You make **possible**

Cisco Software-Defined Access Solution Fundamentals

“A Look Under The Hood”

Shawn Wargo
Principal Engineer - Technical Marketing

BRKCRS-2810

Barcelona | January 27-31, 2020

Cisco Software-Defined Access Solution Fundamentals

“A Look Under The Hood”

Shawn Wargo
Principal Engineer - Technical Marketing

BRKCRS-2810

Barcelona | January 27-31, 2020

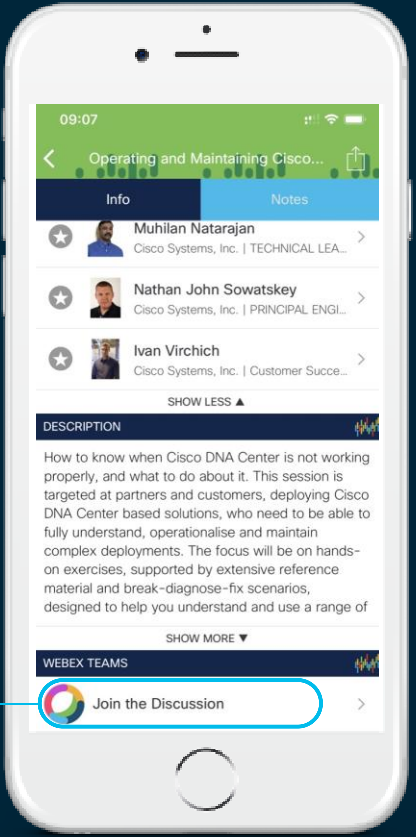
Cisco Webex Teams

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



09:07

Operating and Maintaining Cisco...

Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

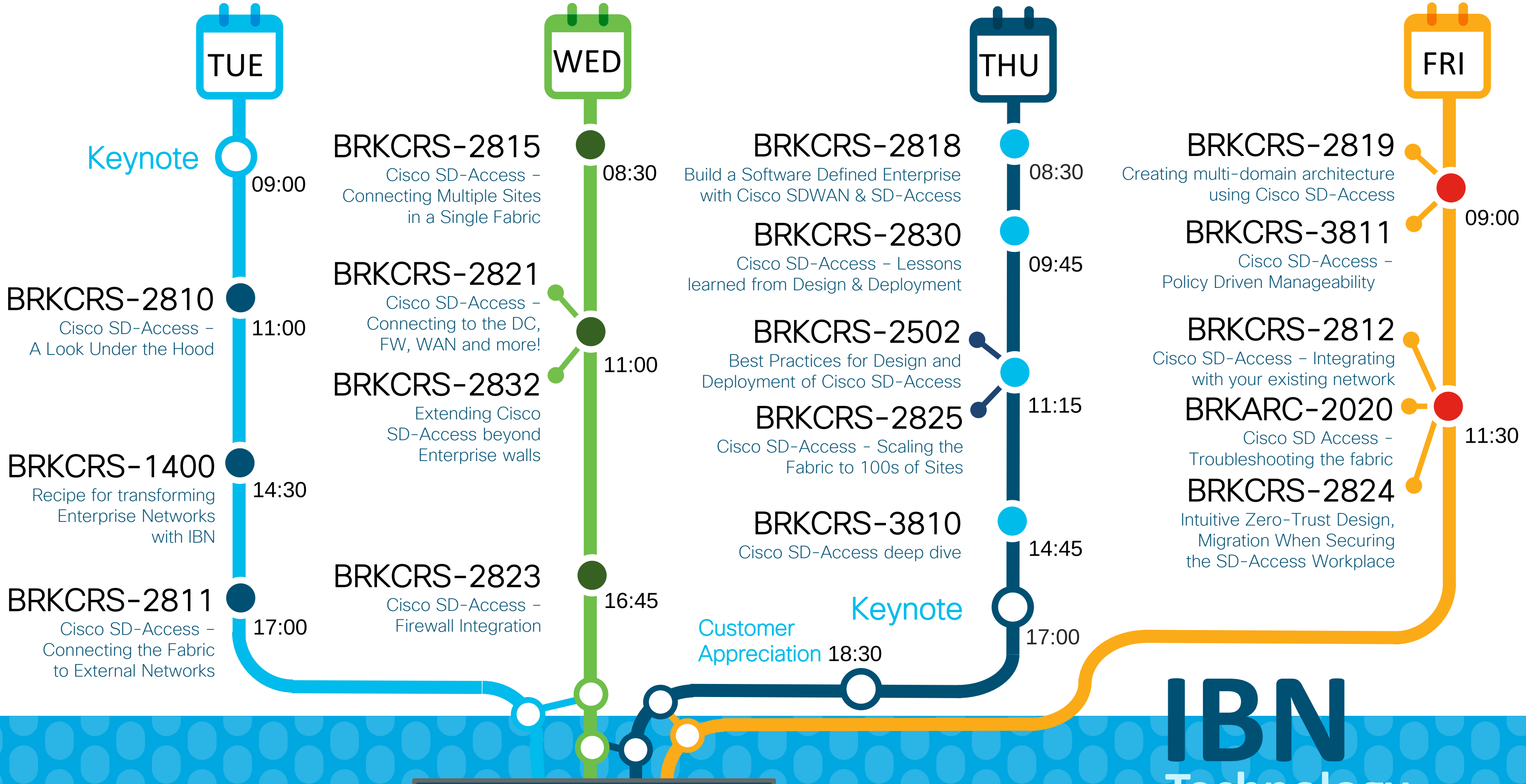
Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

DESCRIPTION

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

WEBEX TEAMS



TUE

Keynote 09:00

BRKCRS-2810 11:00
Cisco SD-Access – A Look Under the Hood

BRKCRS-1400 14:30
Recipe for transforming Enterprise Networks with IBN

BRKCRS-2811 17:00
Cisco SD-Access – Connecting the Fabric to External Networks

WED

BRKCRS-2815 08:30
Cisco SD-Access – Connecting Multiple Sites in a Single Fabric

BRKCRS-2821 11:00
Cisco SD-Access – Connecting to the DC, FW, WAN and more!

BRKCRS-2832 11:00
Extending Cisco SD-Access beyond Enterprise walls

BRKCRS-2823 16:45
Cisco SD-Access – Firewall Integration

THU

BRKCRS-2818 08:30
Build a Software Defined Enterprise with Cisco SDWAN & SD-Access

BRKCRS-2830 09:45
Cisco SD-Access – Lessons learned from Design & Deployment

BRKCRS-2502 11:15
Best Practices for Design and Deployment of Cisco SD-Access

BRKCRS-2825 11:15
Cisco SD-Access – Scaling the Fabric to 100s of Sites

BRKCRS-3810 14:45
Cisco SD-Access deep dive

Keynote 17:00

Customer Appreciation 18:30

FRI

BRKCRS-2819 09:00
Creating multi-domain architecture using Cisco SD-Access

BRKCRS-3811 09:00
Cisco SD-Access – Policy Driven Manageability

BRKCRS-2812 11:30
Cisco SD-Access – Integrating with your existing network

BRKARC-2020 11:30
Cisco SD Access – Troubleshooting the fabric

BRKCRS-2824 11:30
Intuitive Zero-Trust Design, Migration When Securing the SD-Access Workplace

Cisco SD-Access

IBN Technology

cisco Live!

Agenda

Complex
1
2
3
4
5
Time

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?

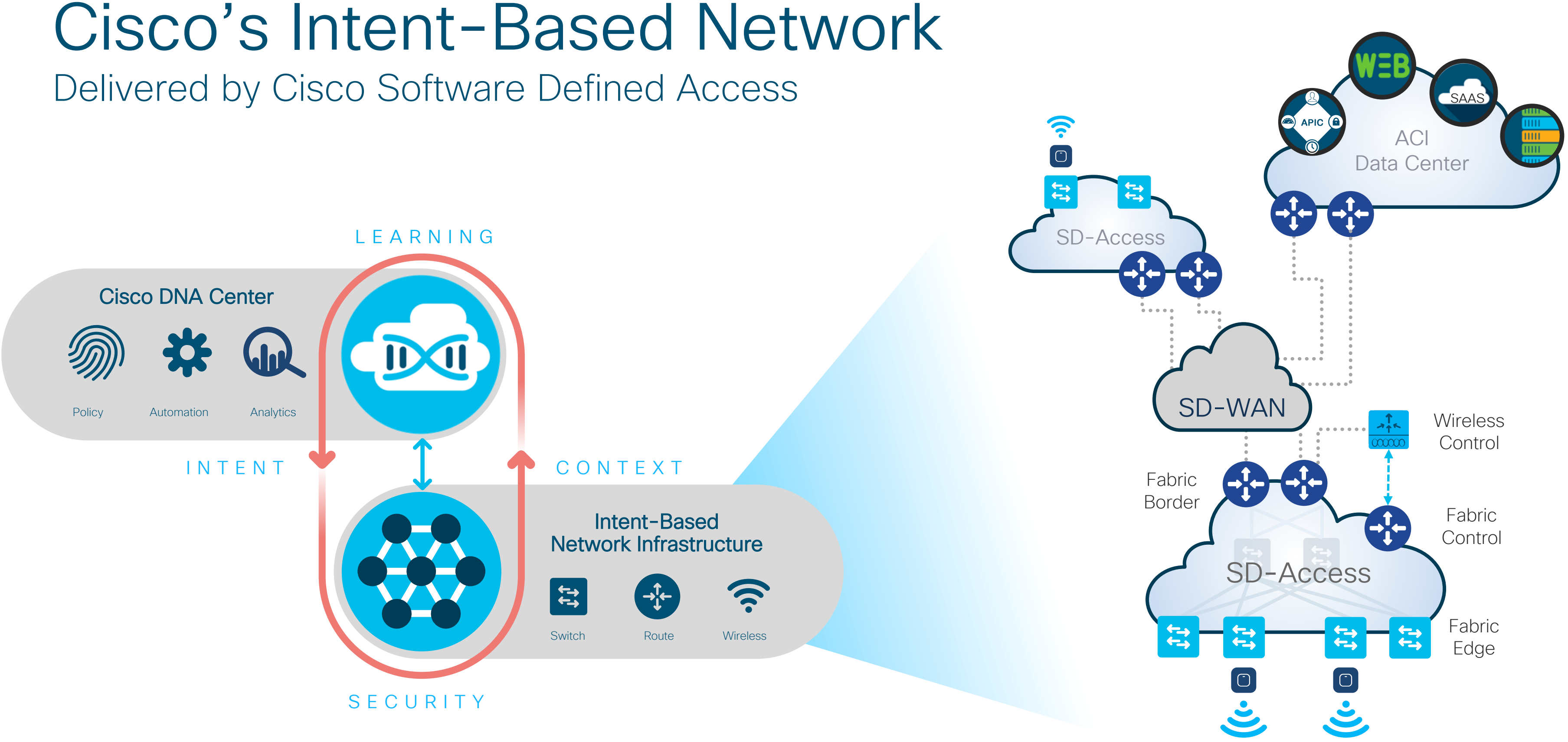
5 **Take Away**
Where to get started?

Why do you care?

Key Benefits

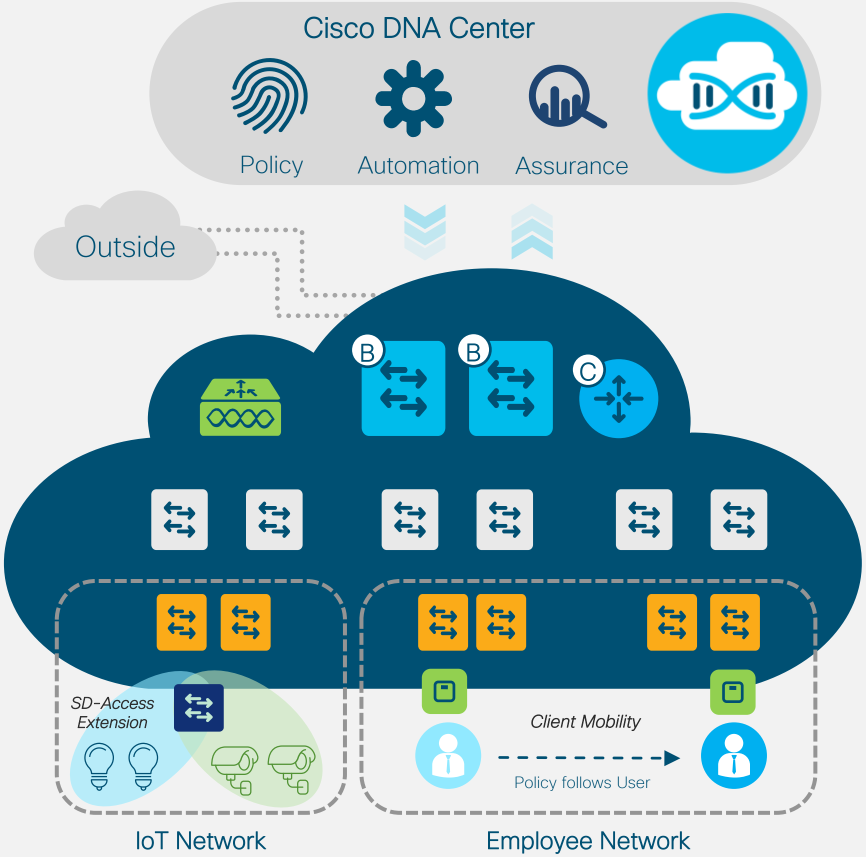
Cisco's Intent-Based Network

Delivered by Cisco Software Defined Access



Cisco Software Defined Access

The Foundation for Cisco's Intent-Based Network



One Automated Network Fabric

Single fabric for Wired and Wireless with full automation

Identity-Based Policy and Segmentation

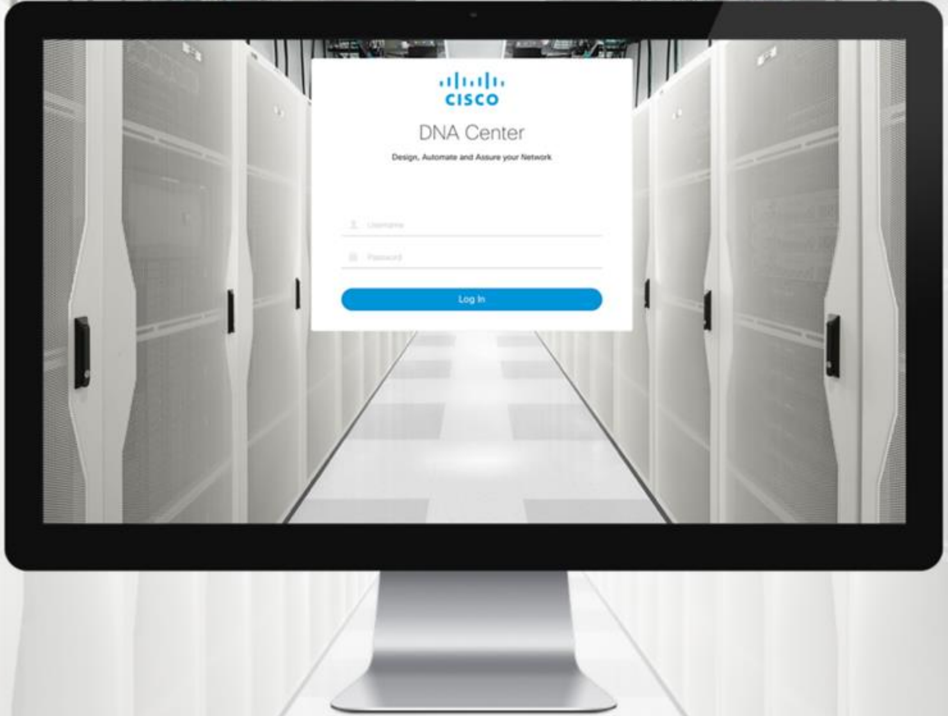
Policy definition decoupled from VLAN and IP address

AI-Driven Insights and Telemetry

Analytics and visibility into User and Application experience

What is Software Defined Access?

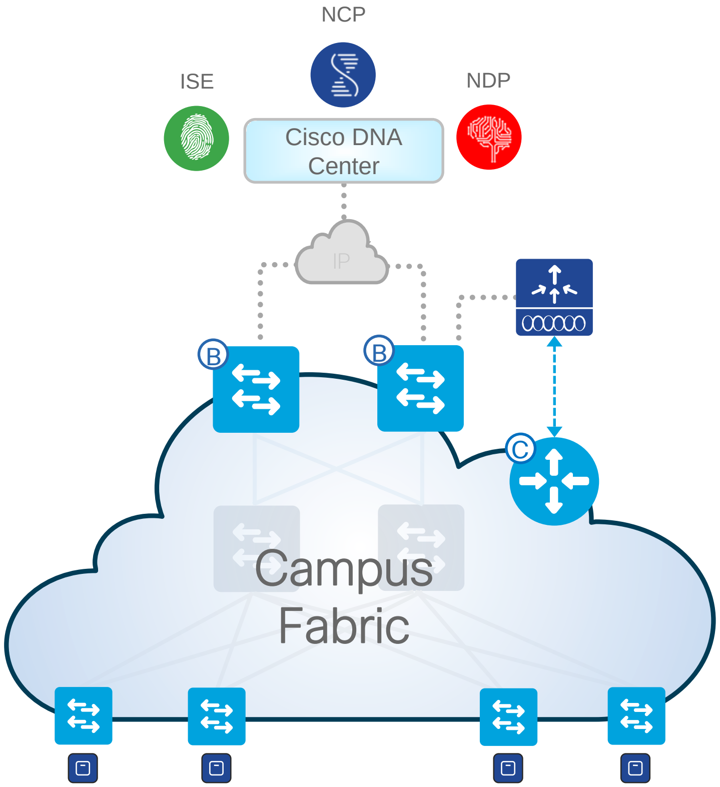
Key Concepts



What is SD-Access?

What is SD-Access?

Campus Fabric + Cisco DNA Center (Automation & Assurance)



- **SD-Access**

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

  Cisco DNA Center integrates multiple management systems, to orchestrate 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 backward compatibility, but management is box-by-box. API provides some automation via NETCONF/YANG, also box-by-box.

  Separate management systems

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

What is Software Defined Access?

Roles & Terminology

SD-Access

What exactly is a Fabric?

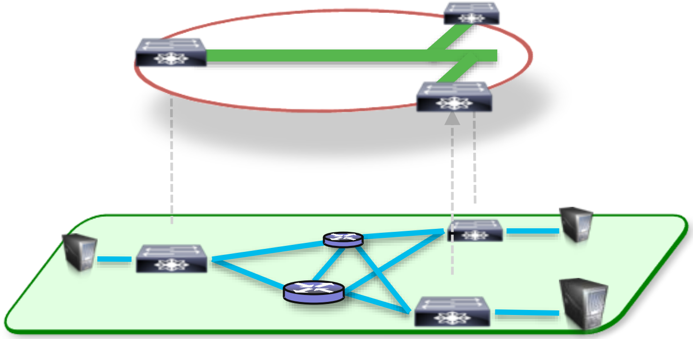
A Fabric is an Overlay

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*.

