CISCO

You make **possible**

Getting Started with Cisco DNA Center

Marcel Rothstein – Technical Solutions Architect
Ivana Lukić – Technical Solutions Specialist

TECNMS-2900

Barcelona | January 27-31, 2020

Getting Started with Cisco DNA Center

Marcel Rothstein

Technical Solutions Architect

Germany

Ivana Lukić

Technical Solutions Specialist

Germany

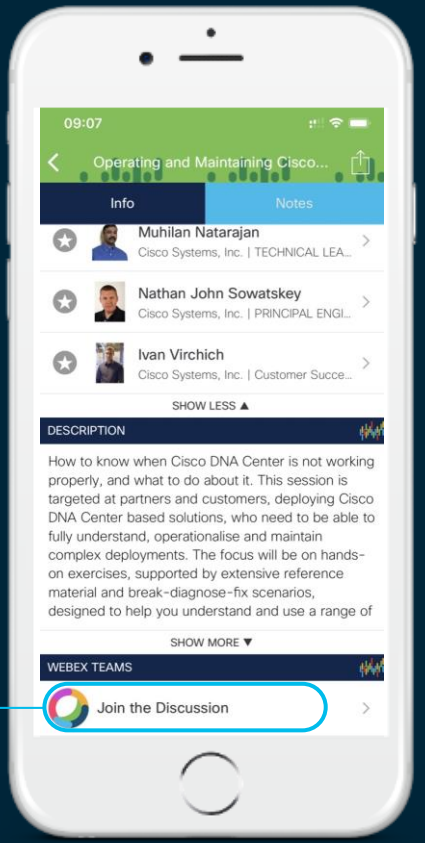
Cisco Webex Teams

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



Agenda

- Cisco DNA Center 10 minutes overview
- Before you deploy – purchase and design considerations
- Base automation for wired and wireless
- Getting started with Cisco SD-Access
- Assurance and application policies
- Key takeaways

It’s a « TAPAS » session

We are here to get you started with Cisco DNA Center

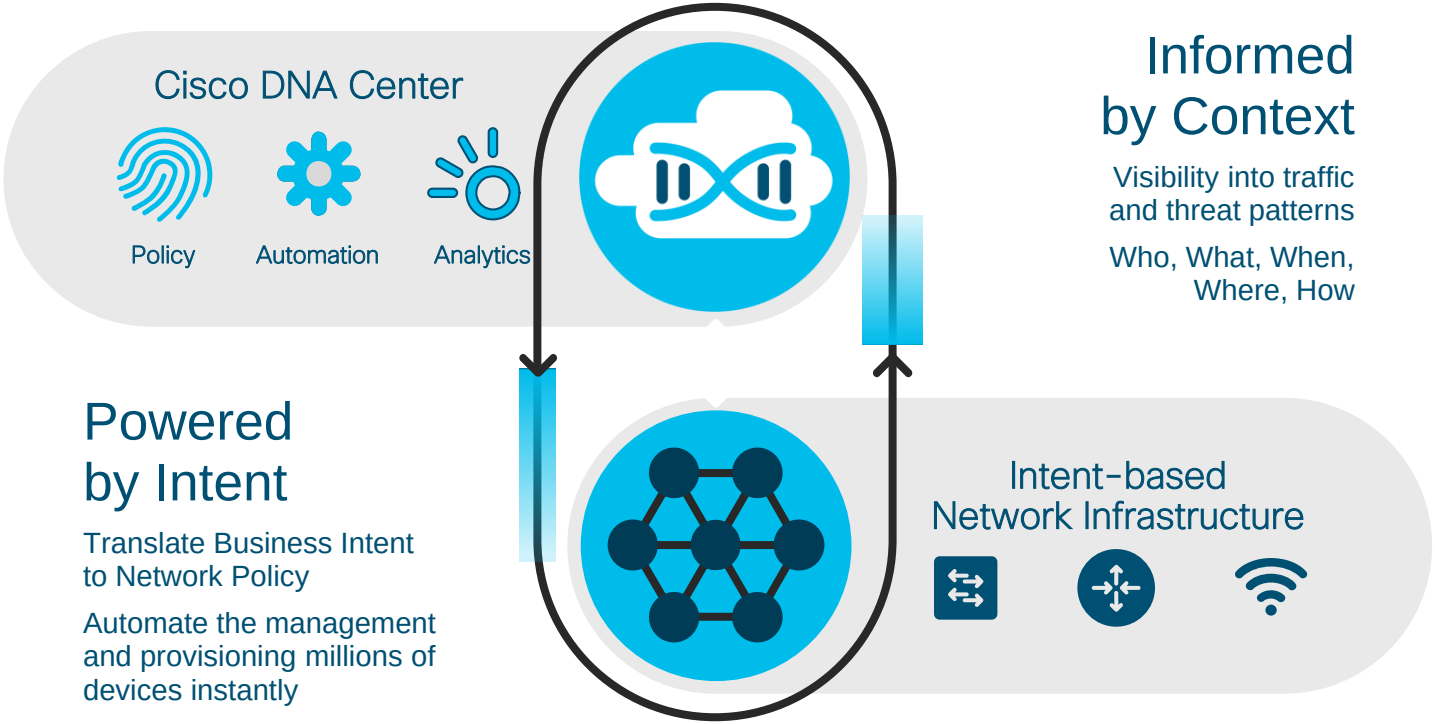
YES

- ✓ Basic actions you’ll most likely have to do
- ✓ Global understanding of Cisco DNA Center
- ✓ Basic network automation and assurance
- ✓ Tips and tricks

NO

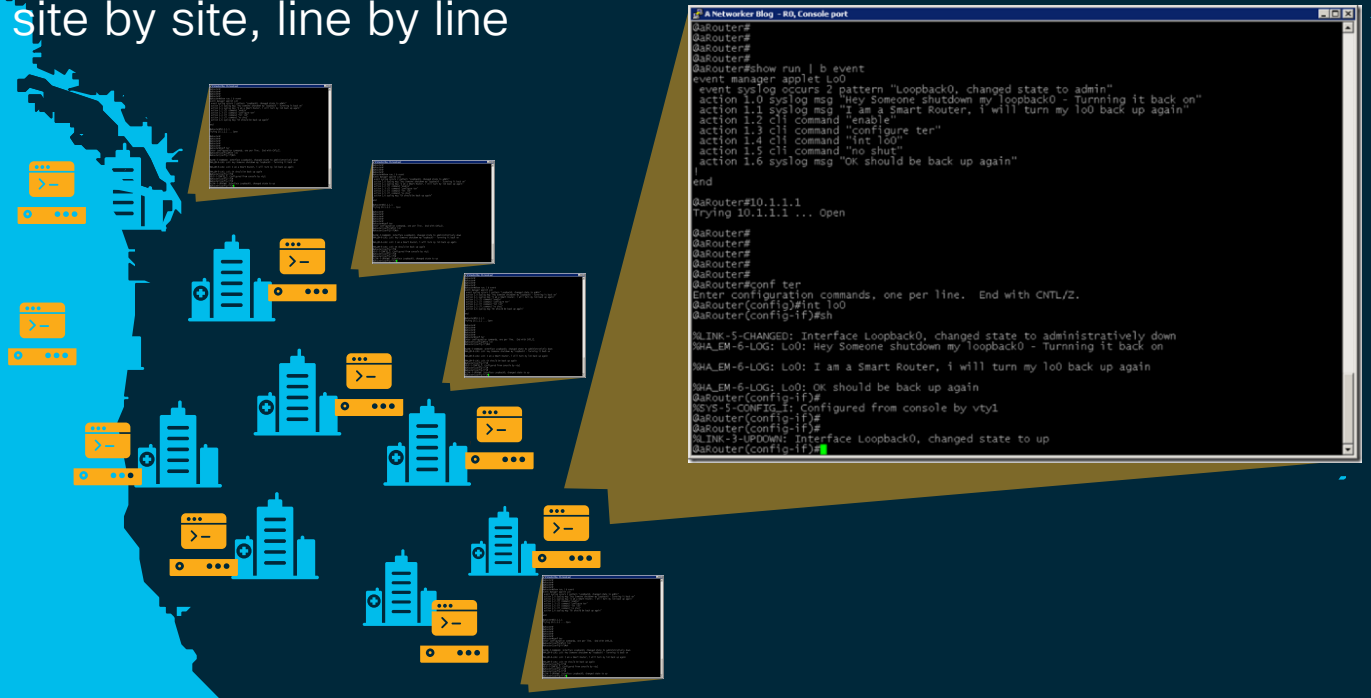
- ✗ Latest features or roadmaps
- ✗ Advanced features you’ll deploy at a second stage
- ✗ Deep dive on the solution
- ✗ API / Programmability

