Worldwide

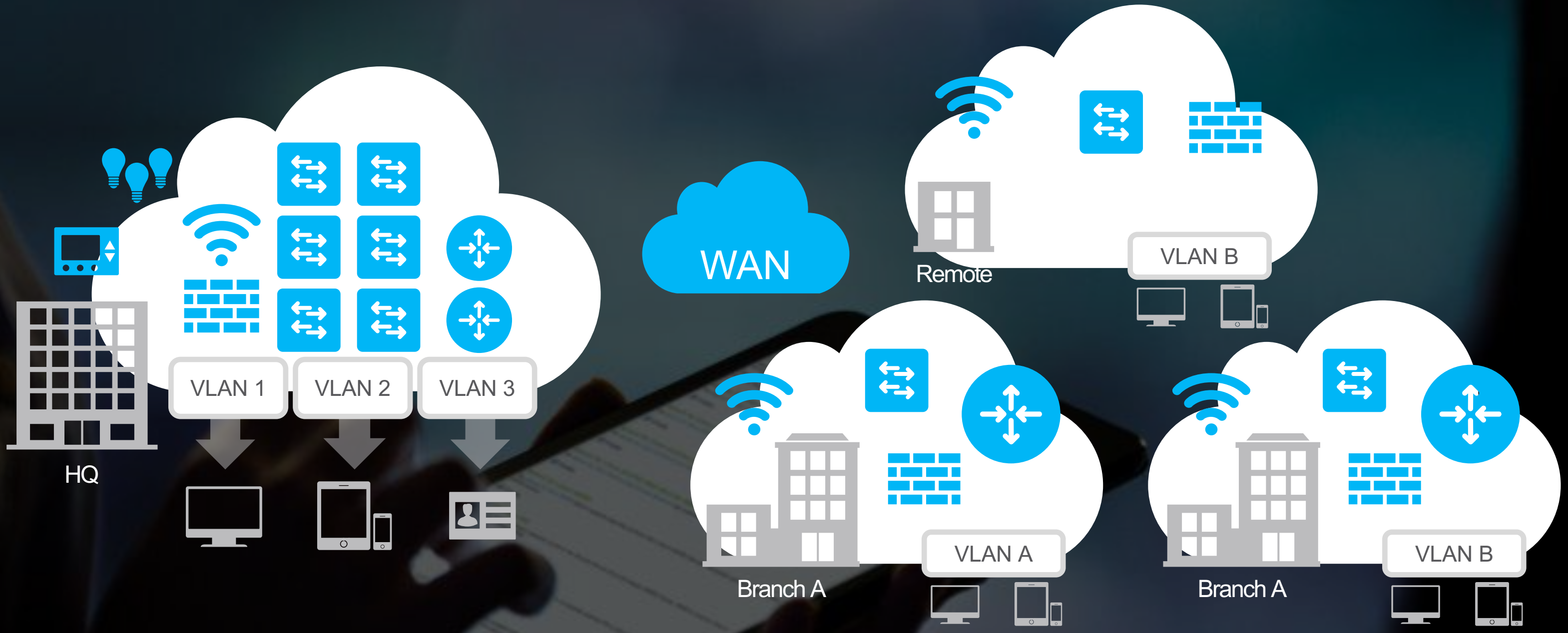
Sales Training

Software-Defined Access
DNA Foundational

Leonardo Montané

Public Sector Systems Engineer

Enterprise Networks Today are Complex…



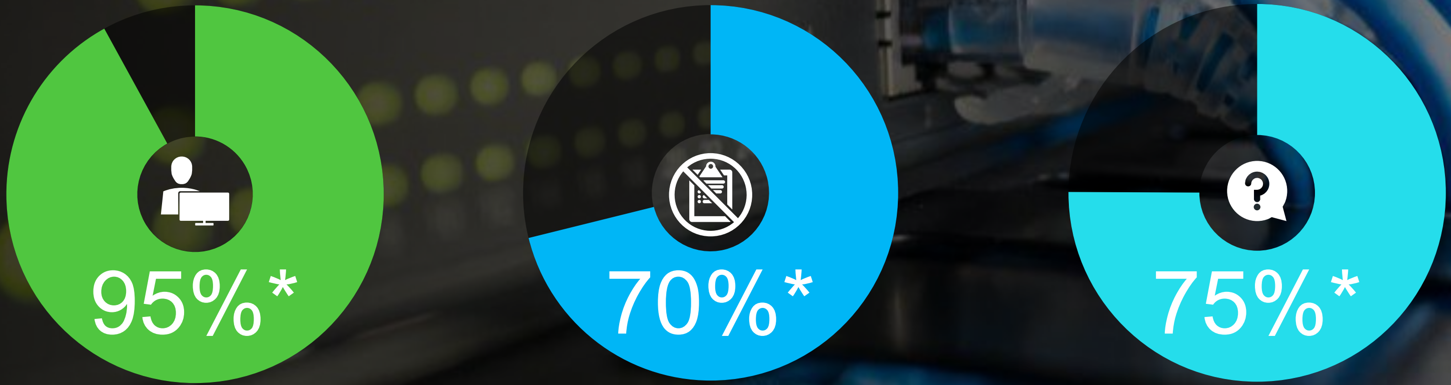
Setting Up Multiple VLANs

Dealing with Disparate Networks

Defining Policies for LAN, W-LAN & WAN

Adding Resources to Scale

…and Have Multiple Operational Challenges



Network Changes Performed Manually

Policy Violations Due to Human Error

OpEx spent on Network Visibility & Troubleshooting

Traditional Networking CANNOT Keep Pace with the Demands of Digital Business

*2016 Internal Customer Study

Digital Transformation
Requires Network Evolution

Information Era: 2000-2015

Connectivity

with High Reliability

Digital Business Era: 2015+

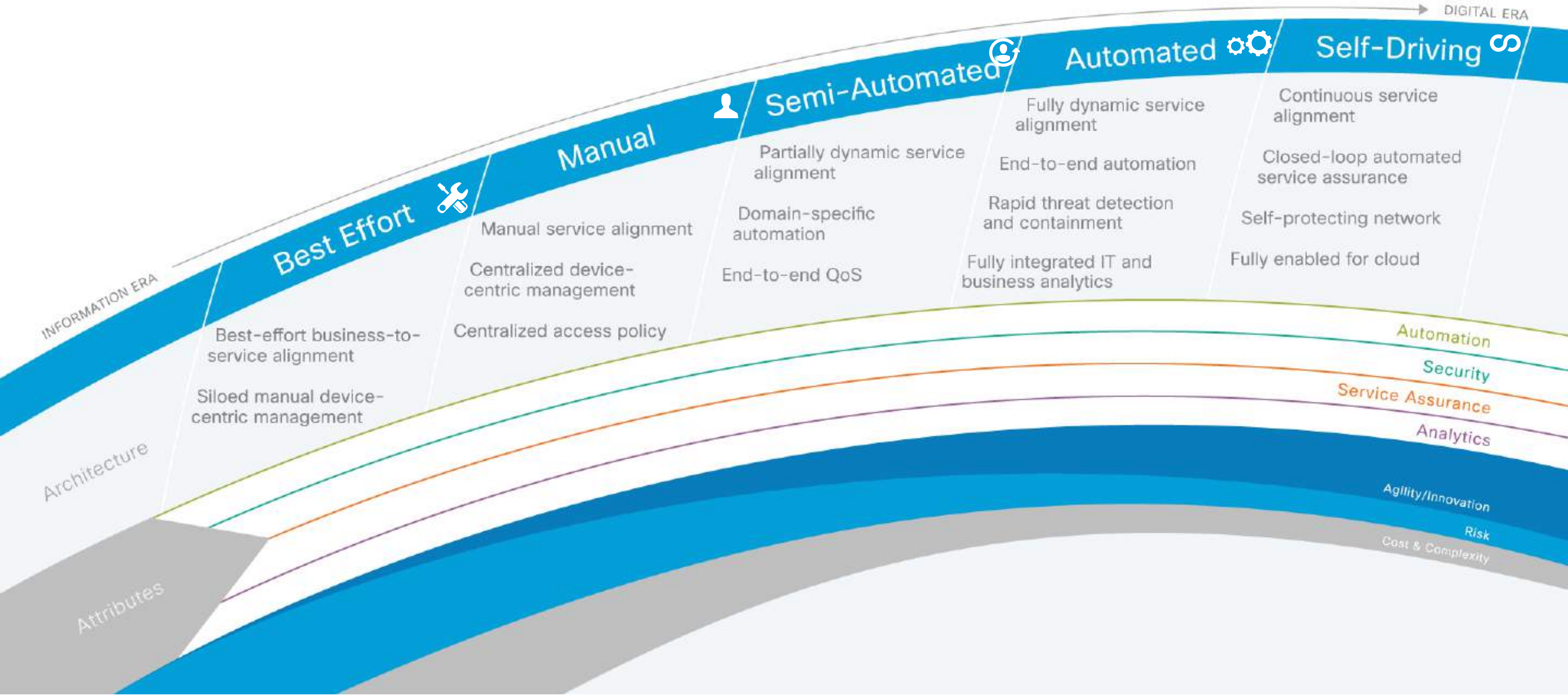
Platform for

Innovation, Agility, Security

Human Scale	IoT Scale (People, Devices, Things)
Physical Appliances	Virtualized Services
Manual Management	Automation, Zero Touch, DevOps
Centralized Enterprise and Web Apps	Distributed SaaS, Mobile, & M2M Apps

Digital Readiness Model

Framework for DNA



Best Effort

Best-effort business-to-service alignment

Siloed manual device-centric management

Manual

Manual service alignment

Centralized device-centric management

Centralized access policy

Semi-Automated

Partially dynamic service alignment

Domain-specific automation

End-to-end QoS

Automated

Fully dynamic service alignment

End-to-end automation

Rapid threat detection and containment

Fully integrated IT and business analytics

Self-Driving

Continuous service alignment

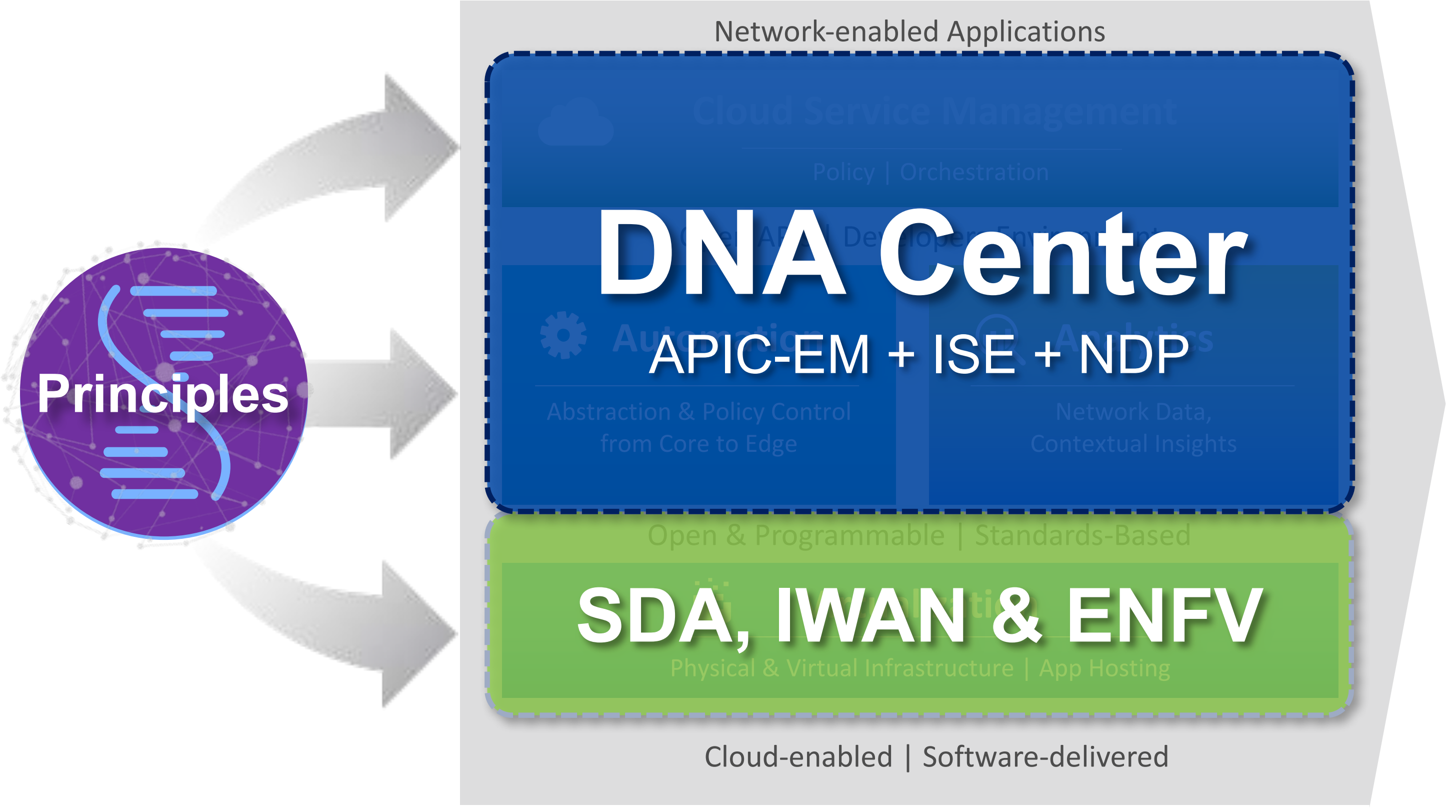
Closed-loop automated service assurance

Self-protecting network

Fully enabled for cloud

Cisco Digital Network Architecture

DNA Overview


Principles
Network-enabled Applications
Cloud Service Management
Policy | Orchestration
DNA Center
APIC-EM + ISE + NDP
Automation
Abstraction & Policy Control from Core to Edge
Analytics
Network Data, Contextual Insights
Open & Programmable | Standards-Based
SDA, IWAN & ENFV
Physical & Virtual Infrastructure | App Hosting
Cloud-enabled | Software-delivered

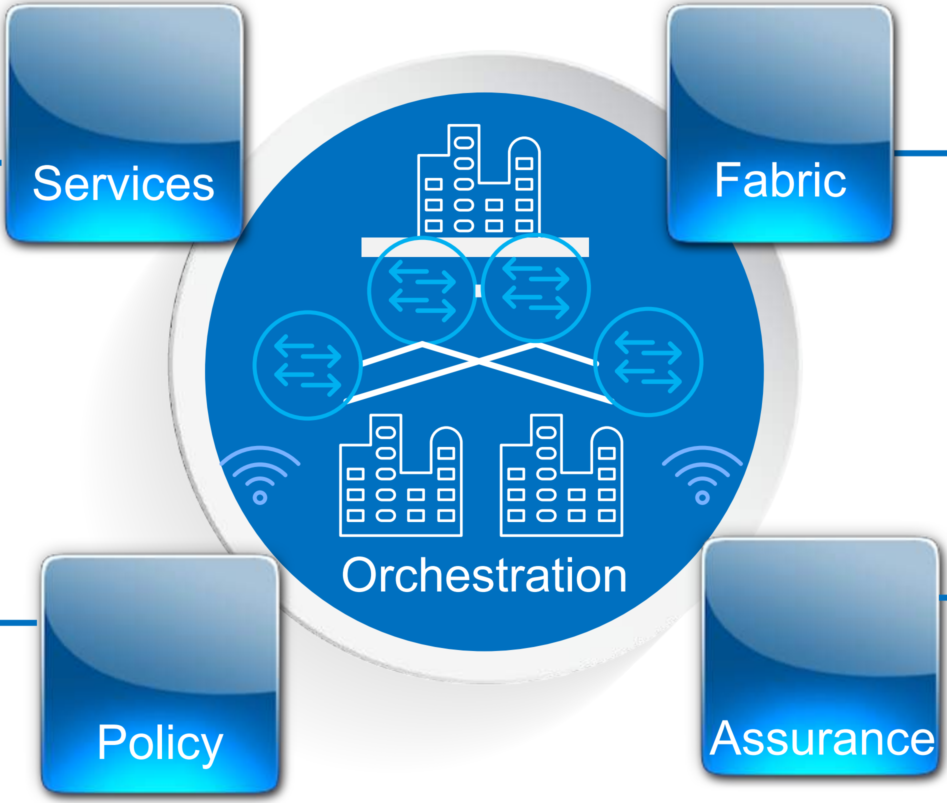
FASTER INNOVATION
Insights & Experiences

REDUCED COST & COMPLEXITY
Automation & Assurance

LOWER RISK
Security & Compliance

Next Generation Enterprise Infrastructure

Foundational Elements Required for New Operational Paradigm



Services enablement through controller based abstraction and open APIs, with fabric aware security and application services integration

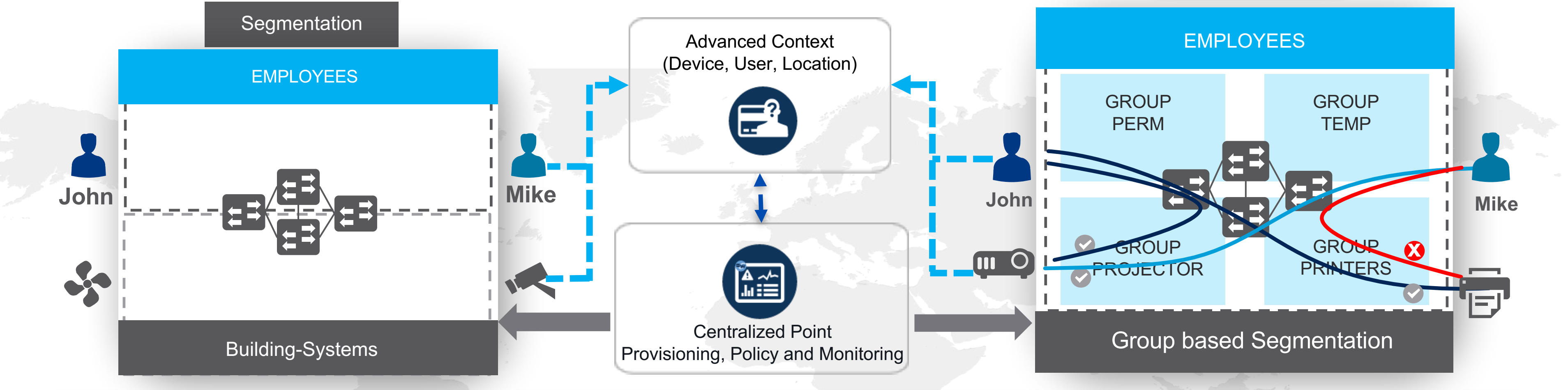
Fabric architecture enabling flexible L2/L3 services on a wired, wireless, and WAN network that is managed as single system

Policy based automated provisioning of network for access, security, application quality of experience, and monitoring, across multiple domains

Assurance for applications, user experience, infrastructure and endpoint function. Network health, availability and function.