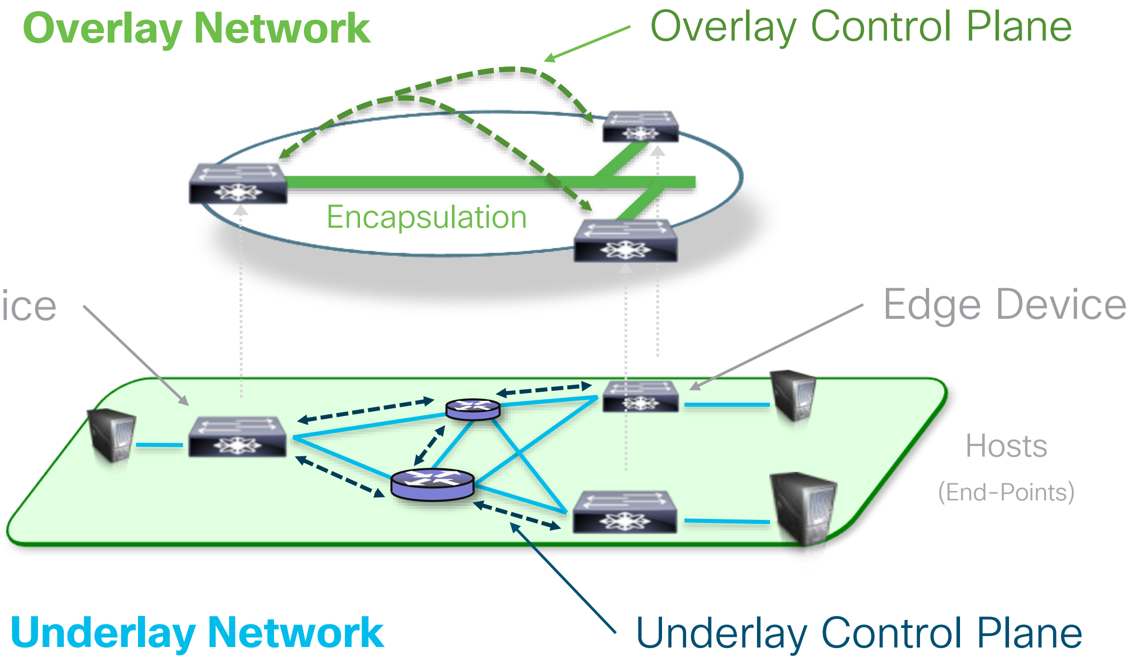
Examples of Network Overlays

- GRE, mGRE
- MPLS, VPLS
- IPSec, DMVPN
- CAPWAP
- LISP
- OTV
- DFA
- ACI



SD-Access

Fabric Terminology



SD-Access

Fabric Underlay – Manual vs. Automated

Manual Underlay

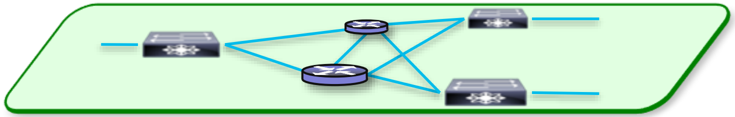
You can reuse your existing IP network as the Fabric Underlay!

- **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)

LAN Automation

Fully automated prescriptive IP network Underlay Provisioning!

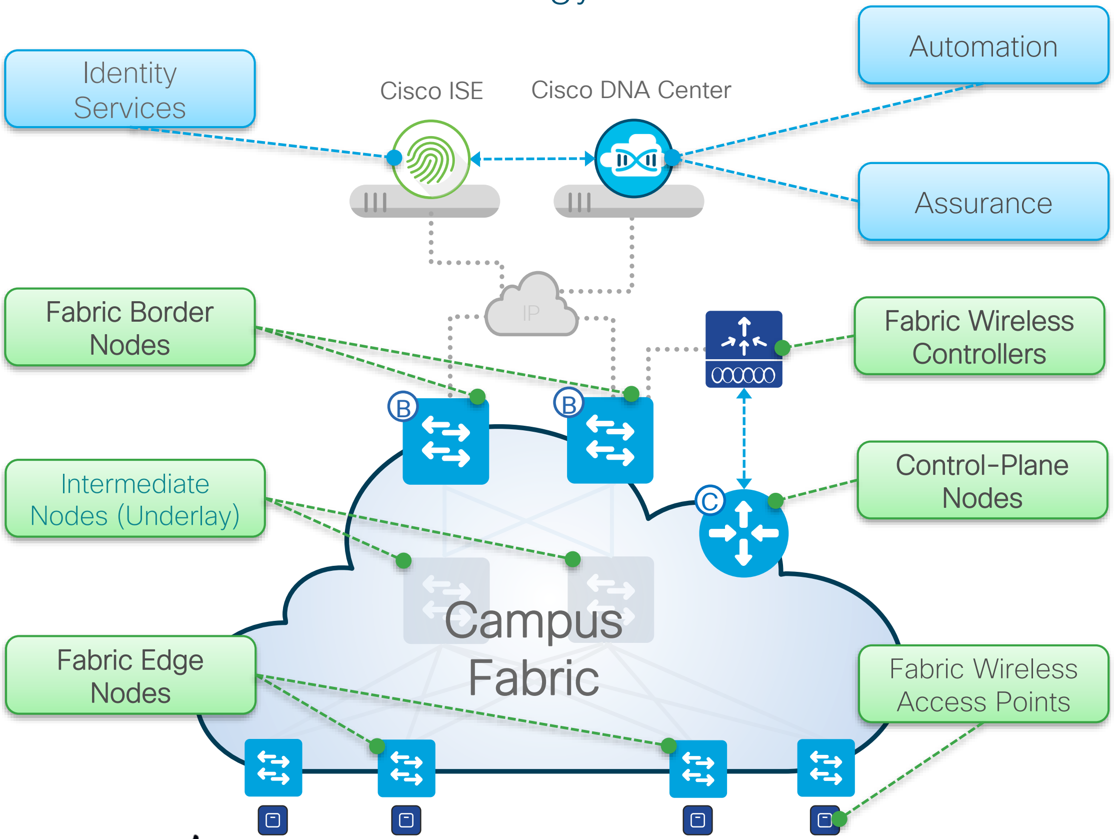
- **Key Requirements**
  - Leverages standard PNP for Bootstrap
  - Assumes New / Erased Configuration
  - Uses a Global "Underlay" Address Pool
- **Key Considerations**
  - Seed Device pre-setup is required
  - 100% Prescriptive (No Custom)



Underlay Network

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 device 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

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

What is Software Defined Access?

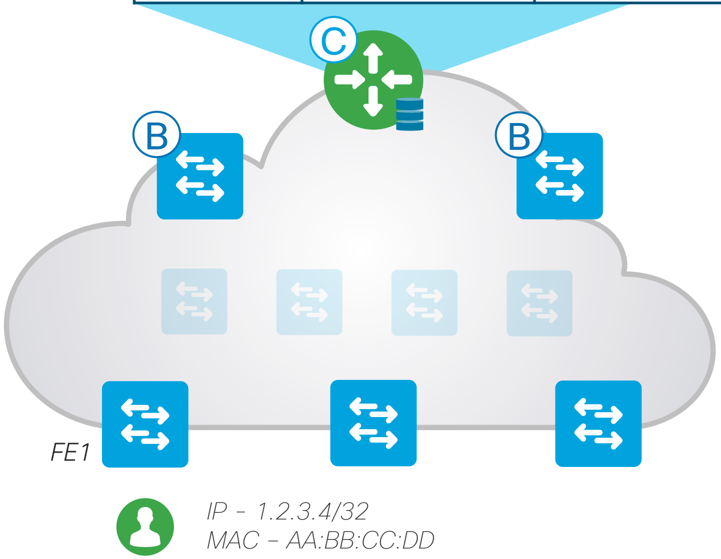
Roles & Terminology

SD-Access Fabric

Control-Plane Nodes – A Closer Look

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

IP to RLOC	MAC to RLOC	Address Resolution
1.2.3.4 → FE1	AA:BB:CC:DD → FE1	1.2.3.4 → AA:BB:CC:DD



- 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

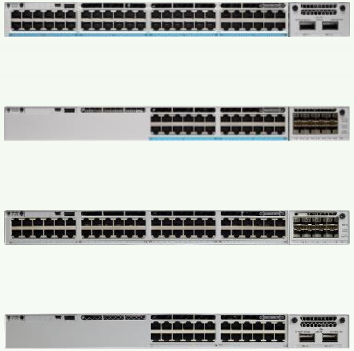
SD-Access Platforms

Fabric Control Plane

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

The Channelco® CRN® Products of the Year 2017, 2018

Catalyst 9300

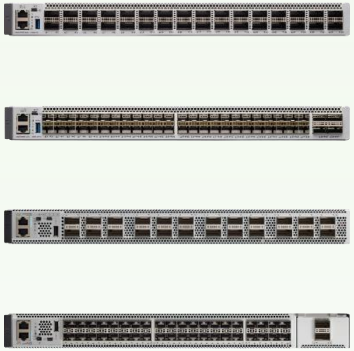


- Catalyst 9300
- 1/mG RJ45
- 10/25/40/mG NM

Catalyst 9400

- Catalyst 9400
- Sup1XL
- 9400 Cards

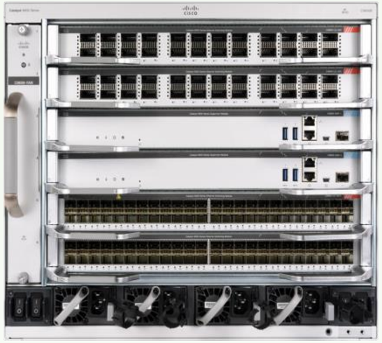
Catalyst 9500



- Catalyst 9500
- 40/100G QSFP
- 1/10/25G SFP

NEW

Catalyst 9600



- Catalyst 9600
- Sup1
- 9600 Cards

SD-Access Platforms

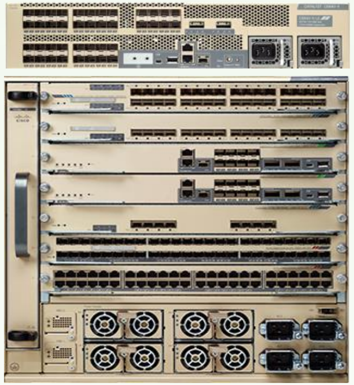
Fabric Control Plane

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

Catalyst 3K

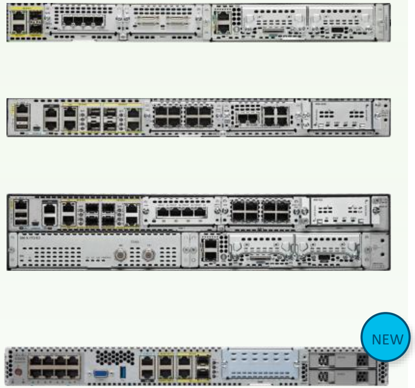
- Catalyst 3650/3850
- 1/mG RJ45
- 1/10G SFP
- 1/10/40G NM Cards

Catalyst 6K



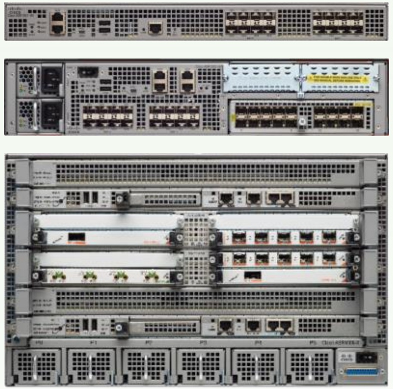
- Catalyst 6500/6800
- Sup2T/Sup6T
- C6800 Cards
- C6880/6840-X

ISR 4K & ENCS



- ISR 4430/4450
- ISR 4330/4450
- ENCS 5400
- ISRv / CSRv

ASR1K



- ASR 1000-X
- ASR 1000-HX
- 1/10G RJ45
- 1/10G SFP

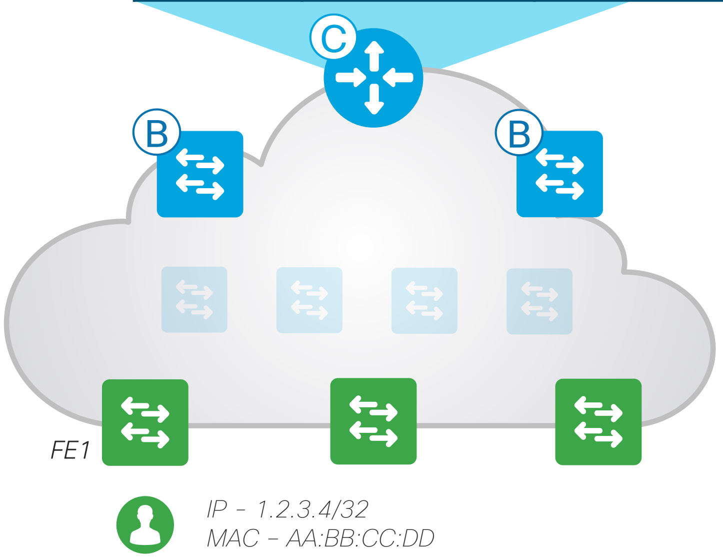
SD-Access Fabric

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

IP to RLOC	MAC to RLOC	Address Resolution
1.2.3.4 → FE1	AA:BB:CC:DD → FE1	1.2.3.4 → AA:BB:CC:DD



SD-Access Platforms

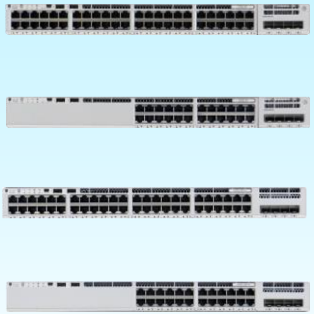
Fabric Edge Node

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

The Channelco®
CRN®
Products of the Year
2017, 2018

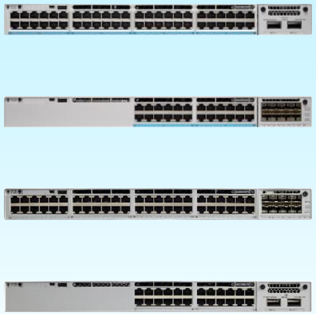
NEW

Catalyst 9200



- Catalyst 9200/L*
- 1/mG RJ45
- 1G SFP (Uplinks)

Catalyst 9300

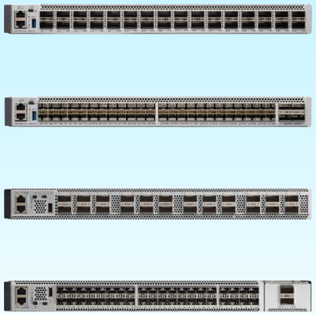


- Catalyst 9300
- 1/mG RJ45
- 10/25/40/mG NM

Catalyst 9400

- Catalyst 9400
- Sup1/Sup1XL
- 9400 Cards

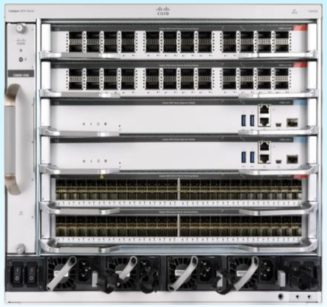
Catalyst 9500



- Catalyst 9500
- 1/10/25G SFP
- 40/100G QSFP

NEW

Catalyst 9600



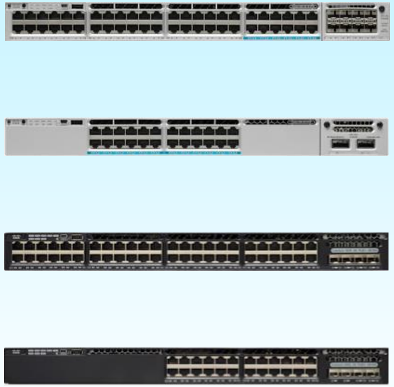
- Catalyst 9600
- Sup1
- 9600 Cards

SD-Access Platforms

Fabric Edge Node

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

Catalyst 3K



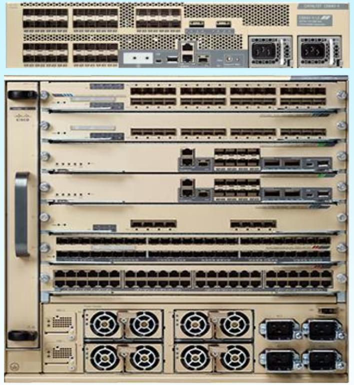
- Catalyst 3650/3850
- 1/mG RJ45
- 1/10G SFP
- 1/10/40G NM Cards

Catalyst 4500E

- Catalyst 4500E
- Sup8E/Sup9E (Uplink)
- 4600/4700 Cards (Host)

NEW

Catalyst 6K



- Catalyst 6500/6800
- Sup2T/Sup6T
- C6800 Cards
- C6880/6840-X

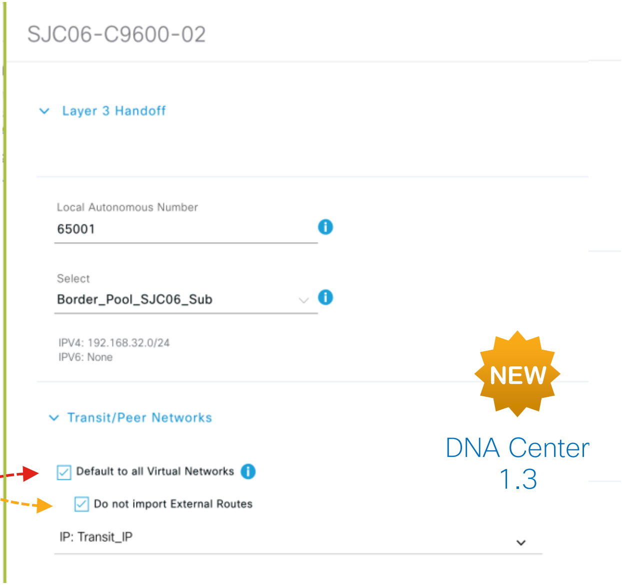
SD-Access Fabric

Border Nodes

Border Node is an Entry & Exit point for data traffic going Into & Out of a Fabric

There are **3 Types** of **Border Node**!