The Network. Intuitive.
Constantly learning, adapting and protecting.



The Old Way

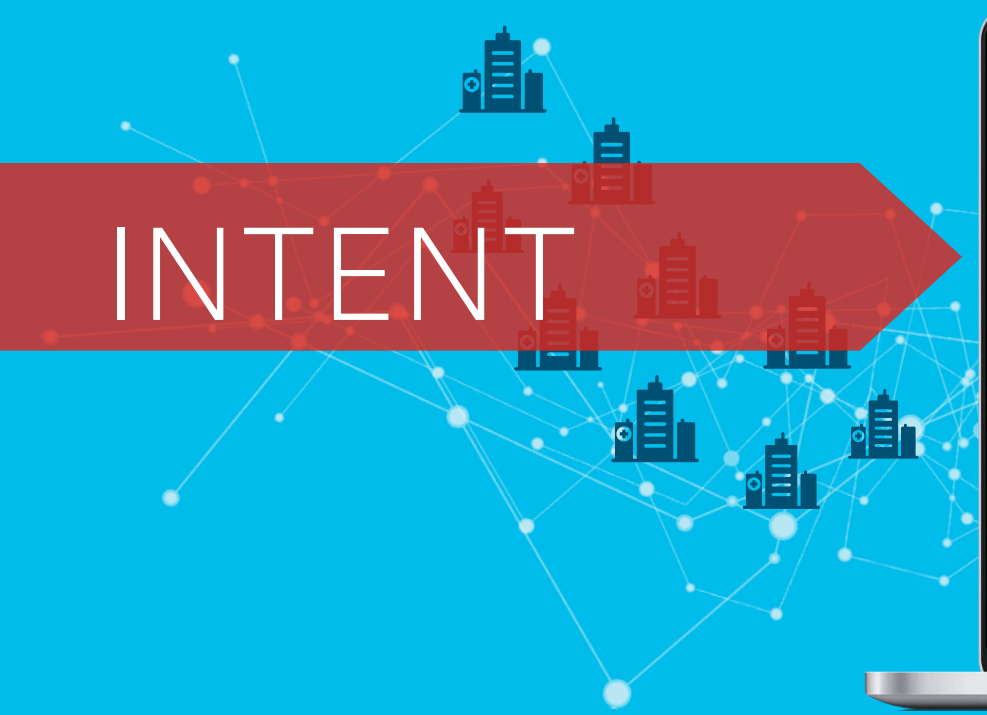
Provisioning site by site, line by line

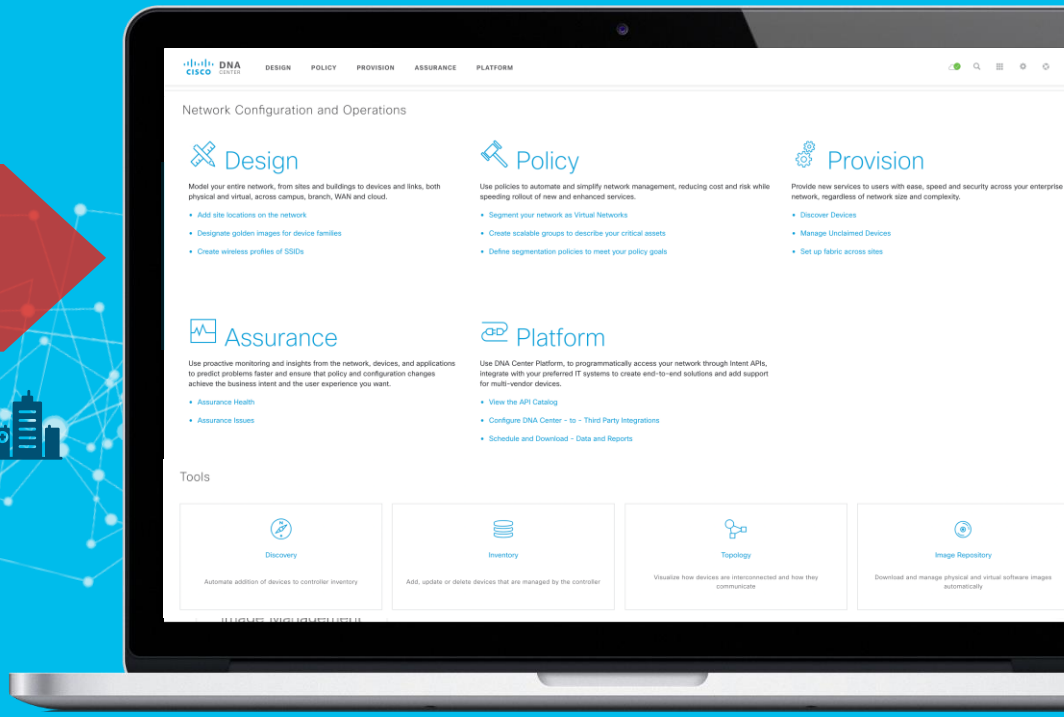


The New Way

Made simple by The Network. Intuitive.

