Cisco ACI und DNA

Veränderungen des Kompetenzprofils des Admins der Zukunft

Jan Haasch
Business Operations Manager
Security and Trust Office

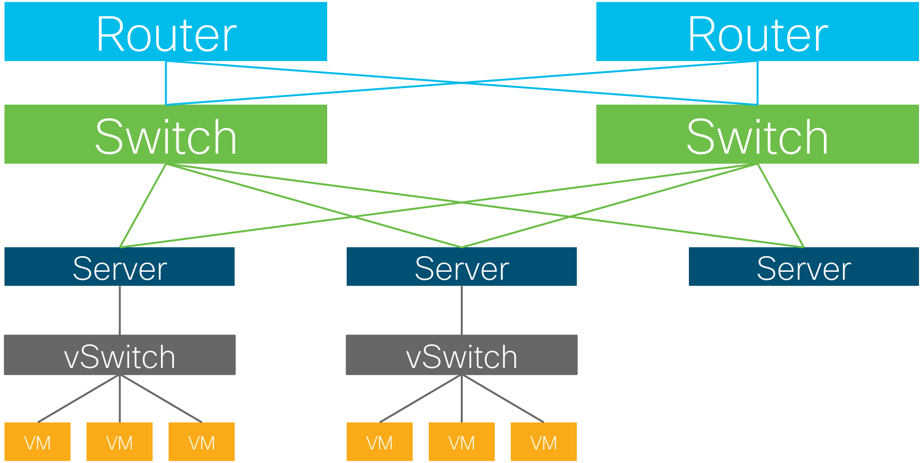
Tim Heckmann
Consulting Engineer
Customer Experience

Agenda

- Classic Network Design
- Software-defined Networking
- Cisco ACI
- Cisco DNA & SDA
- Future Net Admin Skill Set
- Summary and Evaluation

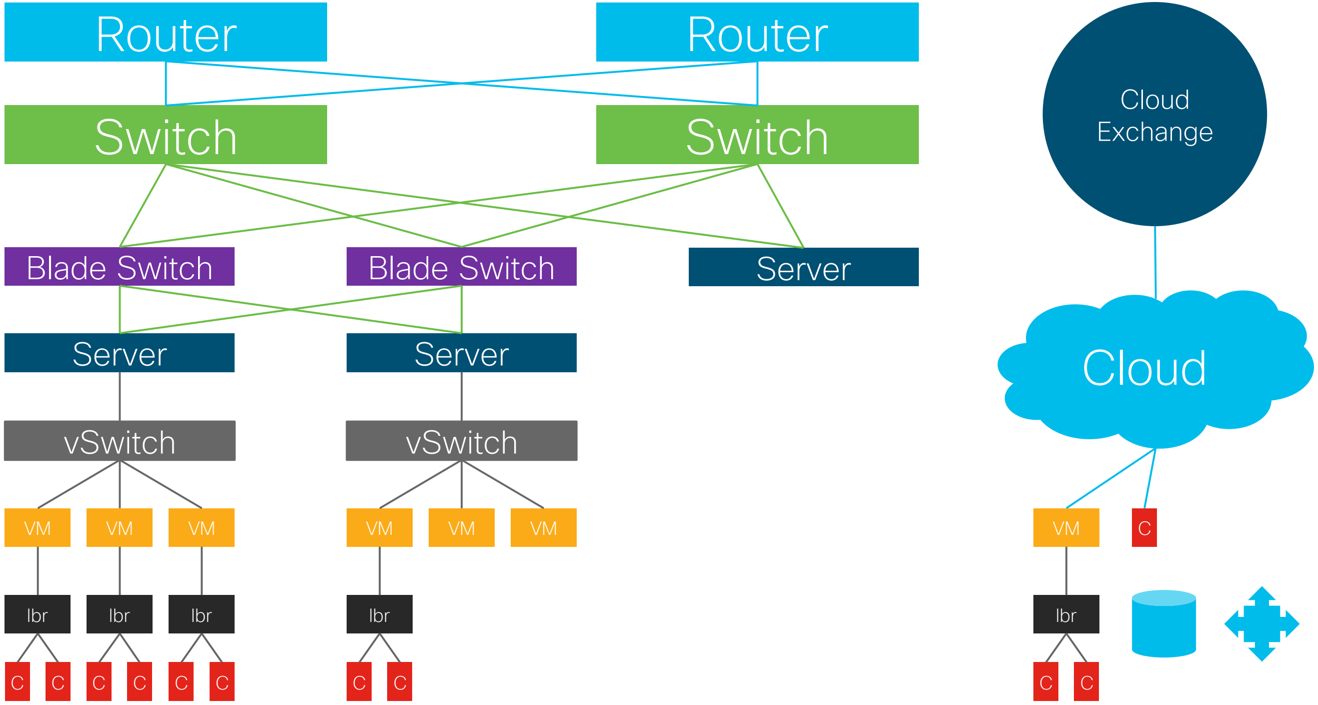
Classic Network Design

Network Evolution



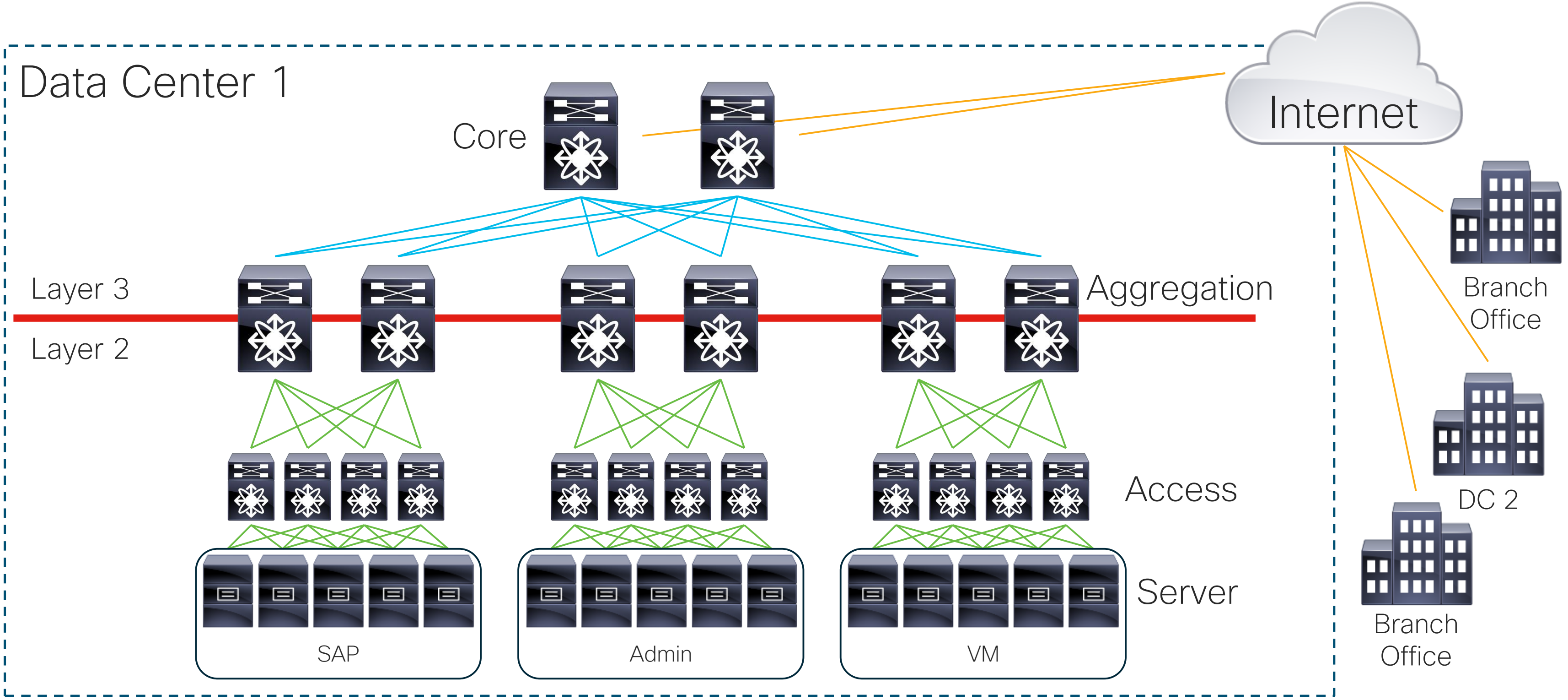
Network Evolution

- Load Balancer
- Firewall
- IPS
- DNS
- Gateways
- Others



Router
Router
Switch
Switch
Blade Switch
Blade Switch
Server
Server
Server
vSwitch
vSwitch
VM VM VM
VM VM VM
lbr lbr lbr
lbr
C C C C C C
C C
Cloud Exchange
Cloud
VM
C
lbr
C C

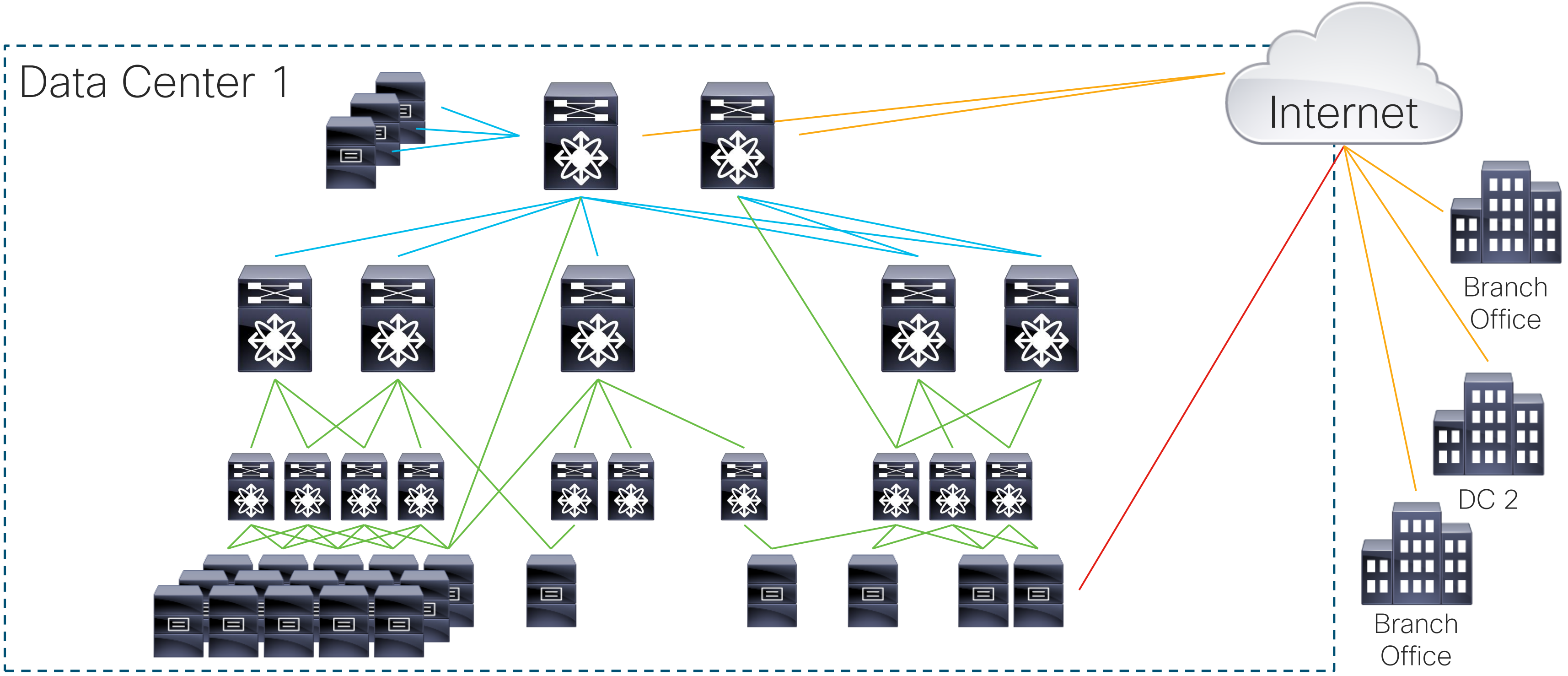
Data Center 3-Tier Design



Data Center 3-Tier Design

“Life is what happens to you while you're busy making other plans.”

Data Center 3-Tier Design



Network Revolution

I want an agile bimodal hybrid cloud so we can develop containerised serverless trustless microservices applications to take us digitial to avoid disruptions from any unicorns. Oh … and I want DevOps … two of those …

What has changed?

- digitization
- cloud computing
- app economy
- Internet of Things
- software-defined networks
- tech unicorns

Four Ages of Networking

Stone Age

Spanning Tree
VLANs

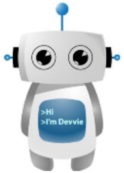
Bronze Age

Routing Protocols
WAN Design
IP-mageddon

Renaissance

SDN
OpenFlow
Controllers
Overlays
MP-BGP
VXLAN
Micro-Segmentation
White Box

Programmable Age



Cloud
Python
REST/APIs
NETCONF/YANG
Fabrics
NFV
Containers
(Net)DevOps

Software-defined Networking

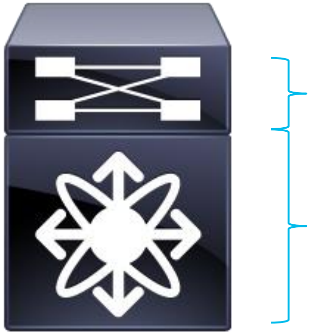
Definition

“Software-defined networking (SDN) technology is a novel approach to cloud computing that felicitates network management and enables programmatically efficient network configuration in order to improve network performance and monitoring.”

-Kamal Benzekki

SDN suggests to centralize network intelligence in one network component by disassociating the forwarding process of network packets (data plane) from the routing process (control plane).