Journey to Secure Automation
Business Driven Architecture

Location and IP Address Independence



Secure, Automated, Flexible

Secure

- Support user/ endpoint authentication, identification, remediation, quarantine
- Integrated scalable security enforcement
- IP Address agnostic and location independent
- Software defined segmentation

Policy Driven

- Simplified endpoint policy development and application
- User Centric : Independent of IP Address
- Pervasive and Systemic Application
- Easy to understand, apply, modify or remove

Automated

- Add/Remove Fabric Elements quickly and easily
- Intuitive User Centric GUI
- Integrates with other tools and open API's

Flexible and Scalable

- Supports L2 and L3 topology overlay with location independence
- Supports thousands of infrastructure devices within the fabric
- Wired and Wireless Integration
- Supports migration and interoperability

Worldwide

Sales Training

SD-Access
High Level Design Considerations

Leonardo Montané

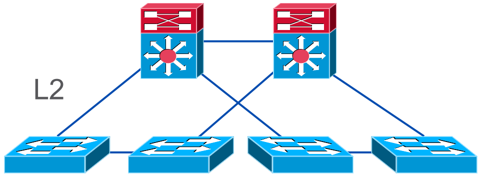
Public Sector Systems Engineer

Common Access Layer Topologies
Design and Deployment Considerations

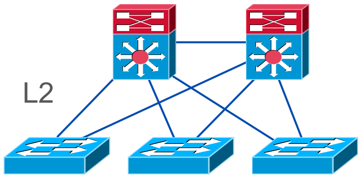
Design Challenges with Growing Needs and New Innovation

- L2/L3 Protocol Tuning
  - STP Priority to HSRP Mapping
- STP Complexity and Limitations
  - STP Root, Priority, Cost
- Failure Domains
  - Topology impact on failover and convergence
- QoS Policy
  - L2 vs. L3 policy enforcement
- Security Policy
  - ACLs statically mapping to MAC and IP

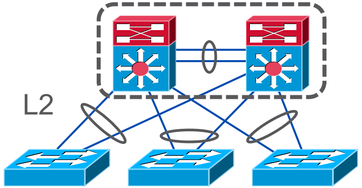
Access Topology Design



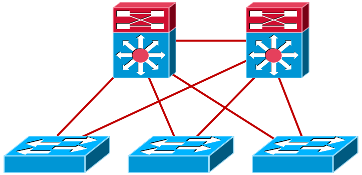
Looped Square



Looped Triangle



VSS/Stack Distribution



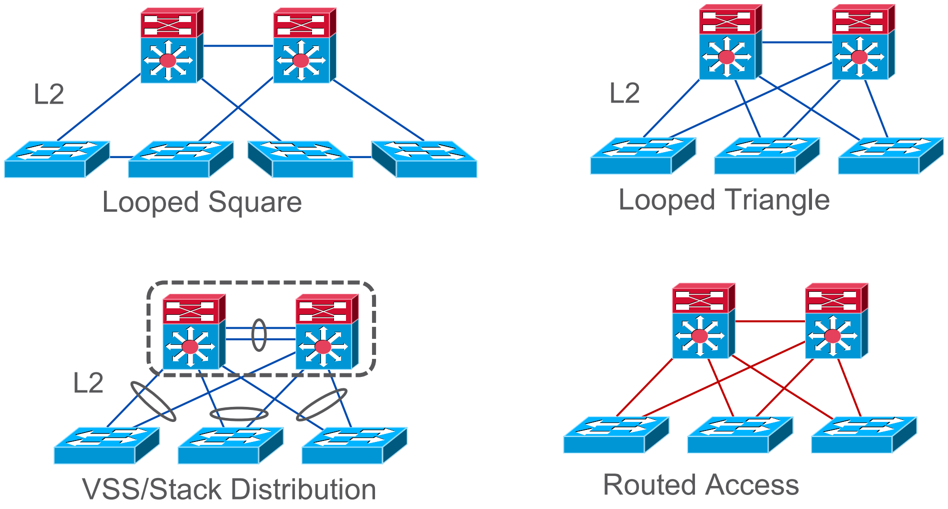
Routed Access

Common Access Layer Topologies
Growing Complexity - Scale, Policy, Segmentation

Complexity Grows with Scale and Changing Business Requirements

- Host Mobility
  - Stretching VLANs introduces risks associated with L2 flooding

Access Topology Design



Looped Square

Looped Triangle

VSS/Stack Distribution

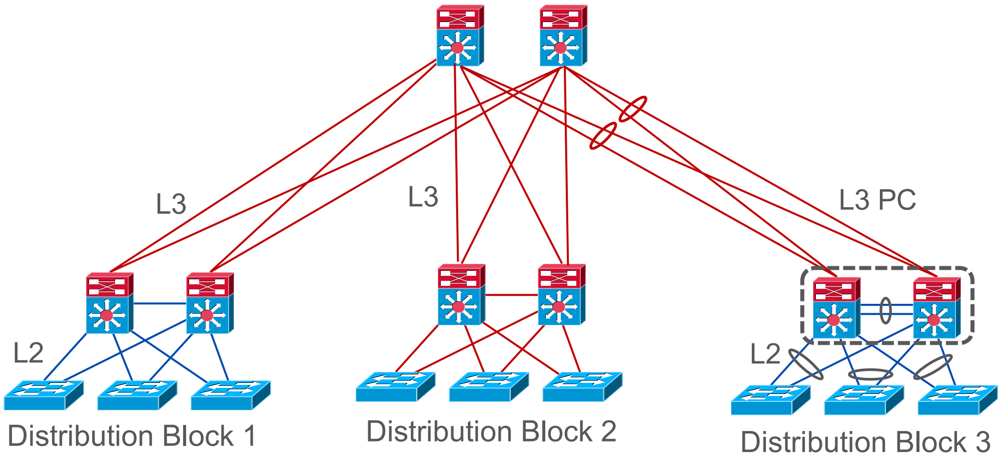
Routed Access

Common Access Layer Topologies
Growing Complexity - Scale, Policy, Segmentation

Complexity Grows with Scale and Changing Business Requirements

- Host Mobility
  - Stretching VLANs introduces risks associated with L2 flooding
  - Challenge to accommodate policy for users roaming between distribution pairs

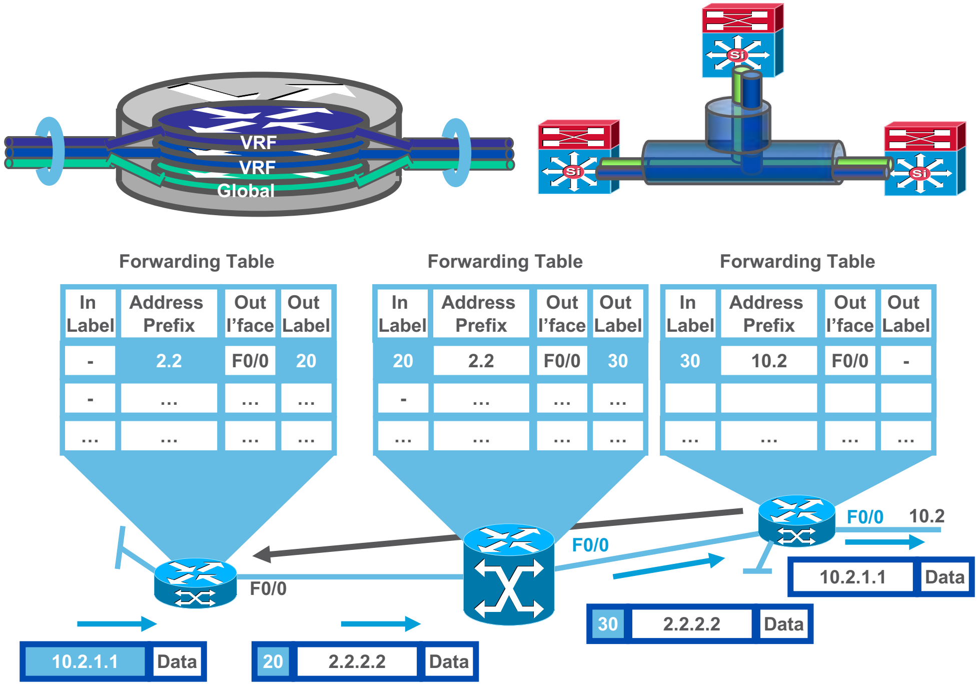
3-Tier Hierarchical View



Common Access Layer Topologies
Growing Complexity - Scale, Policy, Segmentation

Complexity Grows with Scale and Changing Business Requirements

- Host Mobility
  - Stretching VLANs introduces risks associated with L2 flooding
  - Challenge to accommodate policy for users roaming between distribution peers
- Segmentation
  - Growing complexity associated with introduction of VRF and full scale MPLS provisioning
- Manageability
  - Inconsistent, inflexible and complex operational model



Forwarding Table

In Label	Address Prefix	Out I'face	Out Label
-	2.2	F0/0	20
-	...	...	...
...	...	...	...

Forwarding Table

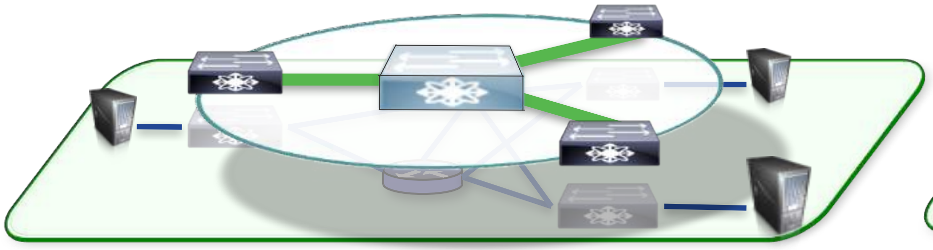
In Label	Address Prefix	Out I'face	Out Label
20	2.2	F0/0	30
-	...	...	...
...	...	...	...

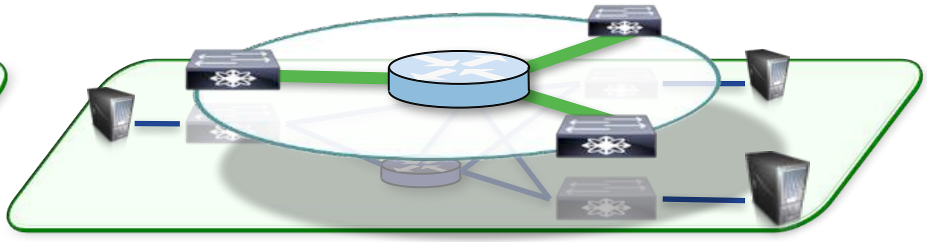
Forwarding Table

In Label	Address Prefix	Out I'face	Out Label
30	10.2	F0/0	-
...	...	...	...

Layer 2 or Layer 3 Access
Dictated by Consumer Device Requirements

What World Do You Live In?





Layer 2 Access

- Stretched LAN segment to extend subnets across multiple closets
- Transport Ethernet Frames (IP & Non-IP)
- Single subnet mobility (L2 domain)
- Exposure to Layer 2 flooding
- STP for loop detection and prevention

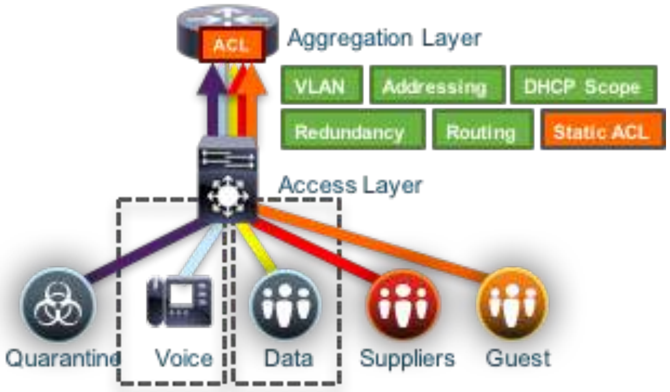
Layer 3 Access

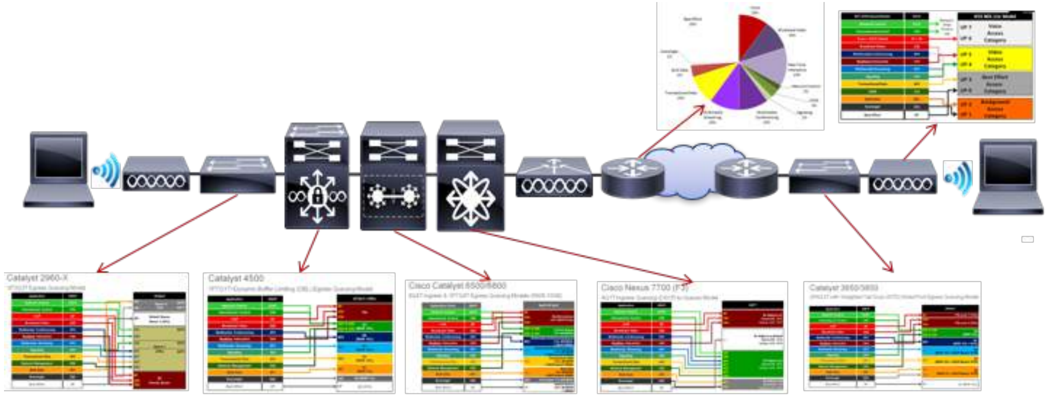
- Modular IP connectivity
- Contain network related failures (floods)
- Transport IP Packets (IPv4 & IPv6)

Layer 2 and Layer 3 Access

Accommodating Security and Differentiated Services

One Can Only Do So Much! What Are You Doing? What Challenges Are You Experiencing?

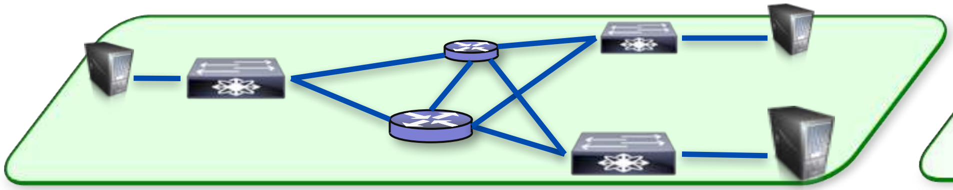


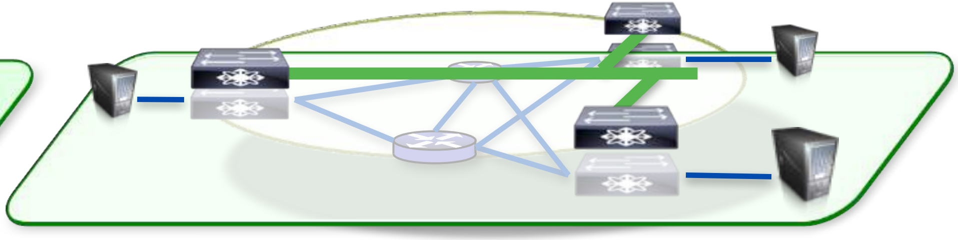


Empower NG Business Driven Infrastructure

Overlay is the Answer

Underlying Transport Built for Forwarding and Optimized Overlay for Services Delivery





Leverage Foundation for Transport Forwarding

- Provision physical devices and paths
- Ensure high speed differentiated forwarding
- Provide resiliency to maximize network availability
- Keep it simple, let the forwarding plane forward

Create Optimized Overlay for Services Delivery

- Design for flexibility and programmability
- Accommodate mobility to track end-points at edges
- Not constrained by the rigidity of the underlay protocols
- Support for L2 and L3 capabilities
- Reduce number of management touch points and the associated nuances
- Distribute state to the network edge to increase scalability

How is Fabric Different from an Overlay?

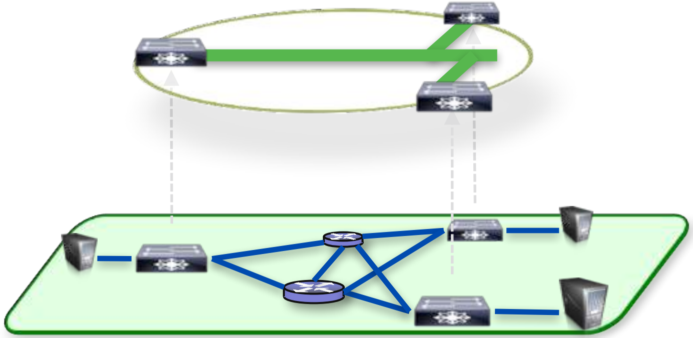
Fabric is an Overlay

An “Overlay” is a *logical topology* used to *virtually connect* devices, built *on top* of an arbitrary physical “Underlay” topology.