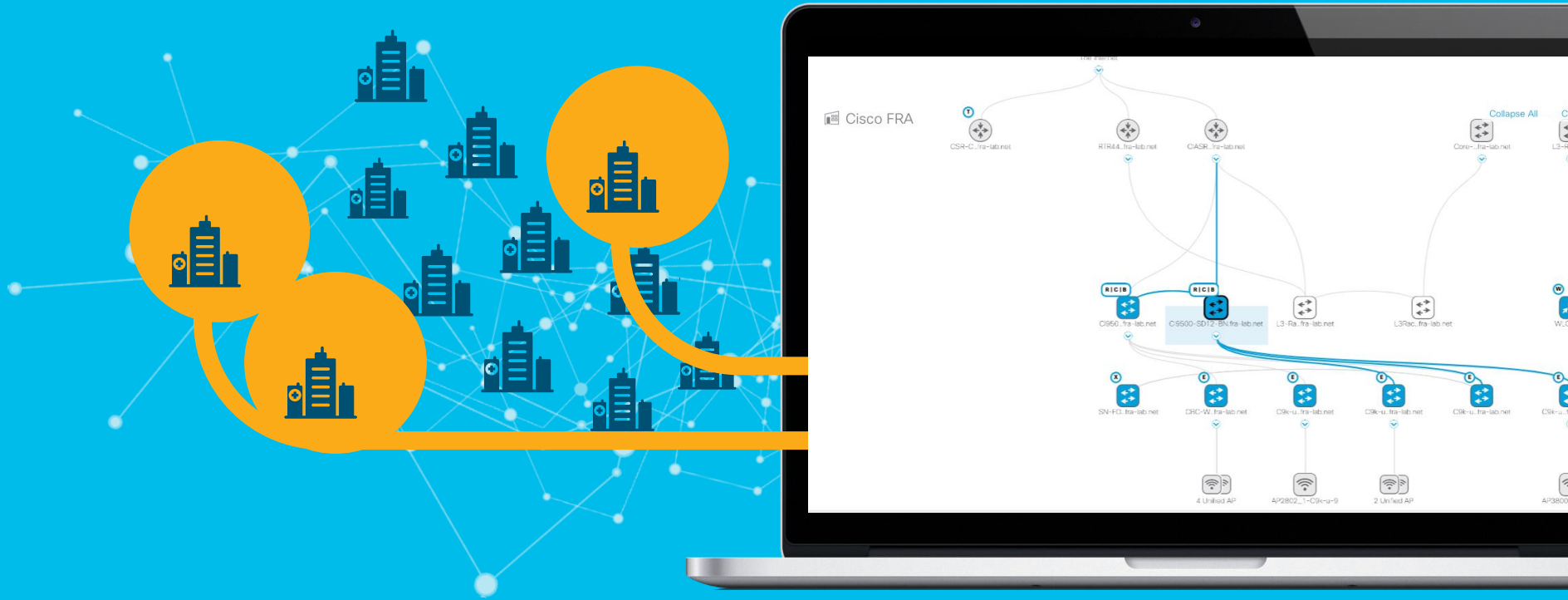
INTENT





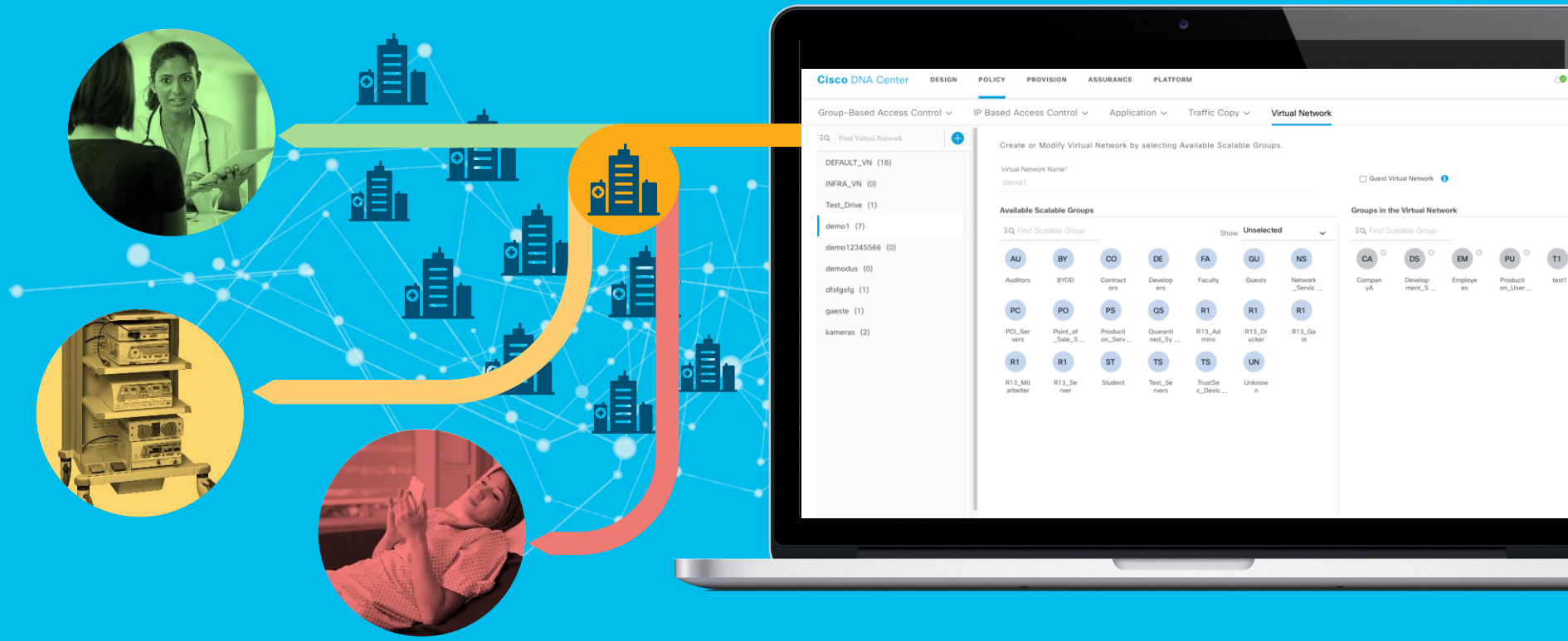
Provision

Bring a new location online and add it to the fabric network



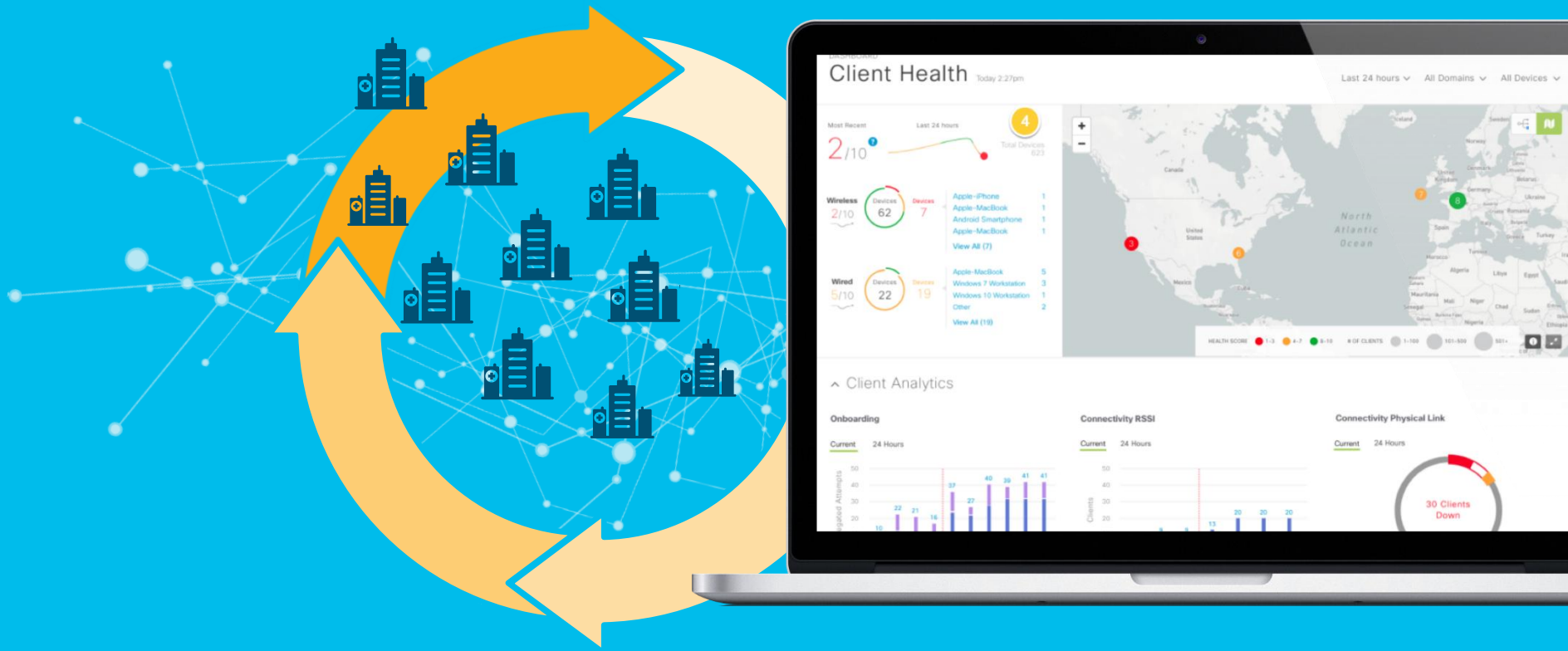
Policy Segmentation

Provide different access rights by user/thing group



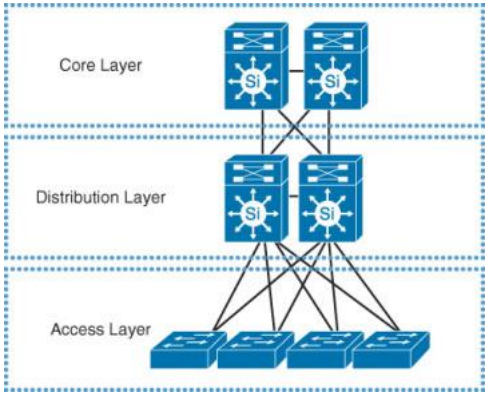
Context

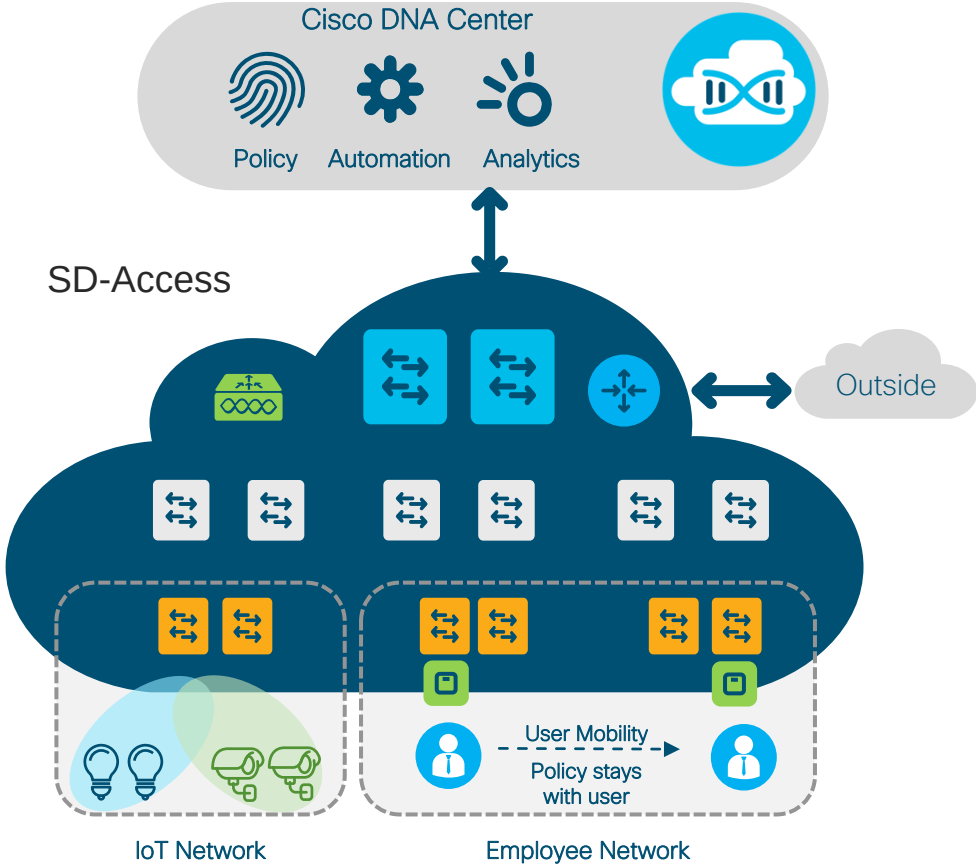
The Network takes the data around users, apps, devices, threats and turns it into context



What Cisco DNA-Center will be used for – you decide!

Classic Design





Cisco DNA Center
Not just a new Network Management System

- Full automation of your network with routed access
- Policy integration
- Active fault management with resolution proposals
- No CLI needed
- Network Segmentation
- Full IT Automation (API & 3rd Party integration)
- Flexible overlays
- Client information
- And much much more…

Agenda

- Cisco DNA Center 10 minutes overview
- **Before you deploy – purchase and design considerations**
- Base automation for wired and wireless
- Getting started with Cisco SD-Access
- Assurance and application policies
- Key takeaways

If your IT Management was very generous this year…

… you found a Cisco DNA Center Appliance under your Christmas Tree

If it was not a Christmas gift, below are the Appliance Ordering Options

Greenfield

- DN2-HW-APL (entry) can be clustered with old one (DN1-HW-APL)