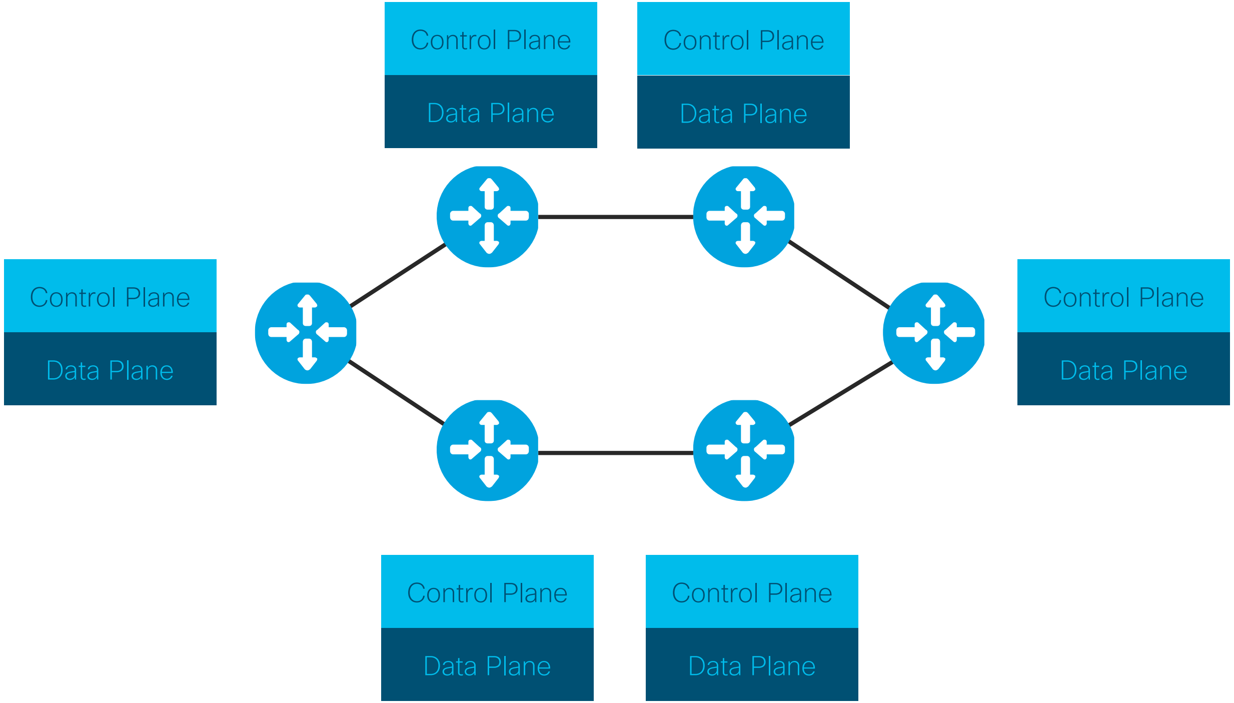
Inside The Box



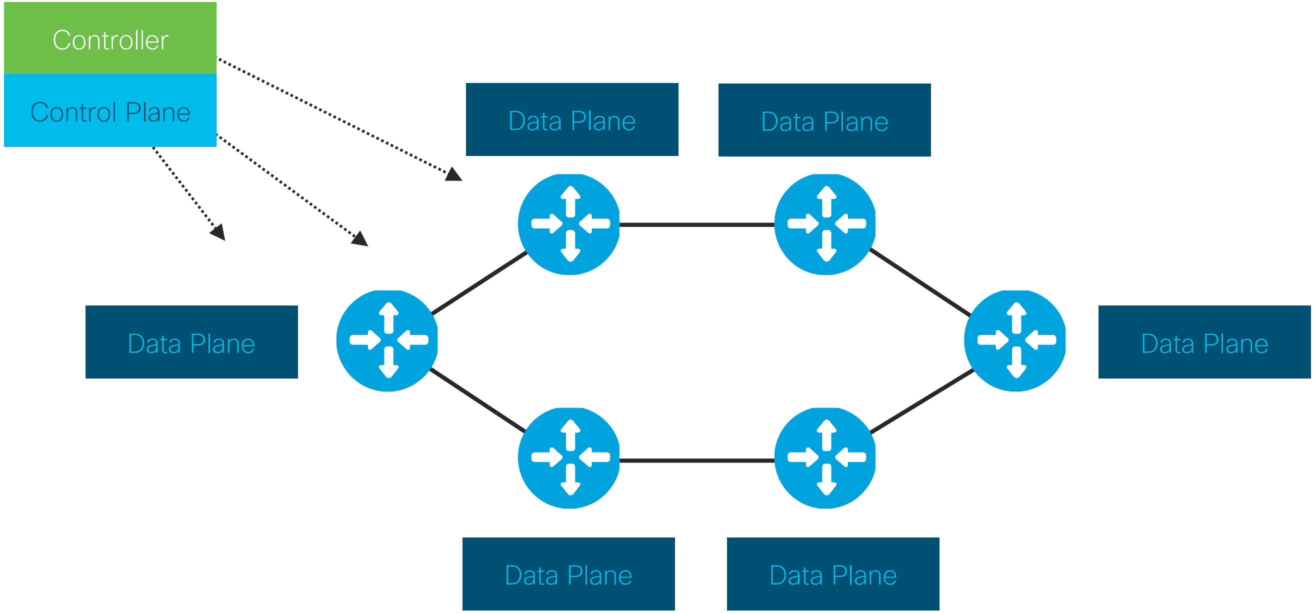
Control Plane | RIP, OSPF, STP, EIGRP, SNMP, CLI, etc.

Data Plane | store-and-forward, ACL, encryption, etc.

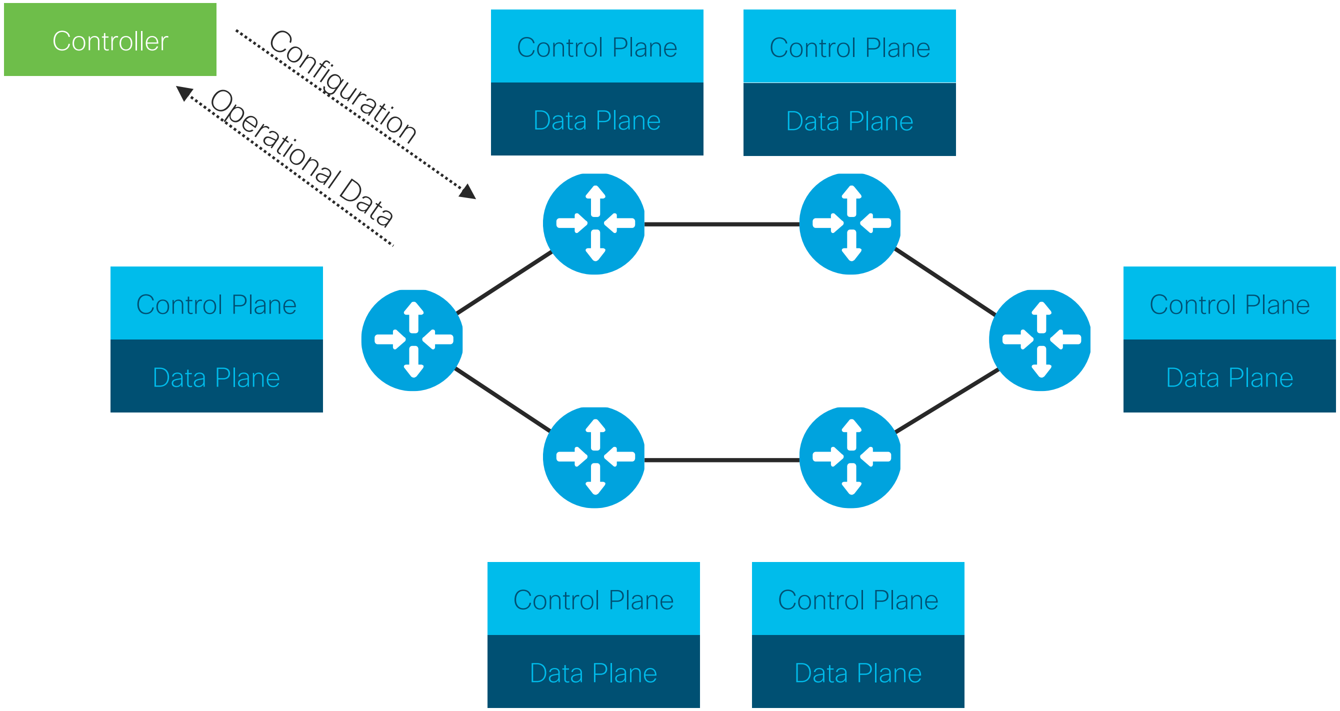
Traditional Networking



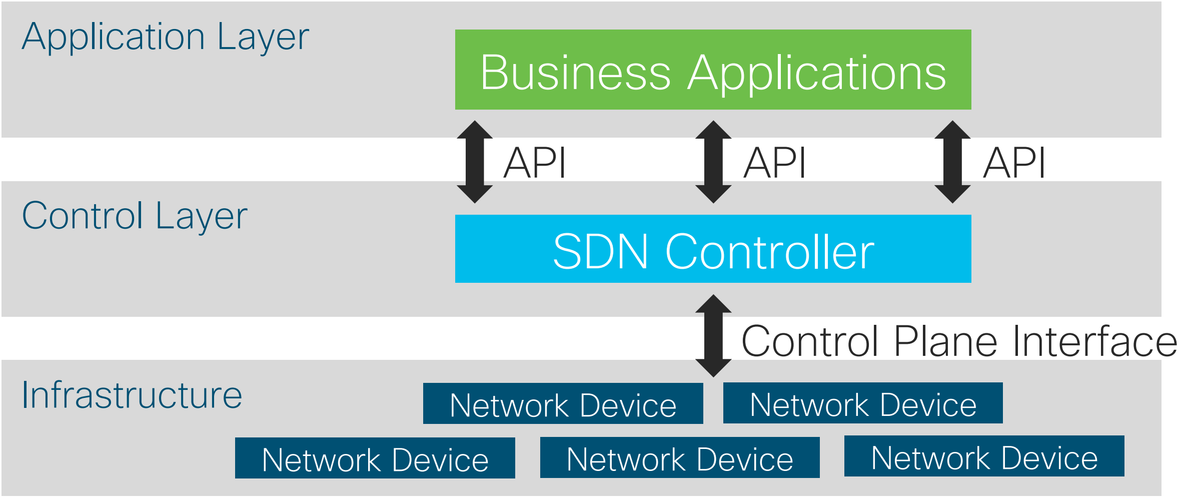
SDN: The Original Idea



SDN: What It Really Is Today



SDN: High Level

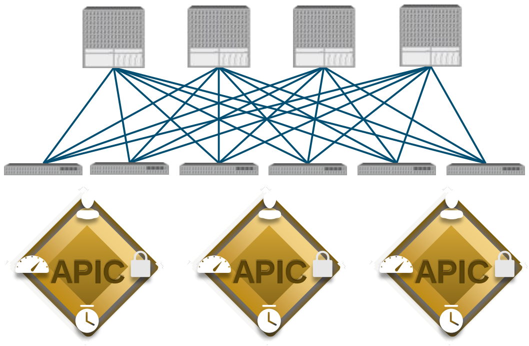


Advantages

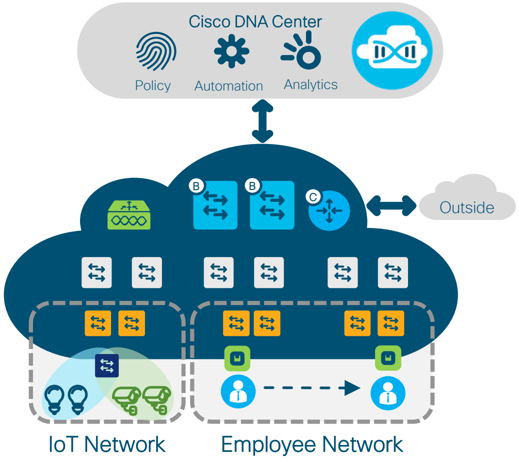
- Flexibility:
  - IT groups can become more agile; deployment backlogs are less problematic.
  - Departments are more easily able to self-select services – including internal, 3rd-party and external cloud services.
- Automation:
  - Features (protect, segment, provision, add policies) are easily added to new workloads, groups, branches, employee devices and cloud resources.
- Visibility drives speed:
  - SDN provides a holistic view of application connectivity and external needs (branch, device).
  - Applications can ask for resources, routes, and instantaneously verify traffic flow (by application) across the campus and data center.