- **Internal Border**
  - connects ONLY to the known areas of the company
- **External Border**
  - connects ONLY to unknown areas outside the company
- **Internal + External**
  - connects transit areas AND known areas of the company



SJC06-C9600-02

Layer 3 Handoff

Local Autonomous Number: 65001

Select: Border_Pool_SJC06_Sub

IPV4: 192.168.32.0/24
IPV6: None

Transit/Peer Networks

☑ Default to all Virtual Networks

☑ Do not import External Routes

IP: Transit_IP

NEW

DNA Center 1.3

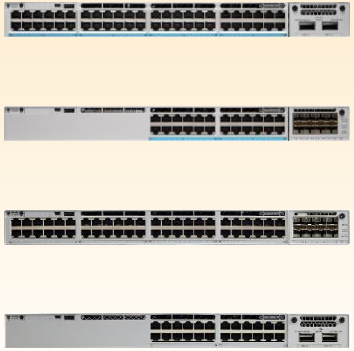
SD-Access Platforms

Fabric Control Plane

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

The Channelco® CRN® Products of the Year 2017, 2018

Catalyst 9300

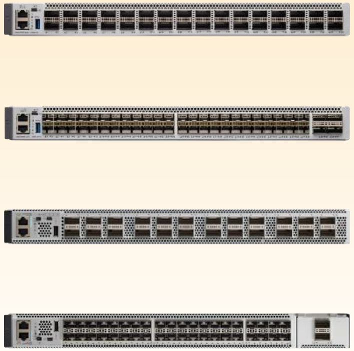


- Catalyst 9300
- 1/mG RJ45
- 10/25/40/mG NM

Catalyst 9400

- Catalyst 9400
- Sup1XL
- 9400 Cards

Catalyst 9500



- Catalyst 9500
- 40/100G QSFP
- 1/10/25G SFP

NEW

Catalyst 9600

- Catalyst 9600
- Sup1
- 9600 Cards

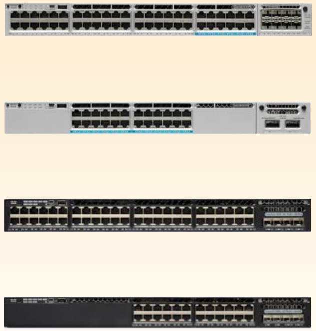
SD-Access Platforms

Fabric Border Node

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

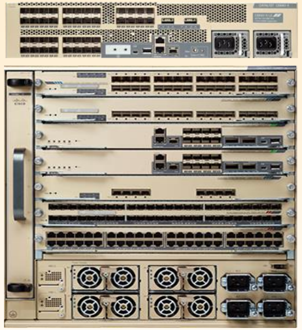
* EXTERNAL ONLY

Catalyst 3K



- Catalyst 3650/3850
- 1/mG RJ45
- 1/10G SFP
- 1/10/40G NM Cards

Catalyst 6K

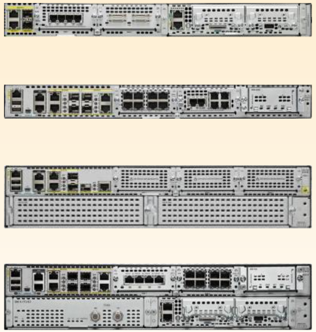


- Catalyst 6500/6800
- Sup2T/Sup6T
- C6800 Cards
- C6880/6840-X

Nexus 7K*

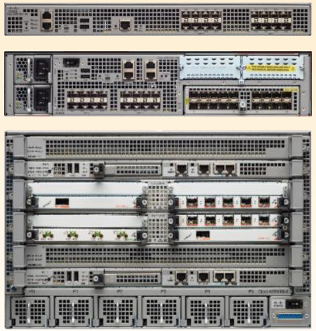
- Nexus 7700
- Sup2E
- M3 Cards
- LAN1K9 + MPLS

ISR 4K



- ISR 4300/4400
- AppX (AX)
- 1/10G RJ45
- 1/10G SFP

ASR 1K



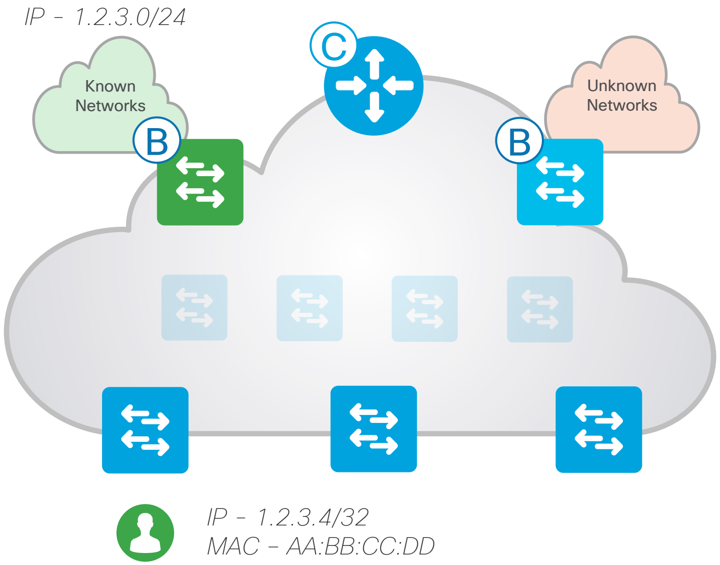
- ASR 1000-X/HX
- AppX (AX)
- 1/10G ELC/EPA
- 40G ELC/EPA

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.

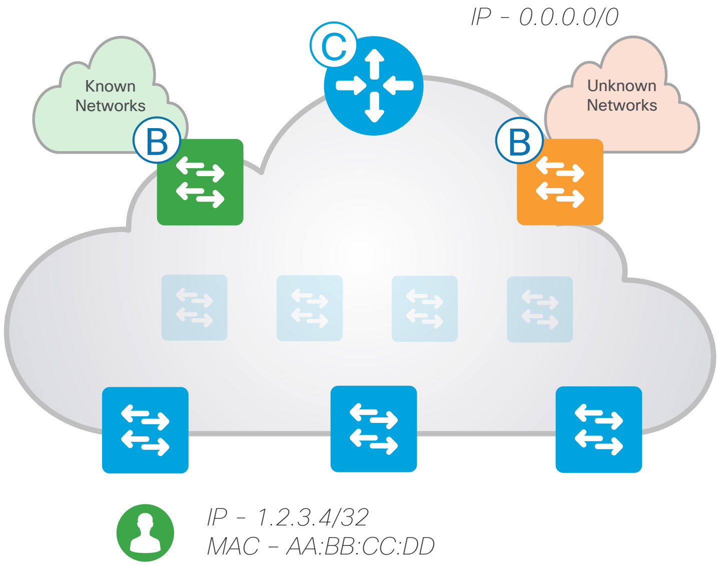


SD-Access Fabric

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.

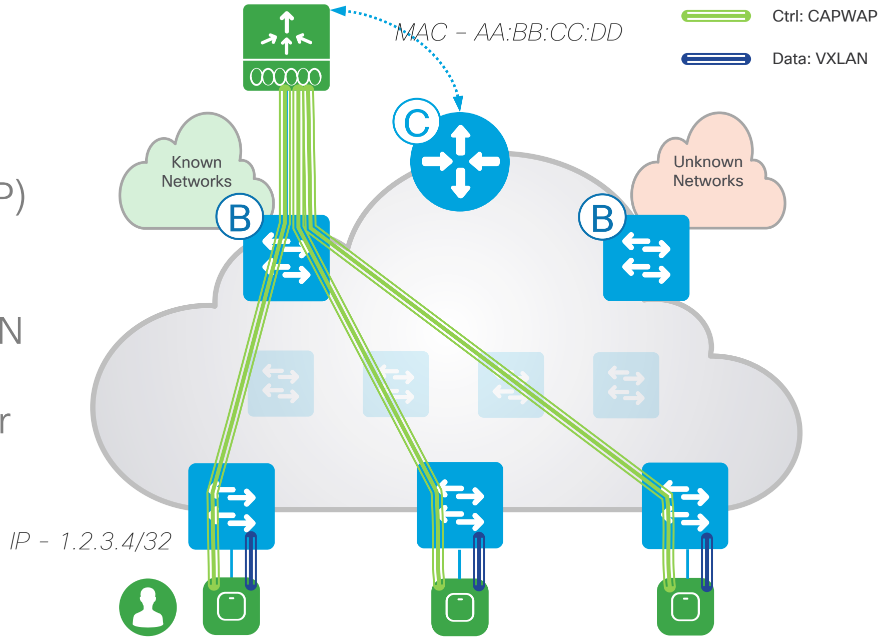


SD-Access Fabric

Fabric Enabled Wireless – A Closer Look

Fabric Enabled WLC is integrated into Fabric for SD-Access 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)



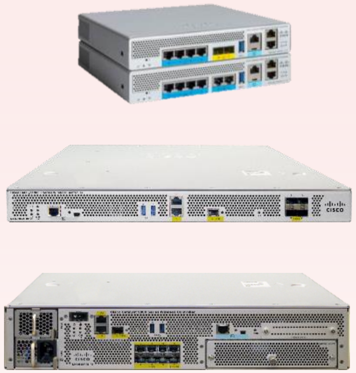
For more details: cs.co/sda-compatibility-matrix

SD-Access Platforms

Fabric Enabled Wireless

Catalyst 9800

NEW



- Catalyst 9800-L
- Catalyst 9800-40
- Catalyst 9800-80
- Catalyst 9800-CL

Catalyst 9100

NEW

- Catalyst 9130
- Catalyst 9120/9115
- 1G/mG RJ45 (Uplink)

AireOS WLC

- AIR-CT3504
- AIR-CT5520
- AIR-CT8540

AireOS AP

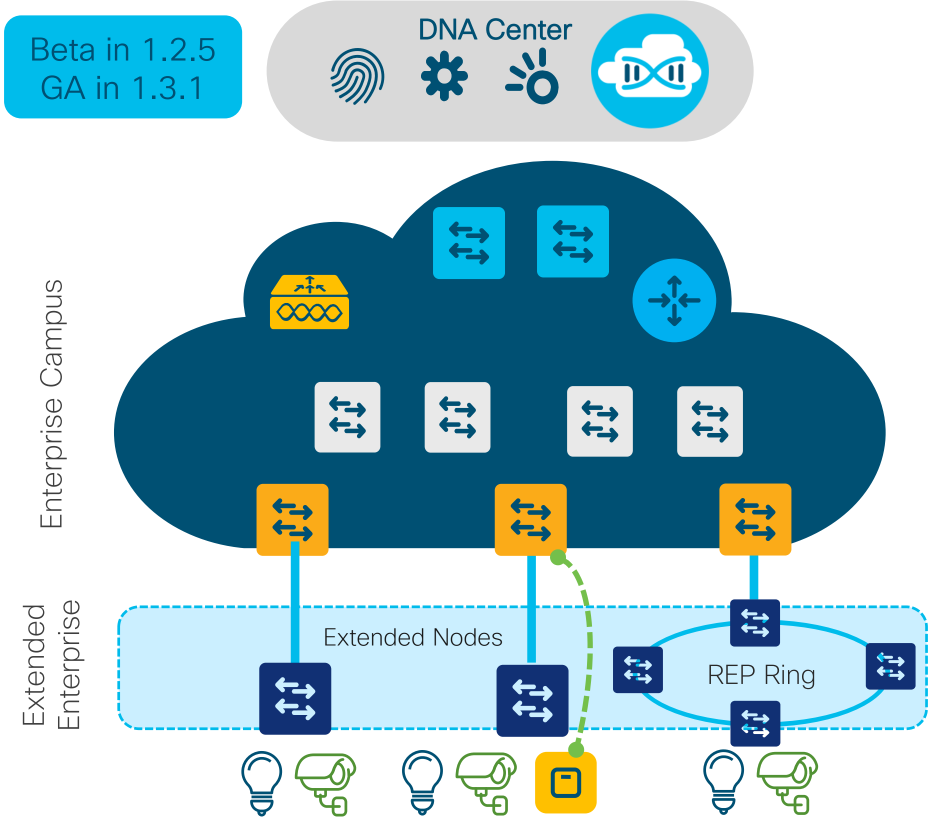
- 1800/2800/3800/4800
- 1700/2700/3700*
- 1G/mG RJ45 (Uplink)

* No IPv6, AVC, FNF

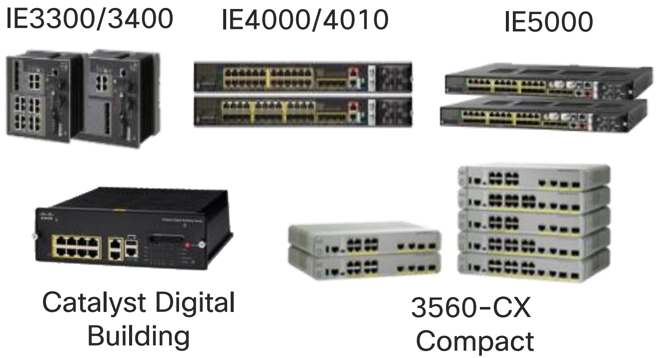
SD-Access Extension for IoT

Securely Consolidate IT and IOT

Beta in 1.2.5
GA in 1.3.1



Extended Node Portfolio



- Operational IOT simplicity (Automation)
  - IT designed and managed -or-
  - IT designed and OT managed
- Greater visibility of IoT devices (Assurance)
- Extended Segmentation & Policy (Security)

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

What is Software Defined Access?

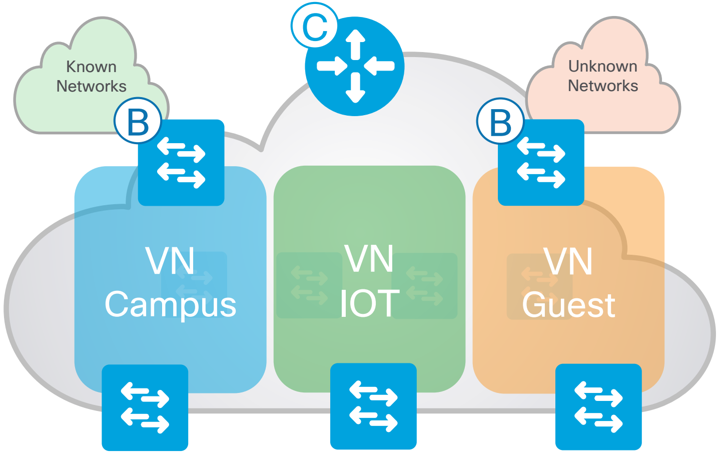
Roles & Terminology

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 a 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)

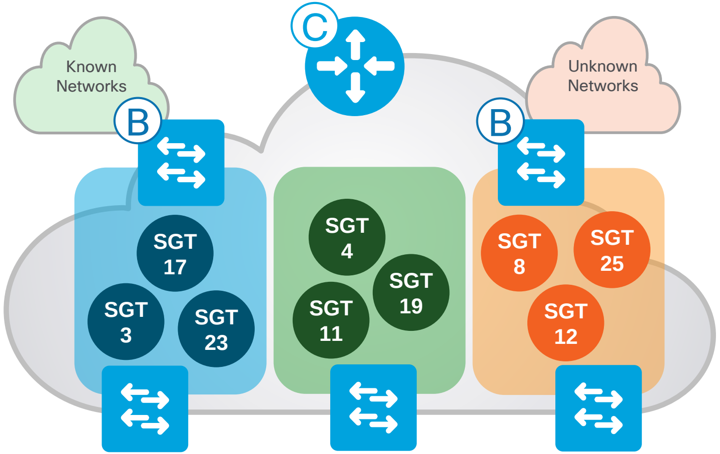


SD-Access Fabric

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 a 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)

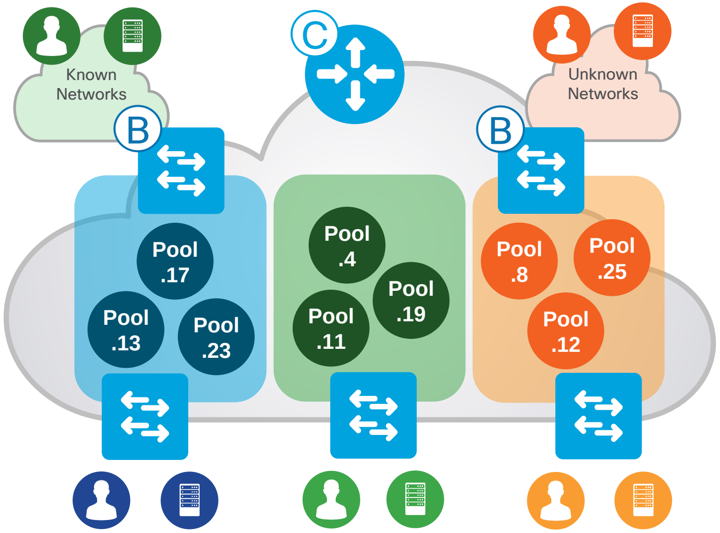


SD-Access Fabric

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 or MAC) advertisement and mobility
- Host Pools can be assigned Dynamically (via Host Authentication) and/or Statically (per port)



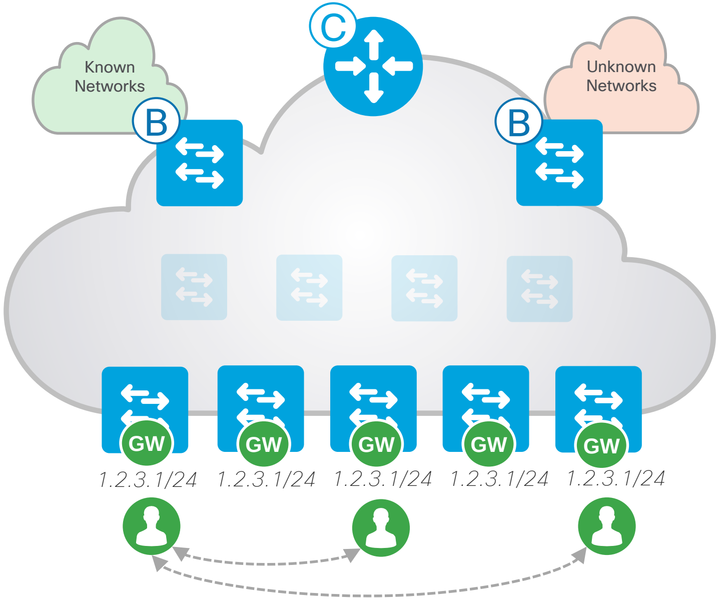
cisco Live!

SD-Access Fabric

Anycast Gateway – A Closer Look

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

- Similar principle and behavior to 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 maintains the Host to Edge relationship
- When a Host moves from Edge 1 to Edge 2, it does not need to change it's Default Gateway ☺

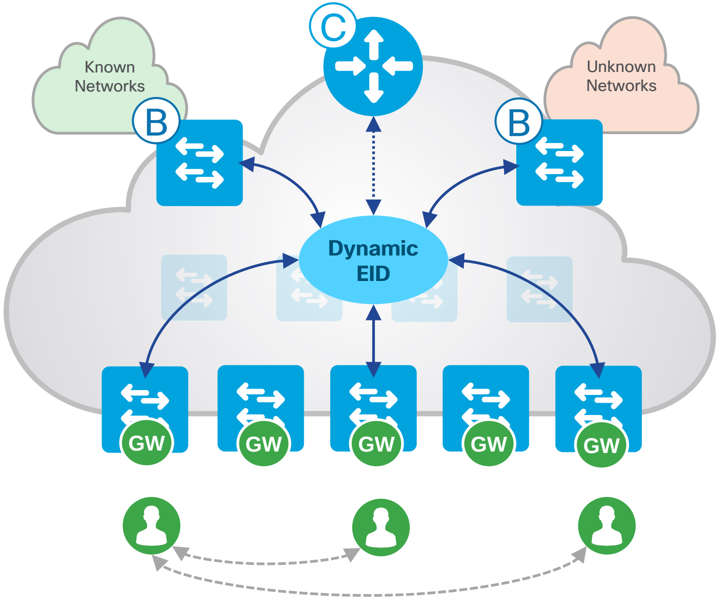


SD-Access Fabric

Layer 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 the 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 ☺

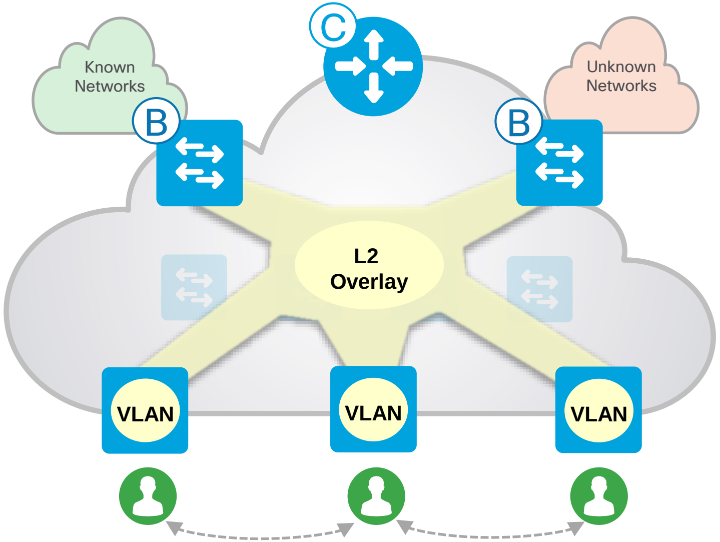


SD-Access Fabric

Layer 2 Overlay – A Closer Look

Layer 2 Overlay 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)



NOTE: L3 Integrated Routing and Bridging (IRB) is not supported at this time.

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

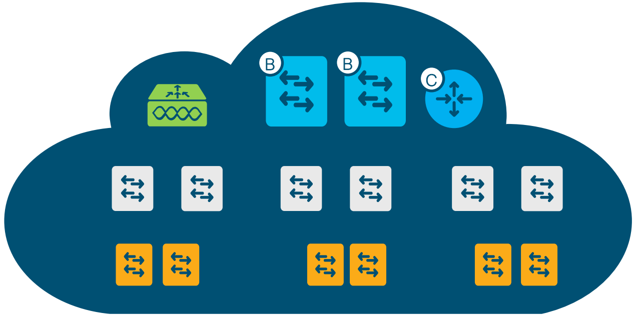
What is Campus Fabric?