- DN2-HW-APL-L (mid-size)
- DN2-HW-APL-XL (large)
- Sizes are referring to the scale numbers / intended deployment

Brownfield – restricted to customers owning the older Appliance

- DN2-HW-APL-U (Identical to DN1-HW-APL*)

SDA Bundles

- SDA-W-LABKIT (wired only option)
- SDA-WW-LABKIT (wired + wireless)

“SeedIT” Program

- FY20 Offer for the first-time buyers (for more information visit www.cisco.com/go/seedit)

*DN1 Appliance is EoS

Cisco DNA Center– Hardware Appliances

DN2 - Entry

- ✓ 44 Core M5
- ✓ 1000 Switches and Routers
- ✓ 4000 APs
- ✓ 20,000 Wireless and 5000 Wired Clients
- ✓ Introduced in 1.2.8 Release

DN2 – Mid Size

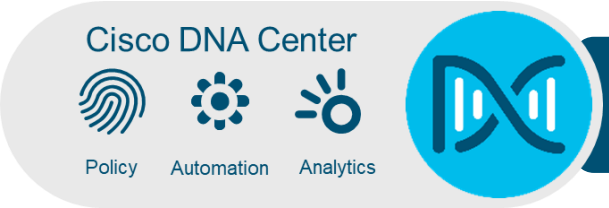
- ✓ 56 Core M5
- ✓ 2000 Switches/Routers
- ✓ 6000 AP
- ✓ 40,000 Clients
- ✓ Introduced in 1.3 Release

DN2 - Large

- ✓ 112 Core M5
- ✓ 5000 Switches/Routers
- ✓ 13,000 AP
- ✓ 100,000 Clients
- ✓ Introduced in 1.3 Release

High Availability available with all models
Cluster members **MUST** be of the same appliance type and SW version

Cisco DNA Center Scale – Scaling Parameters



37 Parameters directly relevant when designing for scale

Main Scale Parameters

- No of Endpoints (Wired, Wireless)
- No of Devices (Includes Sensors, routers, switches, APs, WLCs)

Automation Scale Parameters

- Sites
- Network Profiles
- ISE/IPAM connections, etc.