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

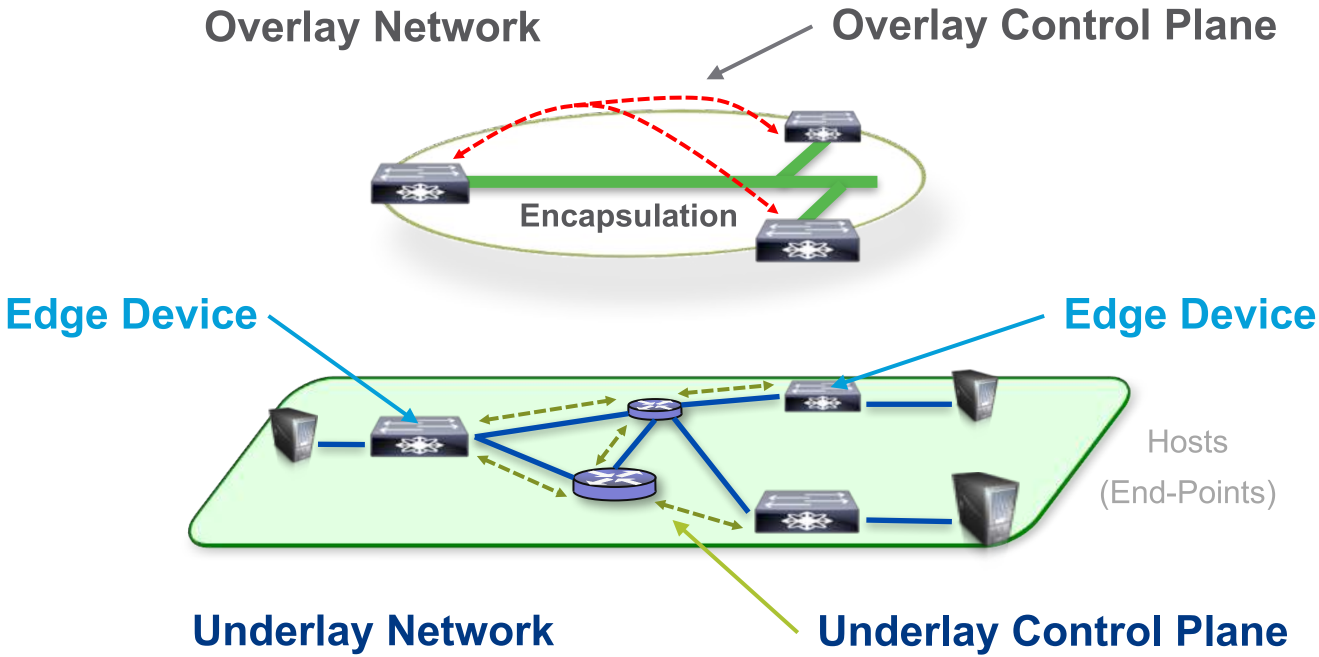
We Live in a World of L2/L3 Overlays

- GRE or mGRE
- L2TPv2 or L2TPv3
- MPLS or VPLS
- IPSec or DMVPN
- CAPWAP
- LISP
- OTV
- DFA
- ACI



Interaction Between Overlay and Underlay

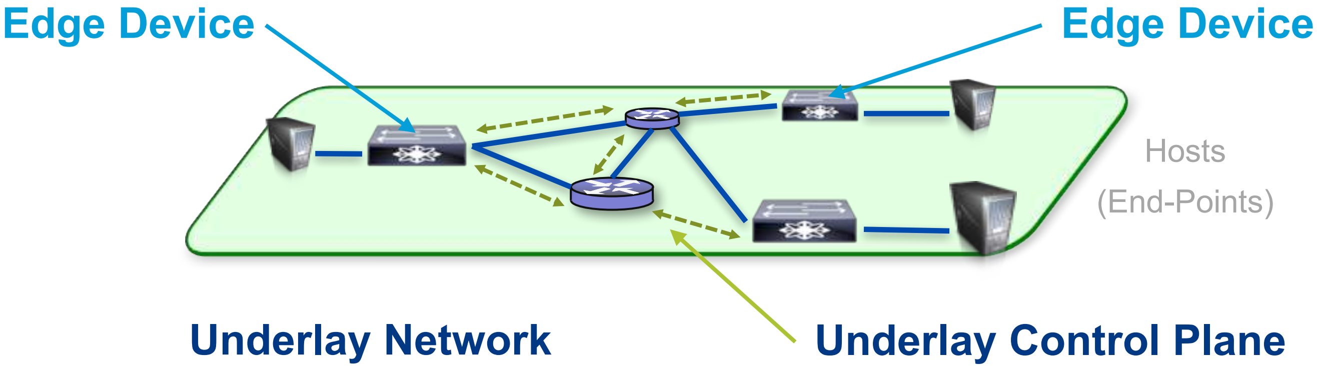
A Picture is Worth a Thousand Words



Design and Deploy for Impact Alignment

Things the Underlay Must Accommodate

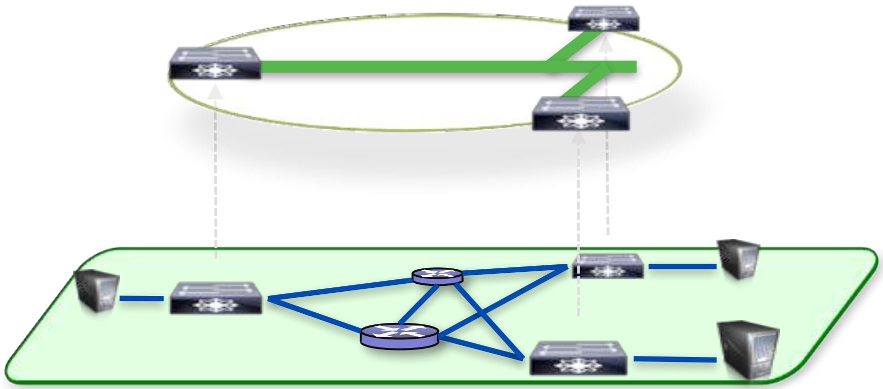
- Routed Network – Intelligent Packet Handling
- Reliability – Maximize Network Availability
- Simplicity – No STP, No Blocking Links, No HSRP, No VSS, etc

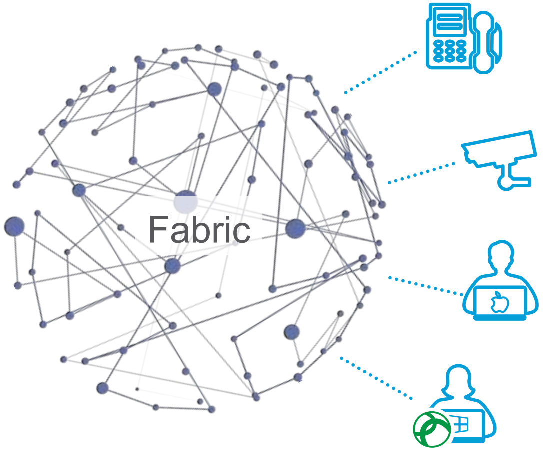


Design and Deploy for Impact Alignment

Things the Campus Fabric Must Accommodate

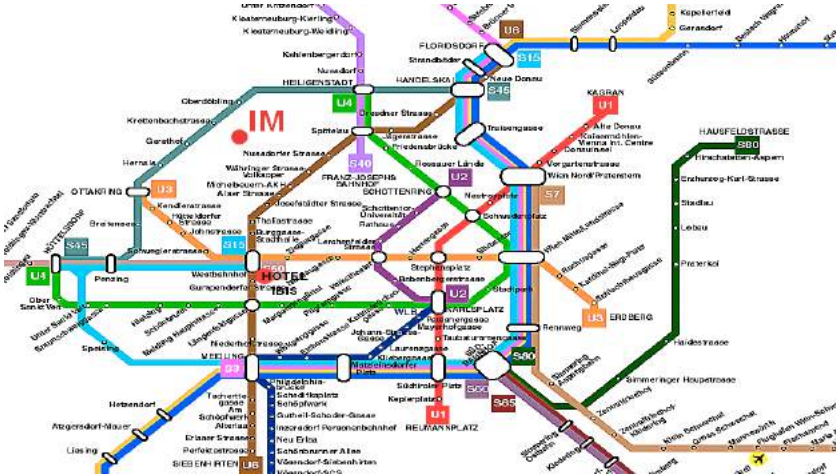
- Host Mobility without stretching VLANs
- Network Segmentation without implementing MPLS
- Role-based Access Control without ‘End-to-End’ TrustSec

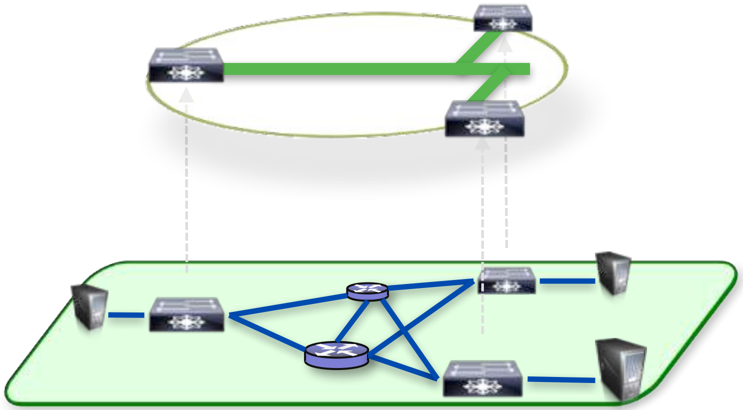




Campus Fabric
Key Components

- LISP based Control-Plane
- VXLAN based Data-Plane
- Platform for seamless TrustSec integration





Key Differences

- L2 + L3 Overlay vs. L2 or L3 Only
- Adds VRF + SGT into Data-Plane
- Host Mobility with Anycast Gateway
- Virtual Tunnel Endpoints (No Static)
- No Topology Limitations (Basic IP)
- Policy and Logical Grouping

SD-Access

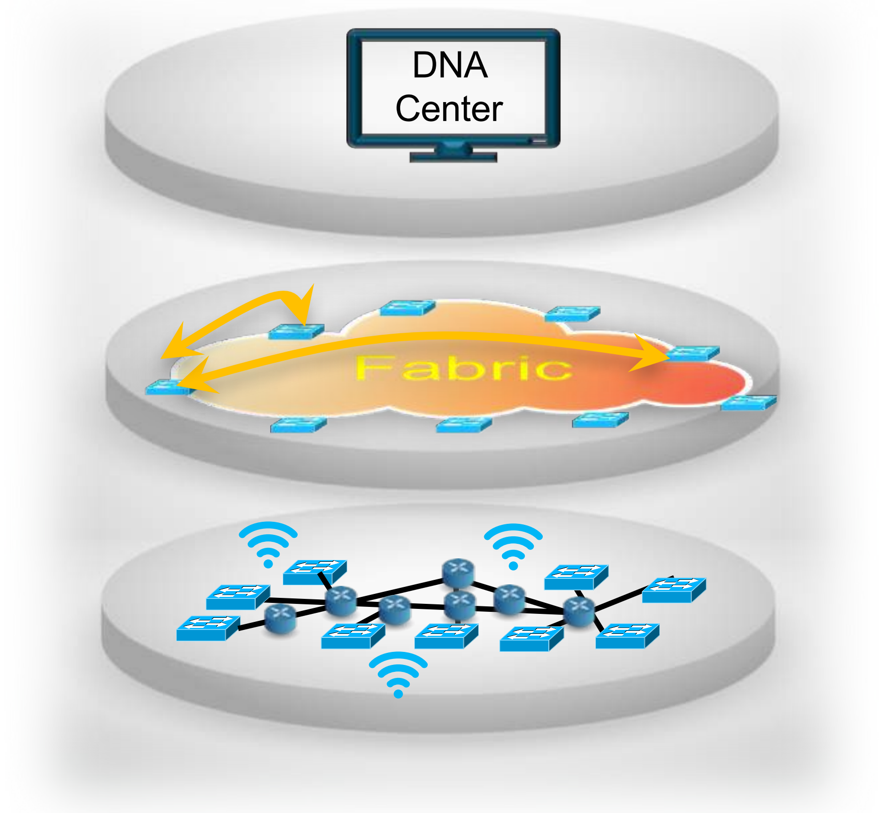
Where DNA Center Meets Campus Fabric

Leonardo Montané

Public Sector Systems Engineer

Software Defined Access (SD-Access)

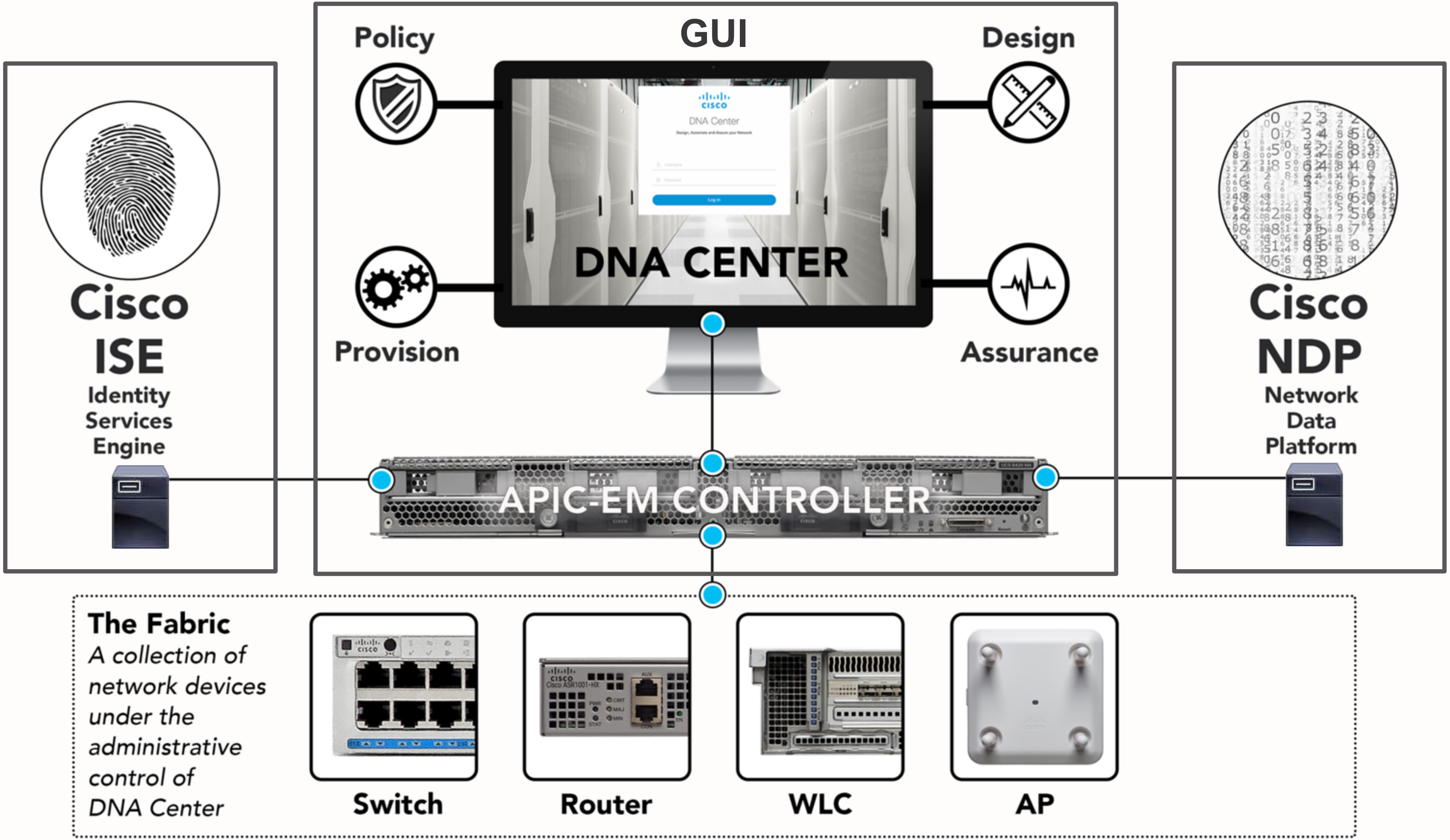
Bringing Everything Together



Controller-based Management

Programmable Overlay

Simplified L3 Underlay



GUI

Policy

Design

Provision

Assurance

DNA CENTER

APIC-EM CONTROLLER

Cisco ISE

Identity Services Engine

Cisco NDP

Network Data Platform

The Fabric

A collection of network devices under the administrative control of DNA Center

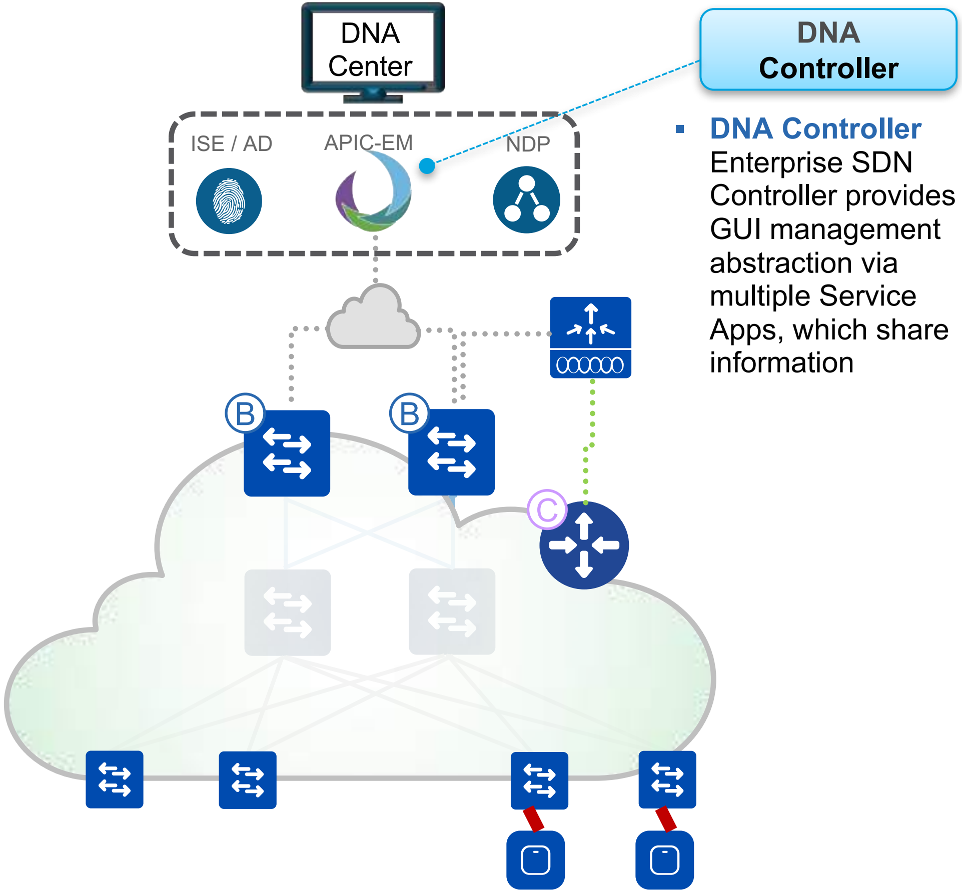
Switch

Router

WLC

AP

SD-Access Architecture
Roles and Terminology



- **DNA Controller**
  Enterprise SDN Controller provides GUI management abstraction via multiple Service Apps, which share information

APIC-EM is a central part of Cisco Digital Network Architecture. It delivers software-defined networking to the enterprise branch, campus, and WAN. Its simple user interface lets you automate policy-based application profiles.