Cisco SDN Portfolio

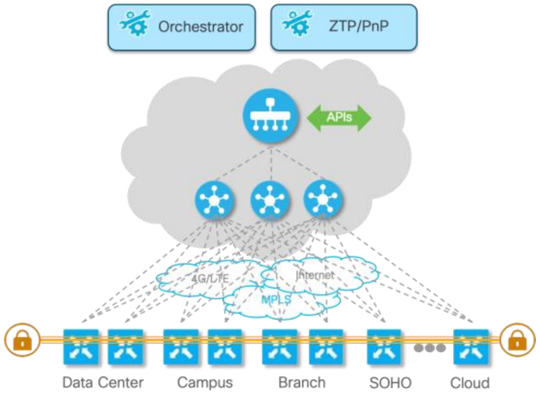
ACI



DNA & SDA



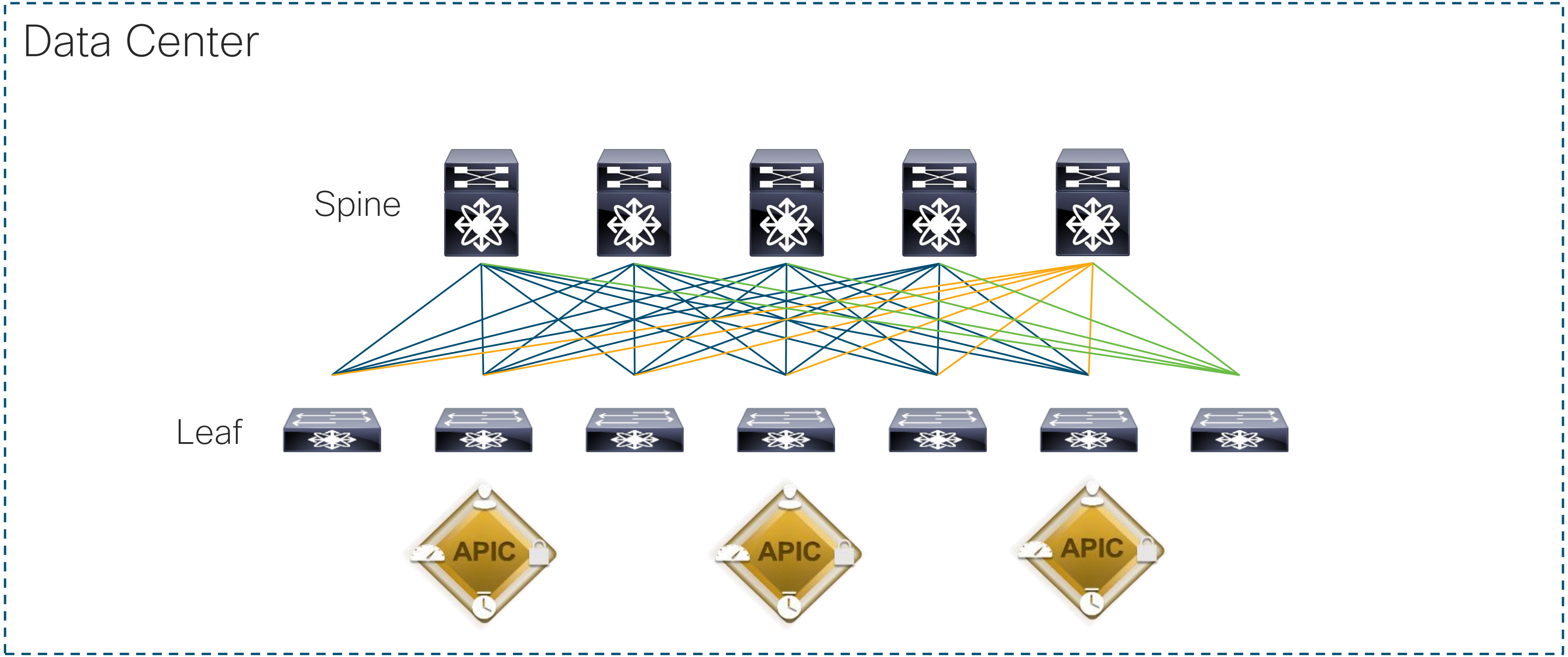
SD-WAN



Cisco Application-Centric Infrastructure

Design Principles

Design Principles

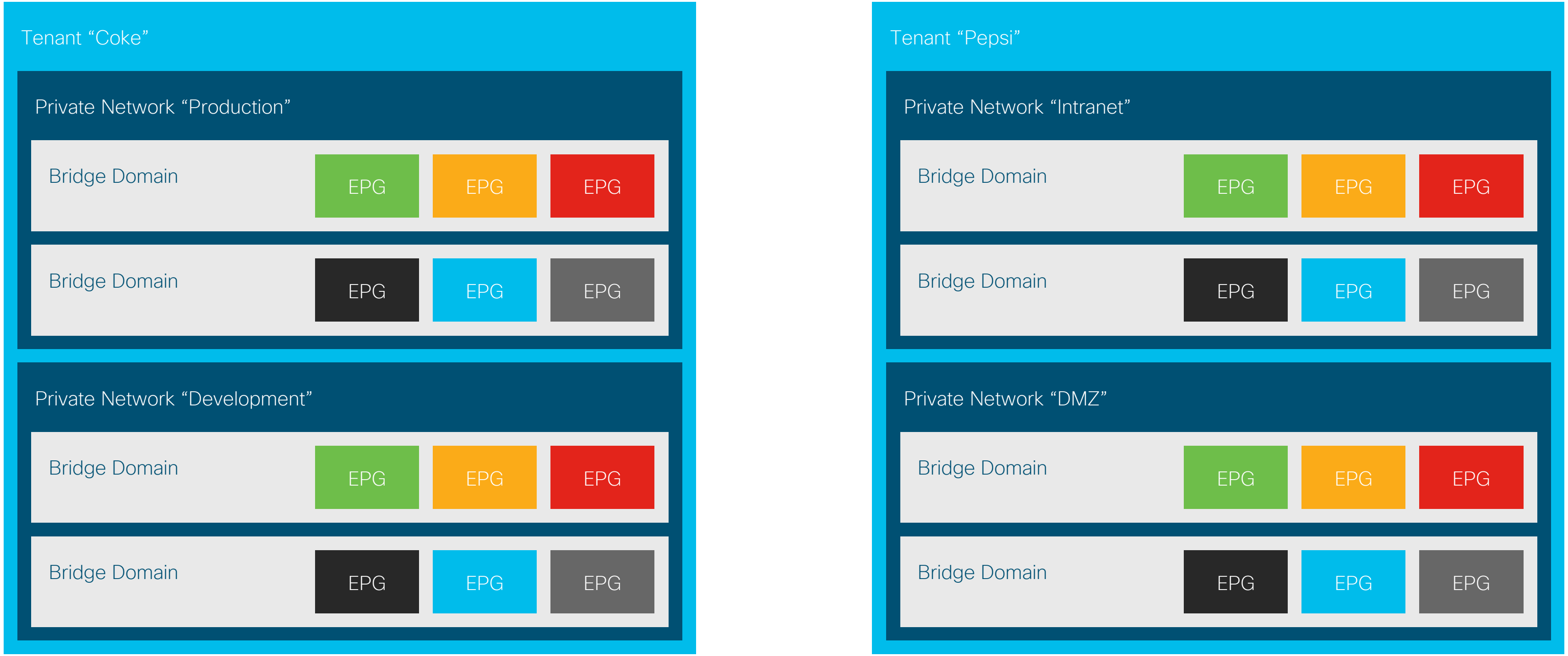


Reference

Design Principles

- spine-leaf architecture
  - add a spine to increase bandwidth
  - add a leaf to increase port count
- APIC cluster controls the fabric
- fabric acts as a single distributed (L3) switch from the application's point of view

Multi-Tenancy



Tenant “Coke”

Private Network “Production”

Bridge Domain EPG EPG EPG

Bridge Domain EPG EPG EPG

Private Network “Development”

Bridge Domain EPG EPG EPG

Bridge Domain EPG EPG EPG

Tenant “Pepsi”

Private Network “Intranet”

Bridge Domain EPG EPG EPG

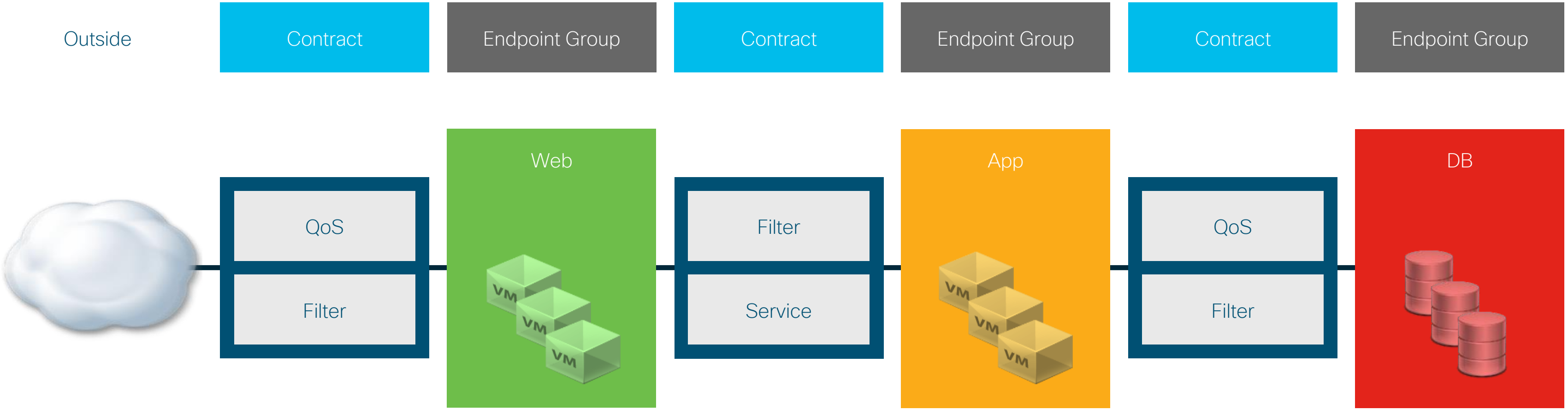
Bridge Domain EPG EPG EPG

Private Network “DMZ”

Bridge Domain EPG EPG EPG

Bridge Domain EPG EPG EPG

Policy Model



Reference

Policy Model

- Endpoint Group (EPG)
  - collection of endpoints with similar functionality
  - possible form factors
    - physical servers
    - virtual servers
    - containers
    - …
- Contract
  - collection of communication rules between EPGs
- whitelist model (all communication is forbidden by default)

Design: Network-centric vs. Application-centric

Network-centric

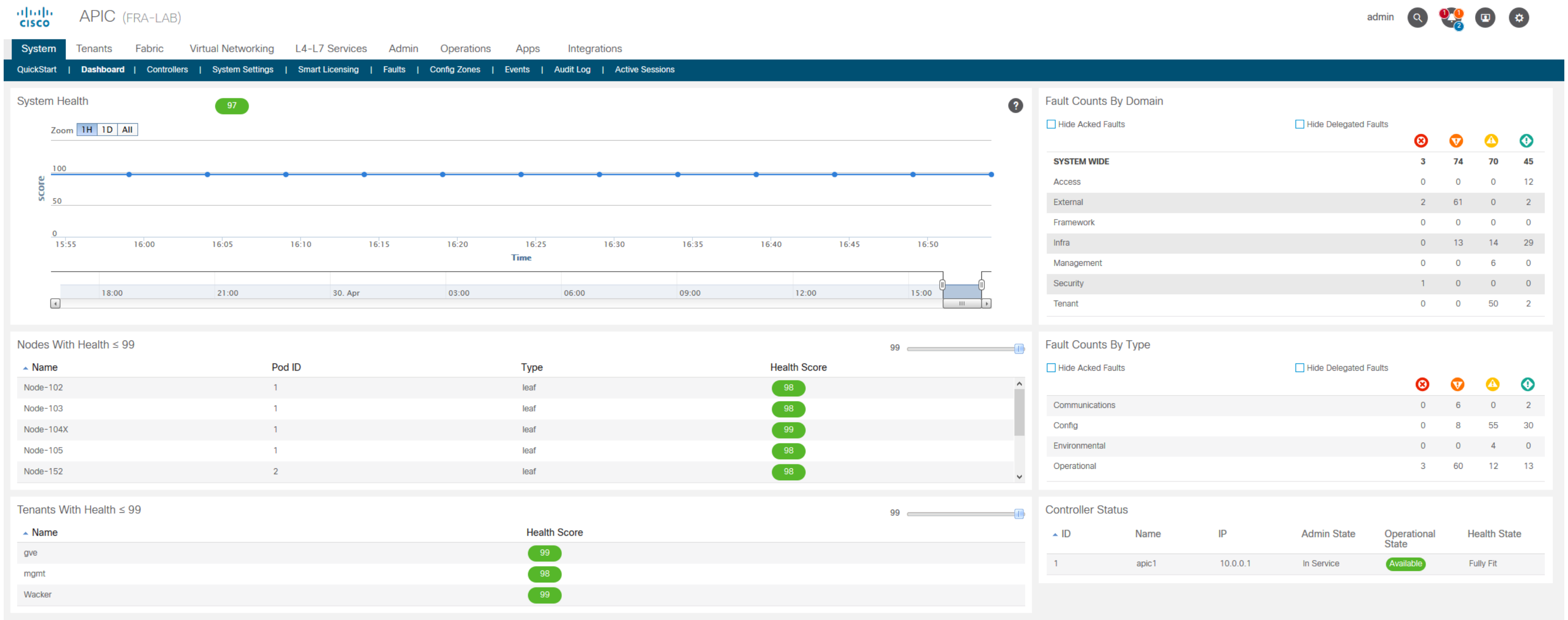
- basically an SDN version of traditional networking:
  - 1 VLAN/subnet → 1 BD → 1 EPG
- mostly an intermediate state on the way to an application-centric deployment

Application-centric

- application connectivity requirements directly mapped onto the network
  - 1 BD → n subnets → n EPGs
- no need for individual network provisioning (VLANs/subnets) per group of servers

Infrastructure Visibility

APIC: Dashboard



Fault Counts By Domain

□ Hide Acked Faults □ Hide Delegated Faults

	⊗	▽	△	ⓘ
SYSTEM WIDE	**3**	**74**	**70**	**45**
Access	0	0	0	12
External	2	61	0	2
Framework	0	0	0	0
Infra	0	13	14	29
Management	0	0	6	0
Security	1	0	0	0
Tenant	0	0	50	2

Nodes With Health ≤ 99

99

Name	Pod ID	Type	Health Score
Node-102	1	leaf	98
Node-103	1	leaf	98
Node-104X	1	leaf	99
Node-105	1	leaf	98
Node-152	2	leaf	98

Fault Counts By Type

□ Hide Acked Faults □ Hide Delegated Faults

	⊗	▽	△	ⓘ
Communications	0	6	0	2
Config	0	8	55	30
Environmental	0	0	4	0
Operational	3	60	12	13