Assurance Scale Parameters

- SNMP, Syslog, Netflow Support,
- Issue Generation, etc.

DNACP Scale Parameters

- No of Concurrent API access
- No of API accessed per second etc.

SDA Scale Parameters

- No of VNs
- No of Border/edge/WLC,
- No of policies etc.

Cisco DNA Center System Scale

For Your Reference

Parameters	DN2-HW-APL	DN2-HW-APL-L	DN2-HW-APL-XL
No of Devices (Switch/Router/WLC)	1000	2000	5000
No of Access Points	4000	6000	13,000[1]
No of Endpoints (Concurrent)	25,000	40,000	100,000
No of Endpoints (Unique) over 14 days	75,000	120,000	250,000
No of endpoints – wired: wireless ratio	Any	Any	Wired: 40,000 Wireless: 60,000
No. of Ports	48,000	192,000	480,000
Number of Site Elements	500	1000	2000
No of WLC	500	1000	2000
API rate limit	50 APIs/min	50 APIs/min	50 APIs/min

[1] For number of supported APs for Fabric, please see the SD-Access table

Cisco DNA Center Software Defined Access (SD-A) Scale

For Your Reference

Parameters	DN2-HW-APL	DN2-HW-APL-L	DN2-HW-APL-XL
No of Fabric Domains	10	20	20
No of Fabric Sites	500	1000	2000
No of Virtual Networks per Fabric Site	64/Site	64/site	256/site
No of Fabric Devices per Fabric/site	500/site	600/site	1200/site
No of Scalable Groups	4000	4000	4000
No of Access Contracts	500	500	500
No of Group-Based Policies	25,000	25,000	25,000
No if IP Pools	100/site	300/site	600/site

Cisco DNA-C 1.3 – Device Support Summary (Attention: for SDA support see next slide!)

For Your Reference

- Cat 2k (2960 C/CG/CPD/CX/L/P/X/XR)
- Cat 3k (3650CX, 3650, 3850 Copper & Fiber)
- Cat 4k (4500X, 4503E/06E/07R+E/10R+E with Sup7E or newer)
- Cat 6k (6503E/04E/06E/09E/13E, 6807, 6840, 6880 with 2T/6T)
- Cat 9k (9200/L, 9300/L, 9400, 9500, 9600)
- CDB (Digital Building Switch)
- N77k with M3
- IE 2k, 3k, 4k, 5k
- ASR 1k, ISR 1k & 4k
- WLC 3504, 5520, 8540, 9800
- Wave 1 & 2 APs, .11ax APs
- https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-device-support-tables-list.html

Cisco DNA-C 1.3 – SD-A Device Matrix

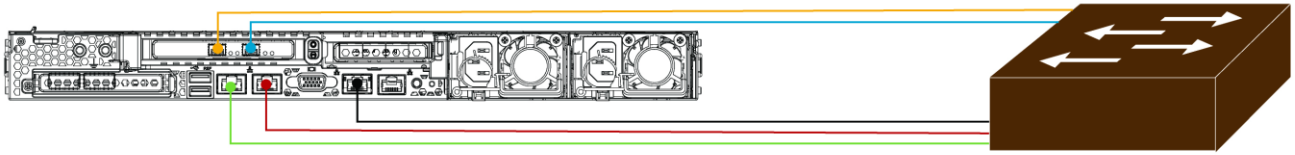
For Your Reference

Features	Hardware	Cisco SD-Access 1.3.0.2[3]	Cisco SD-Access 1.3.0.3[3]	Cisco SD-Access 1.3.0.4 / 1.3.0.5[3] (1.3.0.5 is Cisco Recommended Release for an Upgrade)	Cisco SD-Access 1.3.1.2 / 1.3.1.3[3]	Cisco SD-Access 1.3.1.4[3] (Cisco Recommended Release for New Deployments)
Management	Cisco DNA Center	Cisco DNA Center 1.3.0.2	Cisco DNA Center 1.3.0.3	Cisco DNA Center 1.3.0.4 / 1.3.0.5	Cisco DNA Center 1.3.1.2 / 1.3.1.3	Cisco DNA Center 1.3.1.4
Fabric Edge	Cisco Catalyst 9200 Series Switches including Cisco Catalyst 9200L Series Switches[5] (SD-Access Wireless not supported on 9200L series) (SD-Access Wireless supported on 9200 Series)	IOS XE 16.11.1c[3]	IOS XE 16.11.1c[3]	IOS XE 16.11.1c[3]	IOS XE 16.11.1c[3], IOS XE 16.12.1s[1,4]	IOS XE 16.11.1c[3], IOS XE 16.12.1s[1,4]
	Cisco Catalyst 9300 Series Switches (C9300-24T, C9300-24P, C9300-24U, C9300-24UX, C9300-48T, C9300-48P, C9300-48U, C9300-48UXM)	IOS XE 16.9.3s[1], IOS XE 16.11.1c[3], IOS XE 16.6.4a, IOS XE 16.6.4s, IOS XE 16.6.5, IOS XE 16.6.6, IOS XE 16.9.2s, IOS XE 16.9.3	IOS XE 16.9.3s[1], IOS XE 16.11.1c[3], IOS XE 16.6.4a, IOS XE 16.6.4s, IOS XE 16.6.5, IOS XE 16.6.6, IOS XE 16.9.2s, IOS XE 16.9.3	IOS XE 16.9.3s[1], IOS XE 16.11.1c[3], IOS XE 16.6.4a, IOS XE 16.6.4s, IOS XE 16.6.5, IOS XE 16.6.6, IOS XE 16.9.2s, IOS XE 16.9.3, IOS XE 16.9.4	IOS XE 16.9.3s[1], IOS XE 16.12.1s, IOS XE 16.11.1c[3], IOS XE 16.6.4a, IOS XE 16.6.4s, IOS XE 16.6.5, IOS XE 16.6.6, IOS XE 16.9.2s, IOS XE 16.9.3, IOS XE 16.9.4[1]	IOS XE 16.9.3s, IOS XE 16.12.1s, IOS XE 16.11.1c[3], IOS XE 16.6.4a, IOS XE 16.6.4s, IOS XE 16.6.5, IOS XE 16.6.6, IOS XE 16.9.2s, IOS XE 16.9.3, IOS XE 16.9.4[1]

https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/compatibility-matrix.html
https://content.cisco.com/compatibilitymatrix.html