Features Applications including:

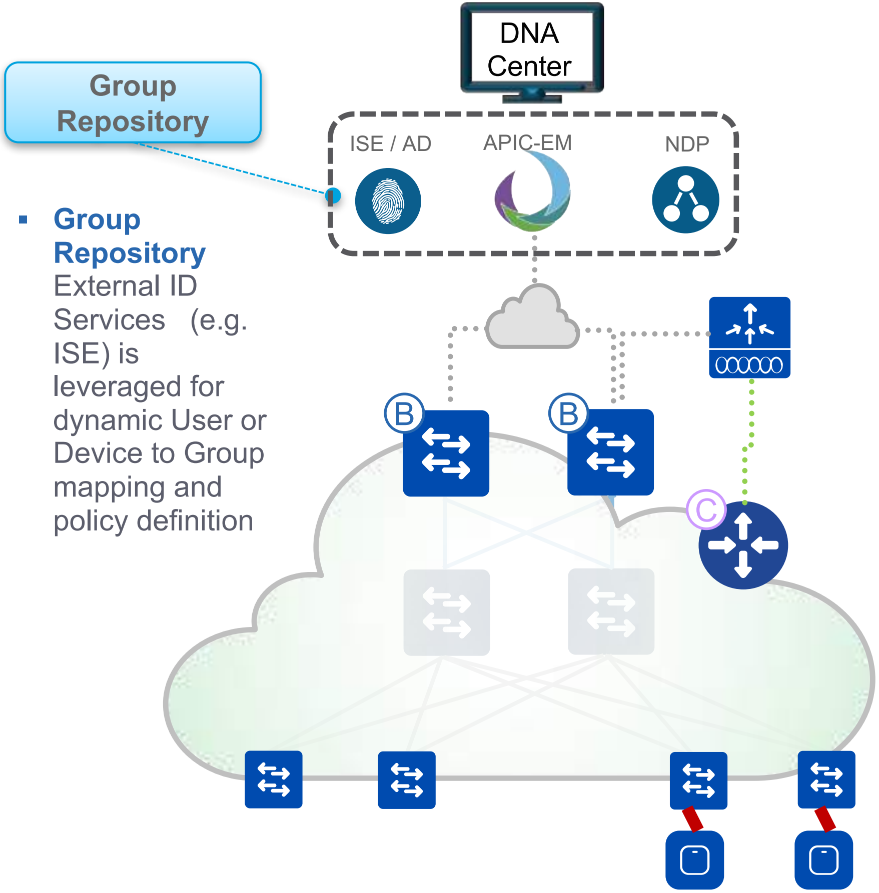
Essential Apps

- Plug-and-Play
- Path Trace
- EasyQoS
- Apple Bonjour Service Discovery Gateway
- Active Advisor

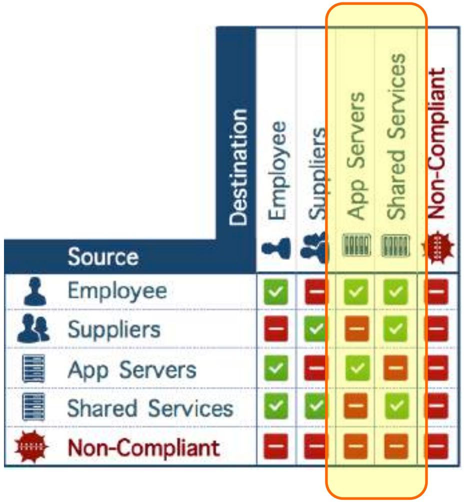
Advanced Apps

- Cisco Intelligent WAN (IWAN)
- Cisco Enterprise Service Automation (ESA)
- Software Defined Access (SD-Access)

SD-Access Architecture
Roles and Terminology



- **Group Repository** External ID Services (e.g. ISE) is leveraged for dynamic User or Device to Group mapping and policy definition



Source \ Destination	Employee	Suppliers	App Servers	Shared Services	Non-Compliant
Employee	✓	🟥	✓	✓	🟥
Suppliers	🟥	✓	🟧	✓	🟥
App Servers	✓	🟥	✓	🟧	🟥
Shared Services	✓	✓	🟧	✓	🟥
Non-Compliant	🟥	🟥	🟧	🟧	🟥

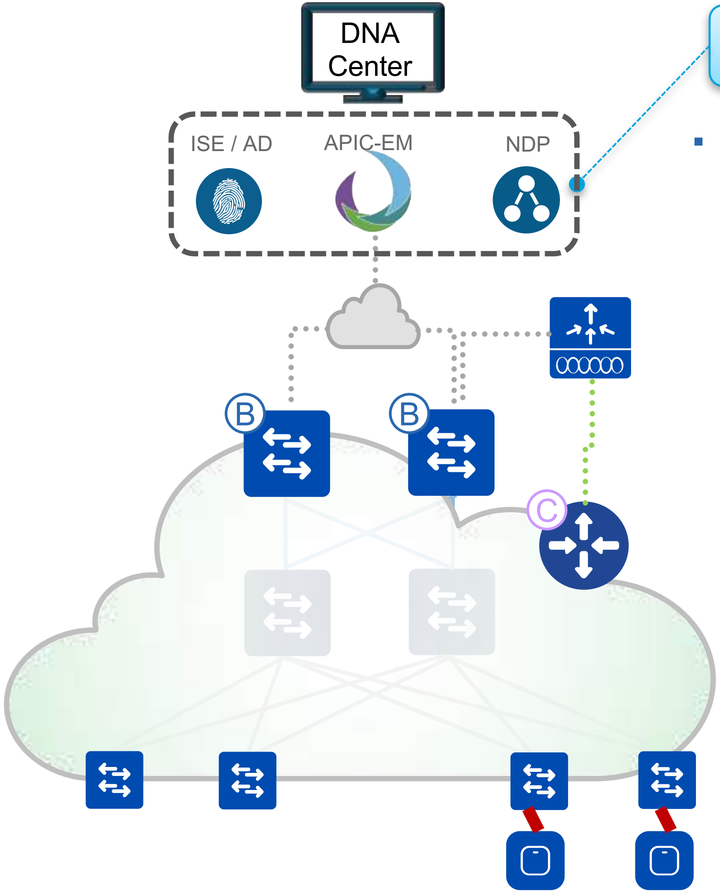
Authenticate Users at Fabric Edge (802.1X, MAC Auth, …)

Segment traffic based on classified group (SGT), not based on topology (VLAN, IP subnet)

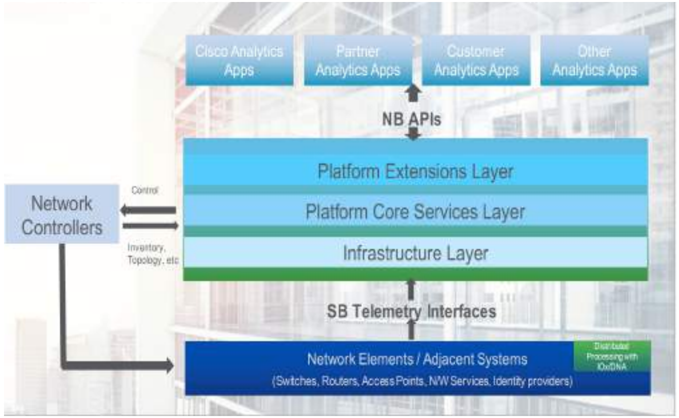
Regardless of location, the “policy” (SGT) stays with users, devices, and applications

CTS simplifies ACL management for all cross-domain traffic

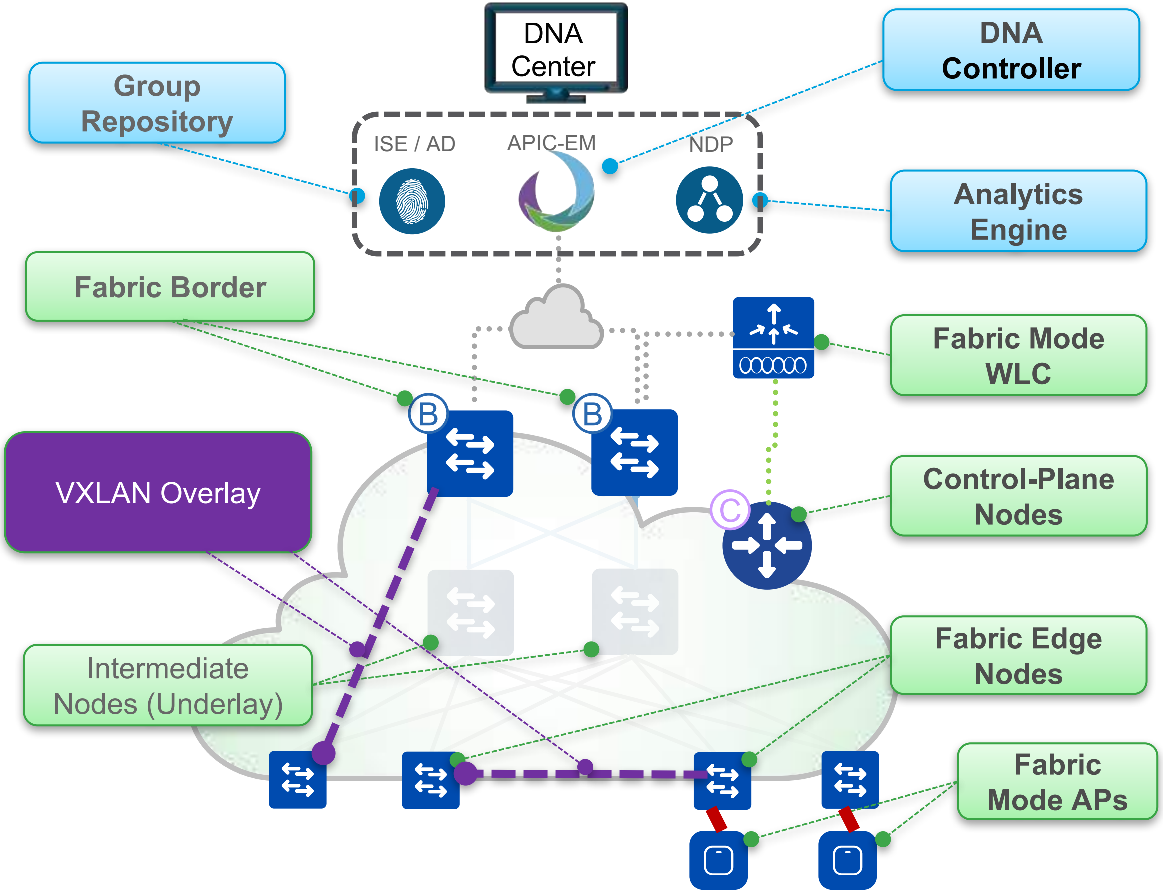
SD-Access Architecture
Roles and Terminology



- **Analytics Engine**
  External Data Collector (e.g. NAE) is leveraged to analyze User or Device to App flows and monitor fabric status

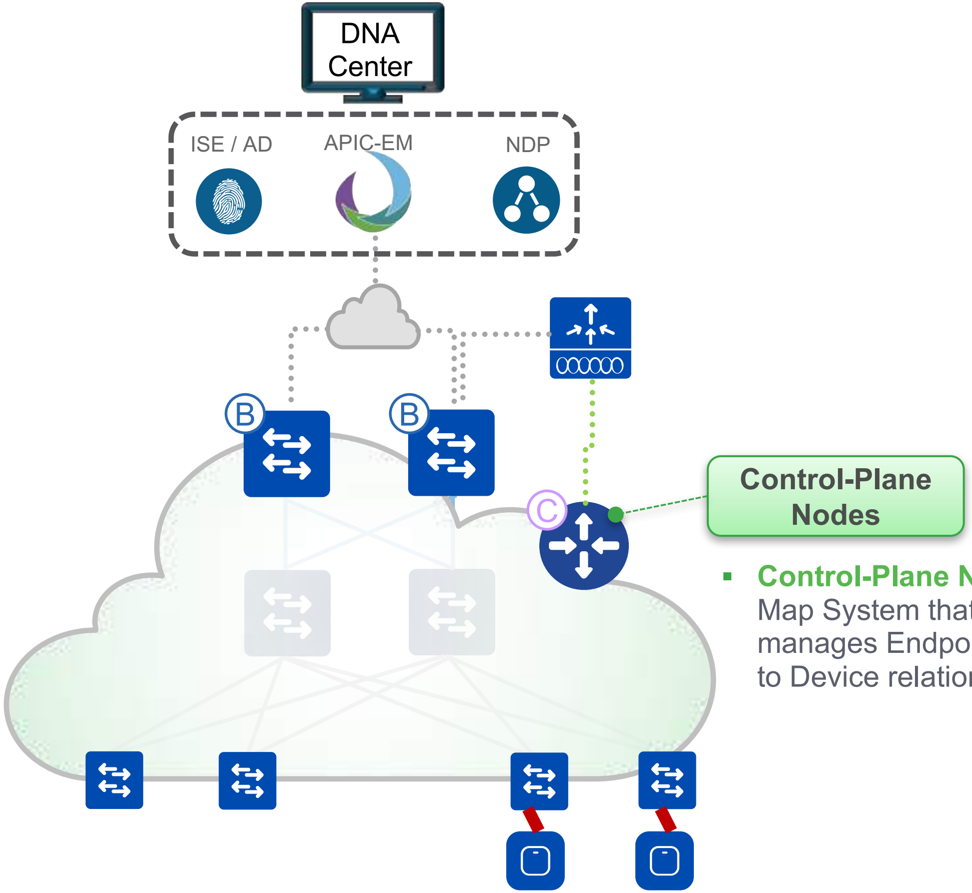

Cisco Analytics Apps
Partner Analytics Apps
Customer Analytics Apps
Other Analytics Apps
NB APIs
Platform Extensions Layer
Platform Core Services Layer
Infrastructure Layer
Network Controllers
Control
Inventory, Topology, etc
SB Telemetry Interfaces
Network Elements / Adjacent Systems
(Switches, Routers, Access Points, N/W Services, Identity providers)
Distributed Processing with IOx/DNA

SD-Access Architecture
Roles and Terminology



- **Control-Plane Nodes** – Map System that manages Endpoint ID to Device relationships
- **Border Nodes** – A Fabric device (e.g. Core) that connects External L3 network(s) to the SD-Access Fabric
- **Edge Nodes** – A Fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SD-Access Fabric
- **Fabric Wireless Controller** – Wireless Controller (WLC) that is fabric-enabled
- **Fabric Mode APs** – Access Points that are fabric-enabled.
- **Intermediate Nodes** – Underlay
- **Overlay** – Endpoint traffic carried within VXLAN frames between Fabric Edges and between Fabric Edges and Border Nodes

SD-Access Architecture
Fabric Control-Plane Node Responsibilities

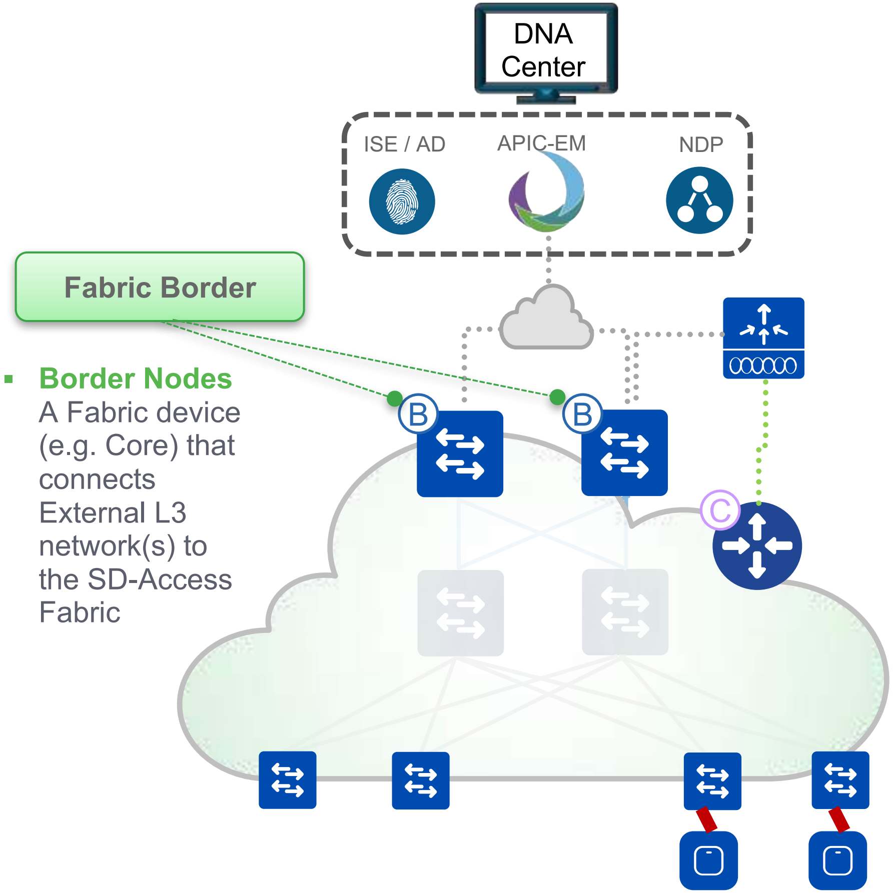


- **Control-Plane Nodes**
  Map System that manages Endpoint ID to Device relationships

Fabric Control-Plane Node is based on a LISP Map Server / Resolver
Runs the Host Tracking Database to provide overlay reachability information

- Receives prefix registrations from Edge Nodes with local Endpoints
- Provides a simple Host Database, that ties the Endpoint to the Edge Node where it resides (includes other relevant attributes)
- Resolves lookup requests from remote Edge Nodes, to locate local Endpoints
- Host Database supports multiple Endpoint ID lookup keys (**IPv4 /32**, IPv6 /128 or MAC)

SD-Access Architecture
Fabric Border Node Responsibilities

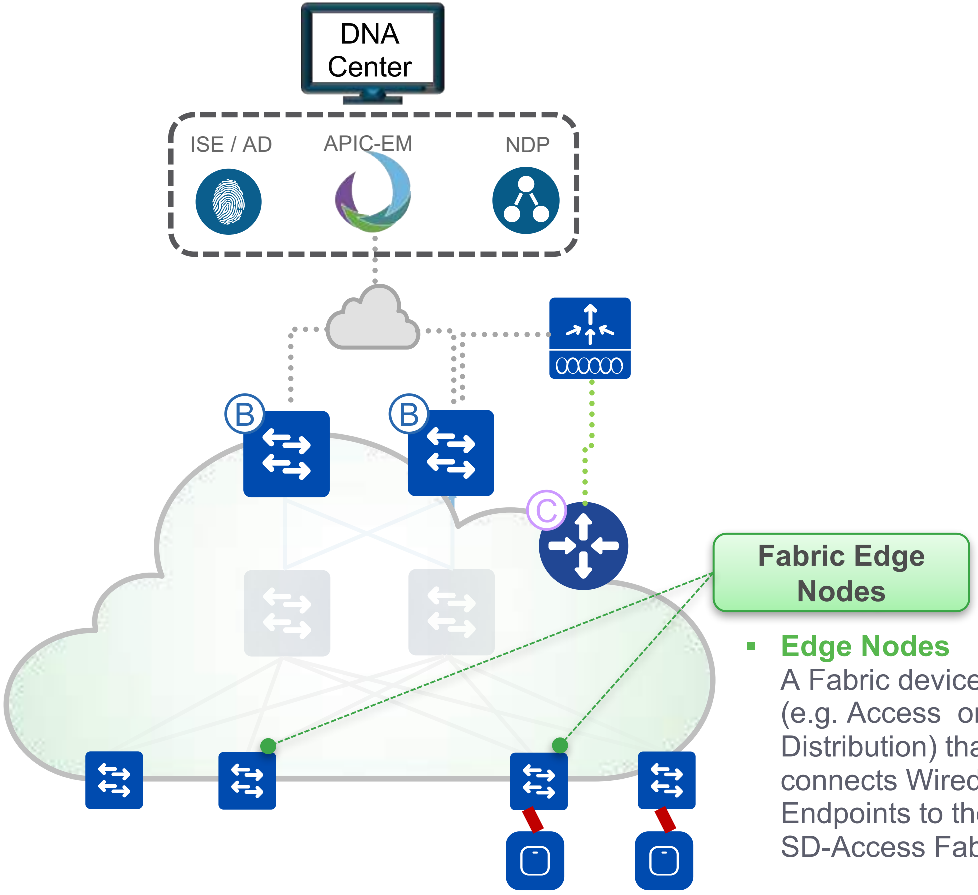


- **Border Nodes**
  A Fabric device (e.g. Core) that connects External L3 network(s) to the SD-Access Fabric

Fabric Border Node is based on a LISP Proxy Tunnel Router (PxTR)
All traffic entering or leaving the Fabric goes through this type of node

- Connects traditional L3 networks and / or different Fabric domains to the local domain
- Where two domains exchange Endpoint reachability and policy information
- Responsible for translation of context (VRF and SGT) from one domain to another
- Provides a domain exit point for all Edge Nodes acting in many ways like a ‘Default-Gateway’