Fabric Fundamentals

SD-Access Fabric

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 - LISP

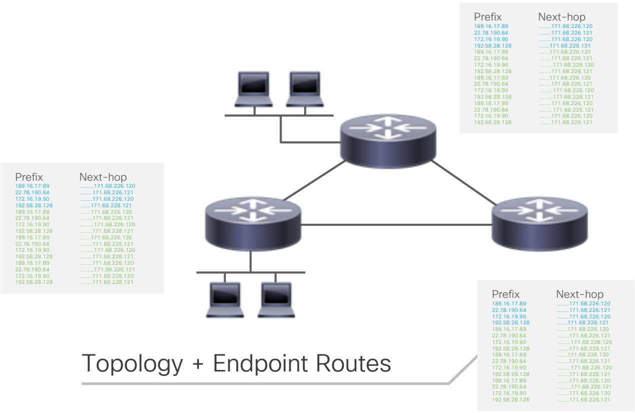
1. Control-Plane based on LISP

Host Mobility

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

BEFORE

IP Address = Location + Identity



Prefix	Next-hop
189.16.17.89	........171.68.226.120
22.78.190.64	........171.68.226.121
172.16.19.90	........171.68.226.120
192.58.28.128	.......171.68.228.121
189.16.17.89	.......171.68.226.120
22.78.190.64	........171.68.226.121
172.16.19.90	.........171.68.226.120
192.58.28.128	........171.68.228.121
189.16.17.89	.......171.68.226.120
22.78.190.64	........171.68.226.121
172.16.19.90	.........171.68.226.120
192.58.28.128	.........171.68.228.121
189.16.17.89	........171.68.226.120
22.78.190.64	.........171.68.226.121
172.16.19.90	........171.68.226.120
192.58.28.128	........171.68.228.121

Prefix	Next-hop
189.16.17.89	.........171.68.226.120
22.78.190.64	........171.68.226.121
172.16.19.90	........171.68.226.120
192.58.28.128	.......171.68.228.121
189.16.17.89	.......171.68.226.120
22.78.190.64	........171.68.226.121
172.16.19.90	.........171.68.226.120
192.58.28.128	........171.68.228.121
189.16.17.89	.......171.68.226.120
22.78.190.64	........171.68.226.121
172.16.19.90	.........171.68.226.120
192.58.28.128	........171.68.228.121
189.16.17.89	........171.68.226.120
22.78.190.64	.........171.68.226.121
172.16.19.90	........171.68.226.120
192.58.28.128	........171.68.228.121

Prefix	Next-hop
189.16.17.89	........171.68.226.120
22.78.190.64	........171.68.226.121
172.16.19.90	........171.68.226.120
192.58.28.128	.......171.68.228.121
189.16.17.89	.......171.68.226.120
22.78.190.64	........171.68.226.121
172.16.19.90	.........171.68.226.120
192.58.28.128	........171.68.228.121
189.16.17.89	.......171.68.226.120
22.78.190.64	........171.68.226.121
172.16.19.90	.........171.68.226.120
192.58.28.128	........171.68.228.121
189.16.17.89	........171.68.226.120
22.78.190.64	.........171.68.226.121
172.16.19.90	........171.68.226.120
192.58.28.128	........171.68.228.121

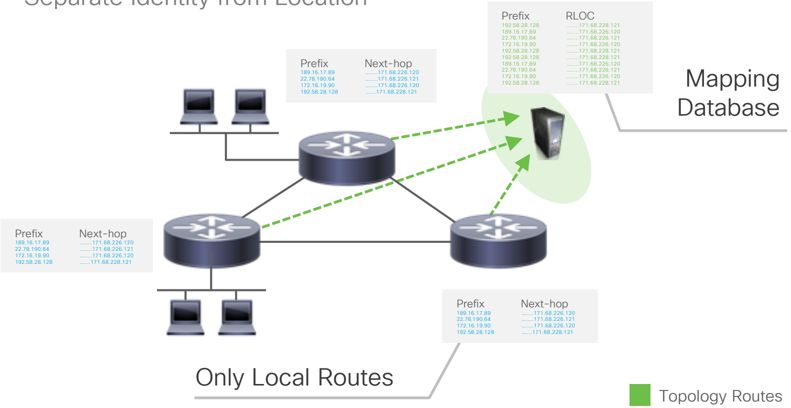
Topology + Endpoint Routes

Endpoint Routes are Consolidated to LISP DB

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

AFTER

Separate Identity from Location



Prefix	RLOC
192.58.28.128	........171.68.228.121
189.16.17.89	........171.68.226.120
22.78.190.64	........171.68.226.121
172.16.19.90	........171.68.226.120
192.58.28.128	........171.68.228.121
192.58.28.128	........171.68.228.121
189.16.17.89	........171.68.226.120
22.78.190.64	........171.68.226.121
172.16.19.90	........171.68.226.120
192.58.28.128	........171.68.228.121

Mapping Database

Prefix	Next-hop
189.16.17.89	........171.68.226.120
22.78.190.64	........171.68.226.121
172.16.19.90	........171.68.226.120
192.58.28.128	.......171.68.228.121

Prefix	Next-hop
189.16.17.89	........171.68.226.120
22.78.190.64	........171.68.226.121
172.16.19.90	........171.68.226.120
192.58.28.128	.......171.68.228.121

Prefix	Next-hop
189.16.17.89	........171.68.226.120
22.78.190.64	........171.68.226.121
172.16.19.90	........171.68.226.120
192.58.28.128	.......171.68.228.121

Only Local Routes

🟩 Topology Routes
🟦 Endpoint Routes

Fabric Operation

Control-Plane Roles & Responsibilities

LISP Map Server / Resolver
(Control-Plane)

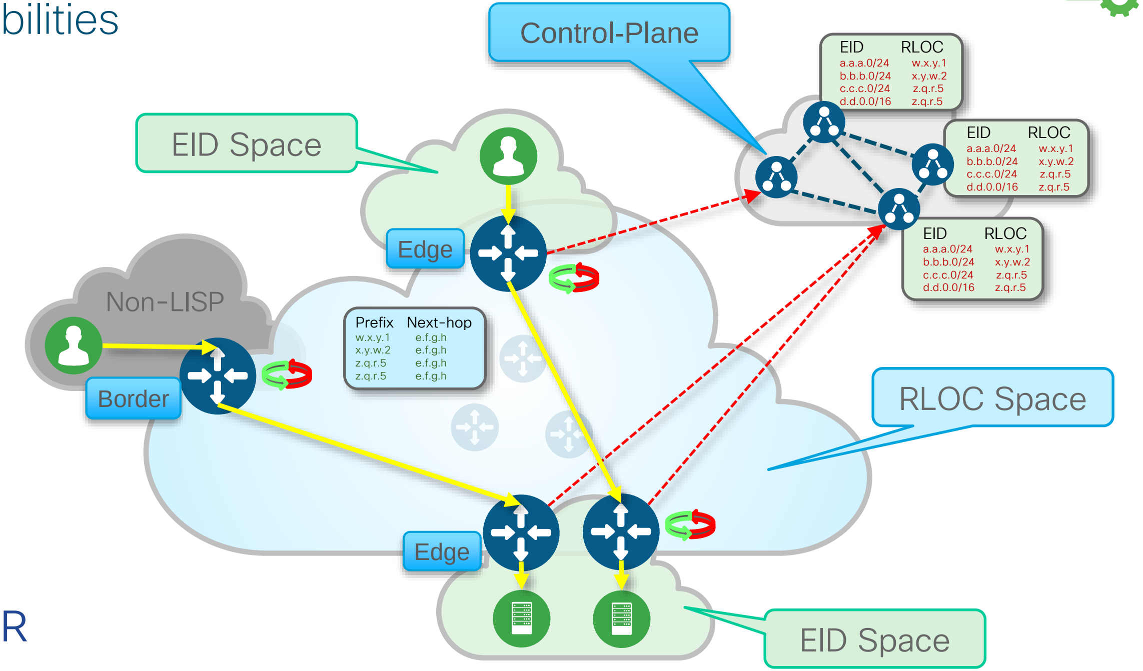
- EID to RLOC mappings
- Can be distributed across multiple LISP devices

LISP Tunnel Router - XTR
(Edge & Internal Border)

- Register EID with Map Server
- Ingress / Egress (ITR / ETR)

LISP Proxy Tunnel Router - PXTR
(External Border)

- Provides a Default Gateway when no mapping exists
- Ingress / Egress (PITR / PETR)



EID	RLOC
a.a.a.0/24	w.x.y.1
b.b.b.0/24	x.y.w.2
c.c.c.0/24	z.q.r.5
d.d.0.0/16	z.q.r.5

EID	RLOC
a.a.a.0/24	w.x.y.1
b.b.b.0/24	x.y.w.2
c.c.c.0/24	z.q.r.5
d.d.0.0/16	z.q.r.5

EID	RLOC
a.a.a.0/24	w.x.y.1
b.b.b.0/24	x.y.w.2
c.c.c.0/24	z.q.r.5
d.d.0.0/16	z.q.r.5

Prefix	Next-hop
w.x.y.1	e.f.g.h
x.y.w.2	e.f.g.h
z.q.r.5	e.f.g.h
z.q.r.5	e.f.g.h

- EID = Endpoint Identifier
    - Host Address or Subnet
- RLOC = Routing Locator
    - Local Router Address

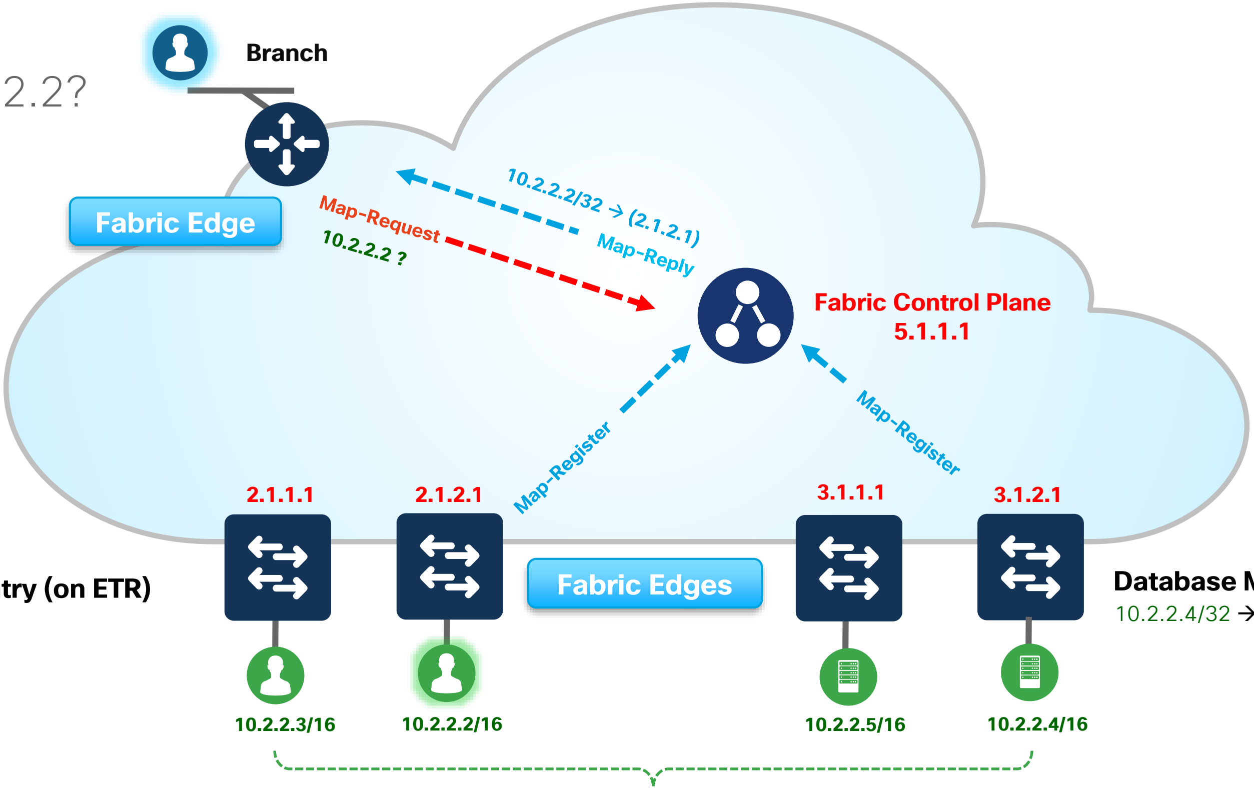
Fabric Operation

Control Plane Register & Resolution

Where is 10.2.2.2?

Cache Entry (on ITR)

10.2.2.2/32 → (2.1.2.1)



Database Mapping Entry (on ETR)

10.2.2.2/32 → (2.1.2.1)

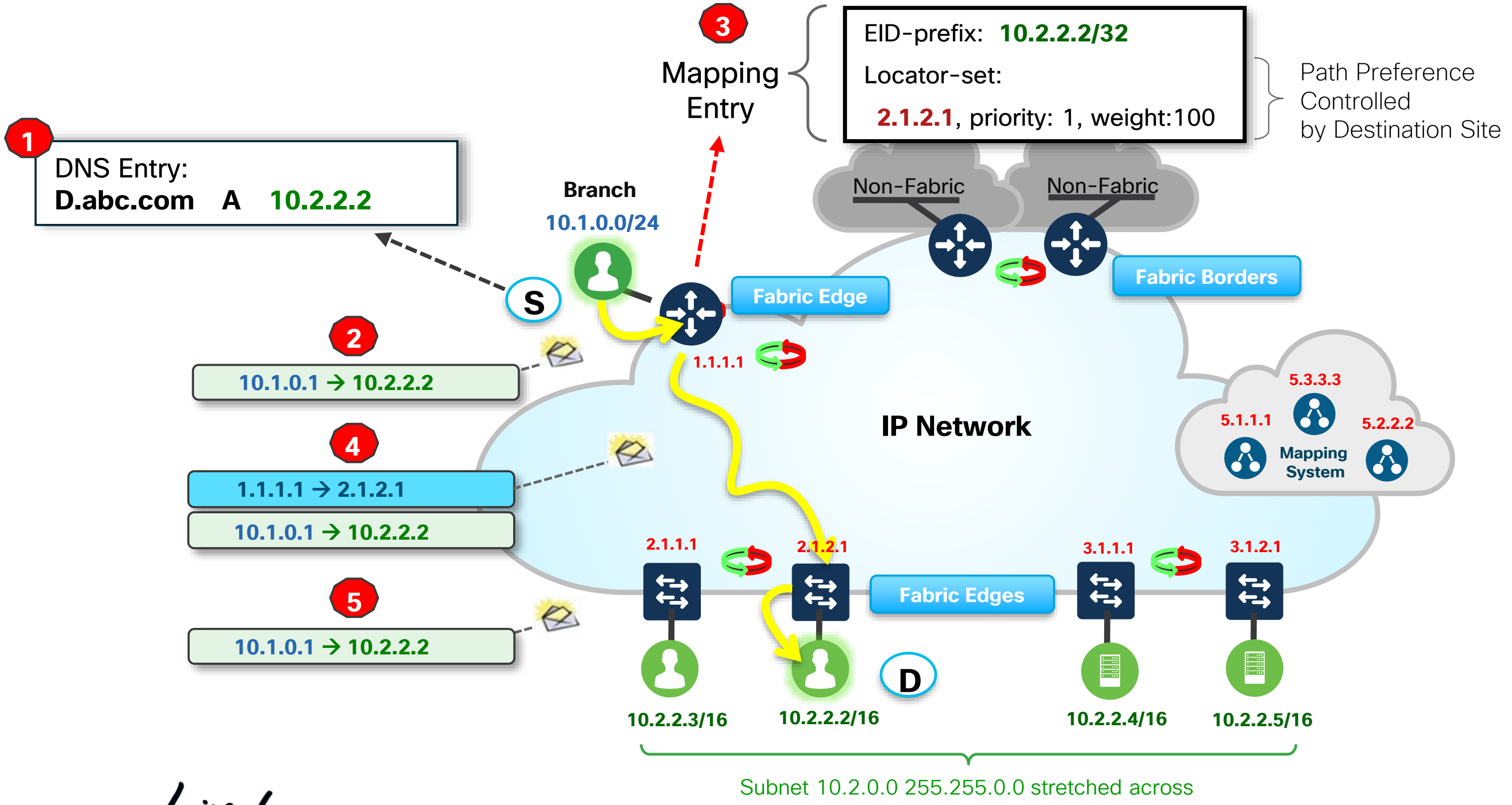
Database Mapping Entry (on ETR)

10.2.2.4/32 → (3.1.2.1)

Subnet 10.2.0.0 255.255.0.0 stretched across

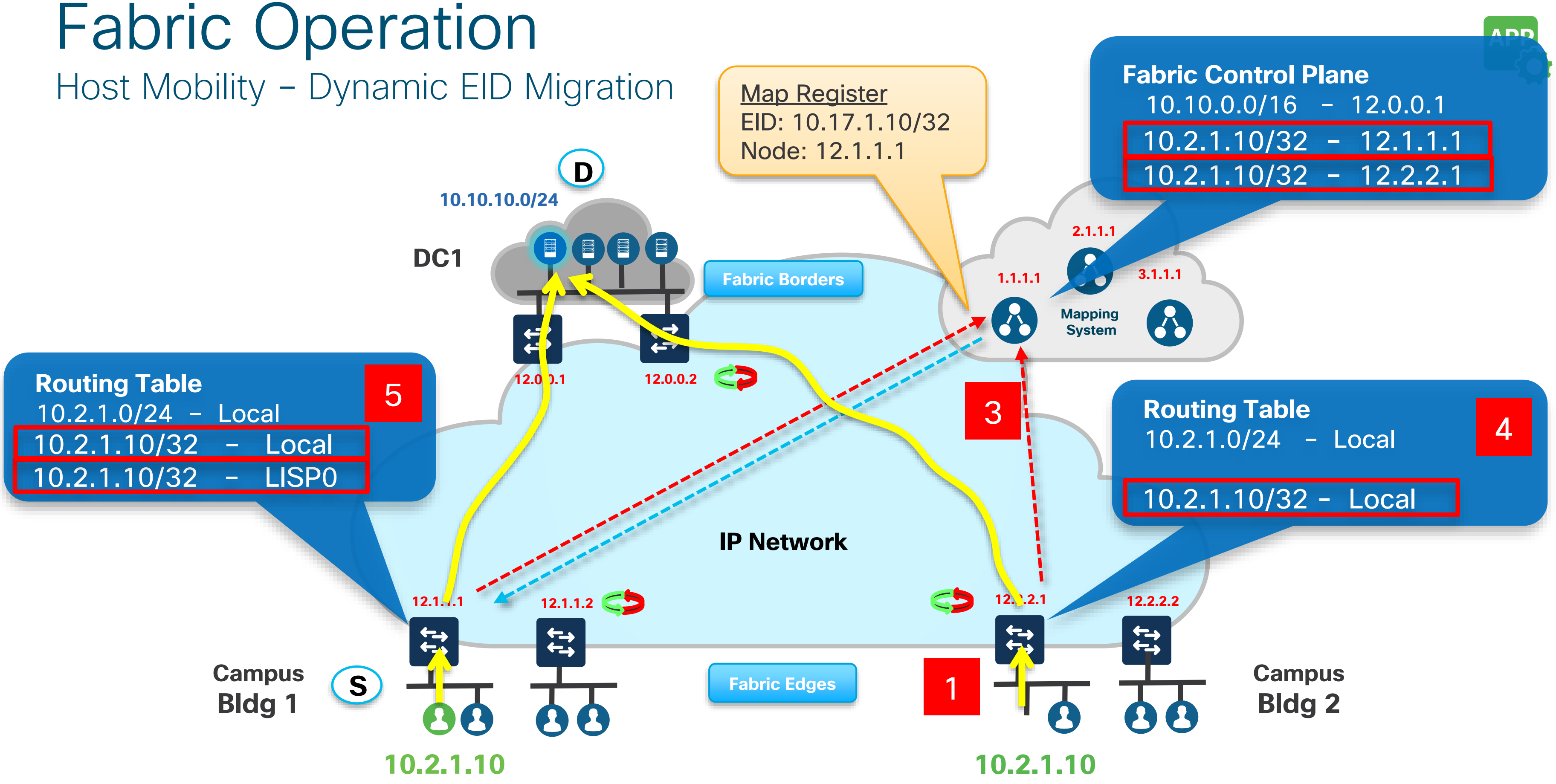
Fabric Operation

Fabric Internal Forwarding (Edge to Edge)



Fabric Operation

Host Mobility – Dynamic EID Migration



Map Register
EID: 10.17.1.10/32
Node: 12.1.1.1

Fabric Control Plane
10.10.0.0/16 – 12.0.0.1
10.2.1.10/32 – 12.1.1.1
10.2.1.10/32 – 12.2.2.1

Routing Table
10.2.1.0/24 – Local
10.2.1.10/32 – Local
10.2.1.10/32 – LISP0

Routing Table
10.2.1.0/24 – Local
10.2.1.10/32 – Local

cisco Live!