Installation + first steps

Before you start the installation 1/3

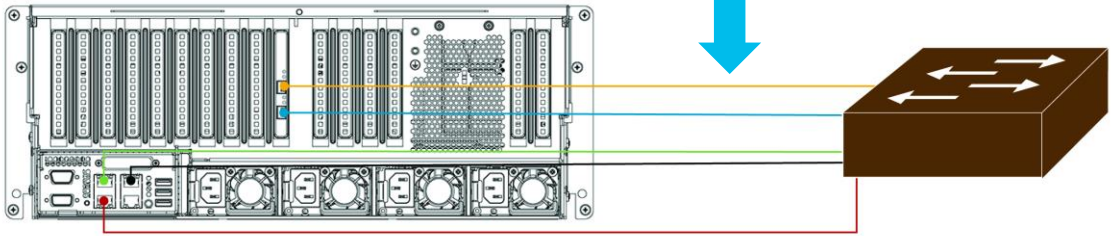


Legend

- 10 Gbps Enterprise Port (enp94s0f0, Network Adapter 3)
- 10 Gbps Cluster Port (enp94s0f1, Network Adapter 4)
- 1 Gbps/10 Gbps Management Port (1, eno1, Network Adapter 1)
- 1 Gbps/10 Gbps Cloud Port (2, eno2, Network Adapter 2
- 1 Gbps CIMC Port

DN2-HW-APL and DN2-HW-APL-L

DN2-HW-APL-XL



Legend

- 10-Gbps Enterprise Port (enp69s0f0, Network Adapter 3)
- 10-Gbps Cluster Port (enp69s0f1, Network Adapter 4)
- 1-Gbps/10-Gbps Management Port (1, enp53s0f0, Network Adapter 1)
- 1-Gbps/10-Gbps Cloud Port (2, enp53s0f1, Network Adapter 2)
- 1-Gbps CIMC Port (3)

439873

Before you start the installation 2/3

Enterprise Network – Interface that is connected to the Enterprise network

- Virtual IP
- All Cisco DNA appliances must be in the same subnet as the Cluster Virtual IP address (see below)

Intra Cluster Link – isolated network used for communication between the Cisco DNA Center cluster nodes

- Virtual IP
- Cluster subnet and Service subnet address pool – min. /21 subnet for each (recommended /20-/16)
  - Must conform with the IETF RFC 1918 or 6598
- The Cluster/Service subnet address pools cannot be changed after installation
- No other machines should be in this network
- Changing the intra-cluster link from one interface to another is not supported

CIMC – Management of the Cisco DNAC Appliance hardware (recommended)

Before you start the installation 3/3

Management – used for Cisco DNA Center management (optional*)

- Virtual IP

Cloud Update Connectivity – used to update the Cisco DNA Center software (optional *)

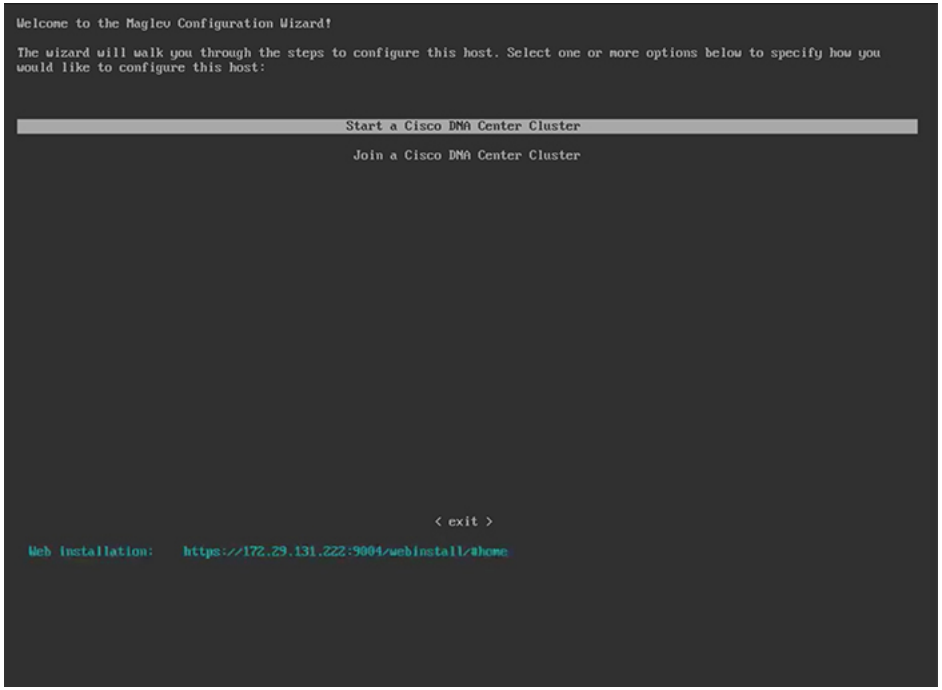
- Virtual IP

*Required only if the Management network and/or the Cloud Update server is not reachable via the Enterprise Network

- **Additional Settings needed**
  - DNS Server IP Address (1 required, 2+ recommended)
  - NTP Server IP Address (1 required, 2+ recommended)
  - Optional Proxy Server IP Address (required if direct internet access is not available – http proxy only)

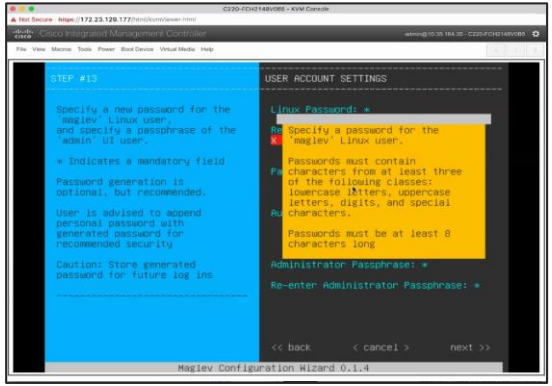
Installation – Let's get started!

- Cluster installation <u>only</u> (new / join)
- Straight forward but takes a little bit

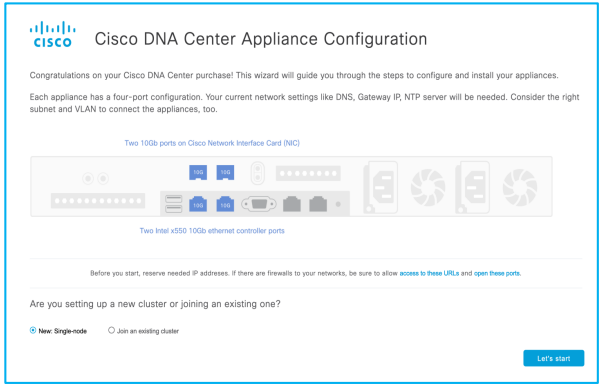


Installation – Let's get started!

