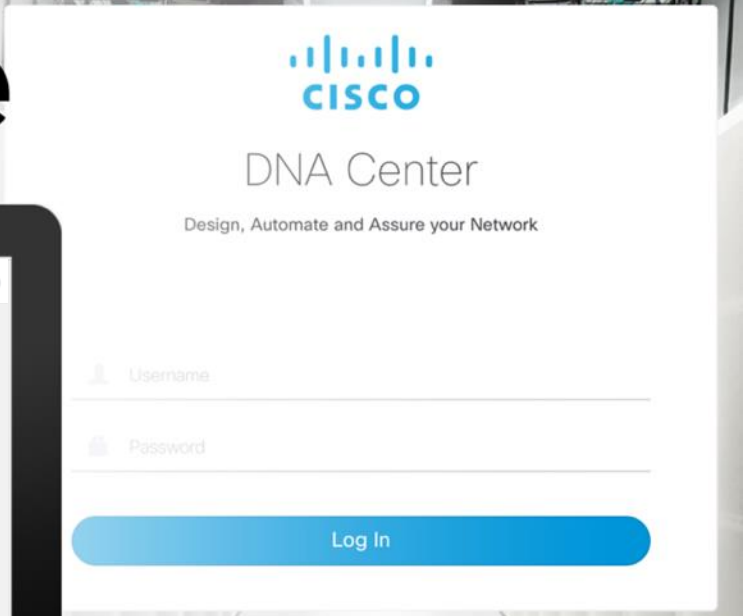




Device On-Boarding
Device Inventory
Fabric Administraton
Host On-Boarding

SDA - Assurance





Health Scores
Client 360
Device 360
Application 360
Click to Resolve

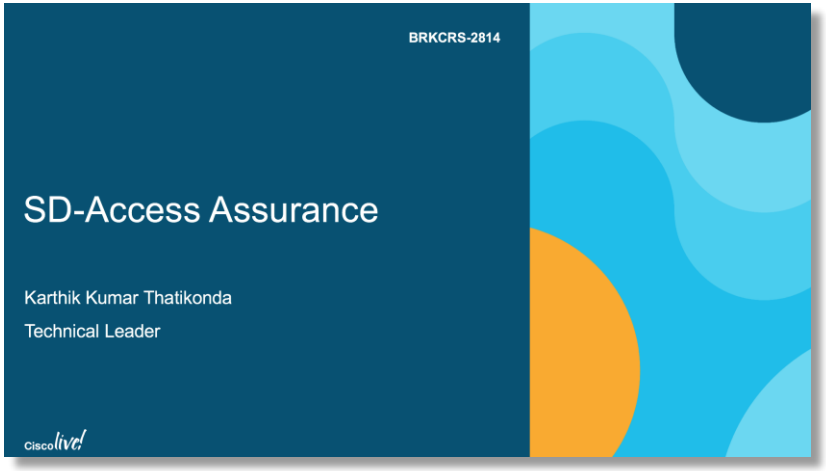
Would you like to know more?

Fabric Assurance

Check out the following session:

BRKCRS-2814

SD-Access - Fabric Assurance



This session covers:

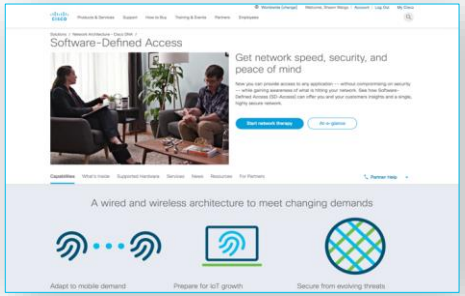
- More details about Fabric Assurance
- How DNA Center uses NDP
- Fabric Assurance best practices & tips

SD-Access Resources

Would you like to known more?