Tenants With Health ≤ 99

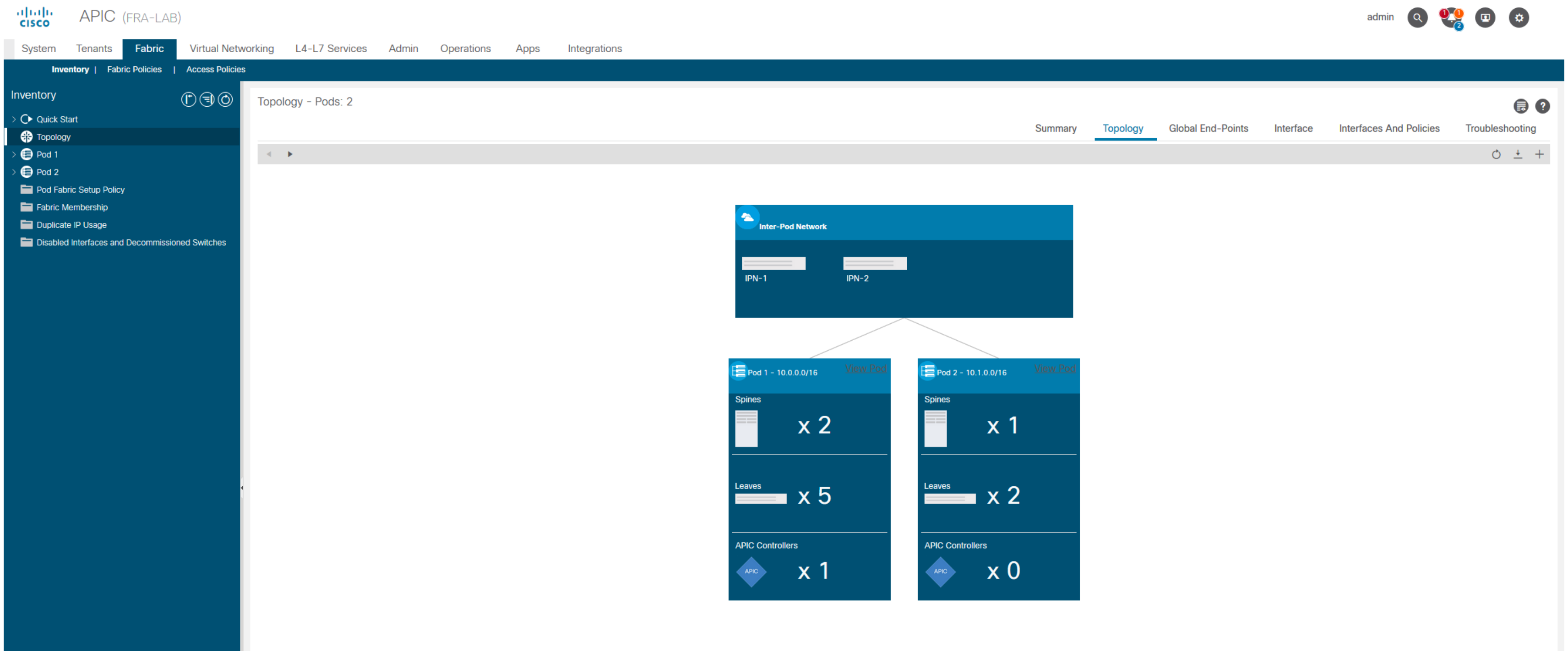
99

Name	Health Score
gve	99
mgmt	98
Wacker	99

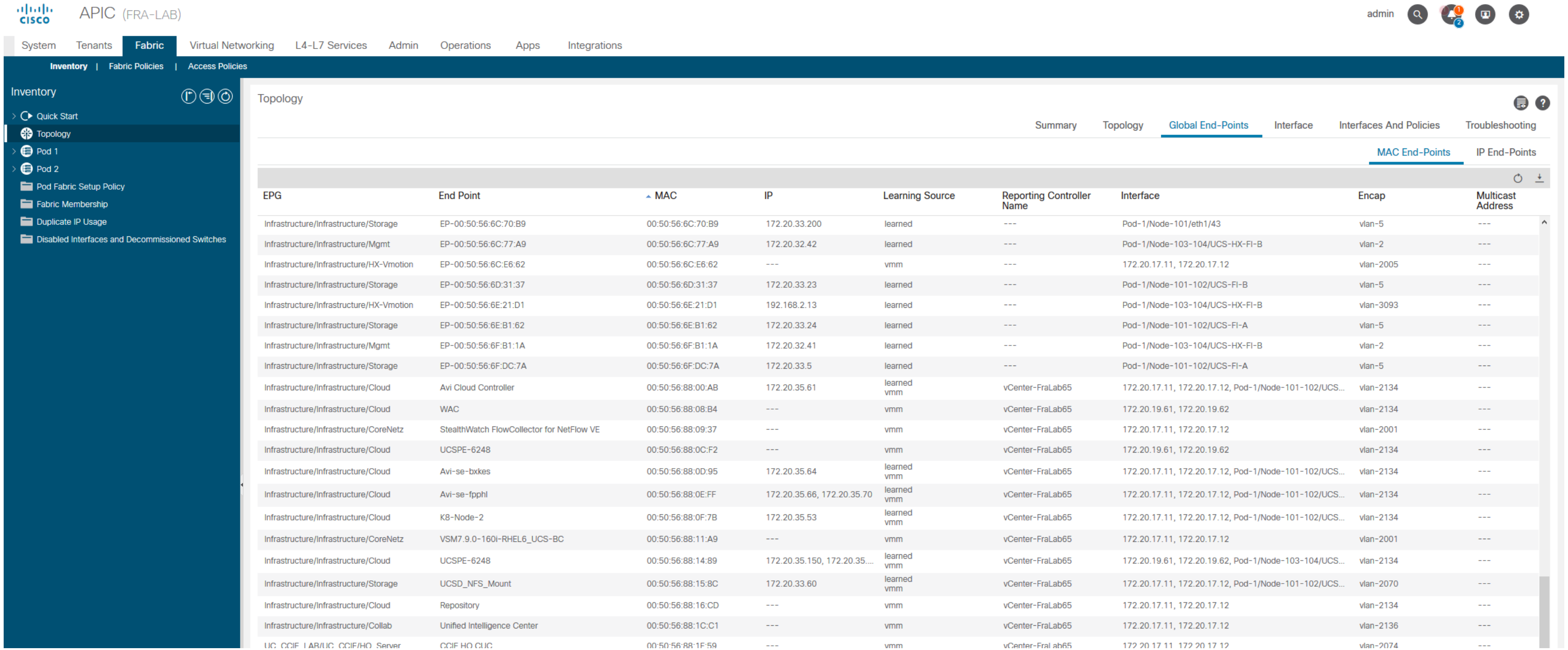
Controller Status

ID	Name	IP	Admin State	Operational State	Health State
1	apic1	10.0.0.1	In Service	Available	Fully Fit

APIC: Topology

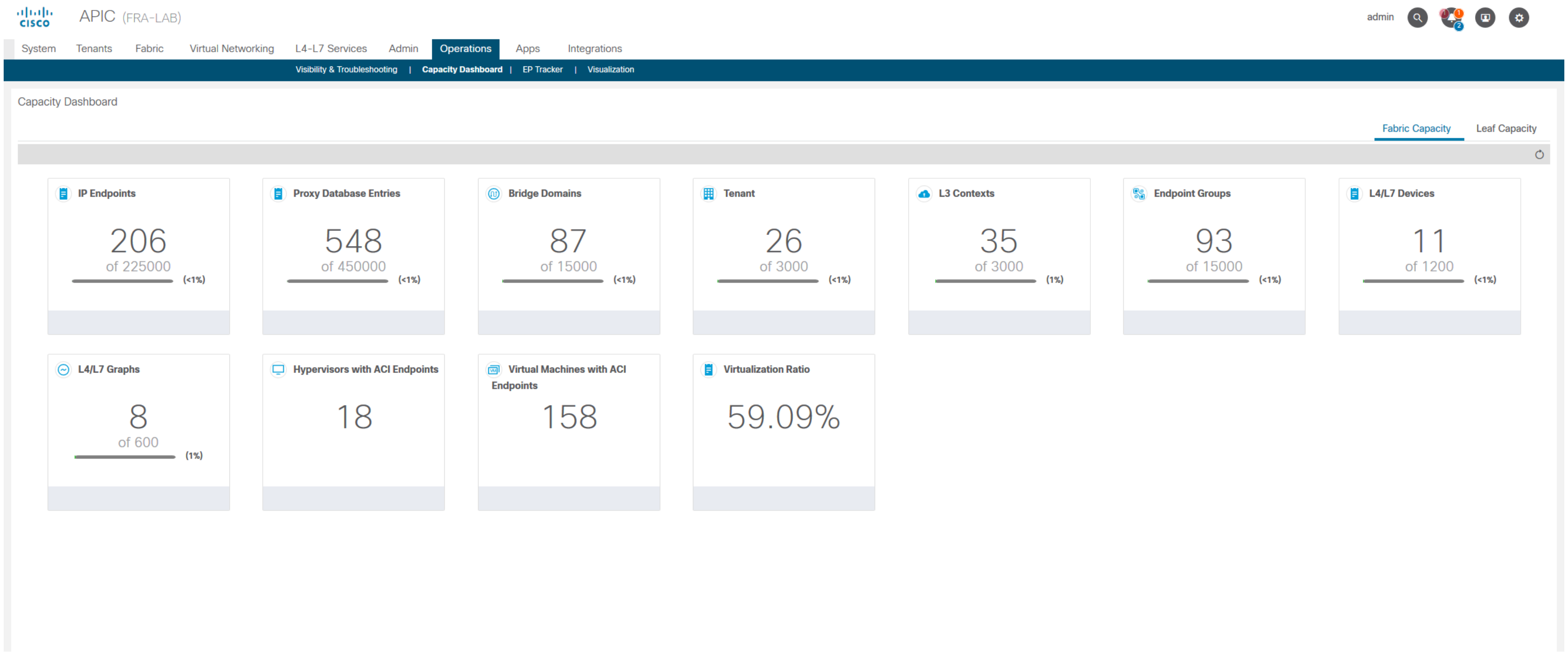


APIC: Endpoints



EPG	End Point	MAC	IP	Learning Source	Reporting Controller Name	Interface	Encap	Multicast Address
Infrastructure/Infrastructure/Storage	EP-00:50:56:6C:70:B9	00:50:56:6C:70:B9	172.20.33.200	learned	---	Pod-1/Node-101/eth1/43	vlan-5	---
Infrastructure/Infrastructure/Mgmt	EP-00:50:56:6C:77:A9	00:50:56:6C:77:A9	172.20.32.42	learned	---	Pod-1/Node-103-104/UCS-HX-FI-B	vlan-2	---
Infrastructure/Infrastructure/HX-Vmotion	EP-00:50:56:6C:E6:62	00:50:56:6C:E6:62	---	vmm	---	172.20.17.11, 172.20.17.12	vlan-2005	---
Infrastructure/Infrastructure/Storage	EP-00:50:56:6D:31:37	00:50:56:6D:31:37	172.20.33.23	learned	---	Pod-1/Node-101-102/UCS-FI-B	vlan-5	---
Infrastructure/Infrastructure/HX-Vmotion	EP-00:50:56:6E:21:D1	00:50:56:6E:21:D1	192.168.2.13	learned	---	Pod-1/Node-103-104/UCS-HX-FI-B	vlan-3093	---
Infrastructure/Infrastructure/Storage	EP-00:50:56:6E:B1:62	00:50:56:6E:B1:62	172.20.33.24	learned	---	Pod-1/Node-101-102/UCS-FI-A	vlan-5	---
Infrastructure/Infrastructure/Mgmt	EP-00:50:56:6F:B1:1A	00:50:56:6F:B1:1A	172.20.32.41	learned	---	Pod-1/Node-103-104/UCS-HX-FI-B	vlan-2	---
Infrastructure/Infrastructure/Storage	EP-00:50:56:6F:DC:7A	00:50:56:6F:DC:7A	172.20.33.5	learned	---	Pod-1/Node-101-102/UCS-FI-A	vlan-5	---
Infrastructure/Infrastructure/Cloud	Avi Cloud Controller	00:50:56:88:00:AB	172.20.35.61	learned vmm	vCenter-FraLab65	172.20.17.11, 172.20.17.12, Pod-1/Node-101-102/UCS...	vlan-2134	---
Infrastructure/Infrastructure/Cloud	WAC	00:50:56:88:08:B4	---	vmm	vCenter-FraLab65	172.20.19.61, 172.20.19.62	vlan-2134	---
Infrastructure/Infrastructure/CoreNetz	StealthWatch FlowCollector for NetFlow VE	00:50:56:88:09:37	---	vmm	vCenter-FraLab65	172.20.17.11, 172.20.17.12	vlan-2001	---
Infrastructure/Infrastructure/Cloud	UCSPE-6248	00:50:56:88:0C:F2	---	vmm	vCenter-FraLab65	172.20.19.61, 172.20.19.62	vlan-2134	---
Infrastructure/Infrastructure/Cloud	Avi-se-bxkes	00:50:56:88:0D:95	172.20.35.64	learned vmm	vCenter-FraLab65	172.20.17.11, 172.20.17.12, Pod-1/Node-101-102/UCS...	vlan-2134	---
Infrastructure/Infrastructure/Cloud	Avi-se-fpphl	00:50:56:88:0E:FF	172.20.35.66, 172.20.35.70	learned vmm	vCenter-FraLab65	172.20.17.11, 172.20.17.12, Pod-1/Node-101-102/UCS...	vlan-2134	---
Infrastructure/Infrastructure/Cloud	K8-Node-2	00:50:56:88:0F:7B	172.20.35.53	learned vmm	vCenter-FraLab65	172.20.17.11, 172.20.17.12, Pod-1/Node-101-102/UCS...	vlan-2134	---
Infrastructure/Infrastructure/CoreNetz	VSM7.9.0-160i-RHEL6_UCS-BC	00:50:56:88:11:A9	---	vmm	vCenter-FraLab65	172.20.17.11, 172.20.17.12	vlan-2001	---
Infrastructure/Infrastructure/Cloud	UCSPE-6248	00:50:56:88:14:89	172.20.35.150, 172.20.35....	learned vmm	vCenter-FraLab65	172.20.19.61, 172.20.19.62, Pod-1/Node-103-104/UCS...	vlan-2134	---
Infrastructure/Infrastructure/Storage	UCSD_NFS_Mount	00:50:56:88:15:8C	172.20.33.60	learned vmm	vCenter-FraLab65	172.20.17.11, 172.20.17.12, Pod-1/Node-101-102/UCS...	vlan-2070	---
Infrastructure/Infrastructure/Cloud	Repository	00:50:56:88:16:CD	---	vmm	vCenter-FraLab65	172.20.17.11, 172.20.17.12	vlan-2134	---
Infrastructure/Infrastructure/Collab	Unified Intelligence Center	00:50:56:88:1C:C1	---	vmm	vCenter-FraLab65	172.20.17.11, 172.20.17.12	vlan-2136	---
UC_CCIE_LAB/UC_CCIE/HQ_Server	CCIE HQ CUC	00:50:56:88:1E:59	---	vmm	vCenter-FraLab65	172.20.17.11, 172.20.17.12	vlan-2074	---

APIC: Capacity Dashboard



Capacity Dashboard

IP Endpoints
206
of 225000 (<1%)

Proxy Database Entries
548
of 450000 (<1%)

Bridge Domains
87
of 15000 (<1%)

Tenant
26
of 3000 (<1%)

L3 Contexts
35
of 3000 (1%)

Endpoint Groups
93
of 15000 (<1%)

L4/L7 Devices
11
of 1200 (<1%)

L4/L7 Graphs
8
of 600 (1%)