SD-Access Fabric

Unique Control-Plane extensions compared to LISP

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

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

What is Campus Fabric?

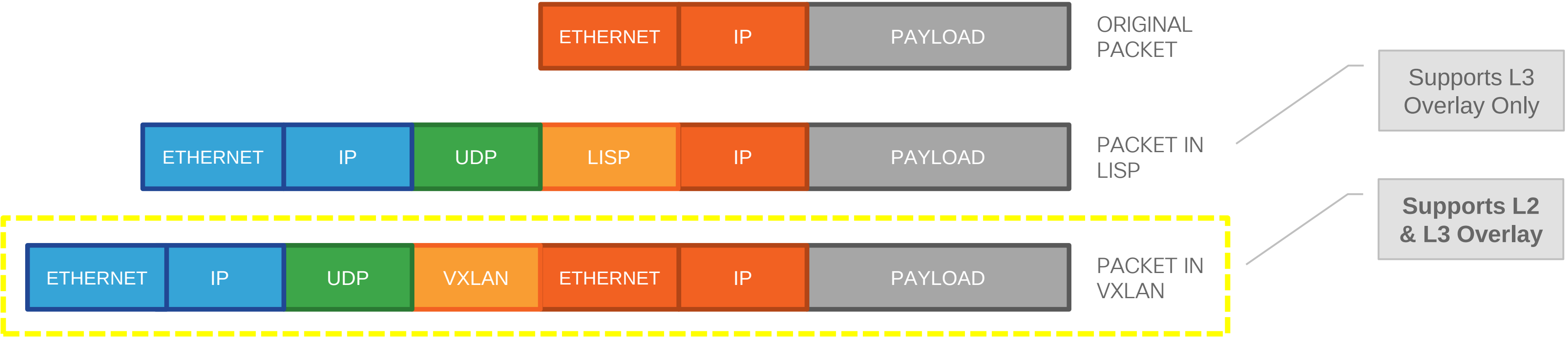
Fabric Fundamentals

SD-Access Fabric

Key Components – VXLAN

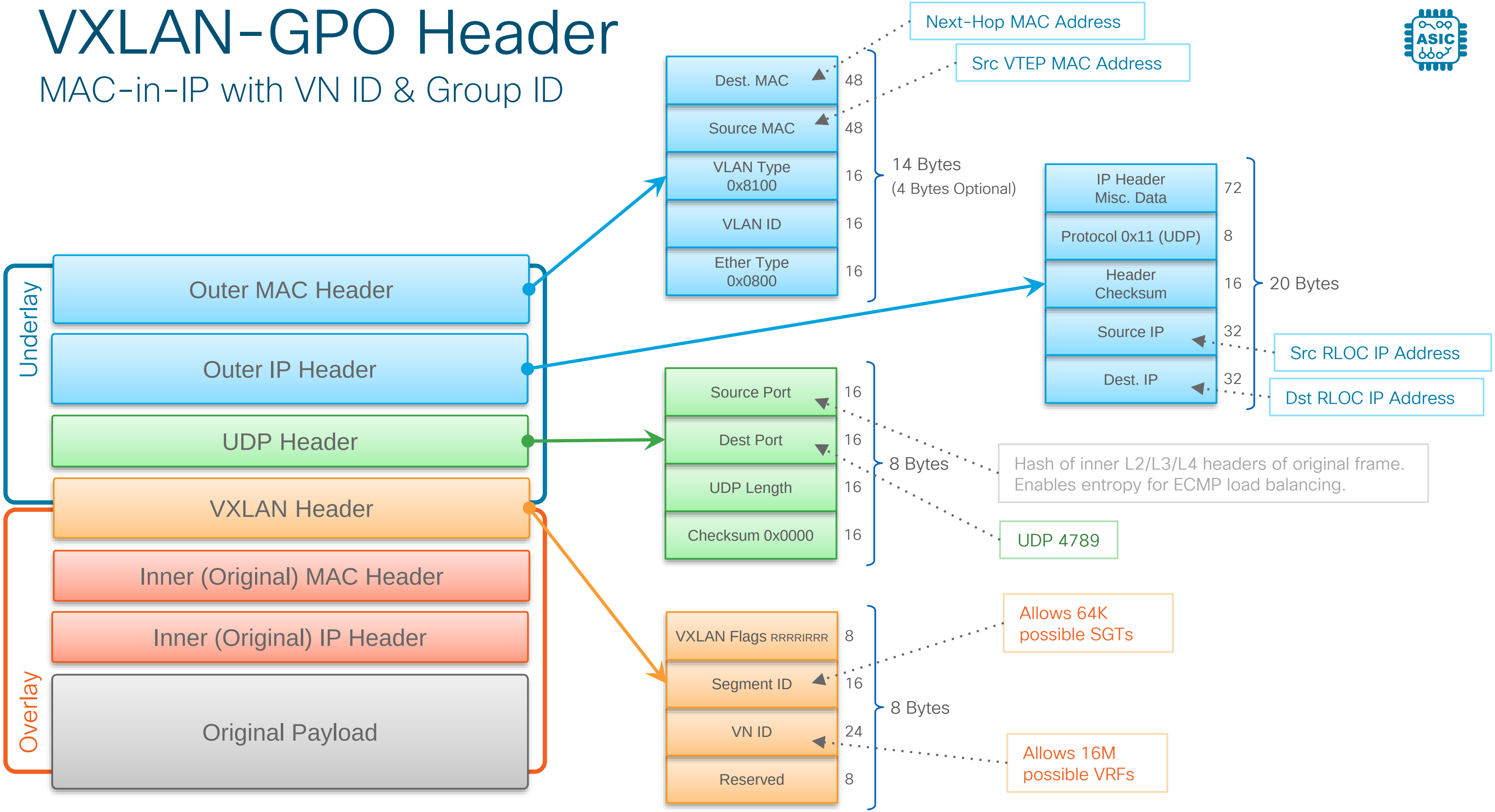
1. **Control-Plane** based on **LISP**

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:

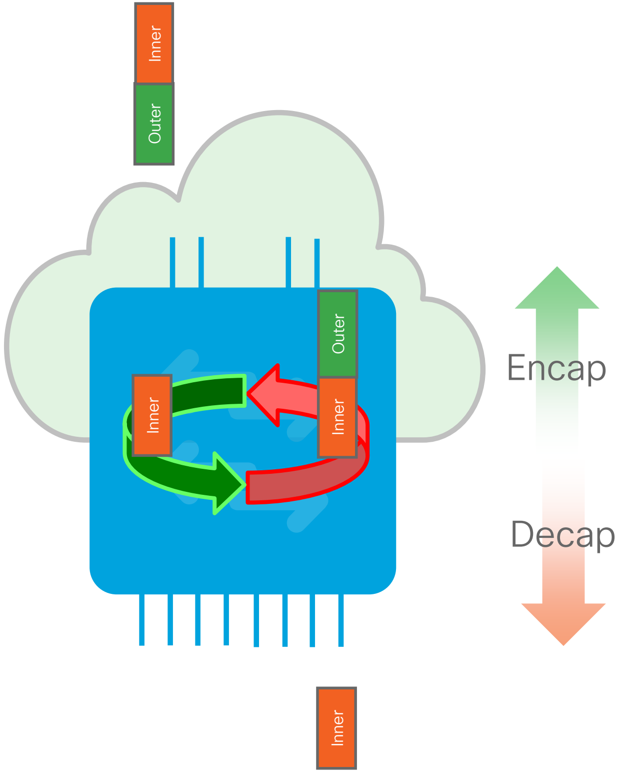
- Underlay address advertisement & mapping
- Automatic tunnel setup (Virtual Tunnel End-Points)
- Frame encapsulation between Routing Locators

Support for LISP or VXLAN header format

- Nearly the same, with different fields & payload
- LISP header carries IP payload (IP in IP)
- VXLAN header carries MAC payload (MAC in IP)

Triggered by LISP Control-Plane events

- ARP or NDP Learning on L3 Gateways
- Map-Reply or Cache on Routing Locators



SD-Access Fabric

Unique Data-Plane Extensions compared to VXLAN

Capability	Traditional LISP/VXLAN	SD-Access Fabric
SGT Tag	No 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)

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

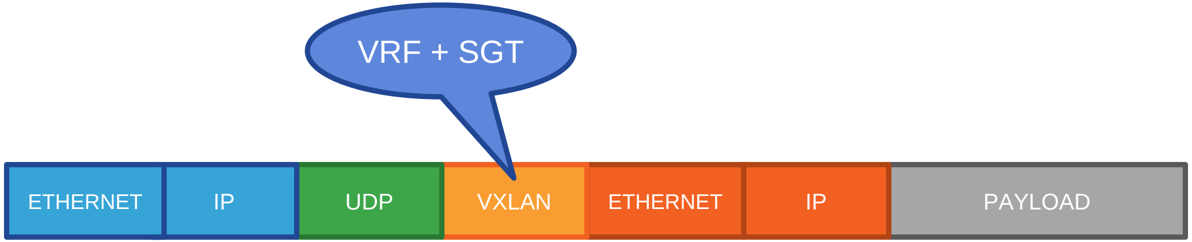
What is Campus Fabric?

Fabric Fundamentals

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**

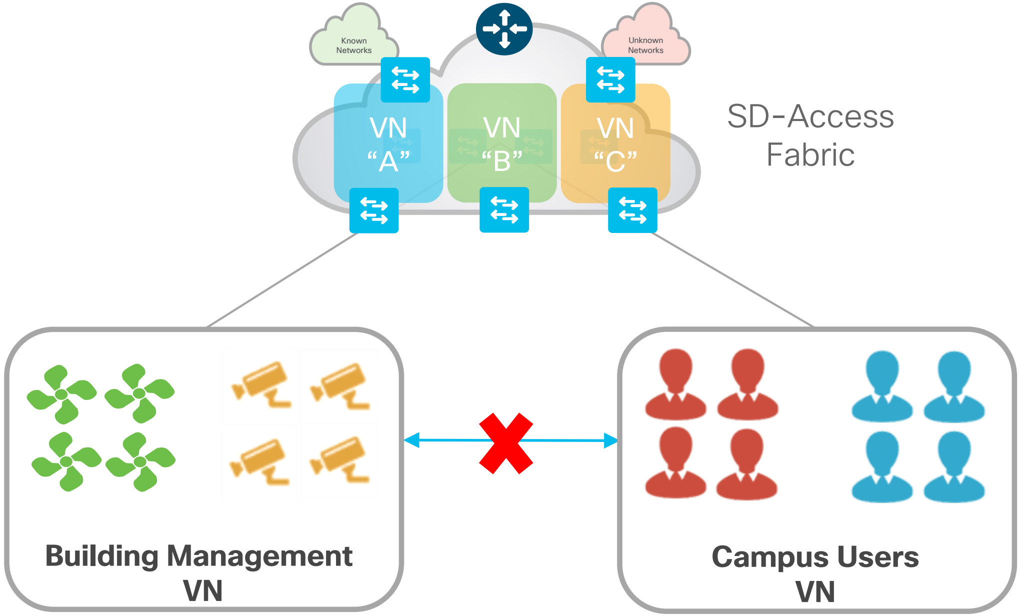


Virtual Routing & Forwarding

Scalable Group Tagging

SD-Access Policy

Two Level Hierarchy - Macro Segmentation

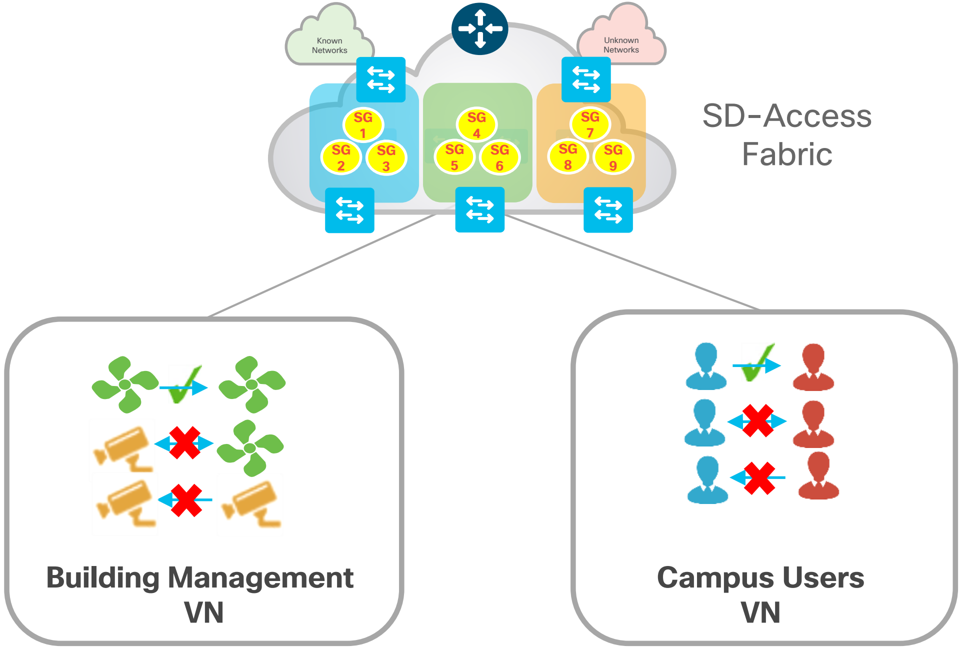


Virtual Network (VN)

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 Segmentation



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

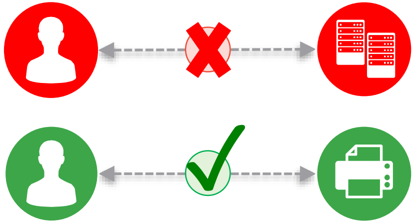
Policy Types

Access Control Policy

↓

Who can access What?

Permit / Deny Rules
for Group-to-Group Access



Application Policy

↓

How to treat Traffic?

QoS for Applications
or Application Caching

Traffic Copy Policy

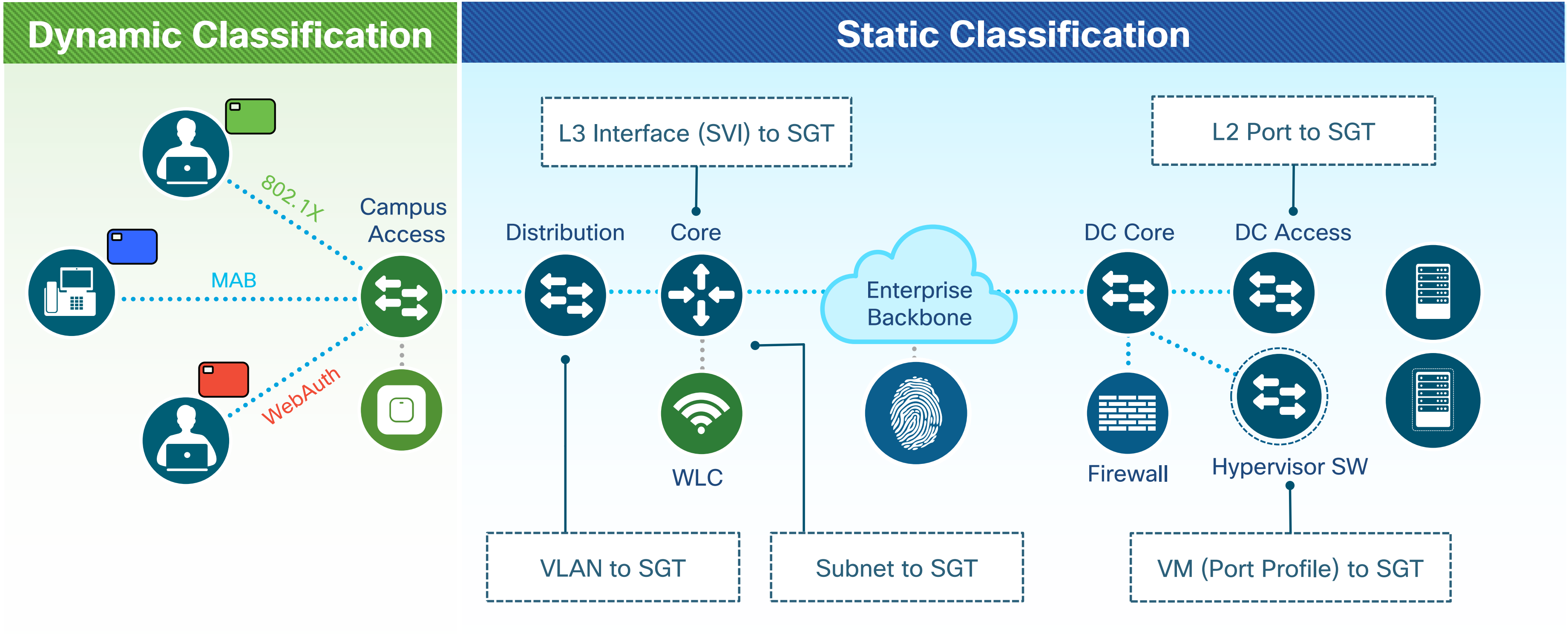
↓

Need to Monitor Traffic?