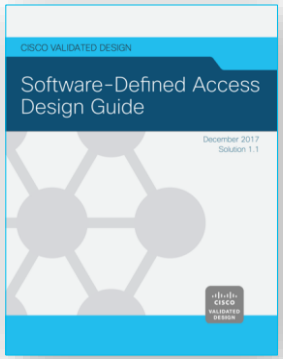
cisco.com/go/sdaccess

- SD-Access At-A-Glance
- SD-Access Design Guide
- SD-Access FAQs
- SD-Access Migration Guide
- SD-Access Solution Data Sheet
- SD-Access Solution White Paper



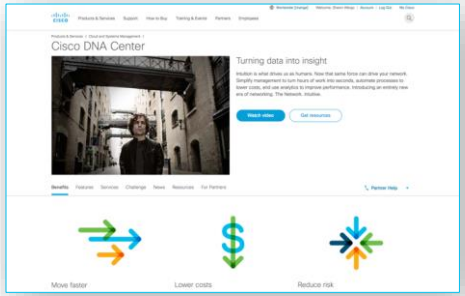
cisco.com/go/cvd

- SD-Access Design Guide - Dec 2017
- SD-Access Deploy Guide - Jan 2018

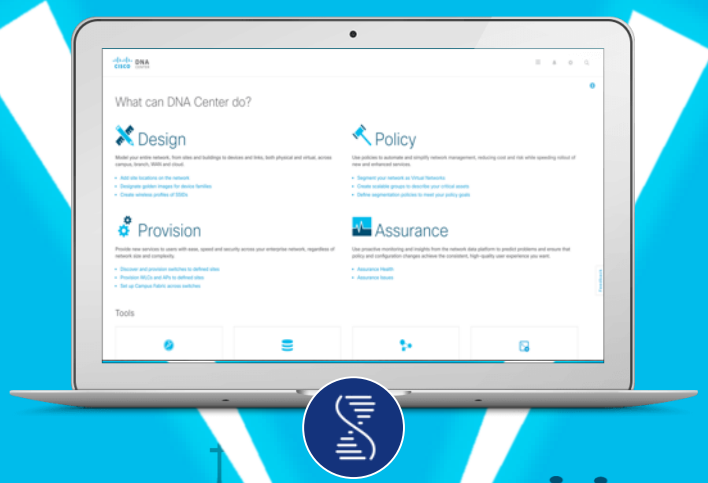


cisco.com/go/dnacenter

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



How about a LIVE Demo?

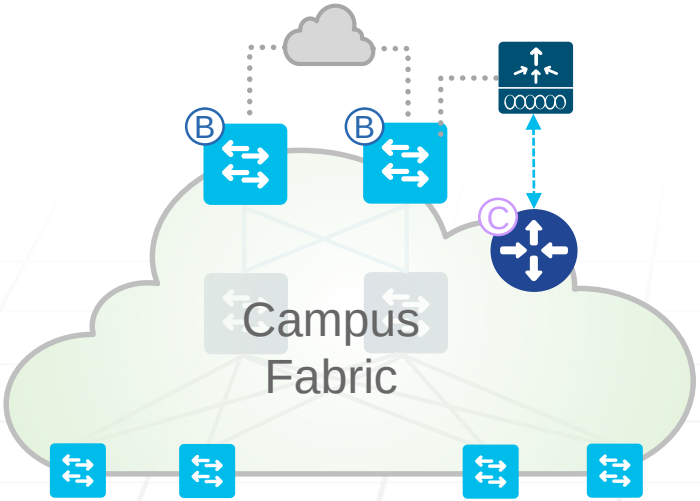


Take Away

Key Points

Session Summary

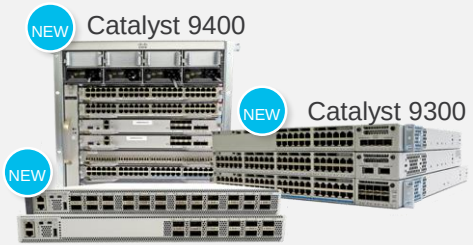
SD-Access = Campus Fabric + DNA Center



SD-Access Support

Fabric ready platforms for your digital ready network

Switching



Catalyst 9500

Catalyst 4500E

Catalyst 6800

Nexus 7700

Catalyst 3650 and 3850

Routing

ASR-1000-X

ASR-1000-HX

ISR 4430

ISR 4450

ISRv/CSRv

Wireless

AIR-CT5520

AIR-CT8540

AIR-CT3504

Wave 2 APs (1800,2800,3800)

Wave 1 APs* (1700,2700,3700)

*with Caveats

Extended

CDB

3560-CX

IE (2K/3K/4K/5K)

What to Do Next?