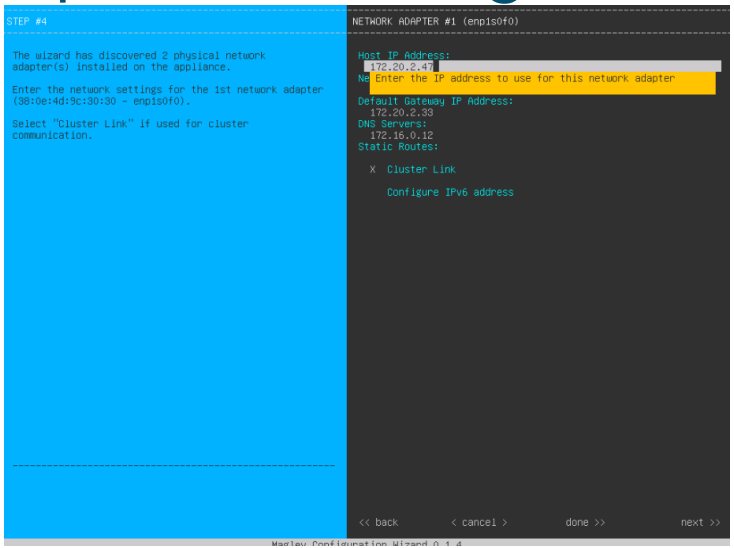
Option 1
Maglev Wizard



Option 2
Browser-Based Wizard



Installation – Option 1 – Maglev Wizard



CISCO
DNA Center
Design, Automate and Assure your Network

Config Wizard:

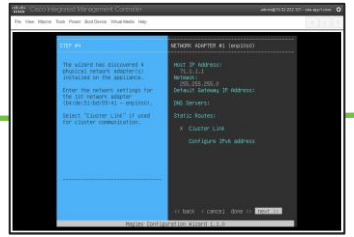
Boot → Enter IP addresses → Change Credentials → Add NTP Server → Finalize Installation ✓

- Enter IP addresses: Enter Cisco DNA Center IP and the other required IPs
- Change Credentials: Shell and UI Username and PWD plus CCO login for update
- Add NTP Server: Enter NTP & DNS Server IP (mandatory!)
- Finalize Installation: Finalize installation and bring up controller

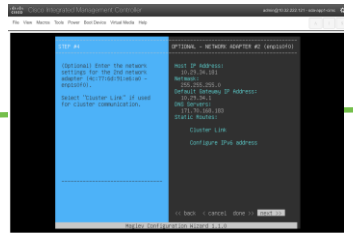
Installation – Option 1 – Maglev Wizard

For Your Reference

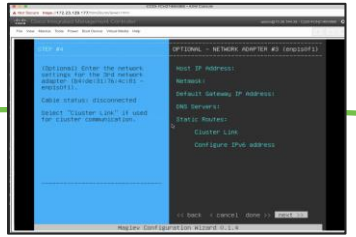
Startup Screen



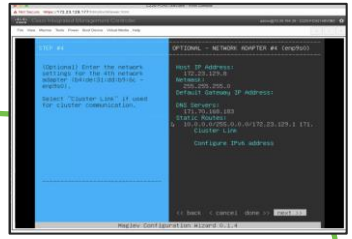
Enterprise NIC Setup



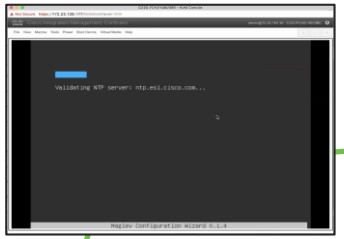
InterCluster NIC Setup



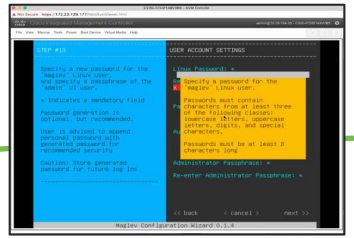
Mgmt. NIC Setup



DMZ NIC Setup

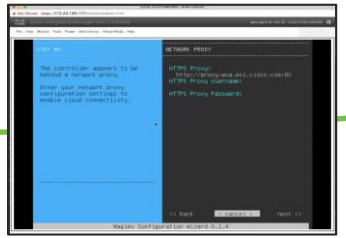


NTP and Cluster Verifications

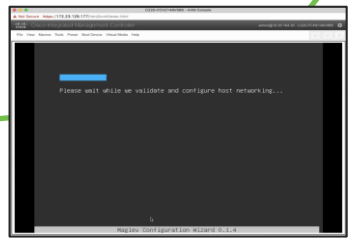


Cluster Settings

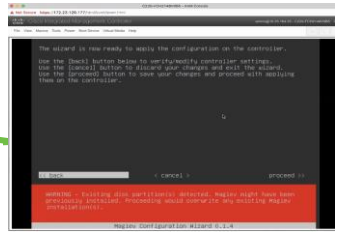
Cluster Settings



Proxy Settings



Host networking verification



Commit for Install

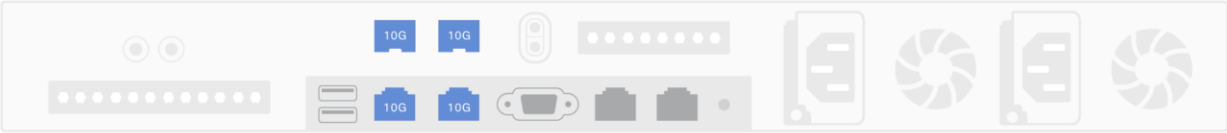
Installation – Option 2 – Browser-Based Wizard

Cisco DNA Center Appliance Configuration

Congratulations on your Cisco DNA Center purchase! This wizard will guide you through the steps to configure and install your appliances.

Each appliance has a four-port configuration. Your current network settings like DNS, Gateway IP, NTP server will be needed. Consider the right subnet and VLAN to connect the appliances, too.

Two 10Gb ports on Cisco Network Interface Card (NIC)