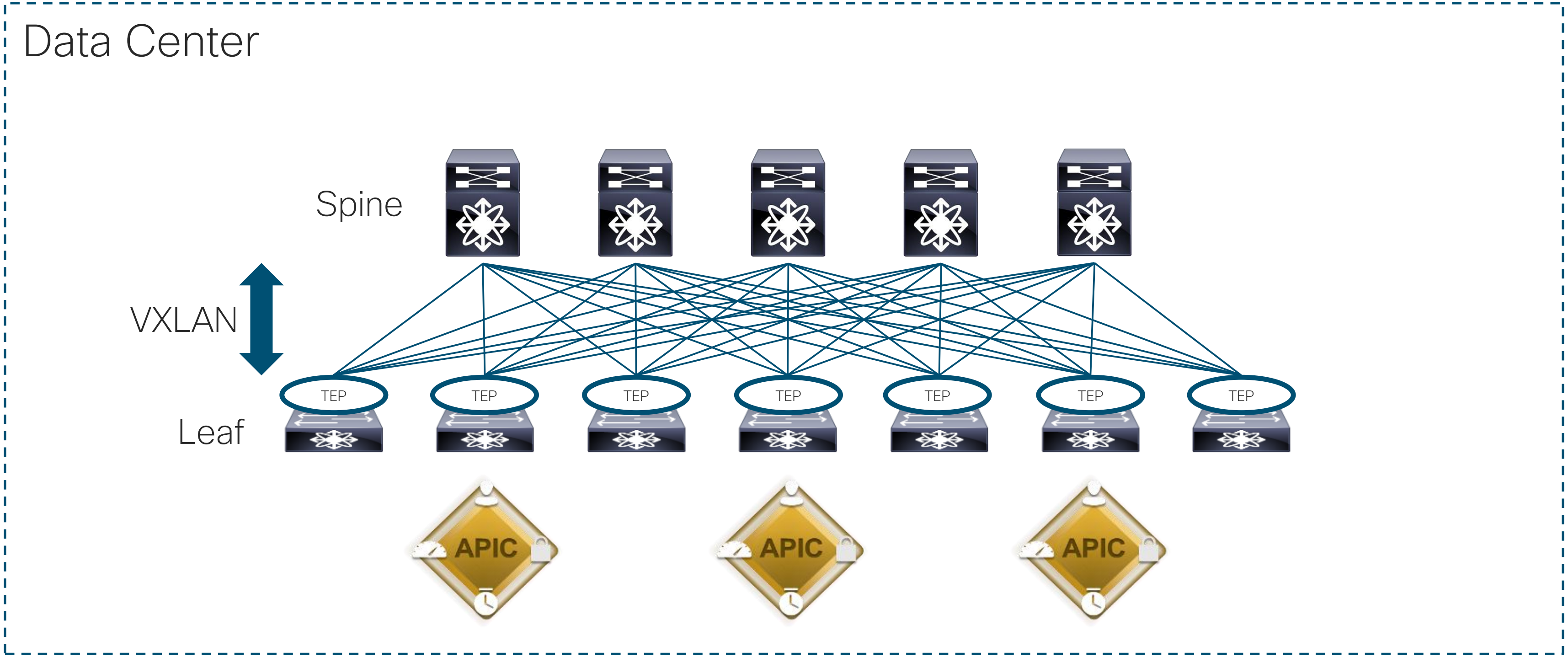
Hypervisors with ACI Endpoints
18

Virtual Machines with ACI Endpoints
158

Virtualization Ratio
59.09%

Under the Hood

Under the Hood



Reference

Under the Hood

- L3 point-to-point links
- loopback interfaces on each node
- VXLAN overlay
  - leaf switches are TEPs
- distributed anycast gateway on all leaf switches
- MP-BGP control plane
- further information → Cisco Live session BRKACI-3545
  "Mastering ACI Forwarding Behavior – A day in the life of a packet"

Example:
Basic Network Provisioning – Traditional vs. ACI-based

Use Case: New Application Onboarding

- 3-tier application (web, application, database)
  - virtual servers
  - application tiers have to be logically separated

Network Provisioning: Traditional vs. ACI Approach

Traditional

- create VLANs
  - per VTP domain
- create SVIs
  - per L3 device
- configure interfaces
  - per device
- configure ACLs
  - per L3 device

ACI

- create Application Profile “XYZ“
  - once
- create EPGs (Web, App, DB)
  - once
- associate endpoints to EPGs
  - once
- associate contracts
  - once

Network Provisioning: Traditional vs. ACI Approach

Traditional

VTP Primary Server

```
vlan 101
name XYZ_Web_Servers
vlan 102
name XYZ_App_Servers
vlan 103
name XYZ_DB_Servers
```

Access Switches

```
interface port-channel 10, ethernet 1/1-8
switchport trunk allowed vlan add 101-103
```

Virtualization Environment

create port groups

connect VMs to port groups

Aggregation Switches

```
<ACL definitions omitted for simplicity>
interface vlan 101
description XYZ_Web_Servers
vrf member Production
ip address 10.0.101.2/24
hsrp 101
ip 10.0.101.1
ip router ospf 1 area 0.0.0.0
<ACL bindings omitted for simplicity>
interface vlan 102
description XYZ_App_Servers
vrf member Production
ip address 10.0.102.2/24
hsrp 102
ip 10.0.102.1
ip router ospf 1 area 0.0.0.0
<ACL bindings omitted for simplicity>
interface vlan 103
description XYZ_DB_Servers
vrf member Production
ip address 10.0.103.2/24
hsrp 103
ip 10.0.103.1
ip router ospf 1 area 0.0.0.0
<ACL bindings omitted for simplicity>

interface port-channel 1, port-channel 10
switchport trunk allowed vlan add 101-103
```

ACI

APIC

create Application Profile "XYZ“

create EPG "Web“

create EPG "App“

create EPG "DB"

create and bind contract between “DB” and “App”

create and bind contract between “App” and “Web”

create and bind contract between “Web” and outside

Virtualization Environment

connect VMs to port groups

Example: Microsegmentation – Traditional vs. ACI-based

Microsegmentation: Traditional vs. ACI Approach

Traditional

- create secondary VLANs
  - per VTP domain
- create PVLAN associations
  - per device
- configure interfaces
  - per device
- configure virtualization environment

ACI

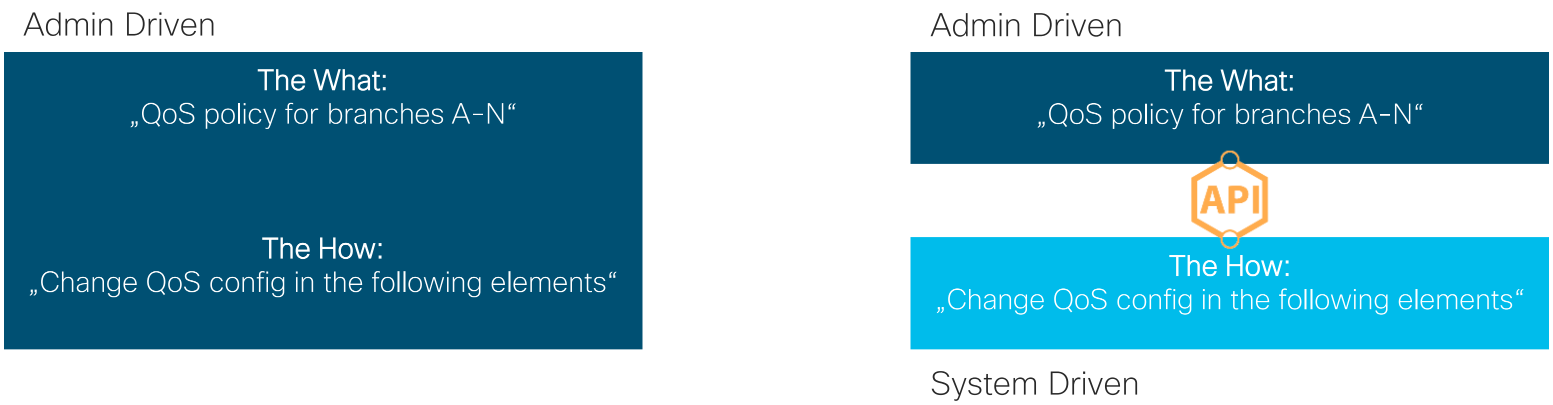
- ☑ intra-EPG isolation
  - per EPG

Cisco
Digital Network Architecture
& Software-defined Access

Intent-based Networking

Manual Policy Deployment

Intent-based Policy Deployment



Admin Driven

The What:
„QoS policy for branches A-N“

The How:
„Change QoS config in the following elements“

Admin Driven

The What:
„QoS policy for branches A-N“

The How:
„Change QoS config in the following elements“

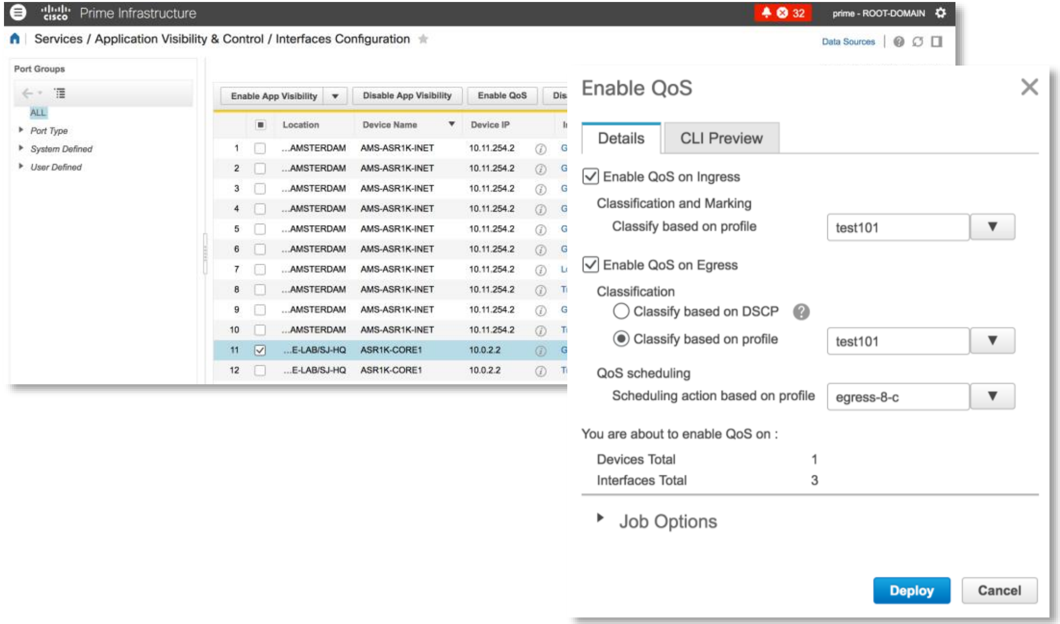
System Driven

Feature Configuration vs. Intent-based Networking

Feature Configuration

- QoS config in Prime:
  - choose device
  - choose interface (ingress/egress)
  - choose configuration
  - admin needs to understand QoS

→ complex and error prone



Services / Application Visibility & Control / Interfaces Configuration

	■	Location	Device Name	Device IP		I
1	□	...AMSTERDAM	AMS-ASR1K-INET	10.11.254.2	ⓘ	G
2	□	...AMSTERDAM	AMS-ASR1K-INET	10.11.254.2	ⓘ	G
3	□	...AMSTERDAM	AMS-ASR1K-INET	10.11.254.2	ⓘ	G
4	□	...AMSTERDAM	AMS-ASR1K-INET	10.11.254.2	ⓘ	G
5	□	...AMSTERDAM	AMS-ASR1K-INET	10.11.254.2	ⓘ	G
6	□	...AMSTERDAM	AMS-ASR1K-INET	10.11.254.2	ⓘ	G
7	□	...AMSTERDAM	AMS-ASR1K-INET	10.11.254.2	ⓘ	L
8	□	...AMSTERDAM	AMS-ASR1K-INET	10.11.254.2	ⓘ	T
9	□	...AMSTERDAM	AMS-ASR1K-INET	10.11.254.2	ⓘ	G
10	□	...AMSTERDAM	AMS-ASR1K-INET	10.11.254.2	ⓘ	T
11	☑	...E-LAB/SJ-HQ	ASR1K-CORE1	10.0.2.2	ⓘ	G
12	□	...E-LAB/SJ-HQ	ASR1K-CORE1	10.0.2.2	ⓘ	T

Enable QoS

Details | CLI Preview

☑ Enable QoS on Ingress

Classification and Marking

Classify based on profile: test101

☑ Enable QoS on Egress

Classification

○ Classify based on DSCP

● Classify based on profile: test101

QoS scheduling

Scheduling action based on profile: egress-8-c

You are about to enable QoS on :

Devices Total	1
Interfaces Total	3

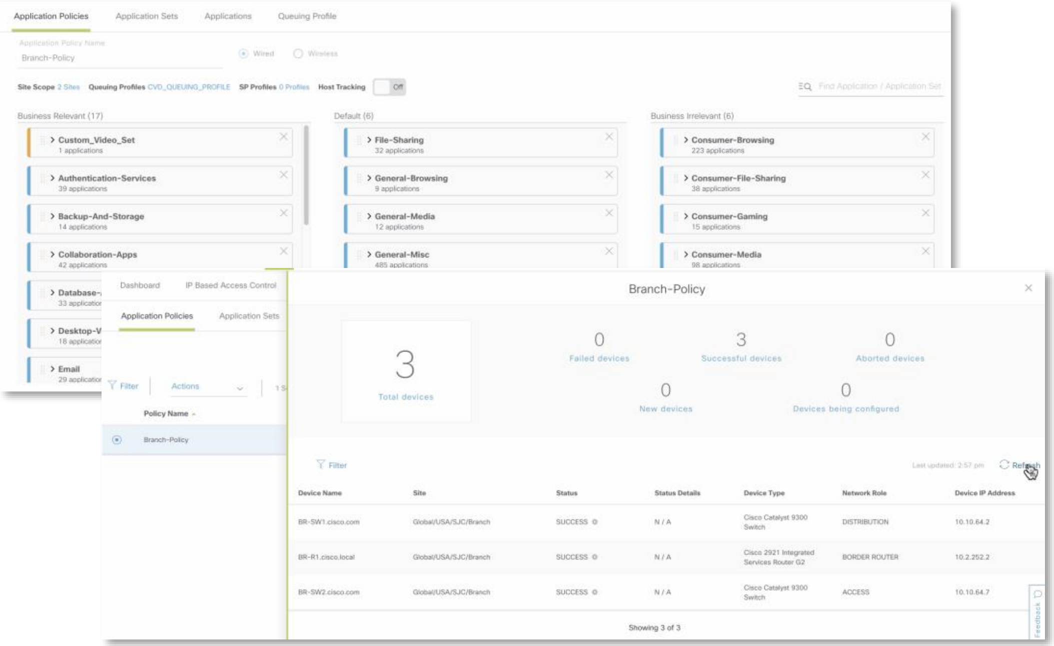
▸ Job Options

Deploy | Cancel

Feature Configuration vs. Intent-based Networking

Intent-based Networking

- QoS in DNA Center
  - application focus
  - configure application policies based on the business requirements
  - configure sites, not devices