SD-Access Capable

DNA Center

Cisco Services

Refresh your Hardware & Software

Get **SD-Access Capable Devices** with **DNA Advantage OS License**

Deploy the DNA Center

Get **DNA Center Appliances** with **DNA Center Software**

Engage with Cisco Services

Cisco Services can help you to **Test** - **Migrate** - **Deploy**

SD-Access - Cisco on Cisco

Live SD-Access Deployment @ Cisco Systems

750

Wired & Wireless

users

2 Fabric Border Control-Plane Nodes

7 Fabric Edge Nodes

98 Fabric Access Points

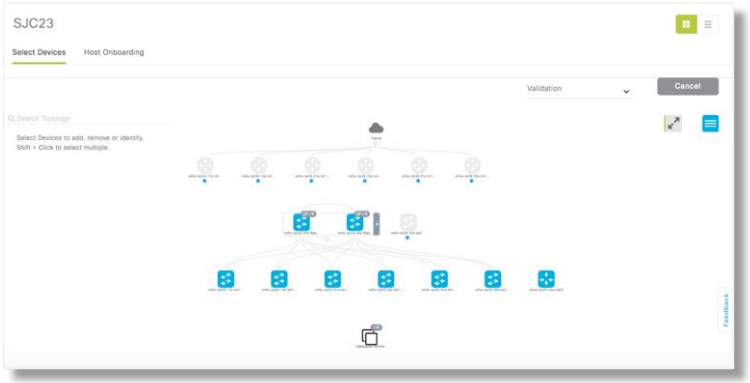
3 Virtual Networks

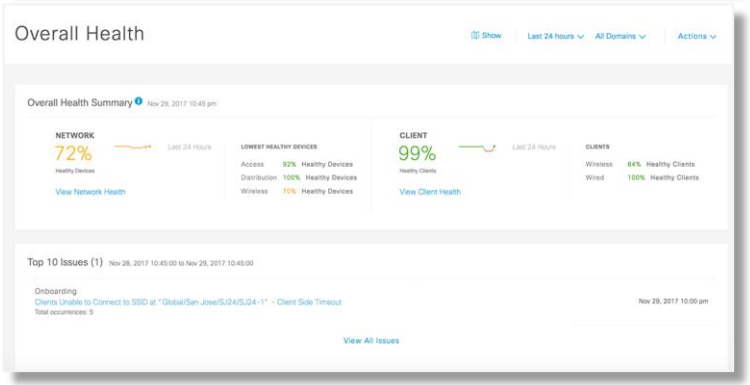
16 Scalable Groups

2 Wireless SSIDs

8 Address Pools

Built and managed by the Cisco Engineering team, in conjunction with Cisco IT Services





Cisco live!


The First Step…
#NewEra
#CiscoDNA
#NetworkIntuitive

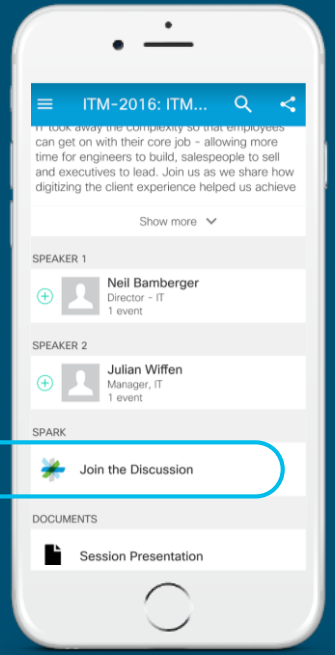
Cisco Spark

Questions?