Enable SPAN Services
for specific Groups or Traffic

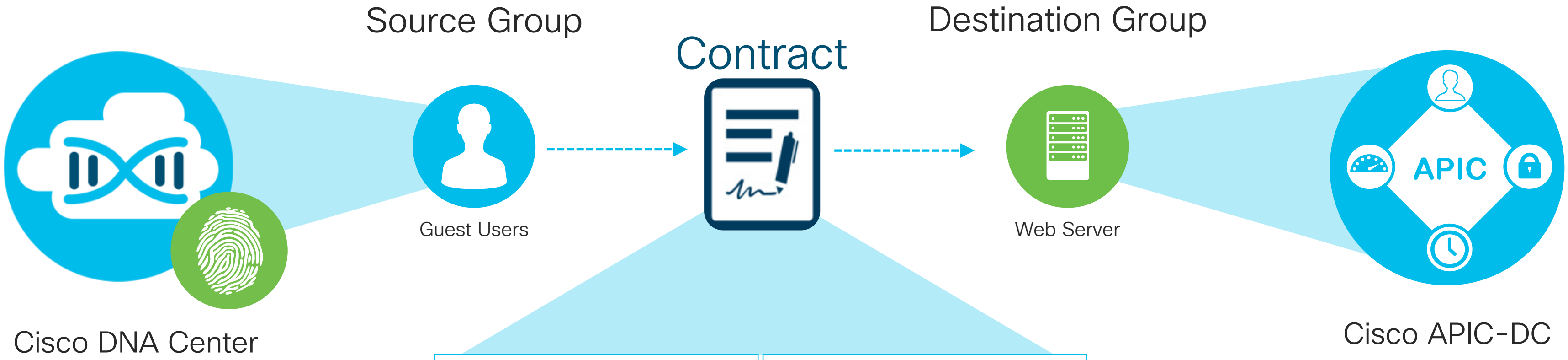
Group Assignment

Two ways to assign SGT



SD-Access Policy

Access Control Policies



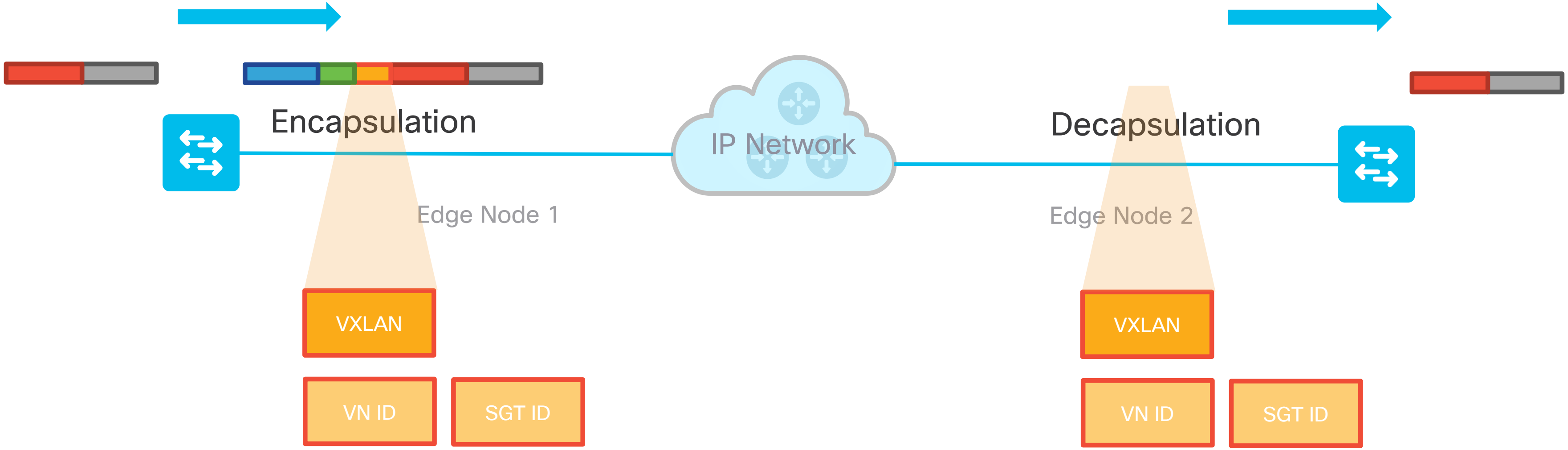
CLASSIFIER: PORT ▼ | ACTION: DENY ▼

Classifier Type	Action Type
Port Number	Permit
Protocol Name	Deny
Application Type	Copy

All groups in a Policy must belong to the same Virtual Network

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

SD-Access Fabric

Unique Policy-Plane Extensions compared to CTS

Capability	Traditional CTS	SD-Access Policy
SGT Propagation	Enabled hop-by-hop, or by 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

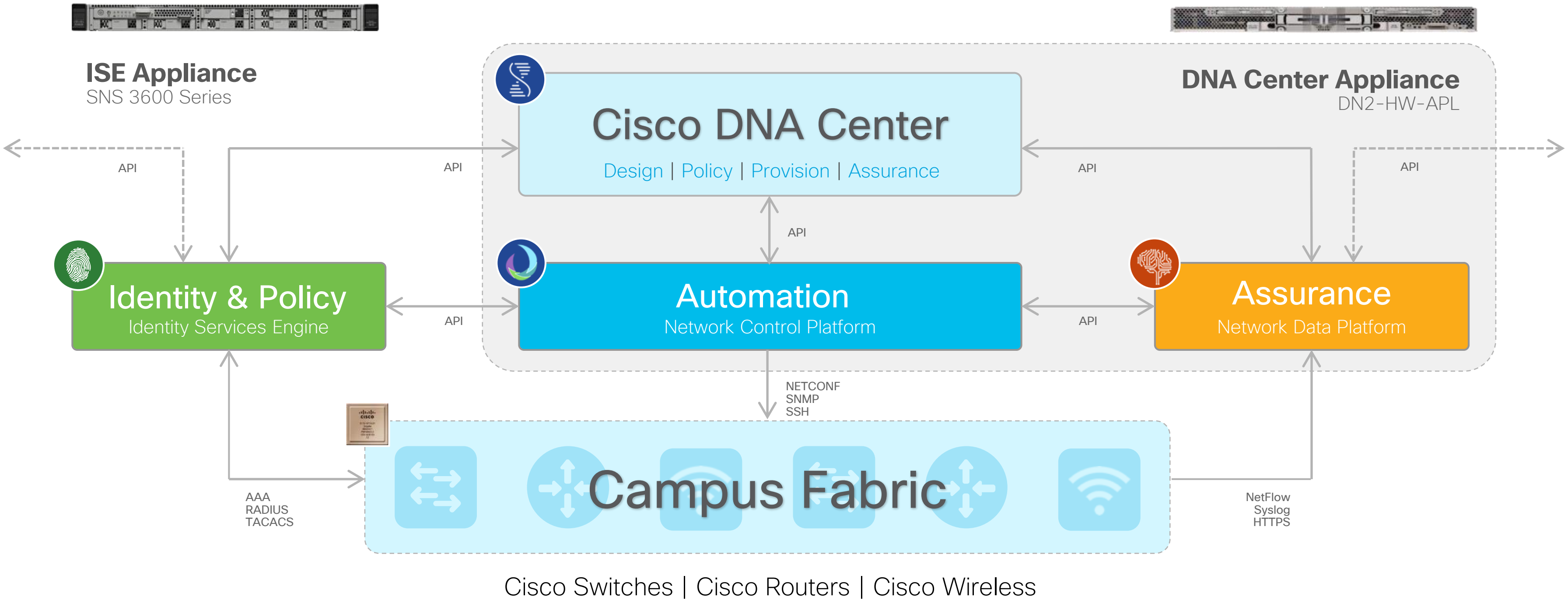
What is Cisco DNA Center?

Controller Fundamentals

1. Architecture
2. User Interface
3. Workflows

Cisco DNA Center

SD-Access – Key Components



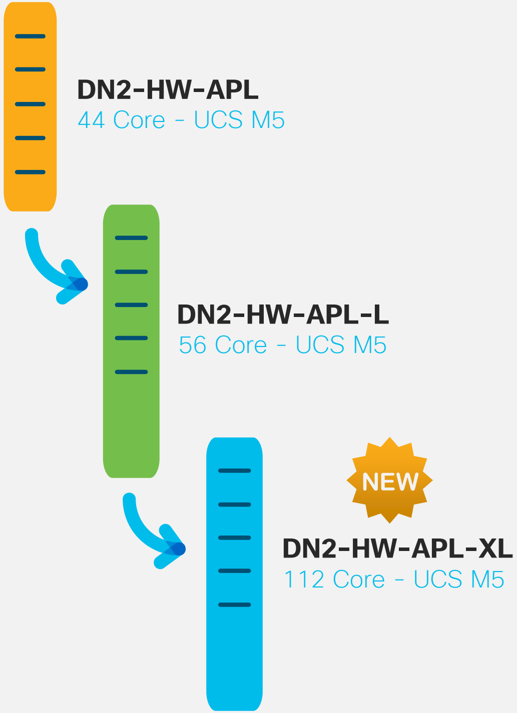
www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/datasheet-listing.html

Cisco DNA Center

Overall “Solution Scale” is Driven by Cisco DNAC

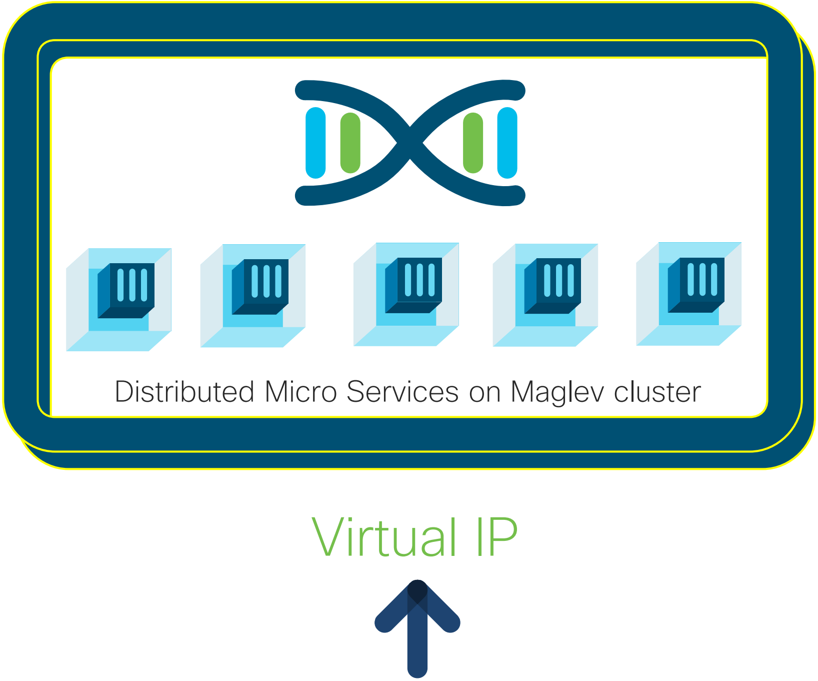
Cisco DNAC 1.3

		Cisco DNA Center		
		DN2-HW-APL 44 Core- UCS M5	**DN2-HW-APL-L** 56 Core- UCS M5	**DN2-HW-APL-XL** 112 Core- UCS M5
Infrastructure	Switches, Routers & WLC	1000	2000	5000
	Access Points	4000	6000	12000
	Endpoints (Wired + Wireless)	25K	40K	100K
	Sites	500	1000	2000
	Fabric Nodes	500/Site	600/Site	1000/Site
	IP Pools	300/Site	500/Site	600/Site
	Virtual Networks	64/Site	64/Site	256/Site
	Access Policies	5K	10K	25K



Cisco DNA Center

High Availability Cluster



1 or 3 appliance HA Cluster (more in future)

- Odd number to achieve quorum of distributed system

Seen as 1 logical DNAC instance

- Connect to Virtual (Cluster) IP
- Rare need to access individual nodes (e.g. SSH)

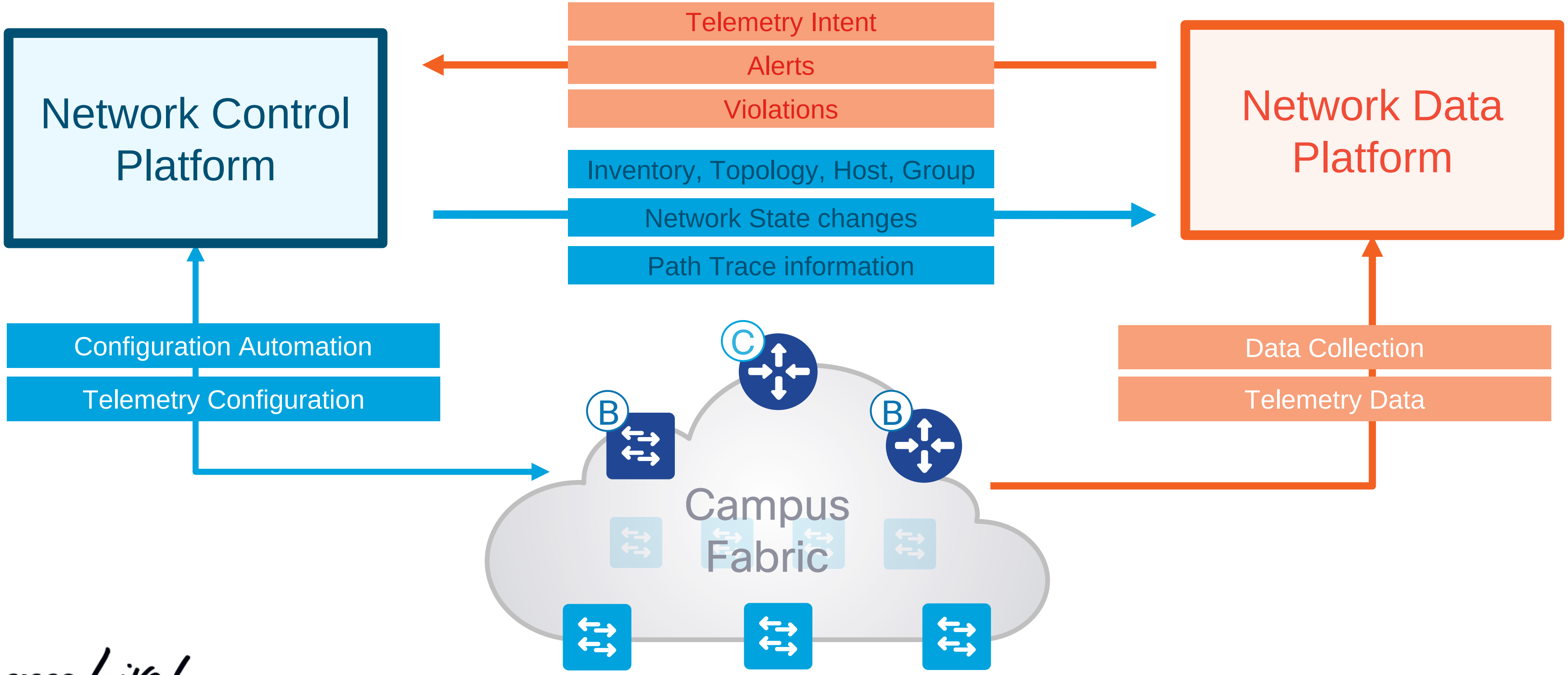
2 nodes active/sharing + 1 redundant

- Some services run multiple copies spread across nodes (e.g. databases)
- Other services run single copy and migrate from failed to redundant node

Single Appliance for Cisco DNA (Automation + Assurance)

Cisco DNA Center

Automated Provisioning and Telemetry Enrichment



Network Control Platform

Telemetry Intent

Alerts

Violations

Inventory, Topology, Host, Group

Network State changes

Path Trace information

Network Data Platform

Configuration Automation

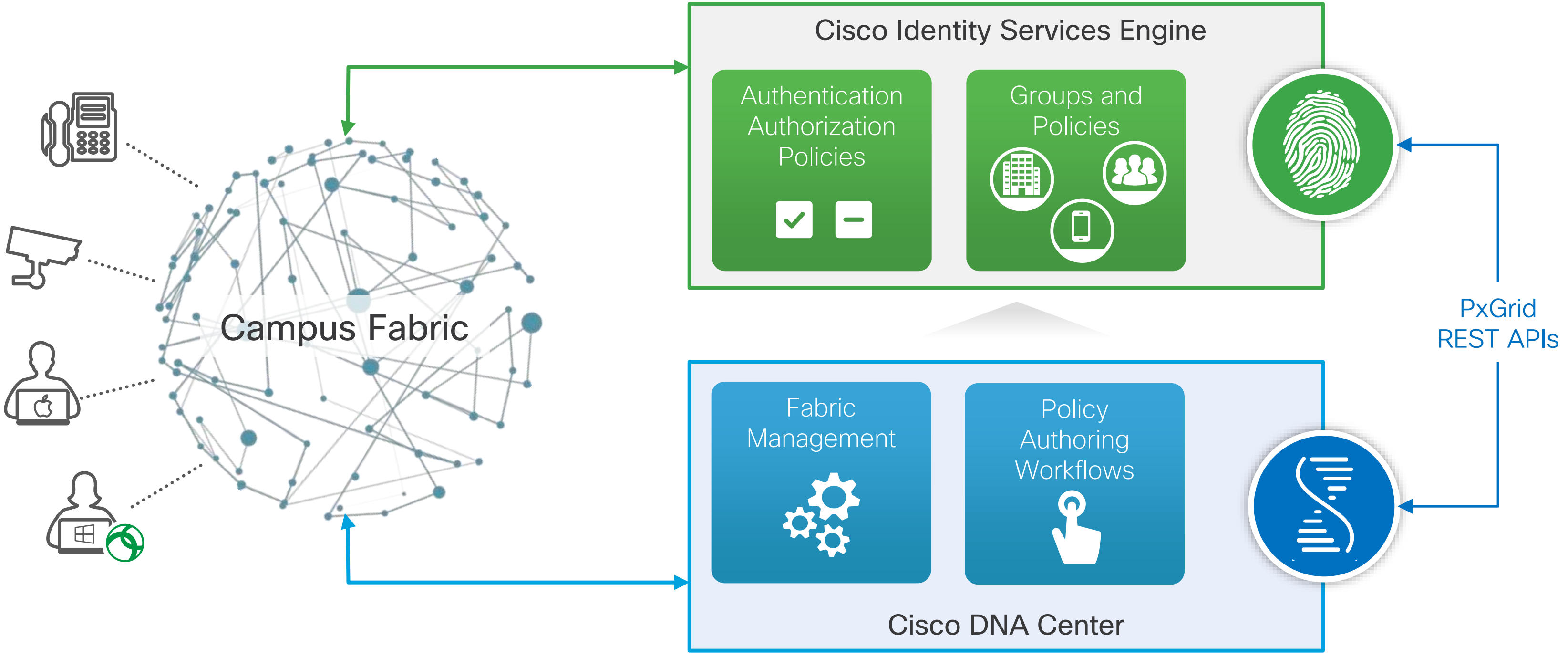
Telemetry Configuration

Data Collection

Telemetry Data

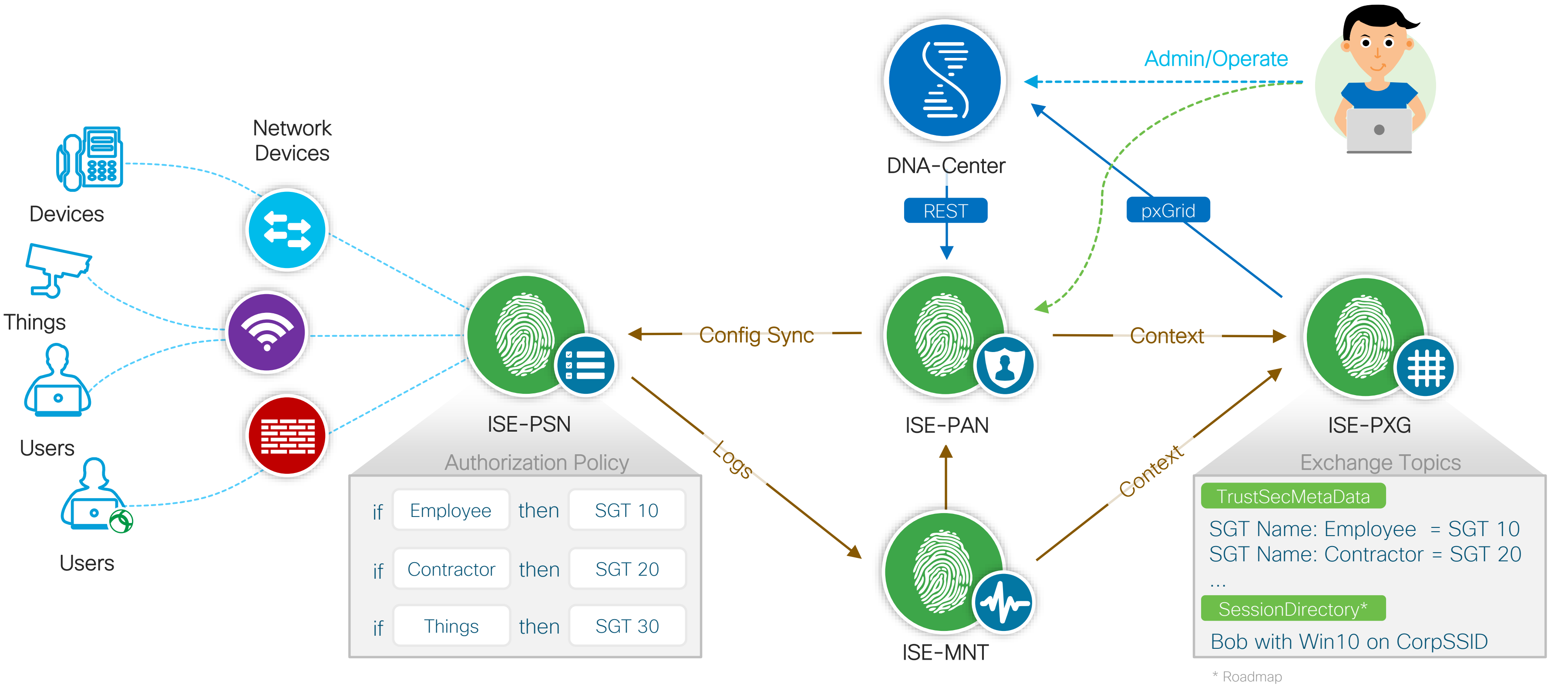
Cisco DNA Center and ISE integration

Identity and Policy Automation


Cisco Identity Services Engine
Authentication Authorization Policies
Groups and Policies
Campus Fabric
PxGrid REST APIs
Fabric Management
Policy Authoring Workflows
Cisco DNA Center

Cisco DNA Center and ISE integration

ISE roles in SD-Access



Authorization Policy

if	Employee	then	SGT 10
if	Contractor	then	SGT 20
if	Things	then	SGT 30

Exchange Topics

TrustSecMetaData

SGT Name: Employee = SGT 10
SGT Name: Contractor = SGT 20
…

SessionDirectory*

Bob with Win10 on CorpSSID

* Roadmap

1. Architecture
2. User Interface
3. Workflows

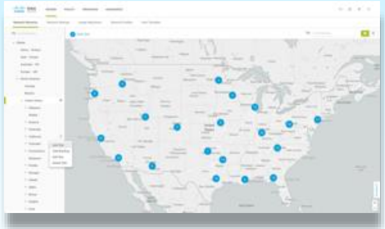
What is Cisco DNA Center?