Application Policy Name: Branch-Policy

● Wired ○ Wireless

Site Scope 2 Sites Queuing Profiles CVD_QUEUING_PROFILE SP Profiles 0 Profiles Host Tracking Off

Business Relevant (17)
- Custom_Video_Set – 1 applications
- Authentication-Services – 39 applications
- Backup-And-Storage – 14 applications
- Collaboration-Apps – 42 applications
- Database-… – 33 applicatio…
- Desktop-V… – 18 applicatio…
- Email – 29 applicatio…

Default (6)
- File-Sharing – 32 applications
- General-Browsing – 9 applications
- General-Media – 12 applications
- General-Misc – 485 applications

Business Irrelevant (6)
- Consumer-Browsing – 223 applications
- Consumer-File-Sharing – 38 applications
- Consumer-Gaming – 15 applications
- Consumer-Media – 98 applications

Policy Name
- ● Branch-Policy

Branch-Policy

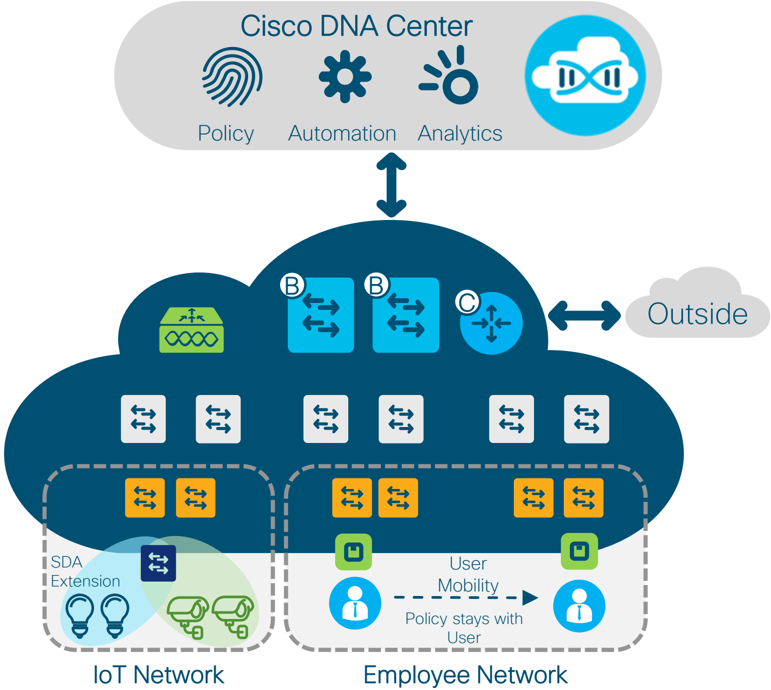
3 Total devices; 0 Failed devices; 3 Successful devices; 0 Aborted devices; 0 New devices; 0 Devices being configured

Last updated: 2:57 pm

Device Name	Site	Status	Status Details	Device Type	Network Role	Device IP Address
BR-SW1.cisco.com	Global/USA/SJC/Branch	SUCCESS	N / A	Cisco Catalyst 9300 Switch	DISTRIBUTION	10.10.64.2
BR-R1.cisco.local	Global/USA/SJC/Branch	SUCCESS	N / A	Cisco 2921 Integrated Services Router G2	BORDER ROUTER	10.2.252.2
BR-SW2.cisco.com	Global/USA/SJC/Branch	SUCCESS	N / A	Cisco Catalyst 9300 Switch	ACCESS	10.10.64.7

Showing 3 of 3

Cisco DNA & SDA



Application to manage the network:

- Design
- Policy
- Provision
- Assurance

Campus Fabric:

- Control plane based on LISP
- Data plane based VXLAN
- Policy plane based on SGT

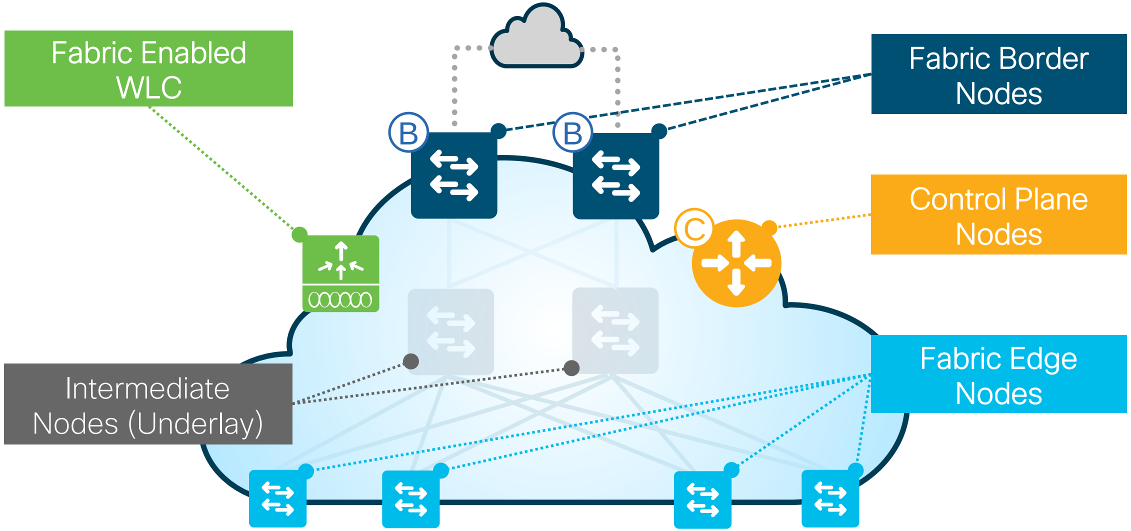
Cisco SD-Access

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 SDA fabric

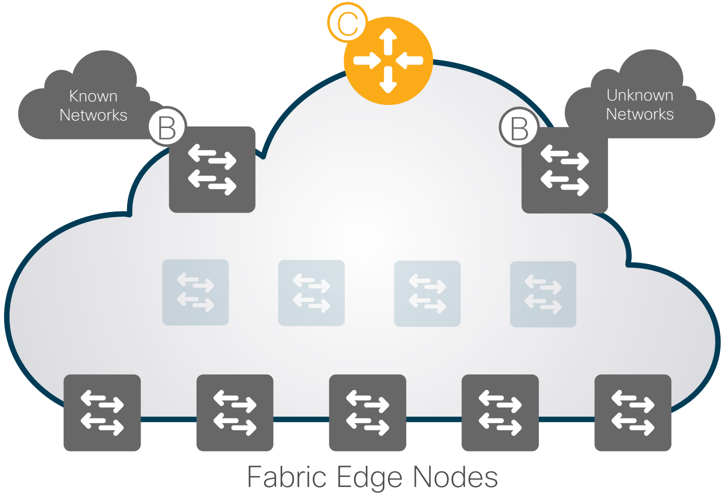
Edge Nodes – A fabric device (e.g. access or distribution) that connects wired endpoints to the SDA fabric

Fabric Wireless Controller – A fabric device (WLC) that connects wireless endpoints to the SDA fabric



SDA – Control Plane Nodes

- runs a host tracking database to map location information
  - A simple host database that maps endpoint IDs to a current location, along with other attributes
  - Host database supports multiple types of endpoint ID lookup types (IPv4, IPv6 or MAC)
  - Receives endpoint ID map registrations from edge and/or border nodes for “known” IP prefixes
  - Resolves lookup requests from edge and/or border nodes, to locate destination endpoint IDs

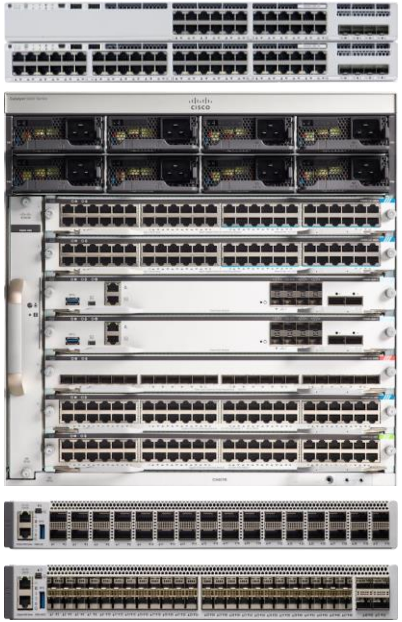


Reference

SDA – Control Plane Nodes

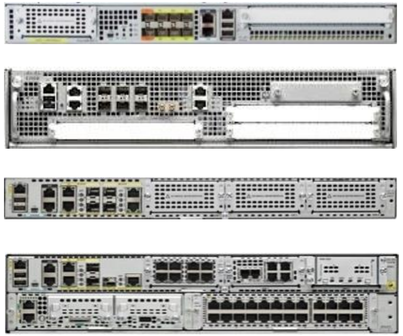
Catalyst 3850

Catalyst 9300/9400/9500



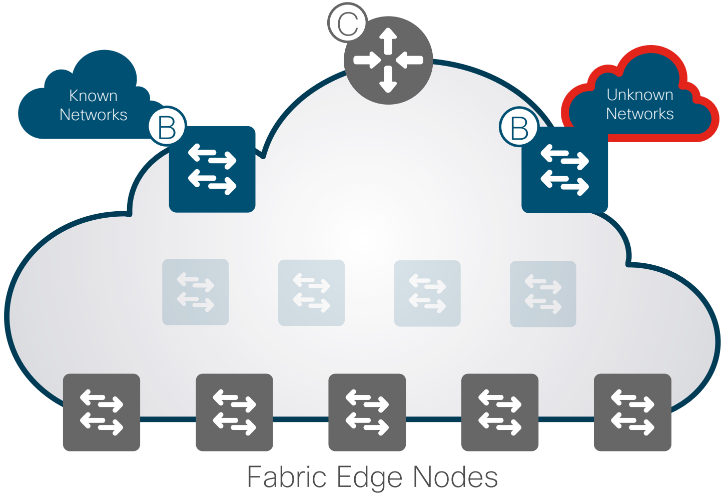
Catalyst 6800

ASR 1000/ISR 4000 & CSRv



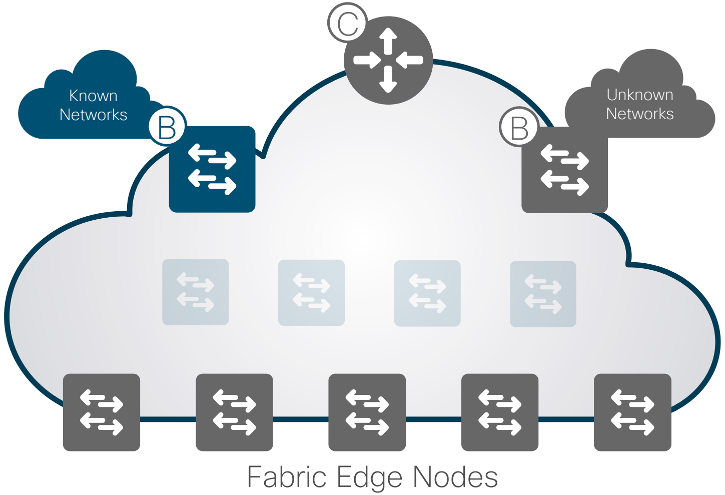
SDA – Border Nodes

- entry and exit point for all data traffic coming in or going out of the fabric
- two types:
  - Fabric Border (internal)
    - used for “known” routes in your company
  - Default Border (anywhere)
    - used for “unknown” routes outside your company



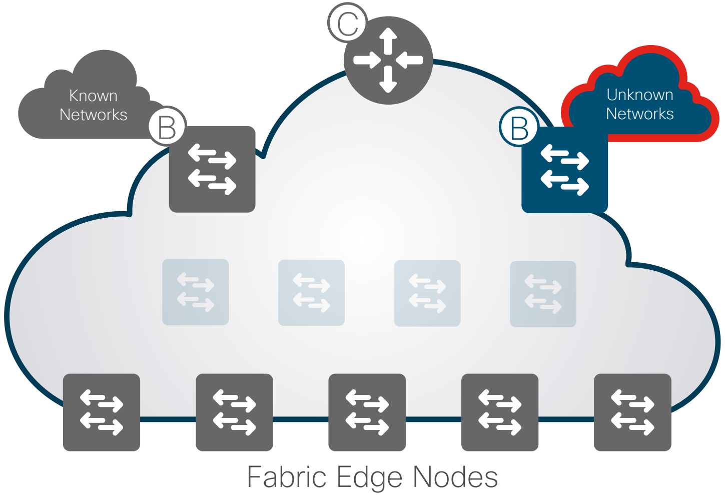
SDA – Fabric Border Nodes

- advertise endpoints to outside and known subnets to inside
  - connect to any “known” IP prefixes (e. g. DC, WLC, FW, etc.)
  - export all internal IP pools outside (as aggregate) using a traditional IP routing protocol(s)
  - import and register (known) IP subnets from outside the fabric to the control plane
  - outside hand-off requires mapping the prefix context (VRF and SGT) from one domain to another



SDA – Default Border Nodes

- gateway of last resort for unknown destinations
  - connect to any “unknown” IP prefixes
    (e. g. internet, public cloud, 3rd party, etc.)
  - export all internal IP pools outside (as aggregate) using a traditional IP routing protocol(s)
  - are a default domain exit point, if no other (specific) entry present in map system
  - outside hand-off requires mapping the prefix context (VRF and SGT) from one domain to another