SD-Access Architecture
Fabric Edge Node Responsibilities



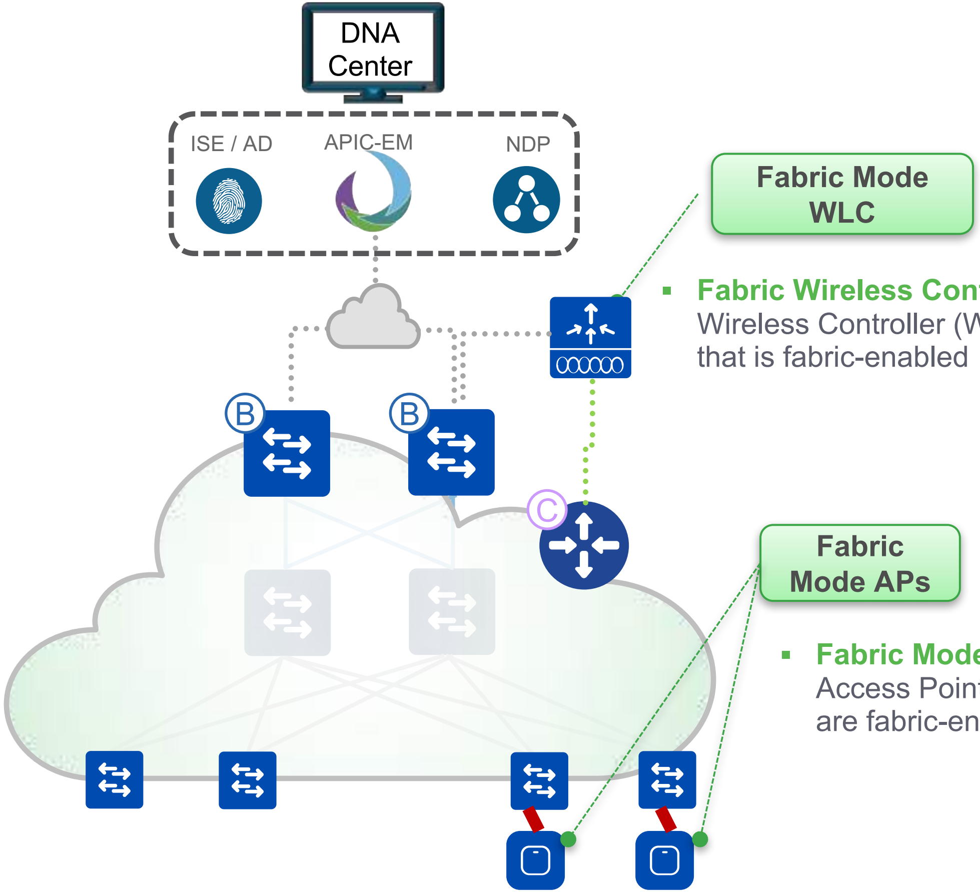
- **Edge Nodes**
  A Fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SD-Access Fabric

Fabric Edge Node is based on a LISP Tunnel Router (xTR)
Provides connectivity for Users and Devices connected to the Fabric

- Responsible for Identifying and Authenticating Endpoints as they move around
- Registers Endpoint ID information with the Control-Plane Node(s)
- Provides Anycast L3 Gateway for connected Endpoints removing the need for HSRP and facilitating seamless host mobility
- Must encapsulate / de-encapsulate host traffic to and from Endpoints connected to the Fabric

SD-Access Architecture

Fabric Mode WLC and AP Responsibilities



- **Fabric Wireless Controller**
  Wireless Controller (WLC) that is fabric-enabled

- **Fabric Mode APs**
  Access Points that are fabric-enabled.

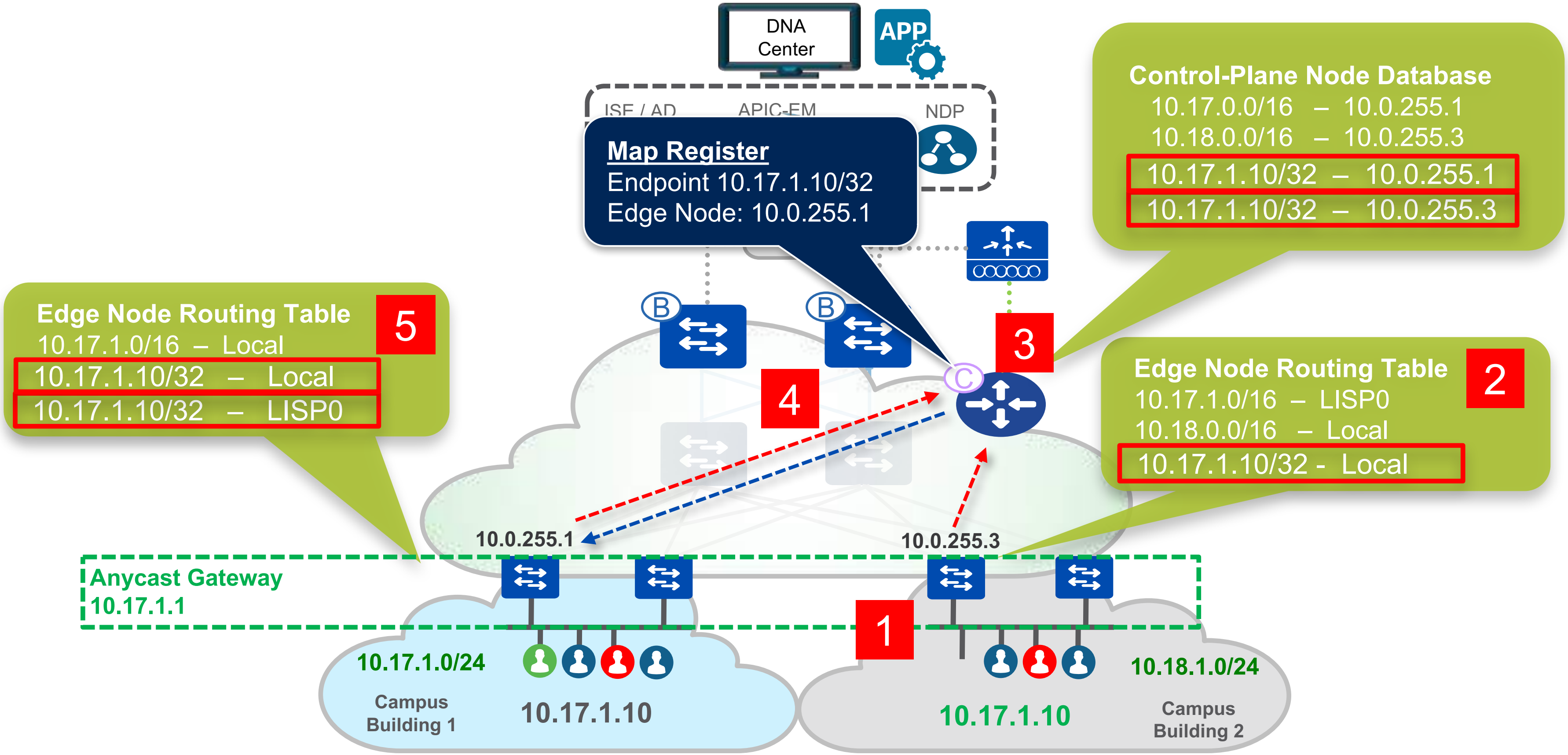
- Centralized control/management plane, distributed data plane, with scalable consistent guest access
- WLC Communicates Client Information to LISP Host Tracking Database (HTDB). It is part of the LISP Control Plane

Mobility

Wired and Wireless

Host Mobility Without Stretching VLANs

Always connect to the same L3 gateway



Map Register
Endpoint 10.17.1.10/32
Edge Node: 10.0.255.1

Control-Plane Node Database
10.17.0.0/16 – 10.0.255.1
10.18.0.0/16 – 10.0.255.3
10.17.1.10/32 – 10.0.255.1
10.17.1.10/32 – 10.0.255.3

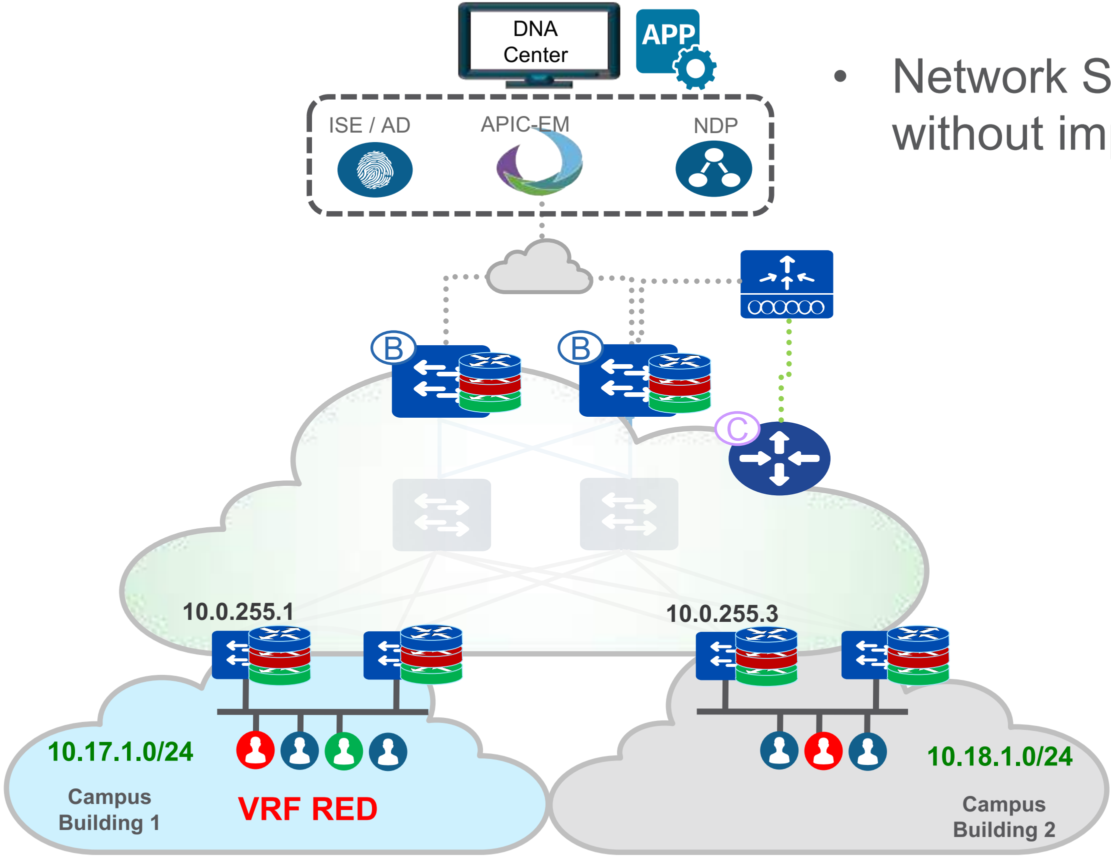
Edge Node Routing Table 5
10.17.1.0/16 – Local
10.17.1.10/32 – Local
10.17.1.10/32 – LISP0

Edge Node Routing Table 2
10.17.1.0/16 – LISP0
10.18.0.0/16 – Local
10.17.1.10/32 - Local

Secure

Segmentation

Simple ***Segmentation*** constructs to build ***Secure*** boundaries for “users and things”

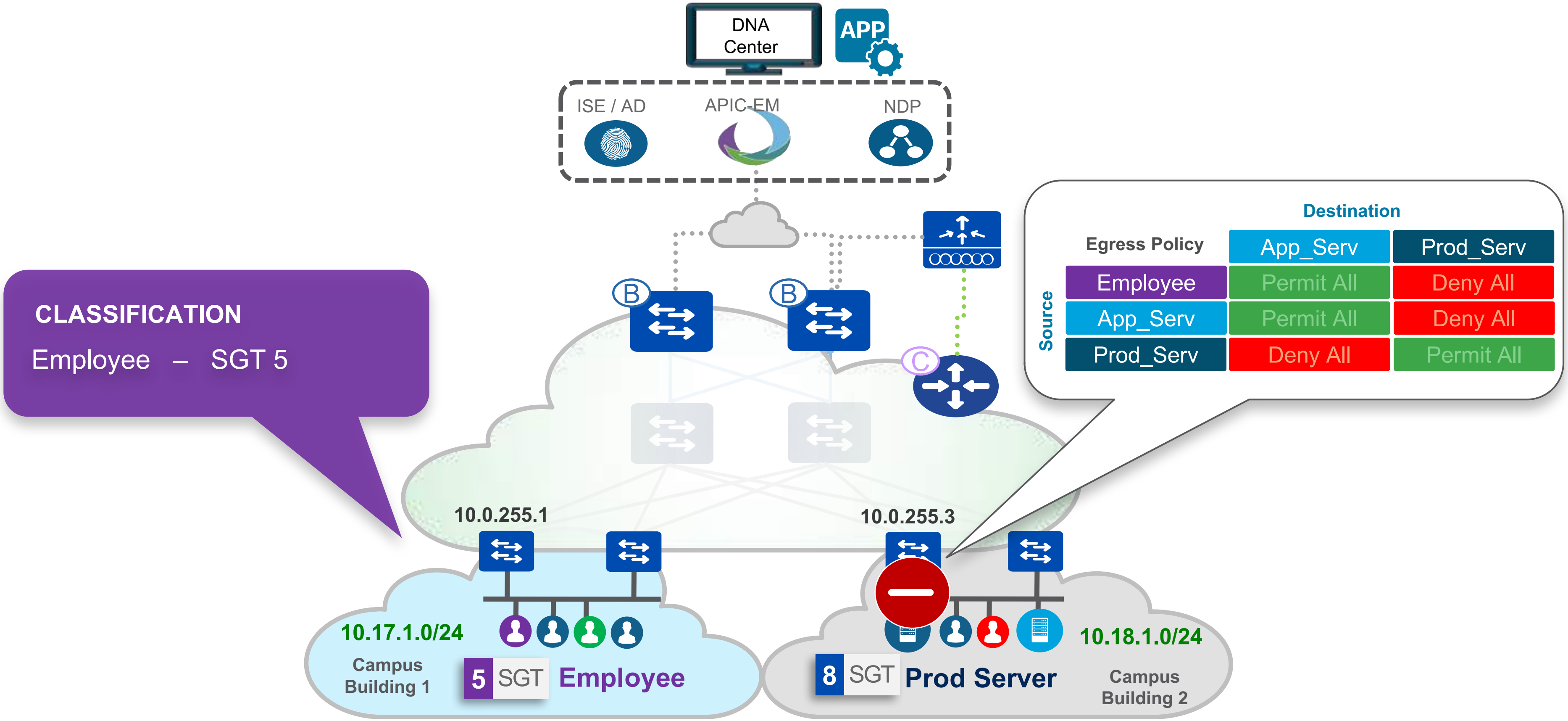


- Network Segmentation without implementing MPLS

Intelligent Policy

Simplified Network Wide *Intelligent Policy* enforcement

Based on your Identity, not on your Address



CLASSIFICATION

Employee – SGT 5

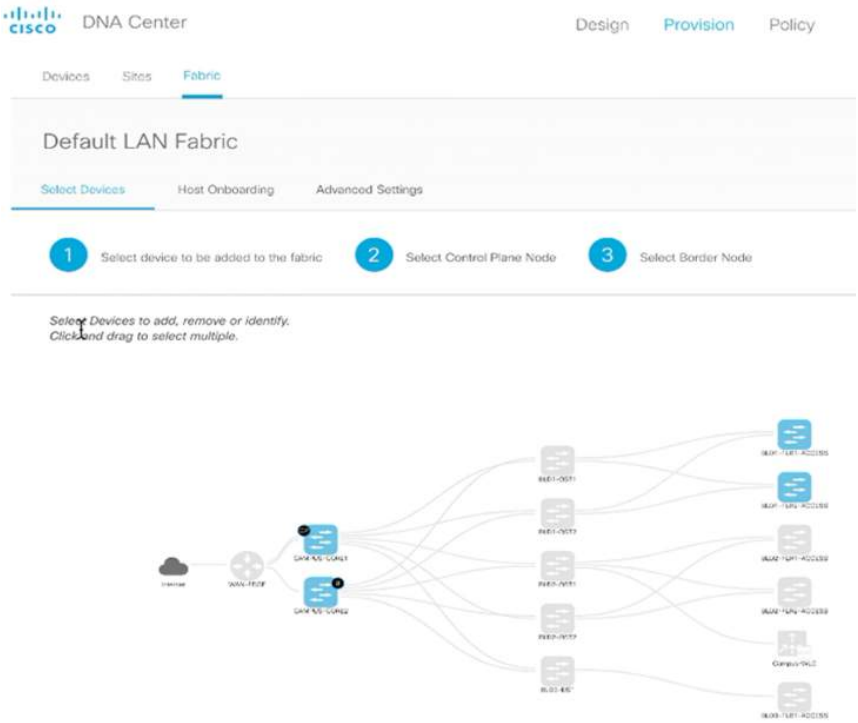
		Destination	
	Egress Policy	App_Serv	Prod_Serv
Source	Employee	Permit All	Deny All
	App_Serv	Permit All	Deny All
	Prod_Serv	Deny All	Permit All

Provision

Simplified Provisioning

Deploy devices using “best practice” configurations

using Smart CLI, Programmability models, Controller capabilities



Default LAN Fabric

1 Select device to be added to the fabric

2 Select Control Plane Node

3 Select Border Node

Select Devices to add, remove or identify.
Click and drag to select multiple.