Controller Fundamentals

Cisco DNA Center

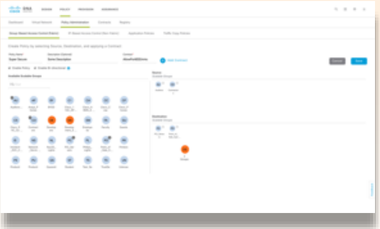
4 Step Workflow

Design



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

Policy

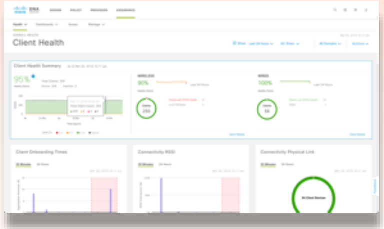


- Virtual Networks
- ISE, AAA, Radius
- Endpoint Groups
- Group Policies

Provision

- Fabric Domains
- CP, Border, Edge
- Fabric WLC, AP
- External Connect

Assurance

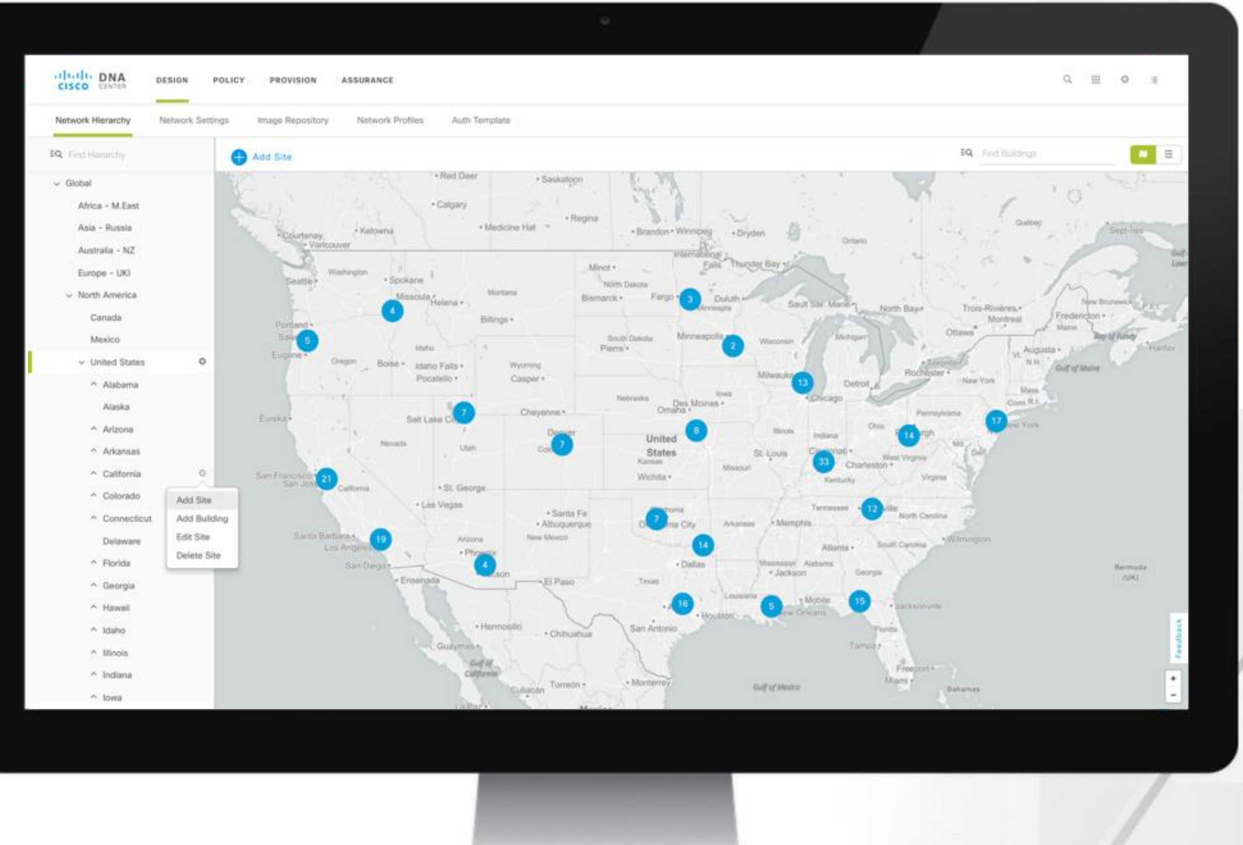


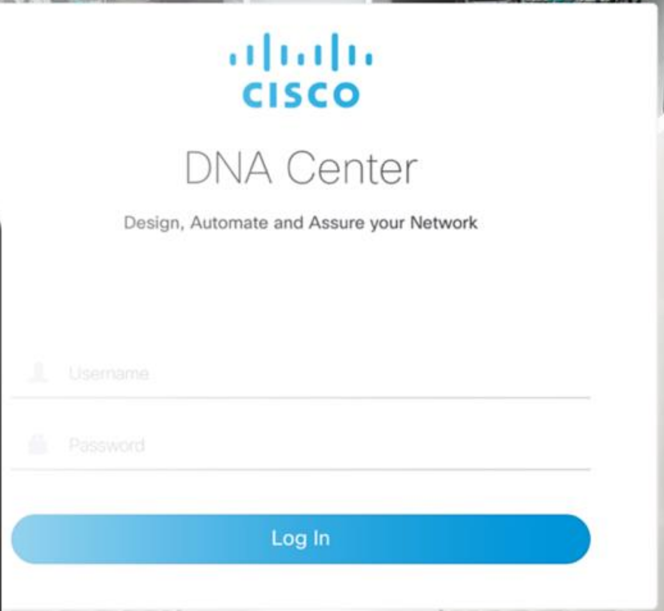
- Health Dashboard
- 360º Views
- Net, Device, Client
- Path Traces

System Settings & Integration

App Management & High Availability

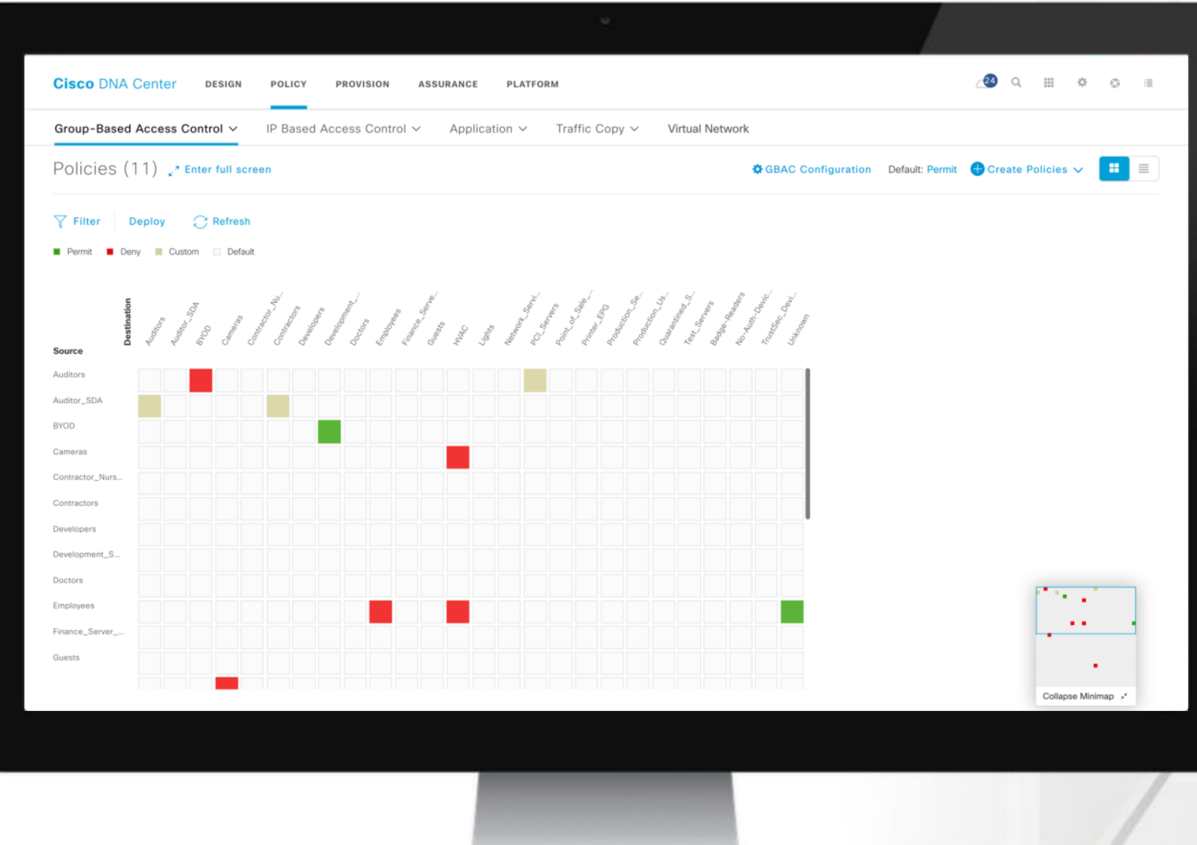
SDA - Design





Network Hierarchy
Network Settings
Image Management
Network Profiles

SDA - Policy



Cisco DNA Center   DESIGN   POLICY   PROVISION   ASSURANCE   PLATFORM

Group-Based Access Control   IP Based Access Control   Application   Traffic Copy   Virtual Network

Policies (11)   Enter full screen   GBAC Configuration   Default: Permit   Create Policies

Filter   Deploy   Refresh

🟩 Permit   🟥 Deny   🟨 Custom   ⬜ Default

Source \ Destination	Auditors	Auditor_SDA	BYOD	Cameras	Contractor_Nu...	Contractors	Developers	Development_...	Doctors	Employees	Finance_Serve...	Guests	HVAC	Lights	Network_Servi...	PCI_Servers	Point_of_Sale_...	Printer_EPG	Production_Se...	Production_Us...	Quarantined_S...	Test_Servers	Badge-Readers	No-Auth-Devic...	TrustSec_Devi...	Unknown
Auditors	⬜	⬜	🟥	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟨	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜
Auditor_SDA	🟨	⬜	⬜	⬜	⬜	🟨	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜
BYOD	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜
Cameras	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟥	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜
Contractor_Nurs...	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜
Contractors	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜
Developers	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜
Development_S...	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜
Doctors	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜
Employees	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟥	⬜	⬜	🟥	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩
Finance_Server_...	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜
Guests	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜
	⬜	⬜	⬜	🟥	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜