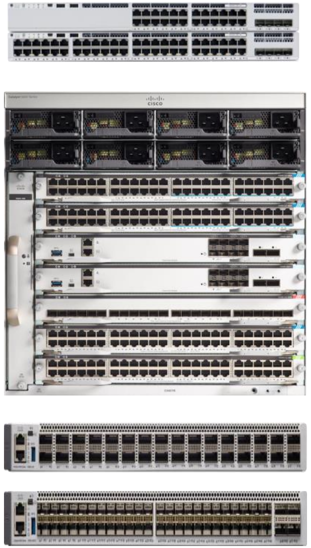


Reference

SDA – Border Nodes

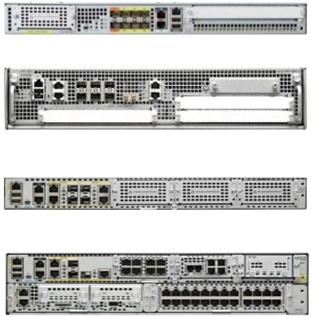
Catalyst 3850

Catalyst 9300/9400/9500



Catalyst 6800

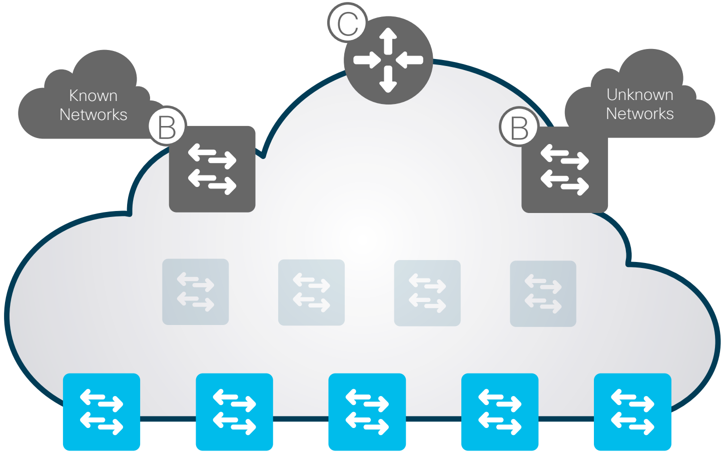
ASR 1000/ISR 4000



Nexus 7700

SDA - Edge Nodes

- provide first-hop services for users/devices connected to the fabric
  - responsible for identifying and authenticating endpoints (e. g. static, 802.1X, Active Directory)
  - register the specific endpoint ID info (e. g. /32 or /128) with the control plane node(s)
  - provides an anycast L3 gateway for connected endpoints (same IP address on all edge nodes)
  - performs encapsulation/decapsulation of data traffic to and from all connected endpoints



Fabric Edge Nodes

Reference

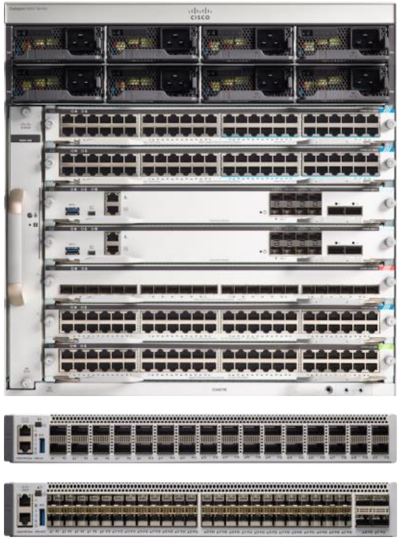
SDA - Edge Nodes

Catalyst 3650/3850

Catalyst 9200/9300

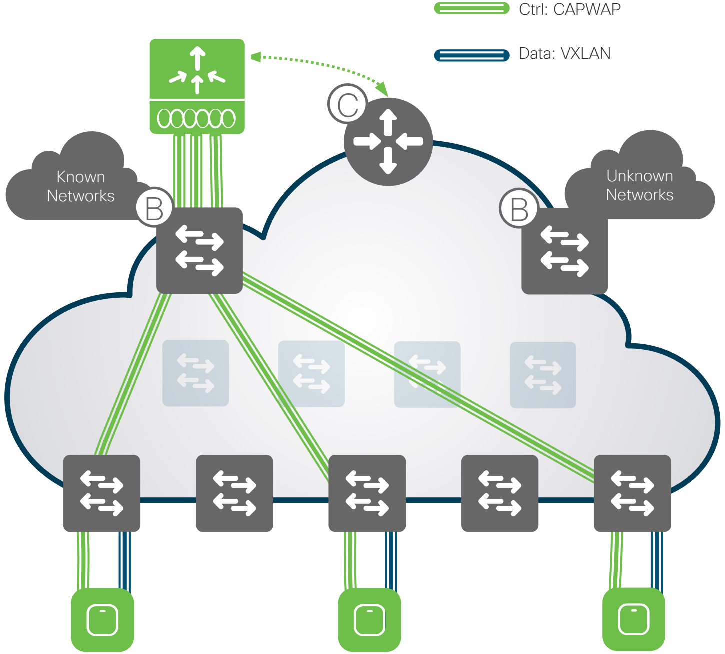
Catalyst 4500-E

Catalyst 9400/9500



SDA – Wireless LAN Controller

- fabric-enabled WLCs are integrated into fabric for SDA wireless clients
  - connect 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)



Reference

SDA – Wireless LAN Controller

Catalyst 9800

CT 3504/5520/8540

Wave 1*/2 APs

Wave 1 APs
(1700,2700,3700)

Wave 2 APs
(1800, 2800, 3800, 4800)

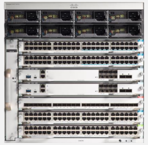
*with caveats

Reference

SDA - Device Portfolio

Switching

Catalyst 9500



Catalyst 9400

Catalyst 9300

Catalyst 9200

Catalyst 4500E

Catalyst 6800

Nexus 7700

Catalyst 3650 & 3850

Routing

ASR-1000-HX

ASR-1000-X

ISR 4451

ISR 4430

ISR 4330

ENCS 5400

Wireless

Catalyst 9800

AIR-CT8540

AIR-CT5520

AIR-CT3504

4800

Wave 2 APs (1800,2800, 3800)

Wave 1 APs* (1700,2700,3700)

Extended$^{\text{BETA}}$

Cisco Digital Building

Catalyst 3560-CX

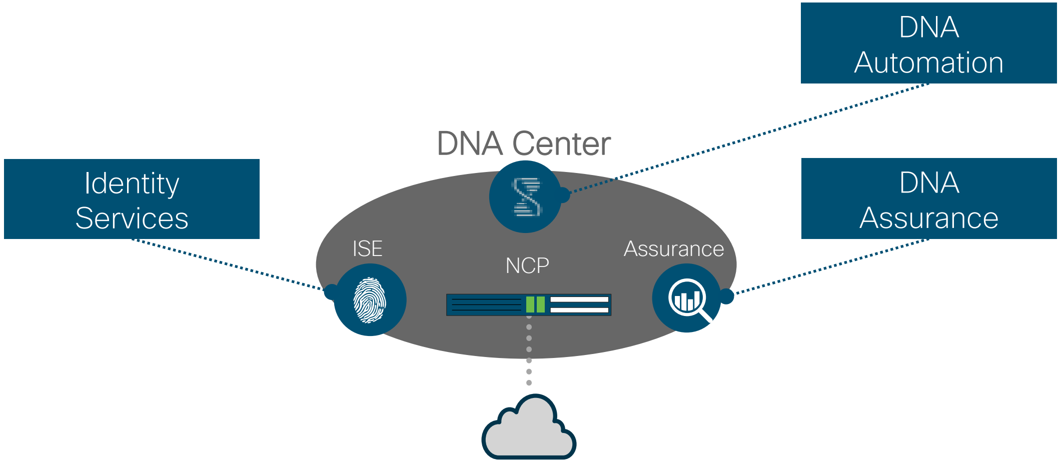
Cisco IE 4K/5K

Cisco DNA Center

DNA Automation – provides simple GUI management and intent-based automation (e. g. NCP) and context sharing

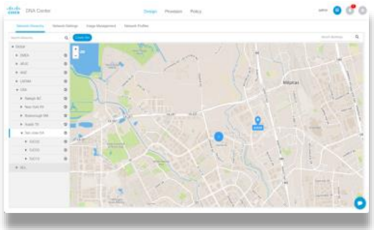
Identity Services – NAC and ID systems (e. g. ISE) for dynamic endpoint to group mapping and policy definition

DNA Assurance – data collectors (e. g. NDP) analyze endpoint to app flows and monitor fabric status



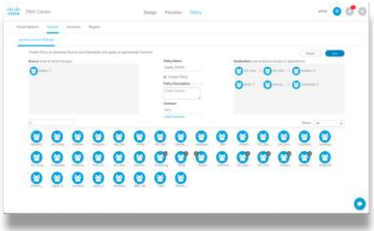
Cisco DNA Center

Design



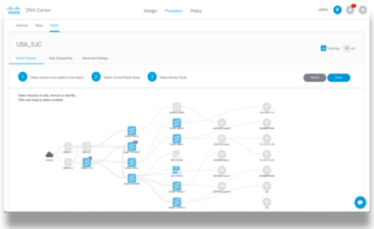
- global settings
- site profiles
- DDI, SWIM, PNP
- user access

Policy



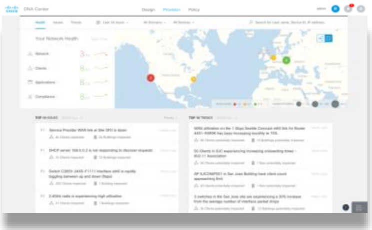
- virtual networks
- ISE, AAA, RADIUS
- endpoint groups
- group policies

Provision



- fabric domains
- CP, Border, Edge
- FEW, OTT WLAN
- external connect

Assurance

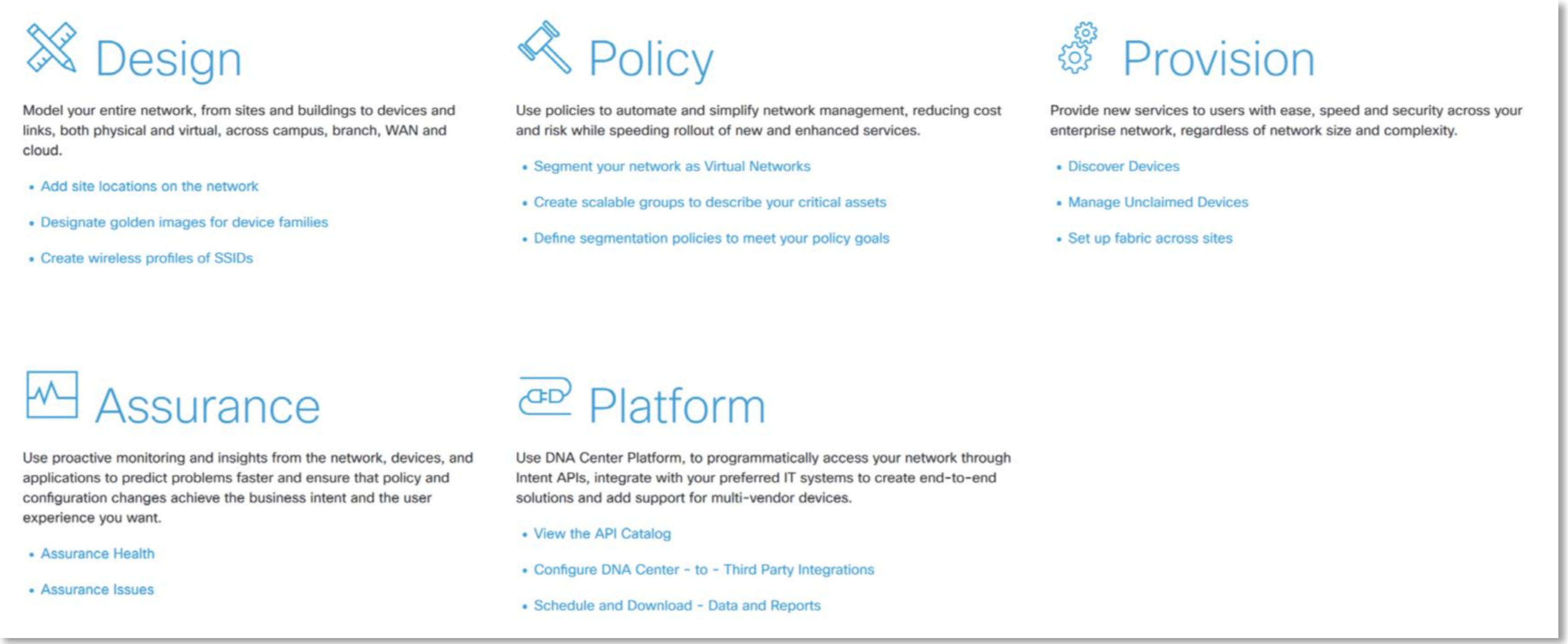


- health dashboard
- 360º views
- FD, Node, Client
- Path Traces

Platform

- allows programmatic access with 3rd-party systems using APIs, using feature set bundles, configurations, a runtime dashboard, and a developer toolkit

Cisco DNA Center



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 scalable groups to describe your critical assets
- Define segmentation policies to meet your policy goals

Provision

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

- Discover Devices
- Manage Unclaimed Devices
- Set up fabric across sites

Assurance

Use proactive monitoring and insights from the network, devices, and applications to predict problems faster and ensure that policy and configuration changes achieve the business intent and the user experience you want.