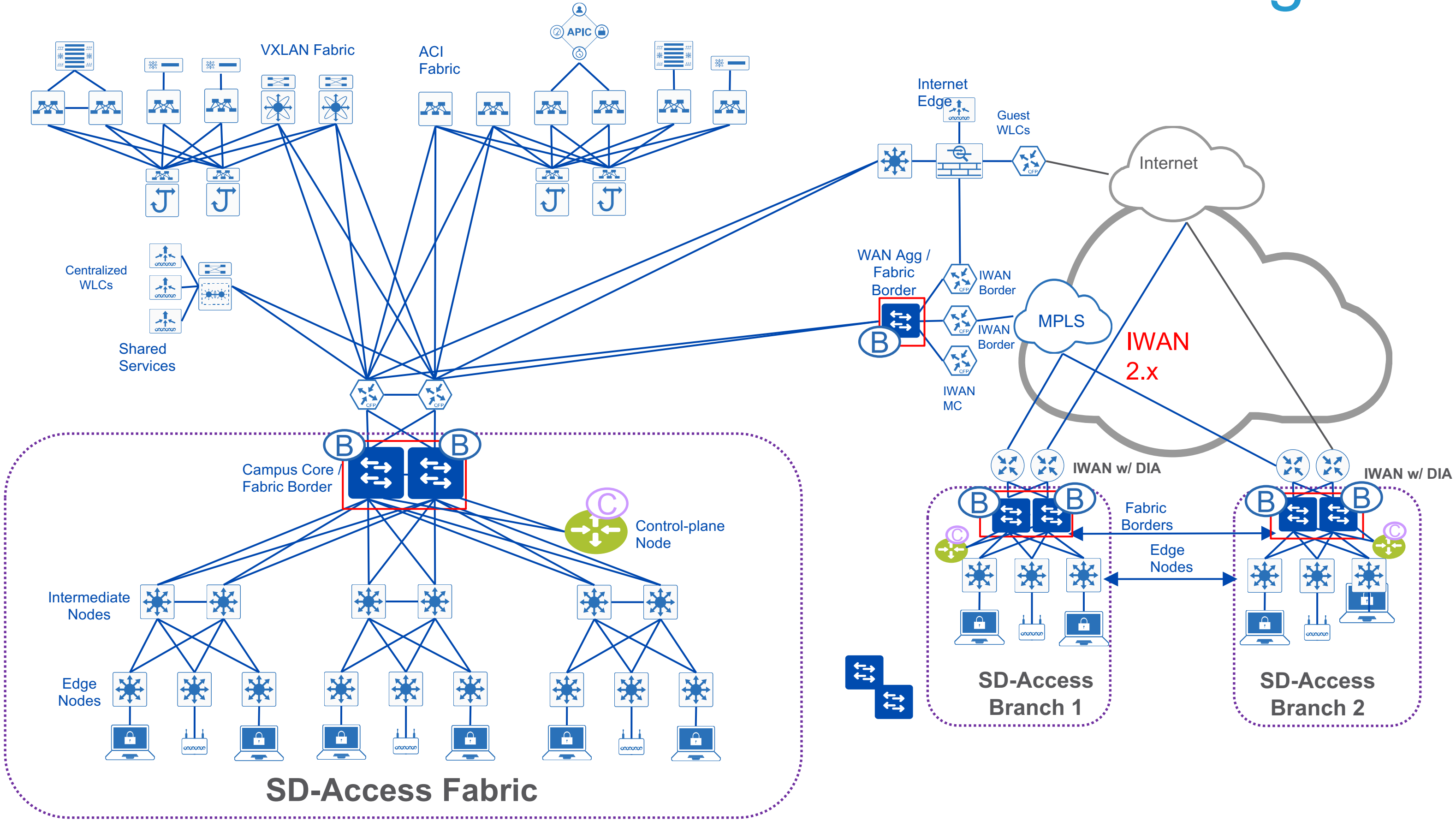
SD-Access
High Level Design Considerations

Leonardo Montané

Public Sector Systems Engineer

SD-Access Branch Design

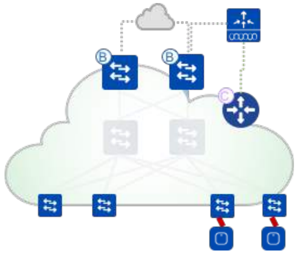
SD-Access Per Site Fabric Distribute Design

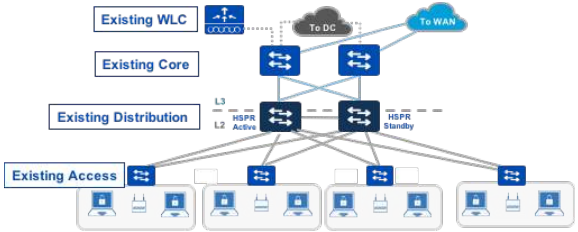


SD-Access Brownfield

Approaches to Integration and Migration

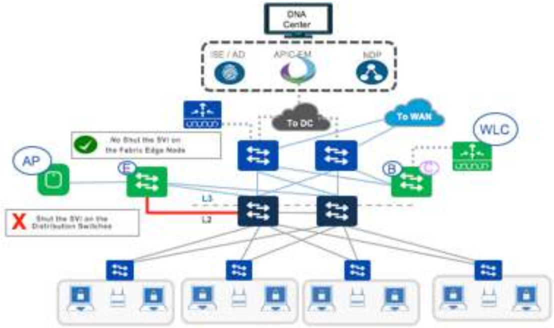
Conditions and Advantages Associated Both Approaches





Parallel Installation Considerations

- Well suited for environments that have mostly legacy hardware
- Requires sufficient facilities (Cabling, Power, Space, etc.)
- Opens up new design and deploy for impact opportunities (underlay connectivity, revised IP addressing schemes, etc.)
- Huge advantages associated with testing prior to cutover as well as ability to rollback
- Typical approach for remote site deployment


DNA Center
ISE / AD
APIC-EM
NDP
To DC
To WAN
WLC
No Shut the SVI on the Fabric Edge Node
AP
E
B
C
L3
L2
Shut the SVI on the Distribution Switches

Migrating One Switch at a Time Considerations

- Ideal for protecting recent investments while upgrading pockets of legacy hardware
- Requires additional fiber runs to distribution switch
- Switch by switch upgrade of certain layers typical
- More risky approach to migration
- Appropriate for both campus and remote site environments

Worldwide
Sales Training

SD-Access
High Level Integration DC & Wireless

Leonardo Montané
Public Sector Systems Engineer

Distinct Doesn’t Necessarily Mean Different

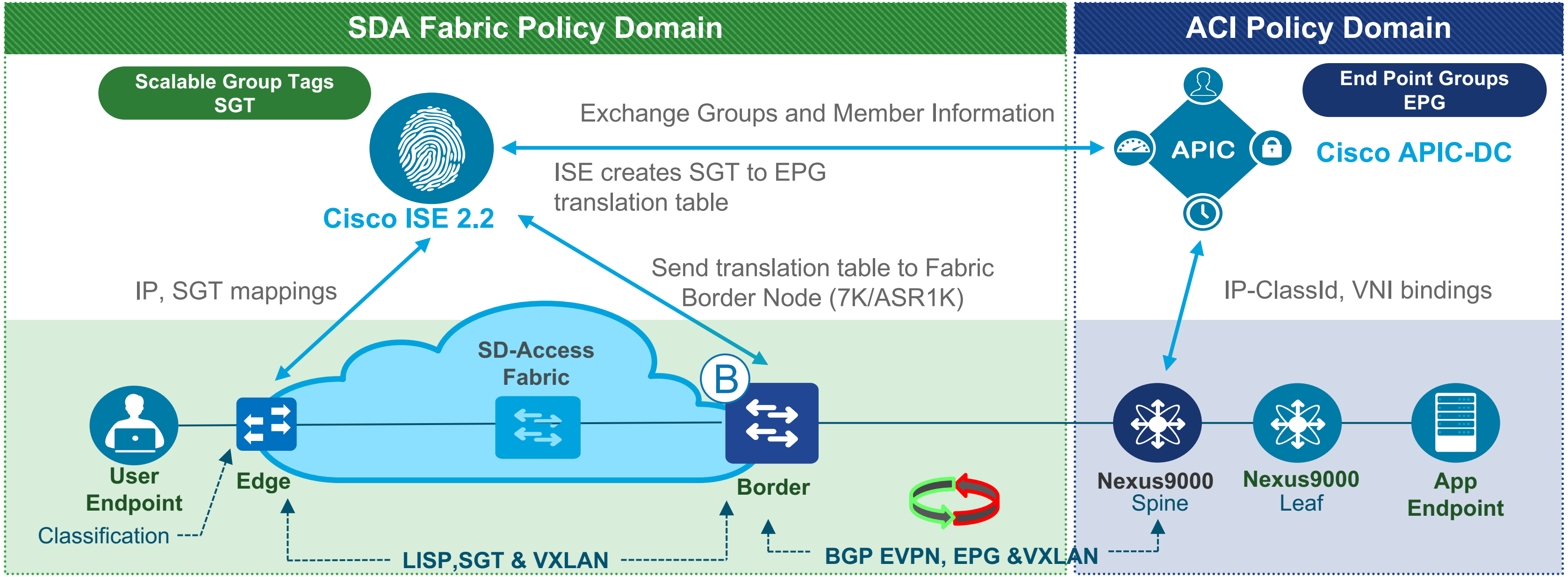
Differences and Commonalities

SD-Access	ACI Fabric
Underlay	Underlay
Overlay	Overlay
Logical constructs	Logical constructs
VNID	VNID
SGT	EPG
User Endpoint	App Endpoint
Group Based Policy	Group Based Policy

SD-Access and DC Policy Integration Design

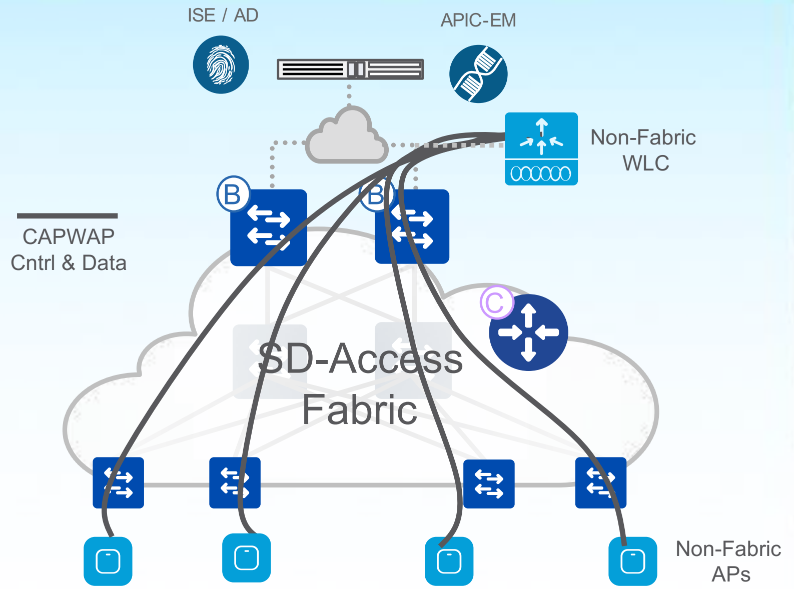
VXLAN Data Plane Between SD-Access and ACI

VXLAN data plane between Internal Border the Cisco ACI fabric to establish communication with the different domains and also to carry the information needed (SGT/EPG) for policy enforcement.



Wireless Integration in SDA Fabric

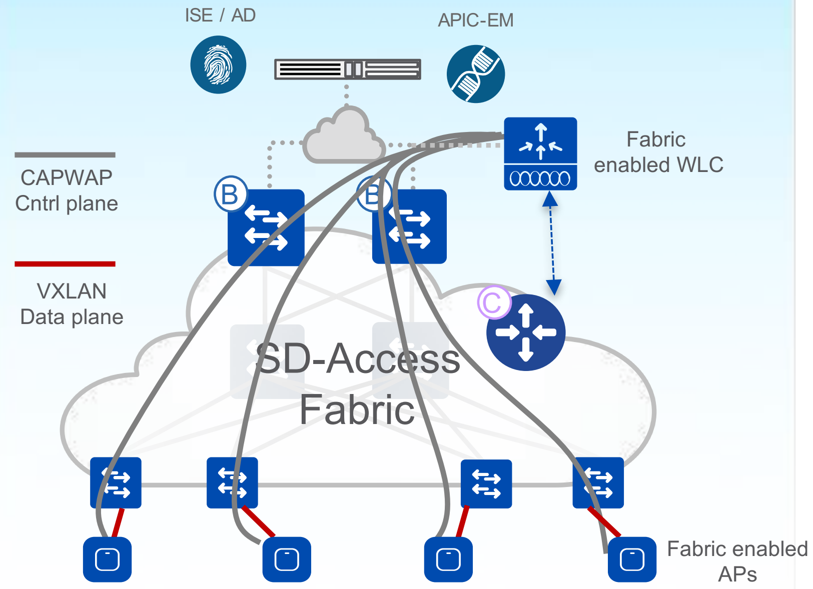
CUWN wireless Over The Top (OTT)



- CAPWAP for Control Plane and Data Plane
- SDA Fabric is just a transport
- Supported on any WLC/AP software and hardware
- Migration step to full SDA

VS.

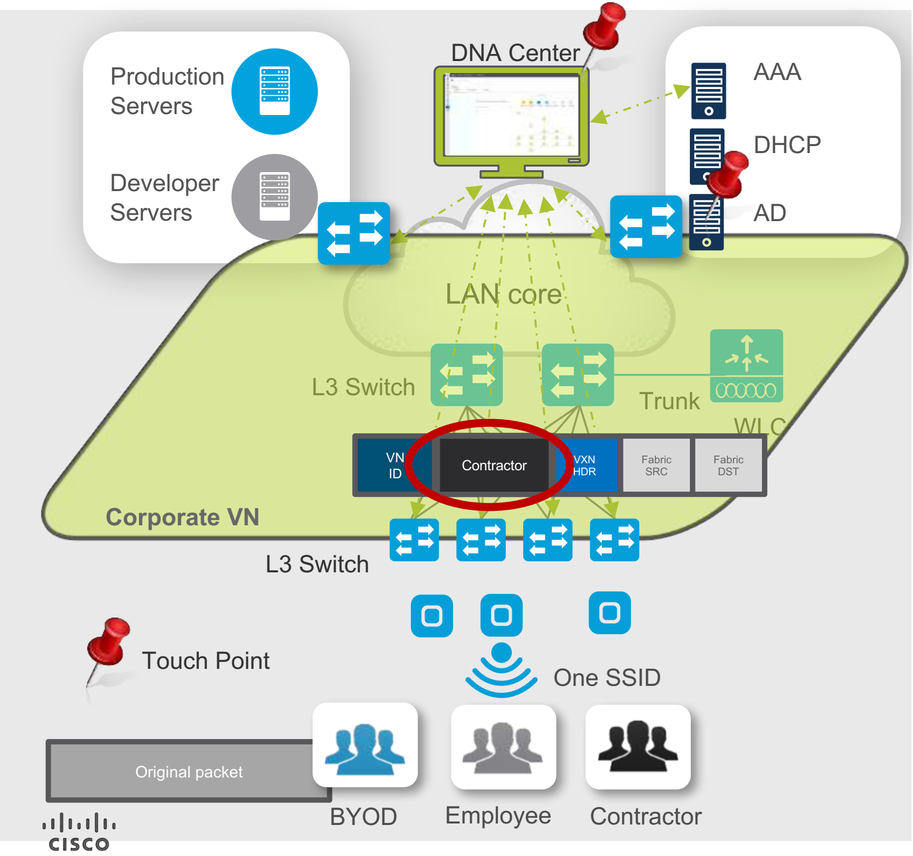
SD-Access Wireless



- CAPWAP Control Plane, VXLAN Data plane
- WLC/APs integrated in Fabric, SD-Access advantages
- Requires software upgrade (8.5+)
- Optimized for 802.11ac Wave 2 APs

SD-Access Wireless Benefits

User Group policy rollout



1. Define Groups in AD

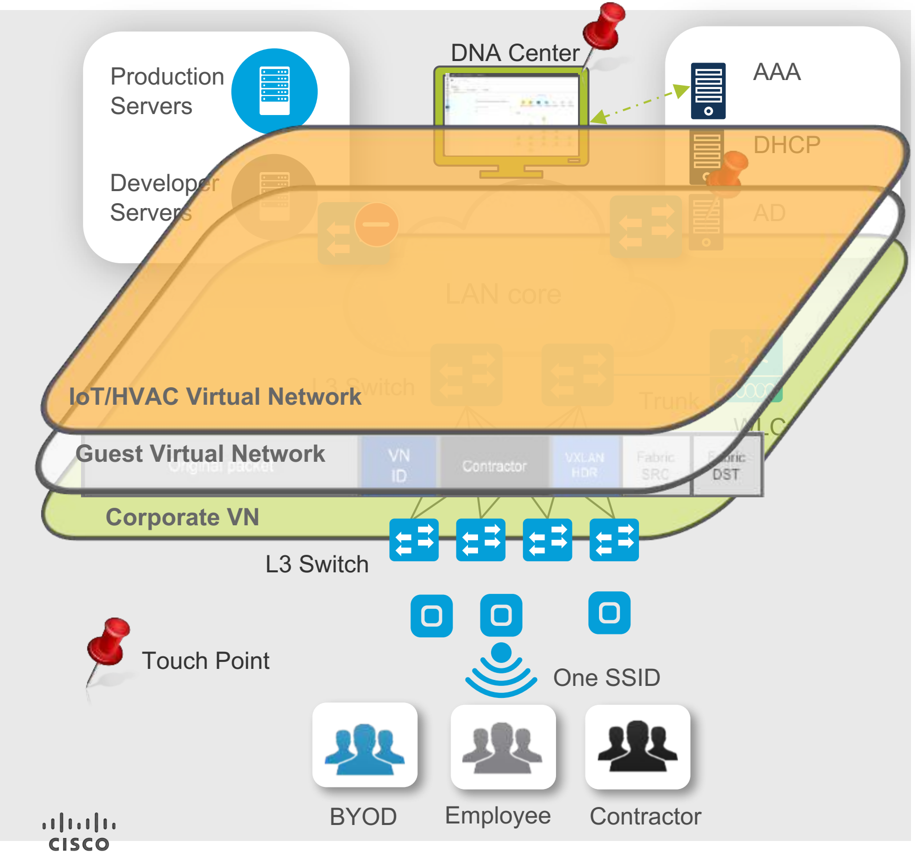
2. Design and Deploy in DNA-C
   - Create Virtual Network for Corporate
   - Define Policies
     - Role/Group based
   - Apply Policies
     - SGT based

	Production Serv. SGT 10	Developer Serv. SGT 20
Employee SGT 100	🟩	🟥
BYOD SGT 200	🟩	🟥
Contractor SGT 300	🟥	🟩

3. Upon user authentication, Policy is automatically applied and carried end to end

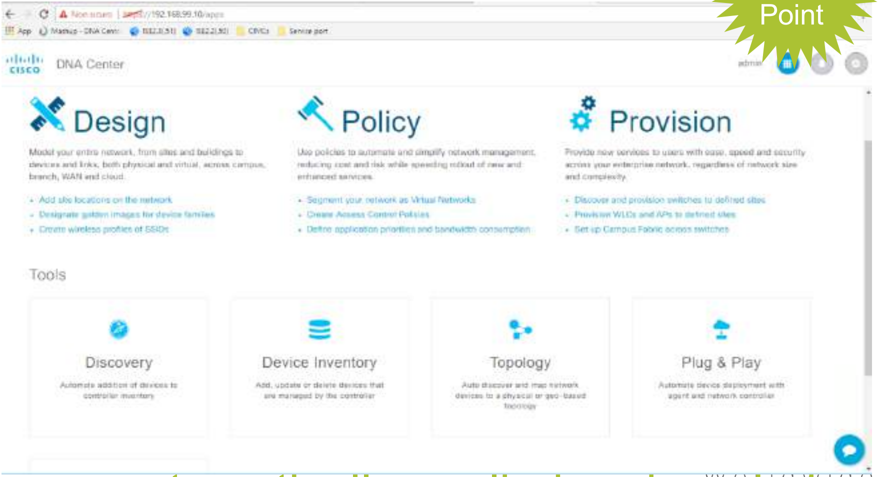
SD-Access Wireless Benefits

User Group policy rollout



1. Define Groups in AD
2. Design and Deploy in DNA-C
   - Create Virtual Network for Corporate
   - Define Policies
     - Role/Group based
   - Apply Policies
     - SGT based

One Touch Point



Design

Model your entire network, from sites and buildings to devices and links, both physical and virtual, across campus, branch, WAN and cloud.

- Add site locations on the network
- Designate golden images for device families
- Create wireless profiles of SSIDs

Policy

Use policies to automate and simplify network management, reducing cost and risk while speeding rollout of new and enhanced services.

- Segment your network as Virtual Networks
- Create Access Control Policies
- Define application priorities and bandwidth consumption

Provision

Provide new services to users with ease, speed and security across your enterprise network, regardless of network size and complexity.