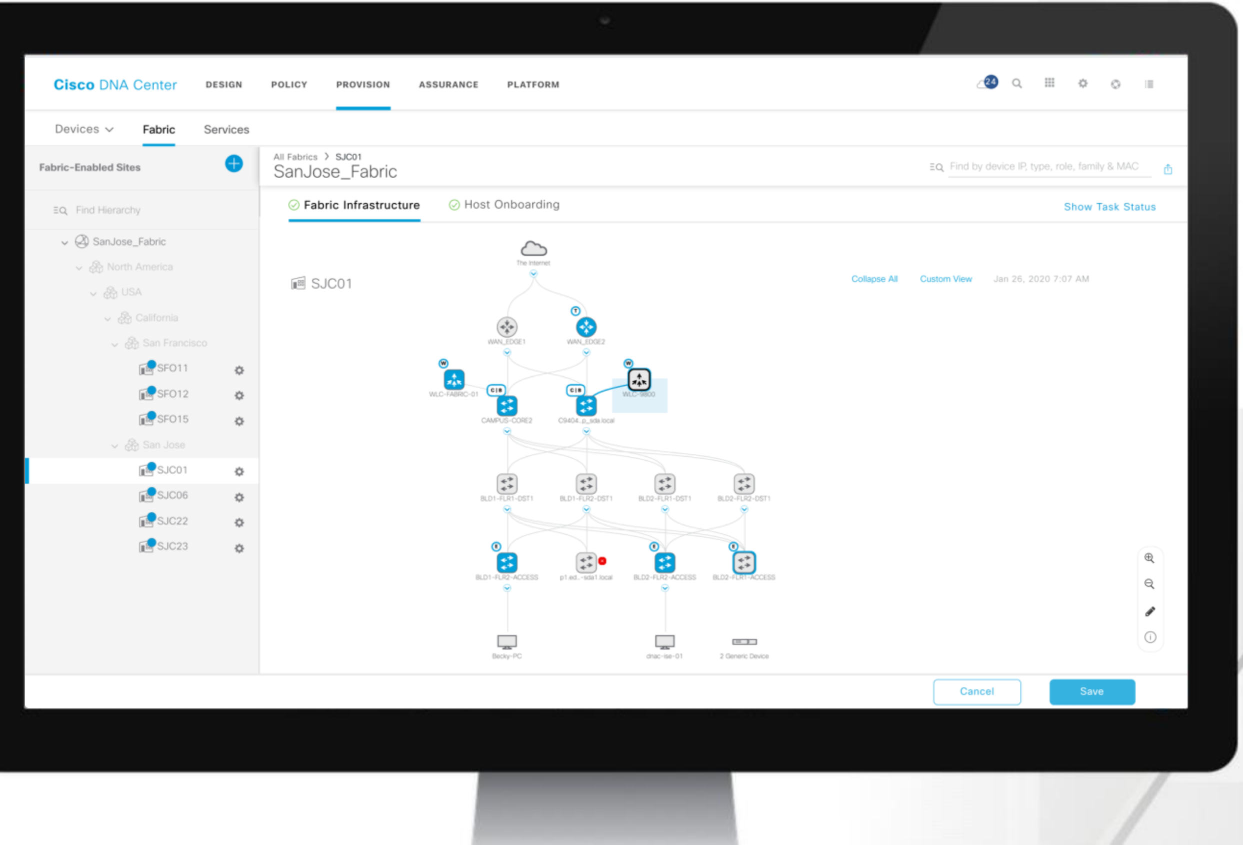
Virtual Networks

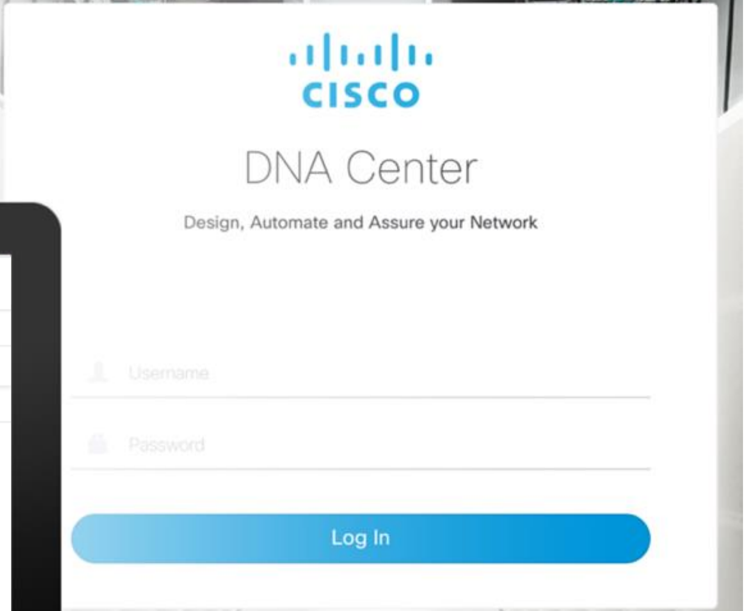
Access Control

Application Priority

Application Registry

SDA - Provision





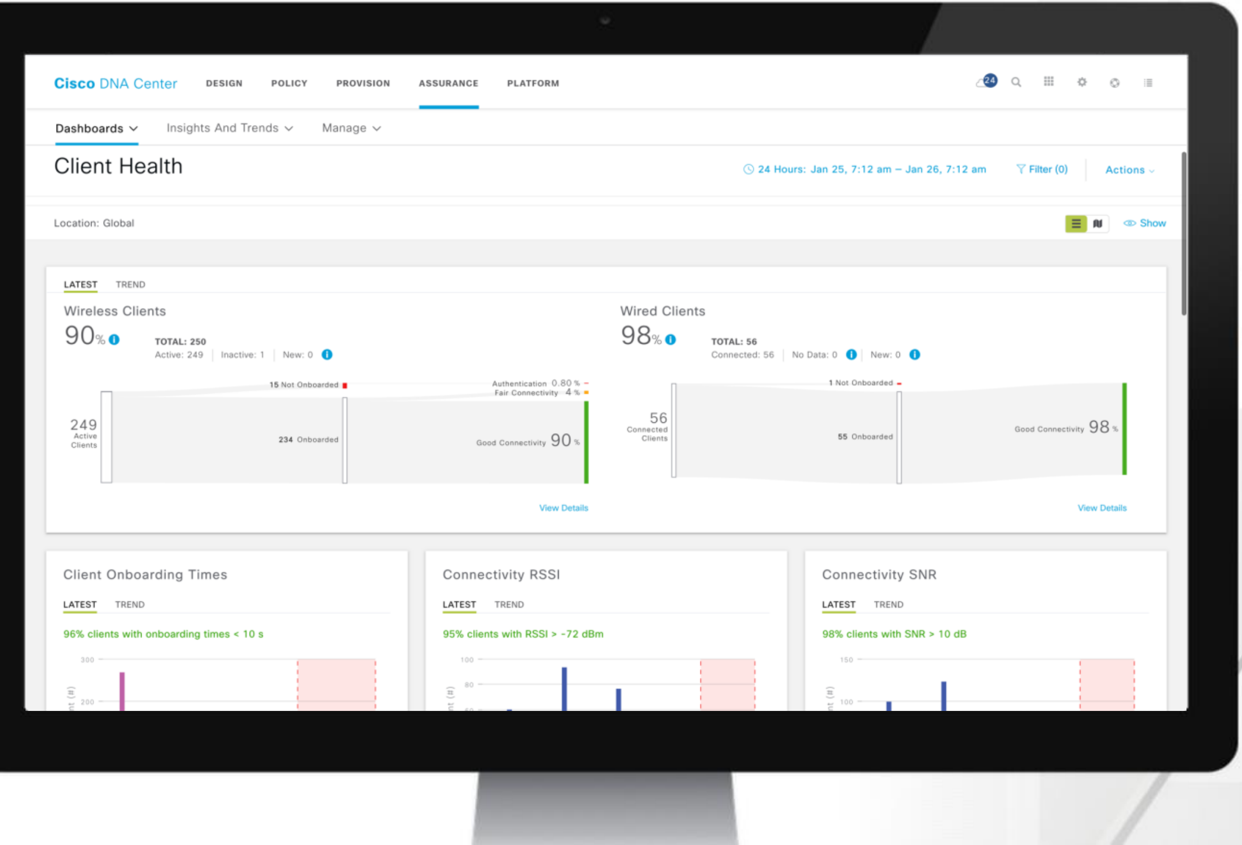
Device On-Boarding

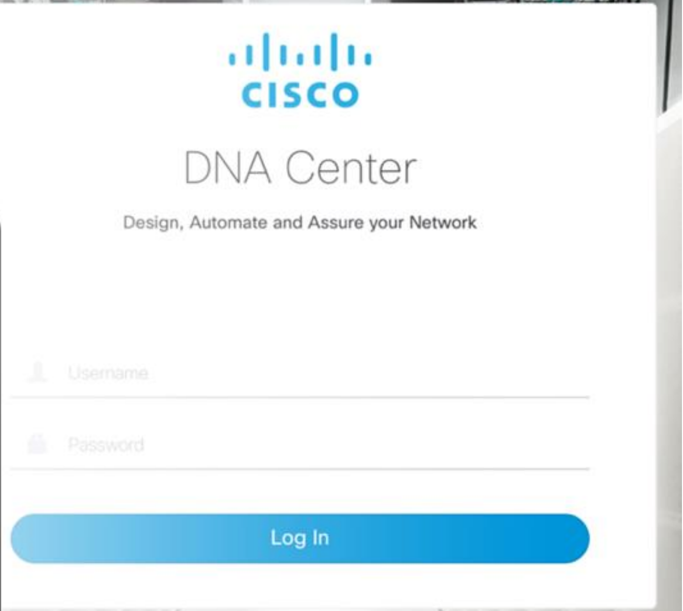
Device Inventory

Fabric Administraton

Host On-Boarding

SDA - Assurance





Health Scores

Client 360

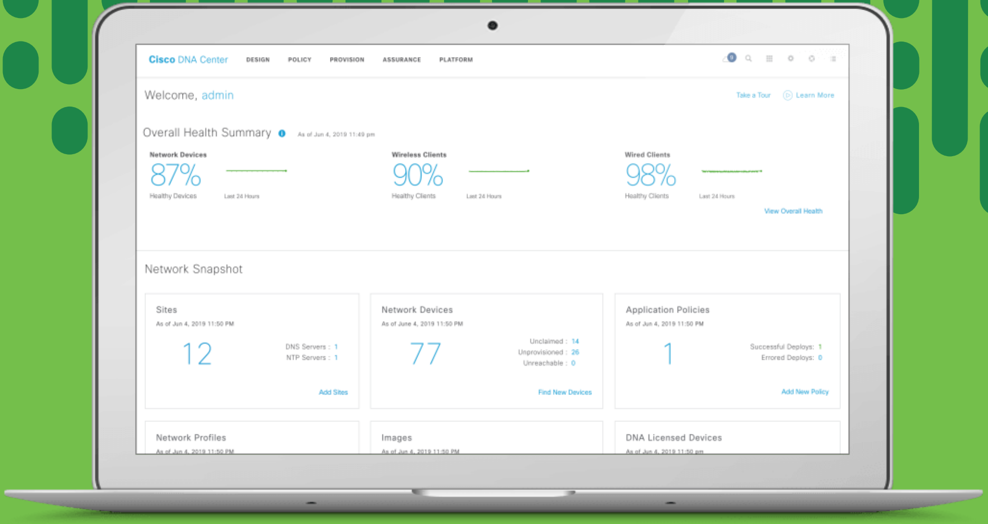
Device 360

Application 360

Click to Resolve

How about a LIVE DEMO?

- Design
- Policy
- Provision
- Assurance



Welcome, admin

Overall Health Summary As of Jun 4, 2019 11:49 pm

Network Devices 87% Healthy Devices Last 24 Hours

Wireless Clients 90% Healthy Clients Last 24 Hours

Wired Clients 98% Healthy Clients Last 24 Hours

Network Snapshot

Sites
As of Jun 4, 2019 11:50 PM
12
DNS Servers : 1
NTP Servers : 1

Network Devices
As of June 4, 2019 11:50 PM
77
Unclaimed : 14
Unprovisioned : 26
Unreachable : 0

Application Policies
As of Jun 4, 2019 11:50 PM
1
Successful Deploys: 1
Errored Deploys: 0

Network Profiles
As of Jun 4, 2019 11:50 PM

Images
As of Jun 4, 2019 11:50 PM

DNA Licensed Devices
As of Jun 4, 2019 11:50 pm

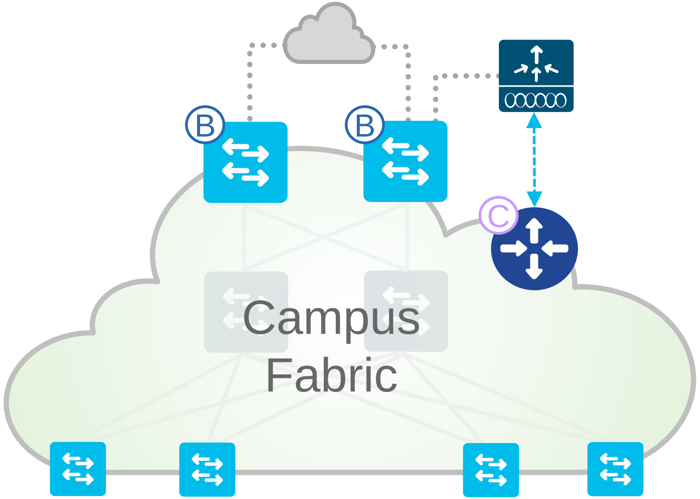
Take Away

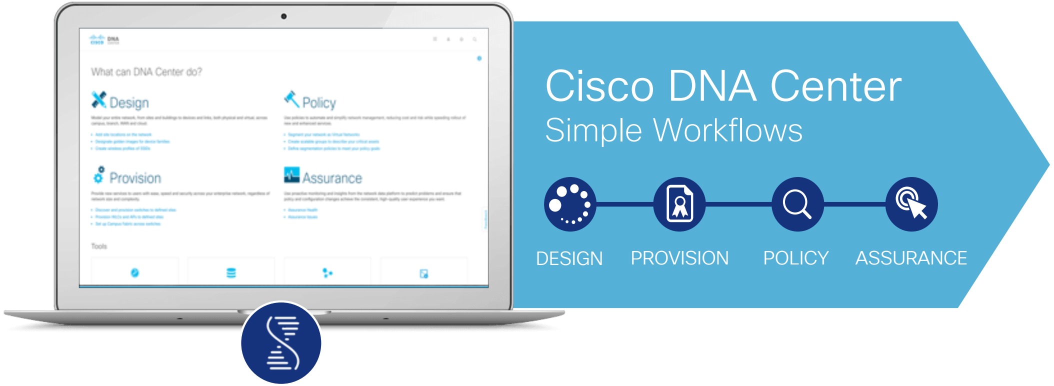
Things to Remember

Session Summary

RECAP

SD-Access = Campus Fabric + Cisco DNA Center



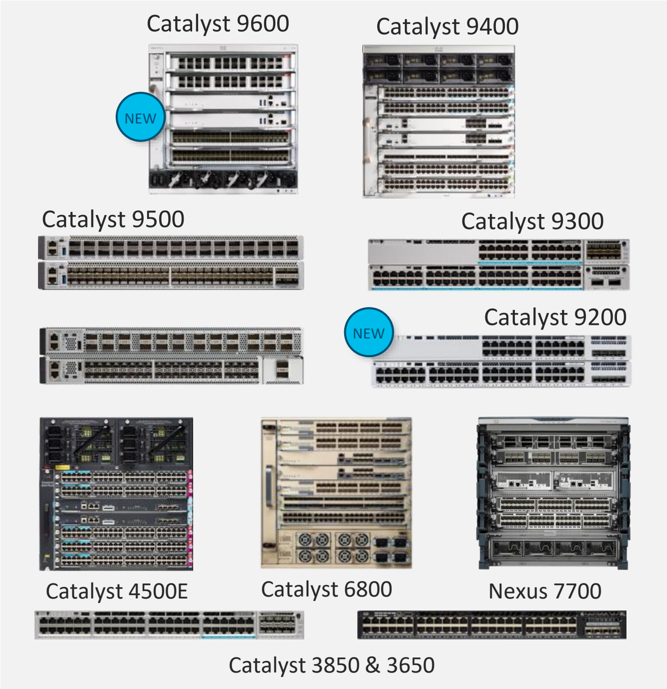


SD-Access Support

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

Digital Platforms for your Cisco Digital Network Architecture

Switching



Catalyst 9600

Catalyst 9400

Catalyst 9500

Catalyst 9300

Catalyst 9200

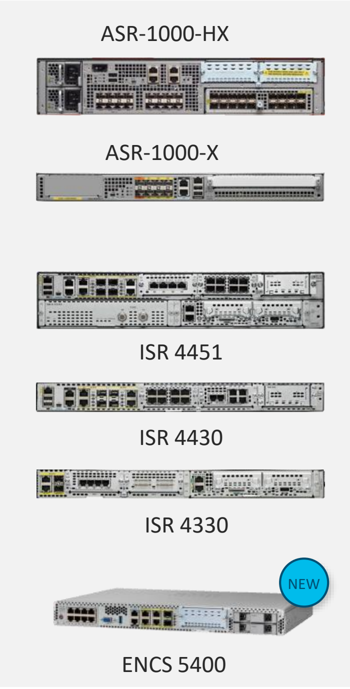
Catalyst 4500E

Catalyst 6800

Nexus 7700

Catalyst 3850 & 3650

Routing



ASR-1000-HX

ASR-1000-X

ISR 4451

ISR 4430

ISR 4330

ENCS 5400

Wireless

Catalyst 9800

Catalyst 9100 APs

AIR-CT8540

AIR-CT3504

AIR-CT5520

Aironet Wave 1 APs*

Aironet Wave 2 APs

Extended BETA

Cisco Digital Building

Catalyst 3560-CX

Cisco IE 3K/4K/5K

What’s New?

Cisco DNA Center 1.3

Optimized for Distribution

SD-Access 1.2.10

February 2019

DNA Center 1.2.10, ISE 2.4 p6, IOS-XE 16.9.2s, AireOS 8.8

- SD-Access Extension for IoT (Beta)
- 3 node DNAC HA for Automation
- Catalyst 9800 Wireless Controller
- Fabric in a Box with Embedded Wireless on Catalyst 9300
- Nexus 7700 Series with M3 as Border, without MPLS license
- SDA-ACI Integration Improvements
- LAN Automation Enhancements

Optimized for Extension

SD-Access 1.3.0

June 2019

DNA Center 1.3.0, ISE 2.6 p1, IOS-XE 16.11.1s, AireOS 8.9

- SD-Access Extension for IoT (FCS)
- IPv6 overlay support for Wired + Wireless (AireOS) Endpoints
- Fabric Edge and Fabric in a Box on Catalyst 9500
- Fabric in a Box with Embedded Wireless on C9400, C9500
- SD-Access Border Simplification
- LAN Automation Enhancements

Optimized for Policy

SD-Access 1.3.3 NEW

January 2020

DNA Center 1.3.3, ISE 2.6 p2, IOS-XE 16.12.2s, AireOS 8.10

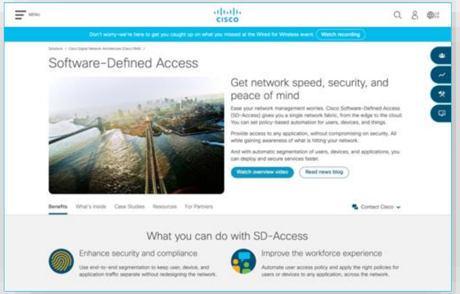
- Group-Based Access Control App (ACA)
- Application Visibility on Switches & WLCs
- Stealthwatch Security Analytics Service
- Cisco DNA Bonjour Service
- Firewall (ASA) support
- StackWise Virtual support
- L2 and Multicast Enhancements
- FiaB and eWLC Enhancements
- Intent APIs for SD-Access

SD-Access Resources

Would you like to know more?

cisco.com/go/sdaccess

- SD-Access At-A-Glance
- SD-Access Ordering Guide
- SD-Access Solution Data Sheet
- SD-Access Solution White Paper



MENU

Don't worry—we're here to get you caught up on what you missed at the Wired for Wireless event. Watch recording

Solutions / Cisco Digital Network Architecture (Cisco DNA) /

Software-Defined Access

Get network speed, security, and peace of mind

Ease your network management worries. Cisco Software-Defined Access (SD-Access) gives you a single network fabric, from the edge to the cloud. You can set policy-based automation for users, devices, and things.

Provide access to any application, without compromising on security. All while gaining awareness of what is hitting your network.

And with automatic segmentation of users, devices, and applications, you can deploy and secure services faster.

Watch overview video | Read news blog

Benefits | What's Inside | Case Studies | Resources | For Partners | Contact Cisco

What you can do with SD-Access

Enhance security and compliance

Use end-to-end segmentation to keep user, device, and application traffic separate without redesigning the network.

Improve the workforce experience

Automate user access policy and apply the right policies for users or devices to any application, across the network.

cisco.com/go/dna

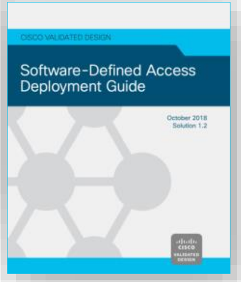
cisco.com/go/cvd

- SD-Access Design Guide
- SD-Access Deployment Guide
- SD-Access Segmentation Guide

CISCO VALIDATED DESIGN

Software-Defined Access Design Guide

December 2018
Solution 1.2



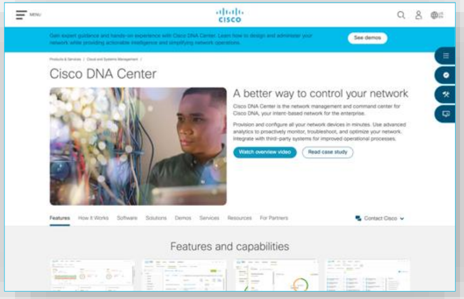
CISCO VALIDATED DESIGN

Software-Defined Access Deployment Guide

October 2018
Solution 1.2

cisco.com/go/dnacenter

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



MENU

Gain expert guidance and hands-on experience with Cisco DNA Center. Learn how to design and administer your network while providing actionable intelligence and simplifying network operations. See demos

Products & Services / Cloud and Systems Management /

Cisco DNA Center

A better way to control your network

Cisco DNA Center is the network management and command center for Cisco DNA, your intent-based network for the enterprise.

Provision and configure all your network devices in minutes. Use advanced analytics to proactively monitor, troubleshoot, and optimize your network. Integrate with third-party systems for improved operational processes.

Watch overview video | Read case study

Features | How It Works | Software | Solutions | Demos | Services | Resources | For Partners | Contact Cisco

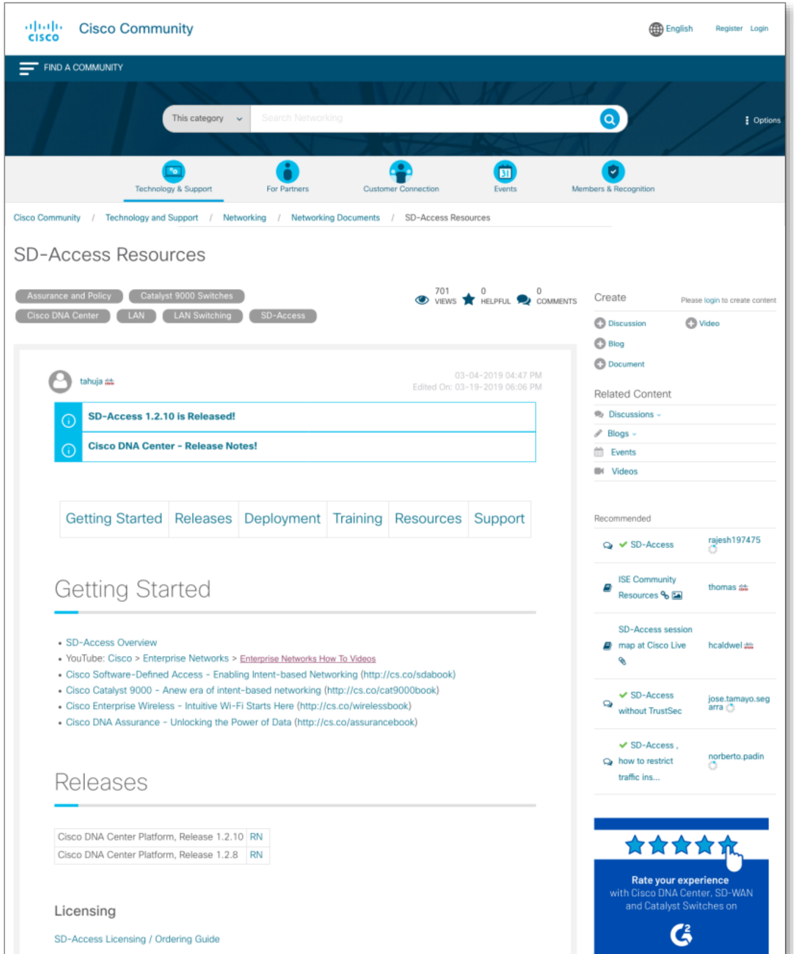
Features and capabilities

SD-Access Resources

Would you like to know more?

- cs.co/sda-resources
- cs.co/sda-community

- Search from your Browser
- Indexed by Search Engines
- Discuss with experts & friends
- Supported by SDA TMEs
- 24-hour First Response
- Questions are marked Answered



Cisco Community / Technology and Support / Networking / Networking Documents / SD-Access Resources

SD-Access Resources

Assurance and Policy · Catalyst 9000 Switches · Cisco DNA Center · LAN · LAN Switching · SD-Access

701 VIEWS 0 HELPFUL 0 COMMENTS

Please login to create content

tahuja

03-04-2019 04:47 PM
Edited On: 03-19-2019 06:06 PM

SD-Access 1.2.10 is Released!

Cisco DNA Center - Release Notes!

Getting Started | Releases | Deployment | Training | Resources | Support

Getting Started

- SD-Access Overview
- YouTube: Cisco > Enterprise Networks > Enterprise Networks How To Videos
- Cisco Software-Defined Access - Enabling Intent-based Networking (http://cs.co/sdabook)
- Cisco Catalyst 9000 - Anew era of intent-based networking (http://cs.co/cat9000book)
- Cisco Enterprise Wireless - Intuitive Wi-Fi Starts Here (http://cs.co/wirelessbook)
- Cisco DNA Assurance - Unlocking the Power of Data (http://cs.co/assurancebook)

Releases

Cisco DNA Center Platform, Release 1.2.10	RN
Cisco DNA Center Platform, Release 1.2.8	RN

Licensing

SD-Access Licensing / Ordering Guide

Recommended

✓ SD-Access	rajesh197475
ISE Community Resources	thomas
SD-Access session map at Cisco Live	hcaldwel
✓ SD-Access without TrustSec	jose.tamayo.segarra
✓ SD-Access , how to restrict traffic ins...	norberto.padin

Rate your experience with Cisco DNA Center, SD-WAN and Catalyst Switches on

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 campus
- Walk-in labs
- Meet the engineer 1:1 meetings
- Related sessions

Thank you

You make **possible**