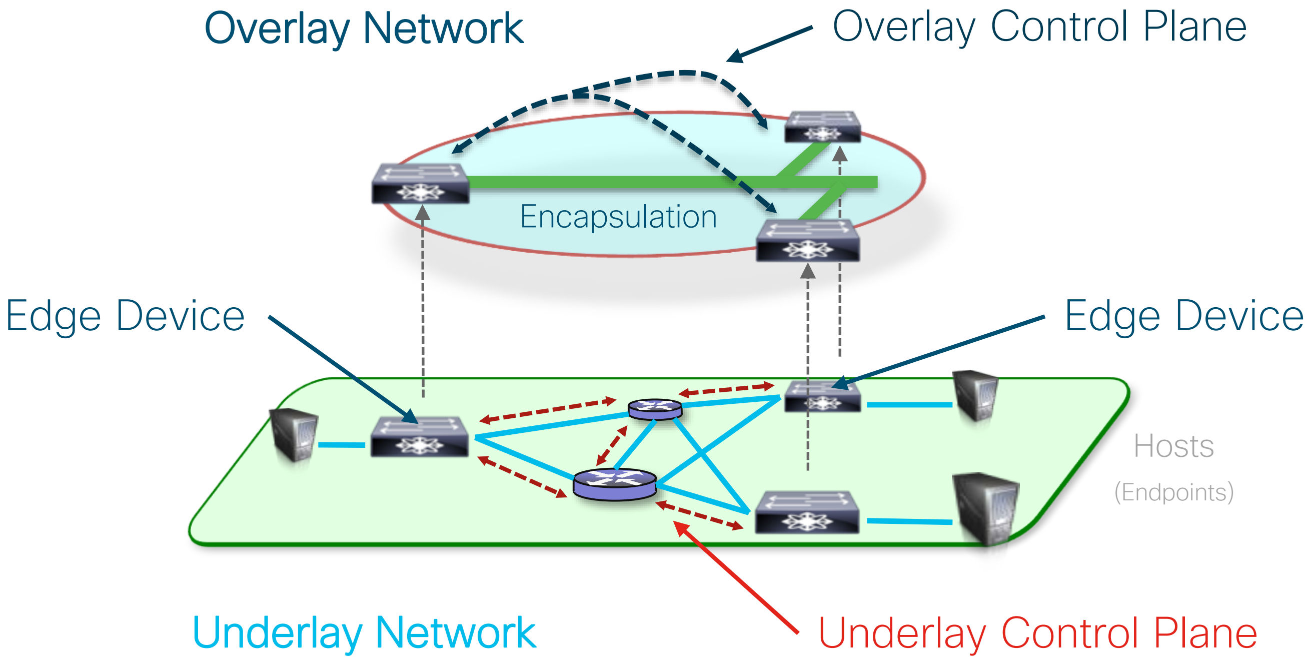
- Assurance Health
- Assurance Issues

Platform

Use DNA Center Platform, to programmatically access your network through Intent APIs, integrate with your preferred IT systems to create end-to-end solutions and add support for multi-vendor devices.

- View the API Catalog
- Configure DNA Center - to - Third Party Integrations
- Schedule and Download - Data and Reports

SDA – Underlay/Overlay



SDA – Control Plane (LISP)

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

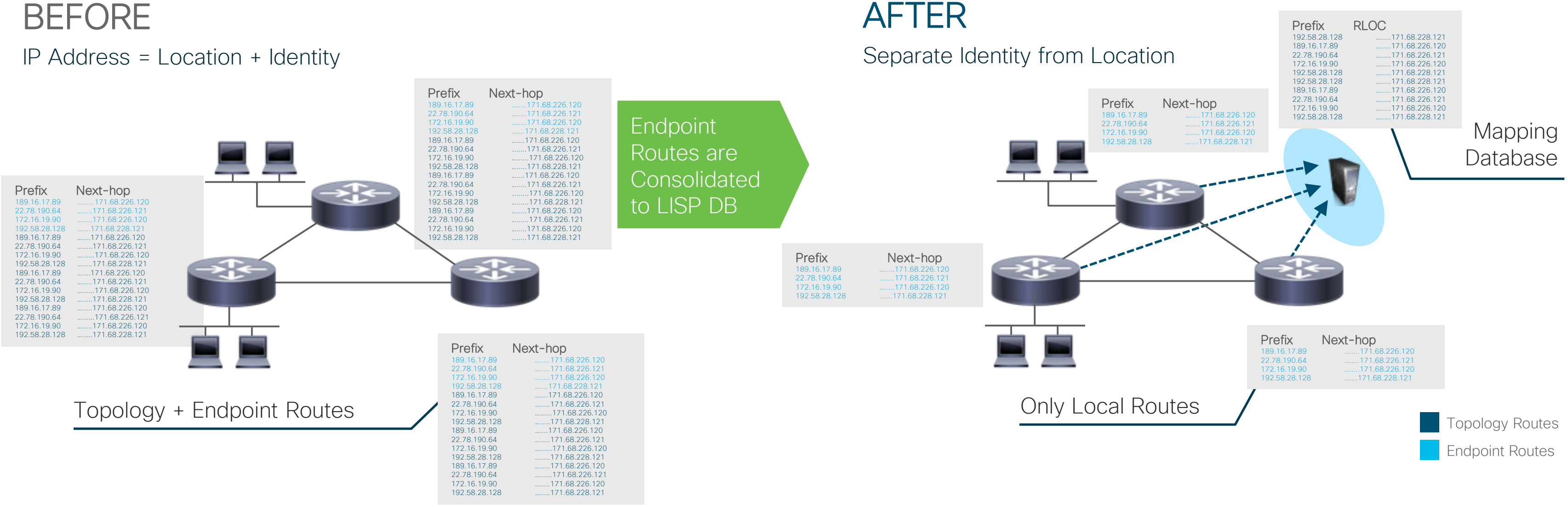
LISP DB + Cache = **Small Tables** & **Less CPU**
with Anycast L3 Gateway

BEFORE

IP Address = Location + Identity

AFTER

Separate Identity from Location



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

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

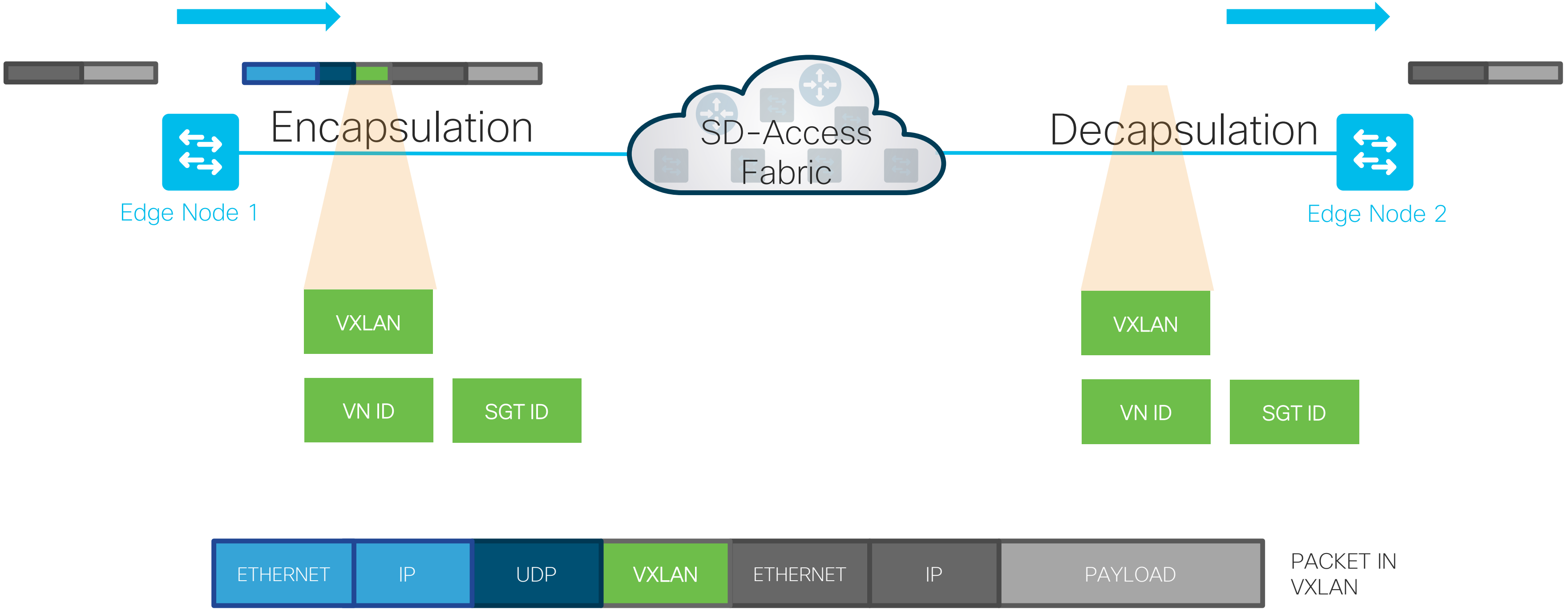
Prefix	Next-hop
189.16.17.89	........171.68.226.120
22.78.190.64	........171.68.226.121
172.16.19.90	........171.68.226.120
192.58.28.128	.......171.68.228.121

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

SDA – Data Plane (VXLAN)

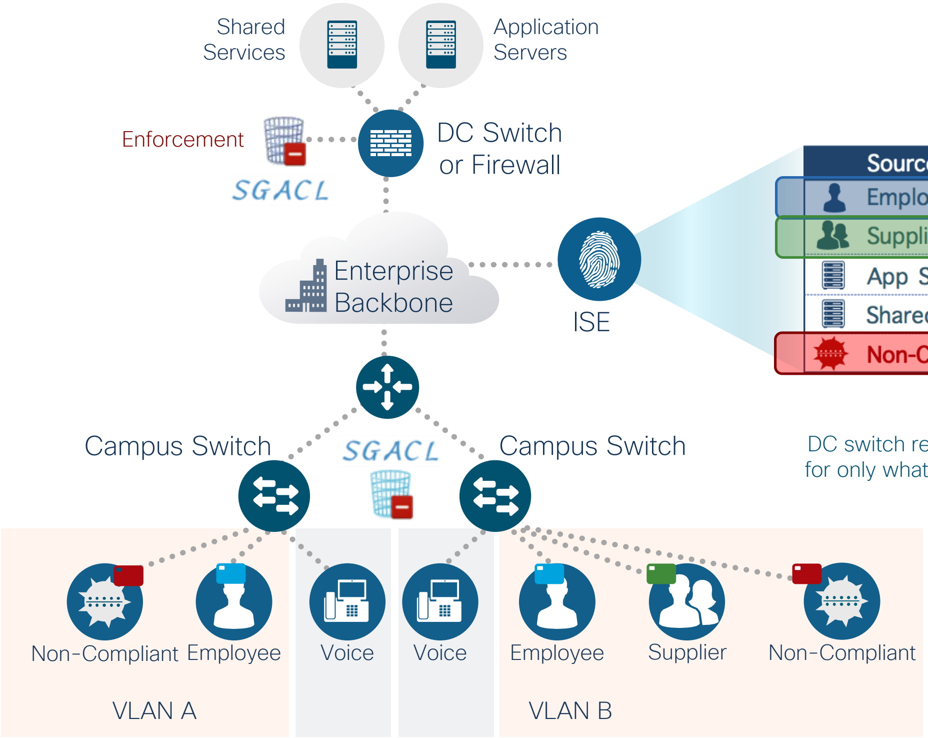


SDA – Policy Plane (SGT)

Enforcement
Group Based Policies
ACLs, Firewall Rules

Propagation
Carry “Group” context through the network using only SGT

Classification
Static or Dynamic SGT assignments



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

DC switch receives policy for only what is connected

🟦 Employee Tag
🟩 Supplier Tag
🟥 Non-Compliant Tag

Cisco DNA & SDA

What we do is the same.

How we do it is different.

Future Net Admin Skill Set

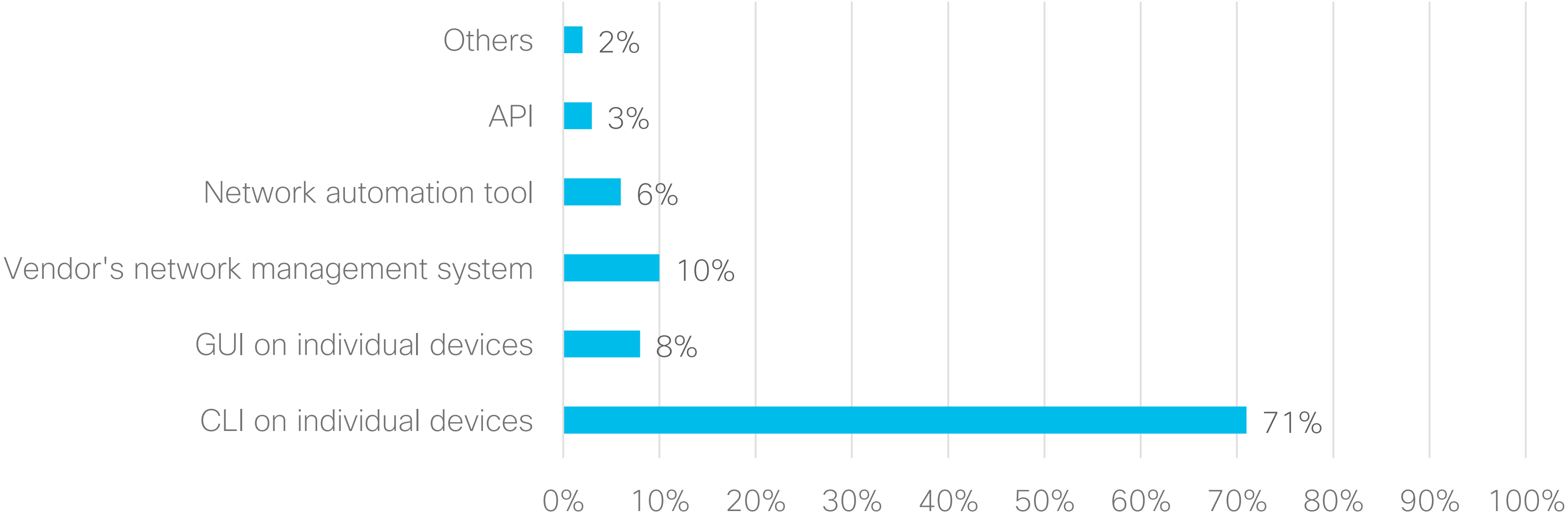
Future Net Admin Skill Set

- understanding of advanced networking concepts
  - (relatively) new technologies/architectures (VXLAN, LISP …)
  - virtualization and container networking
- programming/scripting knowledge to drive automation
  - (REST) APIs
  - data structures (XML, JSON, YAML …)
  - Python, PowerShell, Ansible …

Summary and Evaluation

Critical Observation

What is the primary method of making network changes in your environment?



*https://blogs.gartner.com/andrew-lerner/2018/01/04/checking-in-on-the-death-of-the-cli/

Summary and Evaluation

- What‘s next?
  - Cloud computing is now over 15 years in the market, still evolving/adapting at some customers.
  - SDN is now 5 years in the market, quite new and needs time to be adapted, similar to IoT (Industrie 4.0).
  - But what‘s the next step if we follow up this timeline?

Technology Evolution

- SDN technologies need to be standardized
- orchestration of solutions
- integeration into existing deployments (campus to data center end-to-end)
- extension to other areas (e. g. industrial, mobile and cloud networks)
- connection to business critical applications (ERP, CRM, etc.)

Questions?

More Questions?

Jan Haasch

Business Operations Manager
Security and Trust Office

+49 30 97892414
janhaas@cisco.com

Tim Heckmann

Consulting Engineer
Customer Experience

+49 30 97892888
timheckm@cisco.com

cisco