- Discover and provision switches to defined sites
- Provision WLCs and APs to defined sites
- Set up Campus Fabric across switches

Tools

Discovery
Automate addition of devices to controller inventory

Device Inventory
Add, update or delete devices that are managed by the controller

Topology
Auto discover and map network devices to a physical or geo-based topology

Plug & Play
Automate device deployment with agent and network controller

automatically applied and carried end to end

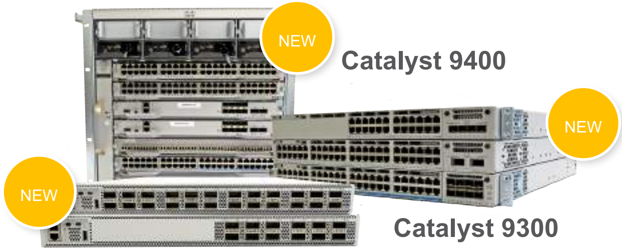
Worldwide
Sales Training

Products

Leonardo Montané
Public Sector Systems Engineer

SD-Access Platform Support
Complete Investment Protection

Switching



Catalyst 9400

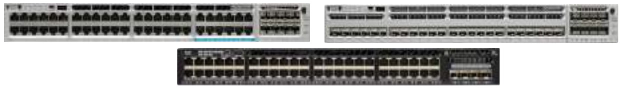
Catalyst 9300

Catalyst 9500

Catalyst 4500E

Catalyst 6K

Nexus 7700



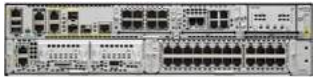
Catalyst 3850 and 3650

Routing

ASR-1000-X

ASR-1000-HX

ISR 4430



ISR 4450

Wireless

AIR-CT5520

AIR-CT8540

AIR-CT3504

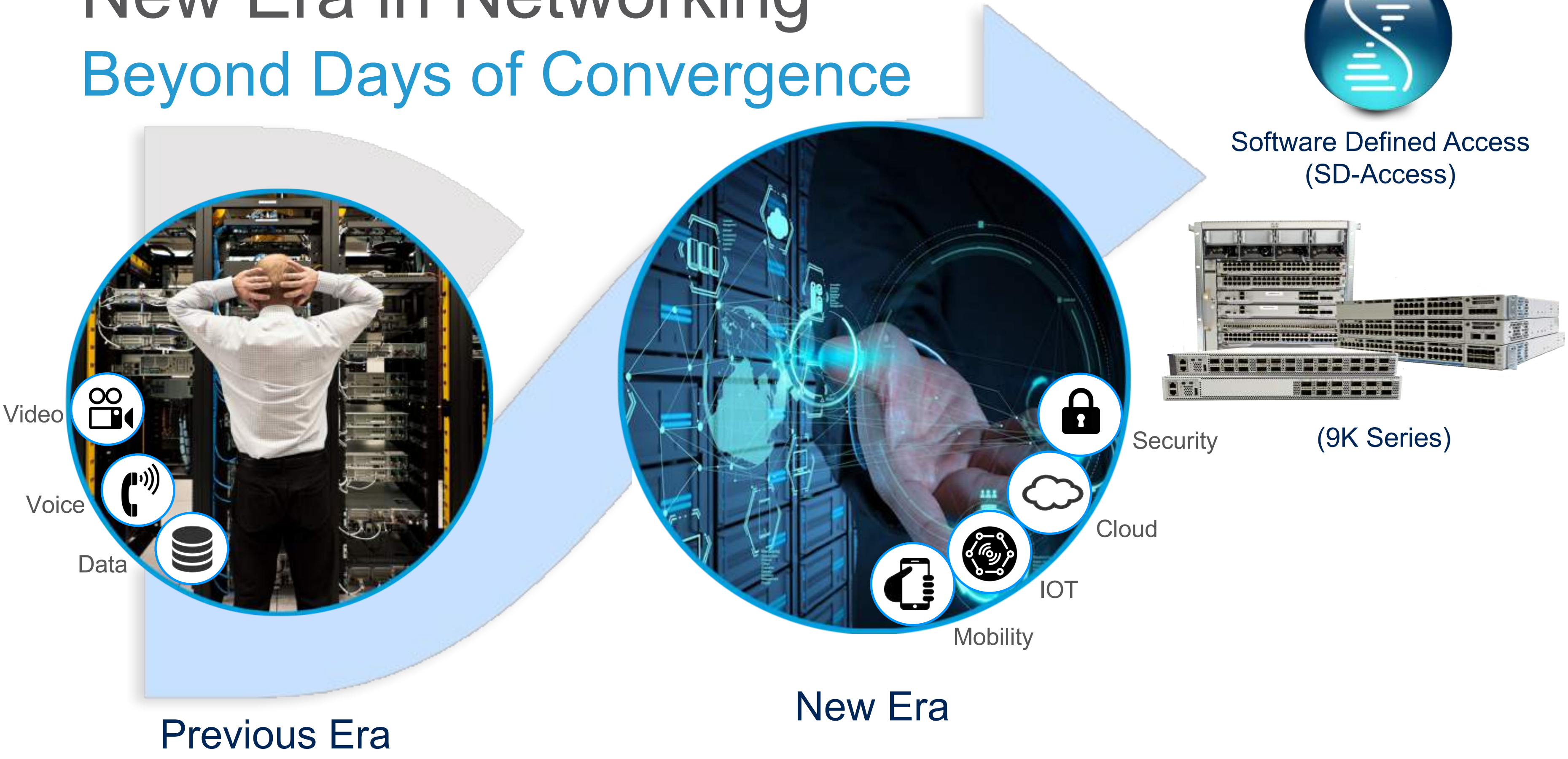
Wave 2 APs (1800, 2800,3800)

Wave 1 APs (1700, 2700,3700)*

* No IPv6 or AVC support

New Era in Networking

Beyond Days of Convergence



SD-Access - *Policy Based Automation from Edge to Cloud*

Future of Enterprise Networking

Platform Transitions

Catalyst 9500

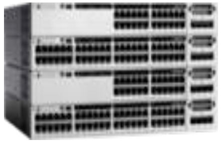
Catalyst 4500X

Catalyst 3850 Fiber 48 port

Backbone Switching

Catalyst 9300

Catalyst 9400



Catalyst 3850 Copper

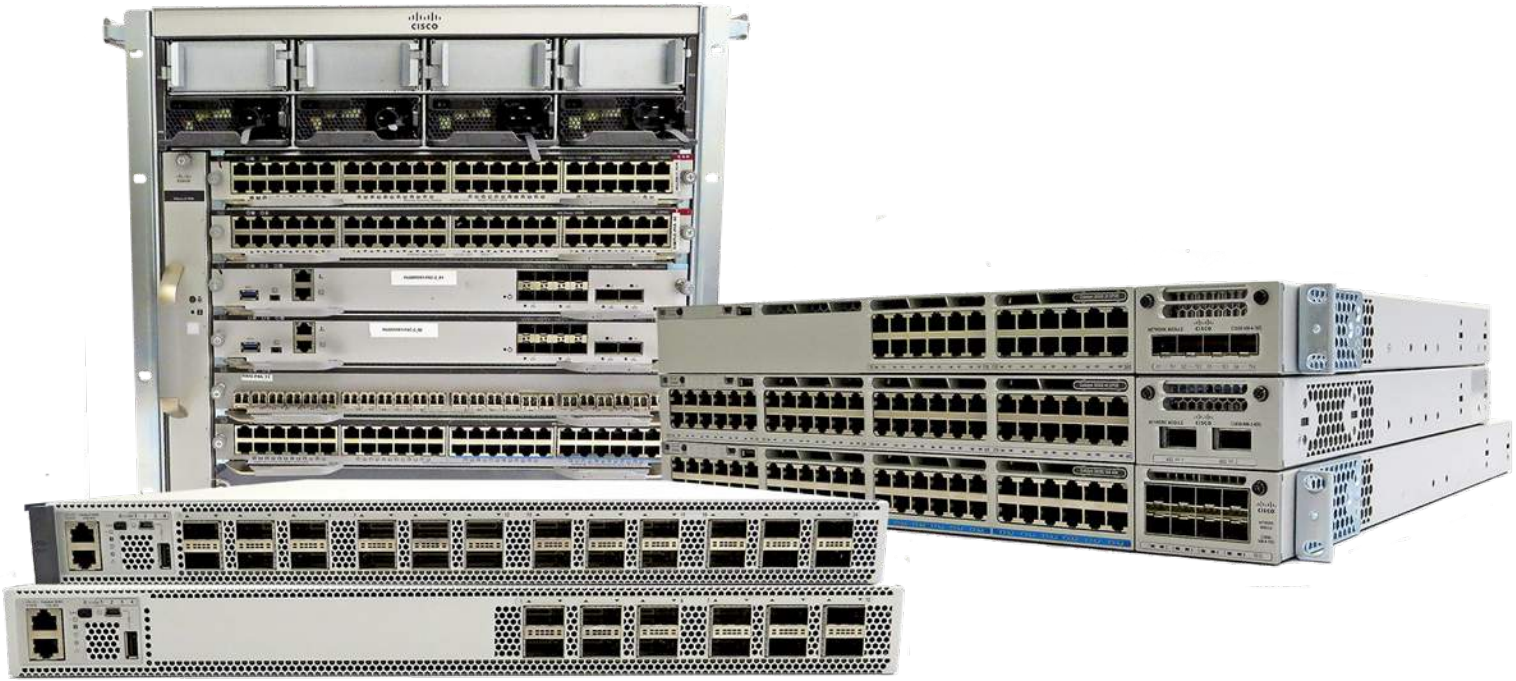
Catalyst 4500-E

Access Switching

Device Bootstrap and Onboarding

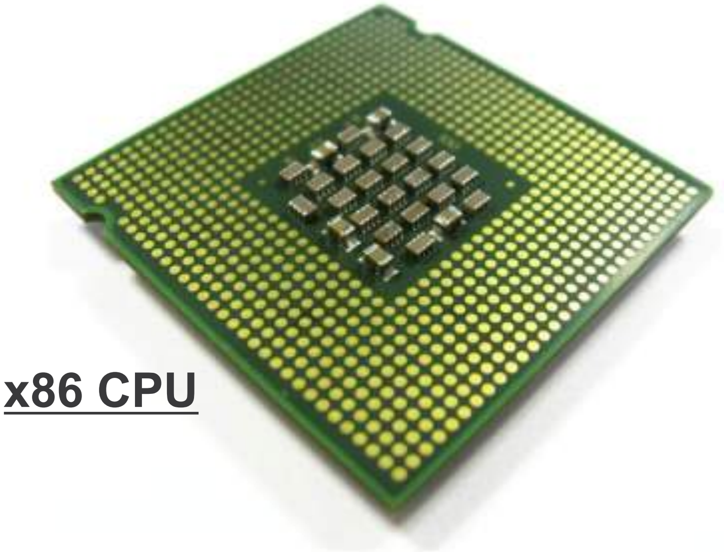
Configuration Automation through Open Interfaces

Server Management Tools on x86 Infrastructure



The Catalyst 9K Family’s Common Attributes

Catalyst 9K Family – x86 CPU



x86 CPU

puppet
ExtraHop
perfSONAR
CHEF
splunk>
Nagios®
kafka

Example x86 based 3rd Party Apps

x86 enables hosting containers and 3rd party apps

Catalyst 9K Family – External Storage Options

SATA SSD Storage

Up to 1 TB

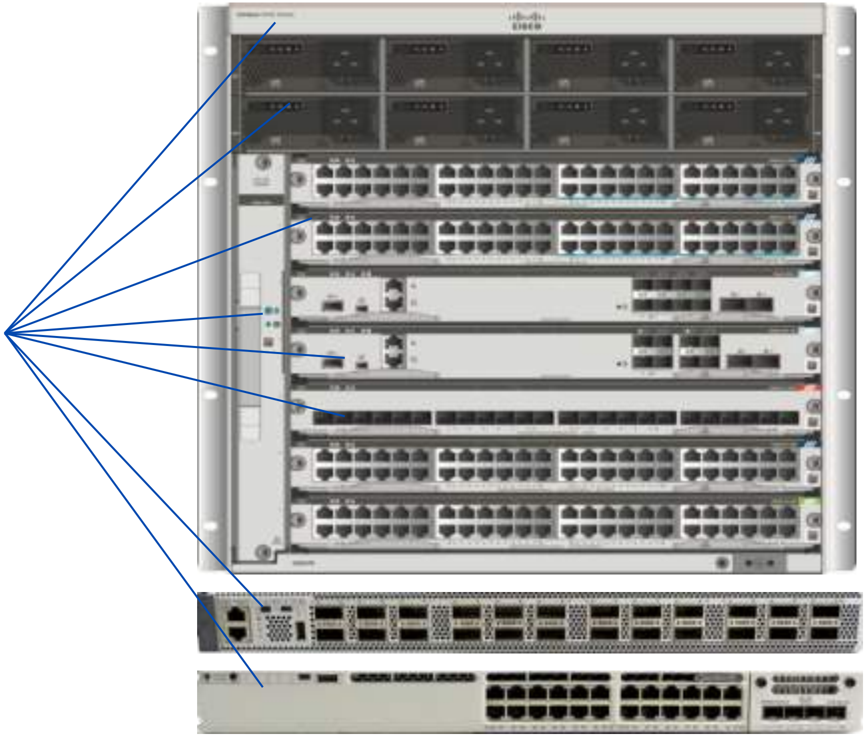
USB 2.0/3.0*

Up to 120 GB

For Local Logging – 3rd Party App Hosting - Containers

Catalyst 9K Family – Blue Beacon

Blue Beacon
on Every System &
Components



Identification of Devices has never been Easier

Catalyst 9K Family – RFID

RFID on Every Device and FRUable Components of Catalyst 9400

Inventory Management (Tracking) has never been Easier

Catalyst 9K Family – Optional Bluetooth

File Transfer

Device Management

```
cat9k (config)# interface bt0
```

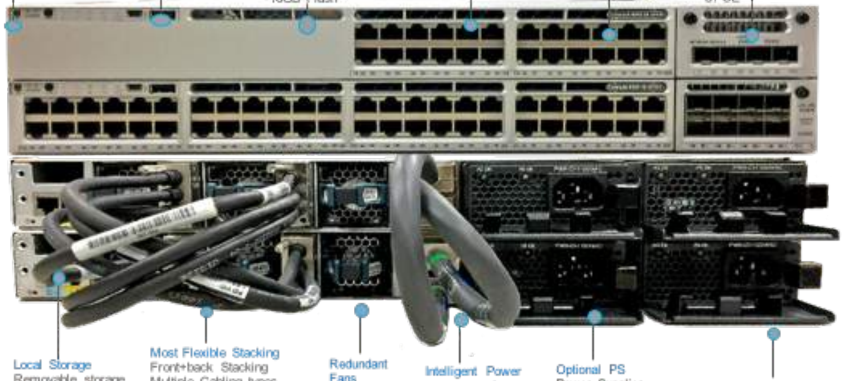
Accessing the Device has never been Easier

Catalyst 9300
Next Generation Fixed Access

2.5G at the Price of 1G 40G at the Price of 10G

Highest 2.5G/mGig Density in the Industry

Only Stackable Switch with 8X 10G Uplinks



Flexible ASIC
UADP 2.0

Optional Bluetooth Management
USB 2.0*

Powerful CPU Complex
Intel X86 CPU
4-core 1.8GHz
8GB Memory
16GB Flash

Wireless Scale
48x Wave 2 APs
in 1RU

Most Dense and Flexible Uplink offering
8x10G, mGig, 25G

Unmatched POE
Resiliency –
Perpetual/Fast
High power - 60W
UPOE

Local Storage
Removable storage
(128GB)

Most Flexible Stacking
Front+back Stacking
Multiple Cabling types – Copper and Fiber
Best HA – NSF/SSO

Redundant Fans

Intelligent Power management
StackPower

Optional PS
Power Supplies
(AC+DC)

mGig UPOE

24xmGig

48xmGig (36 X 2.5G + 12 X 10G)

1G UPOE/POE+

24 Ports

48 Ports

1G Data

24 Ports

48 Ports

Modular Fans

Modular Uplinks

8x10G

2x40G

4x mGig

4x1G

Modular Power Supplies

350W

715W

1100W

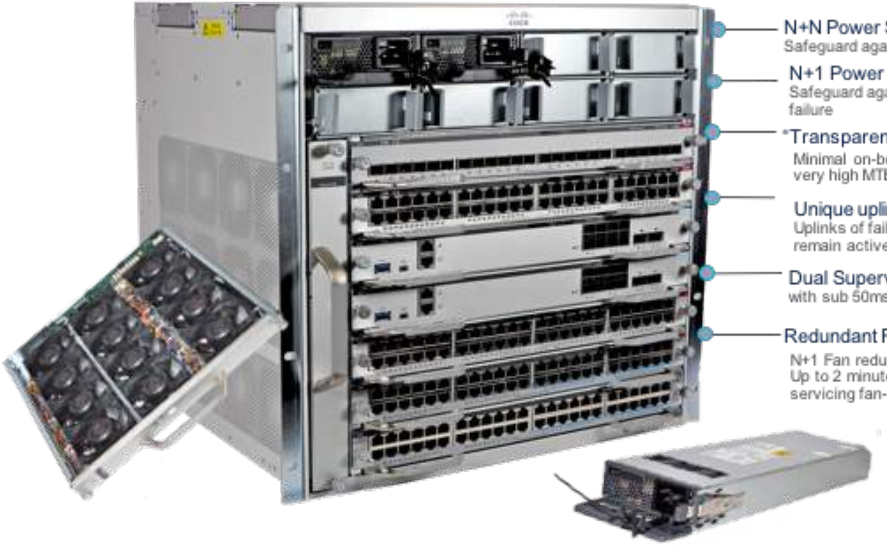
Catalyst 9400

Next Generation Modular Access

Industry's Highest PoE Scale

Redundancy is now Table-stake

9Tbps System b/w



N+N Power Supply Redundancy
Safeguard against power circuit failure

N+1 Power supply redundancy
Safeguard against power supply failure

"Transparent" line card design
Minimal on-board components for very high MTBF

Unique uplink redundancy
Uplinks of failed supervisor continue to remain active

Dual Supervisors
with sub 50ms ISSU & NSF/SSO

Redundant Fans
N+1 Fan redundancy within Fan-tray; Up to 2 minutes of fan-less operation for servicing fan-tray