Use Cisco Spark to communicate with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

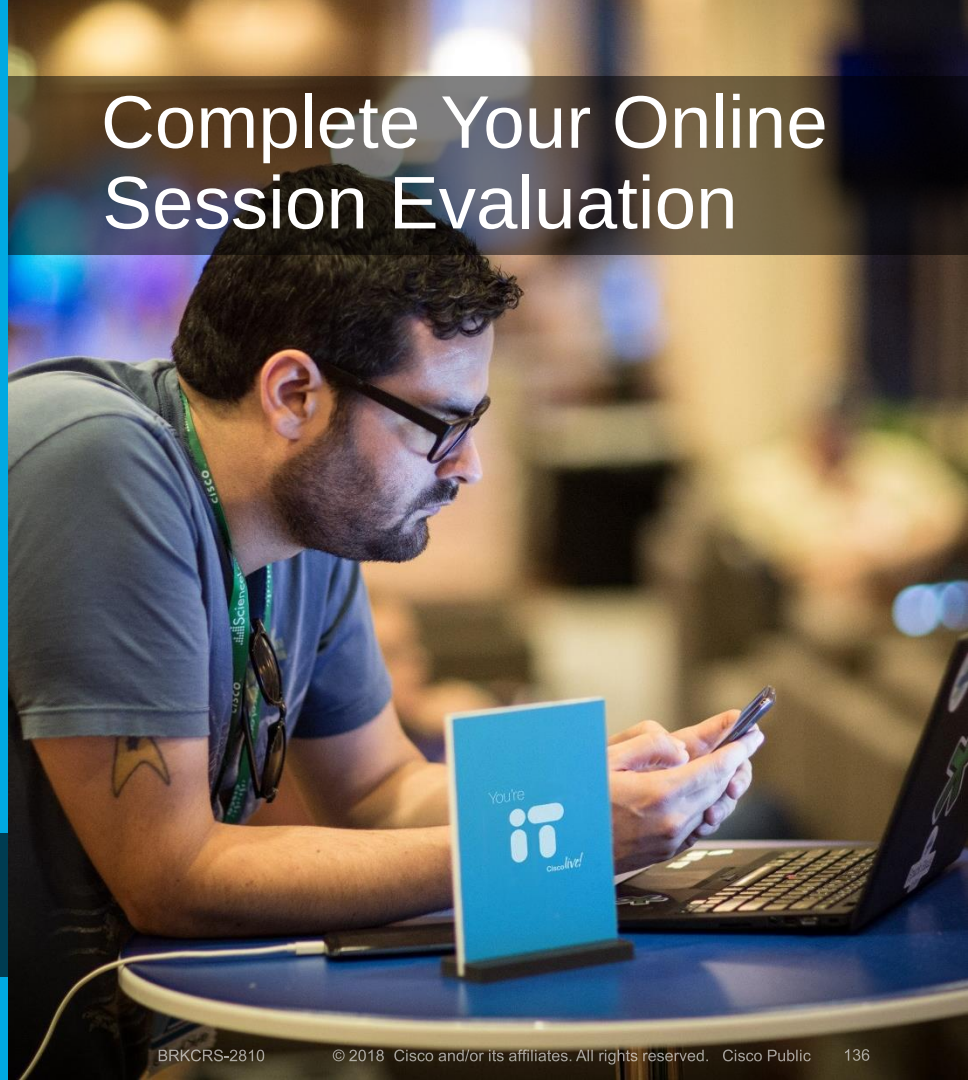


cs.co/ciscolivebot#BRKCRS-2810

Complete Your Online Session Evaluation

- Please complete your Online Session Evaluations after each session
- Complete 4 Session Evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt
- All surveys can be completed via the Cisco Live Mobile App or the Communication Stations

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at www.ciscolive.com/global/on-demand-library/.



Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Tech Circle
- Meet the Engineer 1:1 meetings
- Related sessions

Thank you


You're
Cisco live!