4-Slot*

7-Slot

10-Slot

Supervisor

Sup-1: 80G/Slot Access Optimized
Sup-1XL*: 120G/Slot Core Optimized

Access Linecards

24xmGig + 24xUPOE
48xUPoE
48xPoE+*
48xData

Core Linecards

24x 10G SFP+
48x1G SFP*
24x1G SFP*

Power Supply

3200W AC
3200W DC*
2200W AC*

*not available at FCS

Catalyst 9500

Next Generation Fixed Core/Agg

Redundant platinum rated power supplies

Front to back airflow with N+1 Modular Fans

RFID for Efficient Inventory Management

USB3.0 Storage to host High End Applications

40G at the Price of 10G

8X Buffering vs. Competition

Industry's First 40G Enterprise Switch

Granular Port Densities to Address all Campus Sizes

12Px40G

Catalyst 9500-12Q

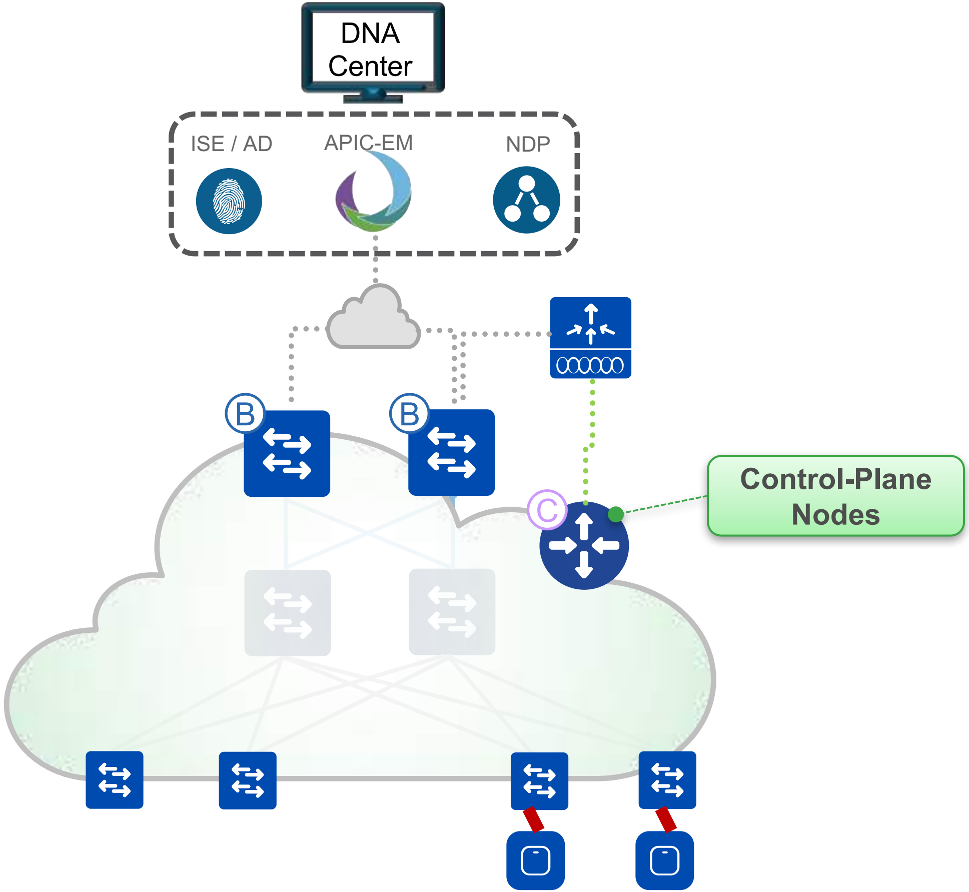
24Px40G

Catalyst 9500-24Q

40Px10G + 8Px10G / 2Px40G

Catalyst 9500-40X

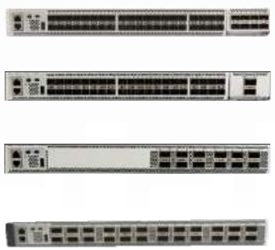
Fabric Control-Plane Node
Supported Hardware/Software



Catalyst 3K

- **Catalyst 3850**
- 1/10G SFP+
- 10/40G NM Cards
- **IOS-XE 16.6.1+**

Catalyst 9500

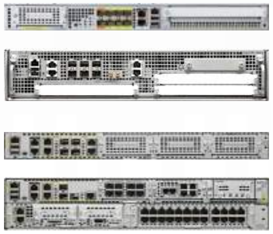


- **Catalyst 9500**
- 40G QSFP
- 1/10G NM Cards
- **IOS-XE 16.6.1+**

Catalyst 6K

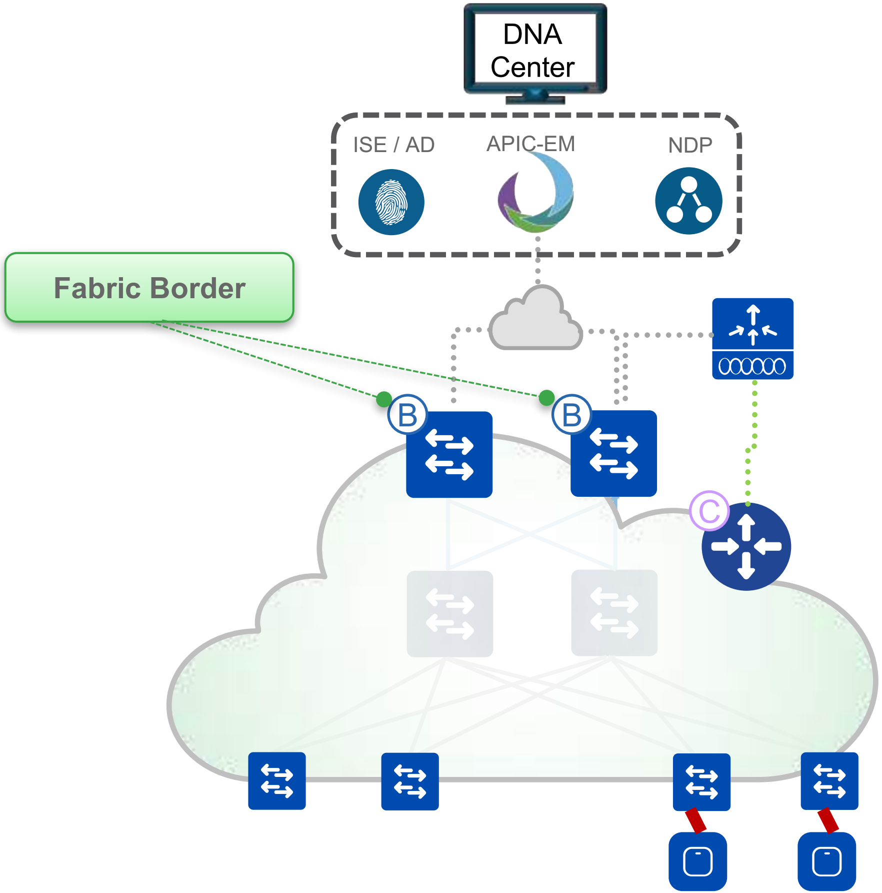
- **Catalyst 6800**
- Sup2T/6T
- 6880-X or 6840-X
- **IOS 15.5.1SY+**

ASR1K & ISR4K



- **ASR 1000-X/HX**
- **ISR 4430/4450**
- 1/10G/40G
- **IOS-XE 16.6.1+**

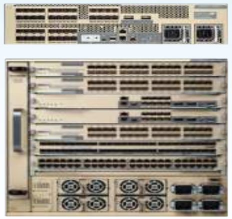
Fabric Border Node
Supported Hardware/Software



Catalyst 9500

- **Catalyst 9500**
- 40G QSFP
- 10/40G NM Cards
- **IOS-XE 16.6.1+**

Catalyst 6K

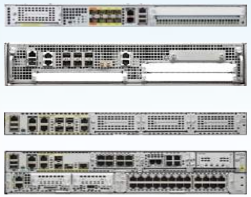


- **Catalyst 6800**
- Sup2T/6T
- 6880-X or 6840-X
- **IOS 15.5.1SY+**

Nexus 7K

- **Nexus 7700**
- Sup2E
- M3 Cards
- **NXOS 7.3.2+**

ASR1K & ISR4K

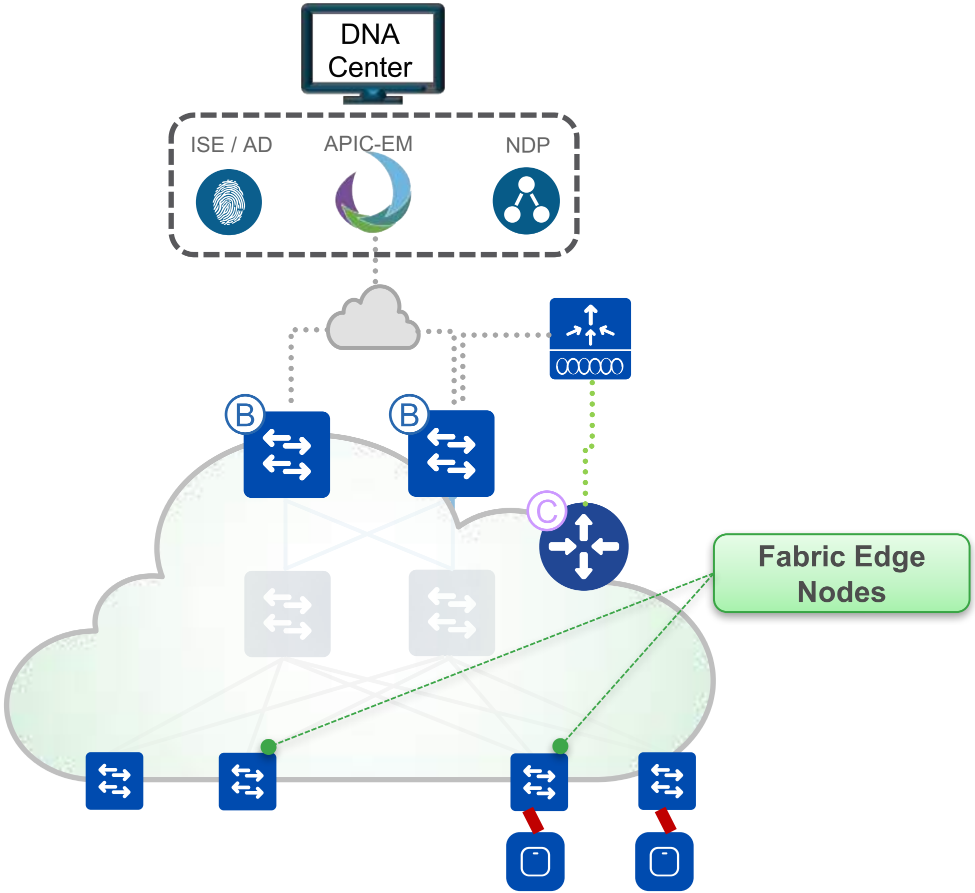


- **ASR 1000-X/HX**
- **ISR 4430/4450**
- 1/10G/40G
- **IOS-XE 16.6.1+**

Catalyst 3K

- **Catalyst 3850**
- 1/10G SFP+
- 10/40G NM Cards
- **IOS-XE 16.6.1+**

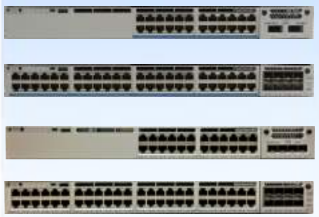
Fabric Edge Node
Supported Hardware/Software



Catalyst 3K

- **Catalyst 3650/3850**
- 1/MGIG RJ45
- 10/40G NM Cards
- **IOS-XE 16.6.1+**

Catalyst 9300



- **Catalyst 9300**
- 1/MGIG RJ45
- 10/40G NM Cards
- **IOS-XE 16.6.1+**

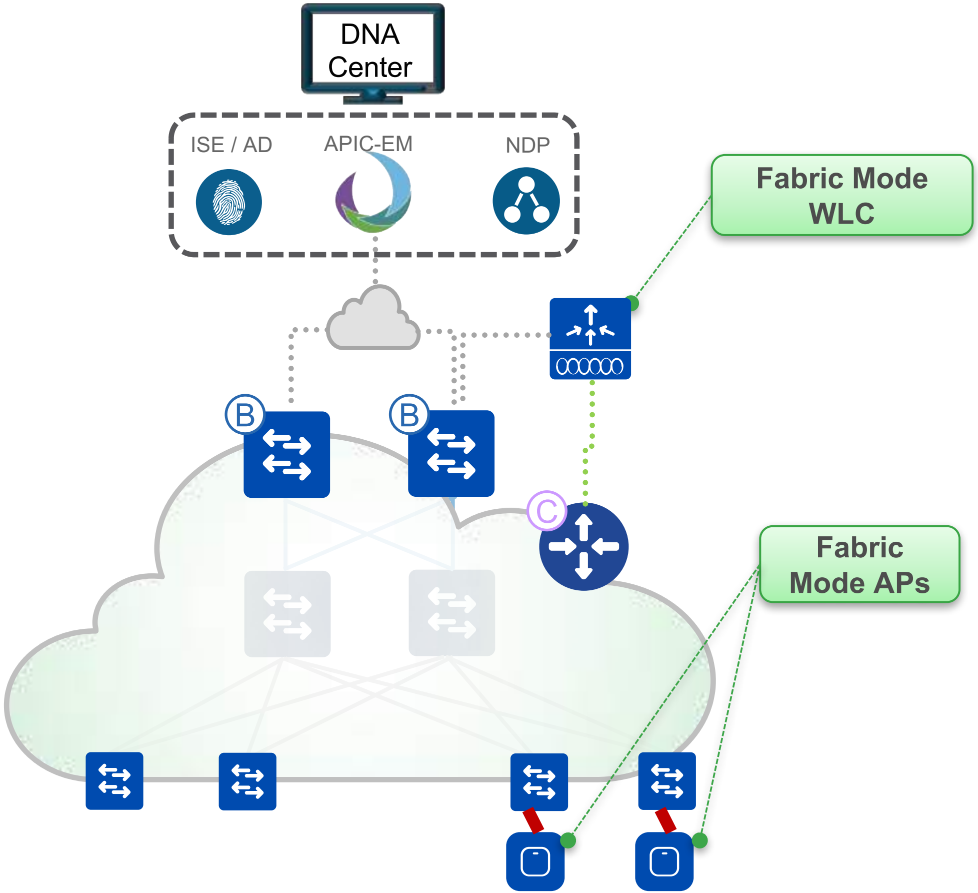
Catalyst 4500E

- **Catalyst 4500**
- Sup8E/9E (Uplinks)
- 4700 Cards (Down)
- **IOS-XE 3.10.1+**

Catalyst 9400

- **Catalyst 9400**
- Sup1E
- 9400 Cards
- **IOS-XE 16.6.1+**

Fabric Mode WLC & APs
Supported Hardware/Software



Fabric Mode WLC

Fabric Mode APs

5500 WLC

- **AIR-CT5520**
- No 5508
- 1G/10G SFP+
- **AireOS 8.5.1+**

8500 WLC

- **AIR-CT8520/40**
- No 8510
- 1G/10G SFP+
- **AireOS 8.5.1+**

WAVE 1 APs

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

WAVE 2 APs

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

Key Foundation Takeaways

Summary

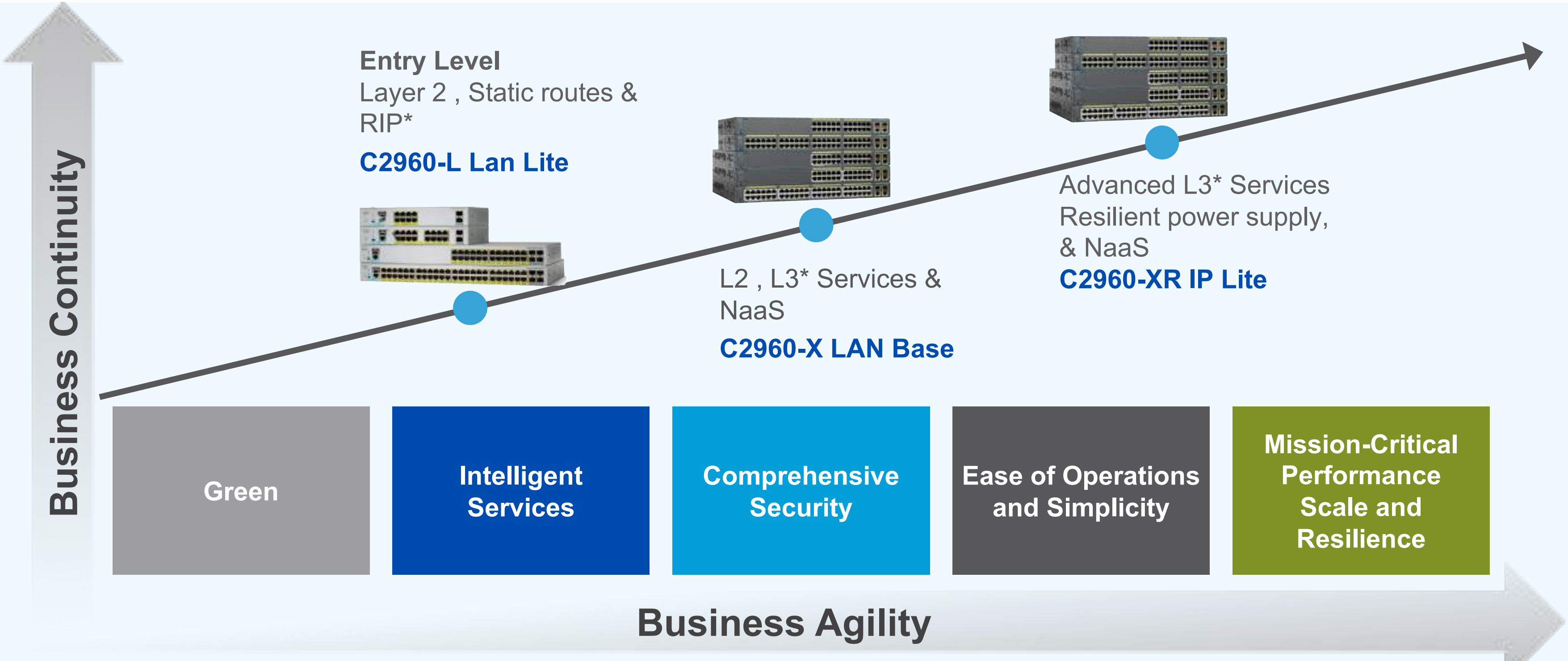
- The Catalyst 3650, 3850, 4500E, 6800, 9300, 9400, 9500 and the Nexus 7700 leveraging M3 cards are all supported from a switching perspective as part of the SD-Access solution
- The Catalyst 9K platform has been built to address security risks posed by advanced persistent threats, operational complexities associated with IoT convergence, evolving mobility requirements and a need to take advantage of Cloud agility & consumption models
- The Catalyst 9500 is the ideal choice to address both Fabric Control-Plane Node and Fabric Border Node requirements
- The Catalyst 9300 and 9400 are the ideal choice to address Fabric Edge Node requirements

Worldwide
Sales Training

Catalyst 2900 Family

Addressing Business Transformation

New Unified Access Cisco Catalyst Switching Solution



Entry Level
Layer 2 , Static routes & RIP*

C2960-L Lan Lite

L2 , L3* Services & NaaS

C2960-X LAN Base

Advanced L3* Services
Resilient power supply, & NaaS

C2960-XR IP Lite

Business Continuity

Green

Intelligent Services

Comprehensive Security

Ease of Operations and Simplicity

Mission-Critical Performance Scale and Resilience

Business Agility

*RIP support in 3.10 release
*L3 services – access routing protocols
*Advances L3 – access routing protocols + vrf lite etc

CISCO TOMORROW starts here.