Two Intel x550 10Gb ethernet controller ports

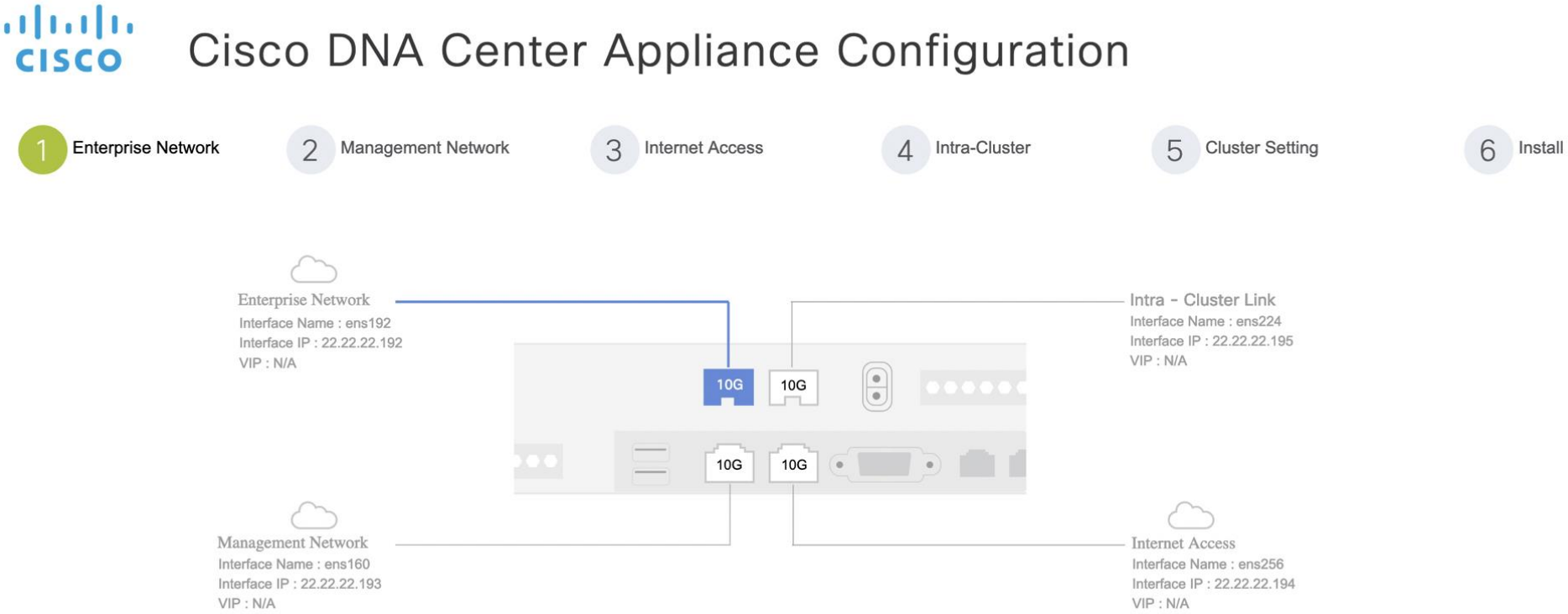
Before you start, reserve needed IP addreses. If there are firewalls to your networks, be sure to allow access to these URLs and open these ports.

Are you setting up a new cluster or joining an existing one?

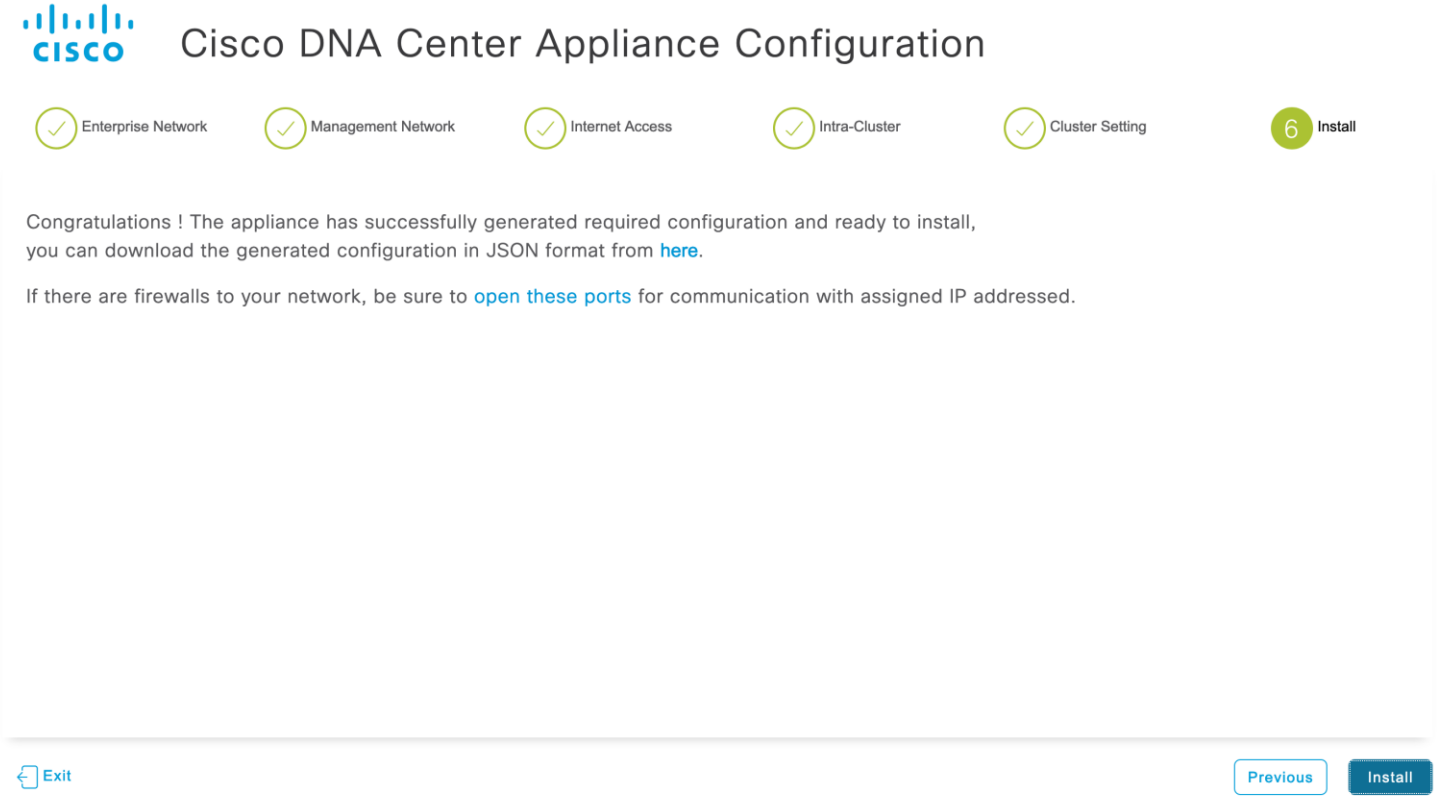
- (•) New: Single-node
- ( ) Join an existing cluster

Let's start

Installation – Option 2 – Browser-Based Wizard



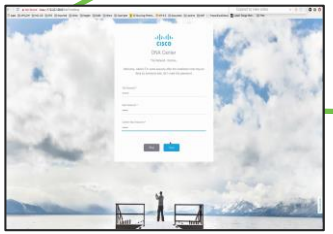
Installation – Option 2 – Browser-Based Wizard



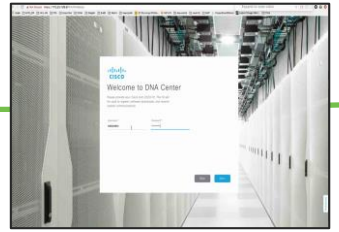
Day 0 setup after installation

For Your Reference

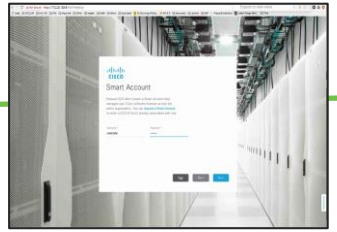
After-Installation



Register CCO



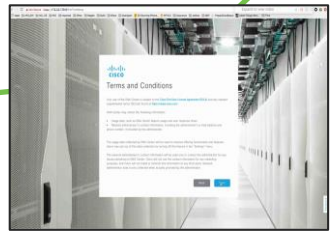
Setup Smart Account



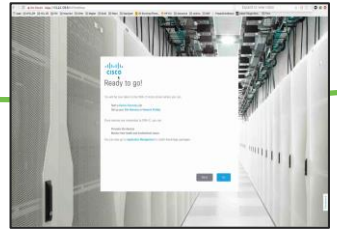
IPAM Setup

Proxy Setup

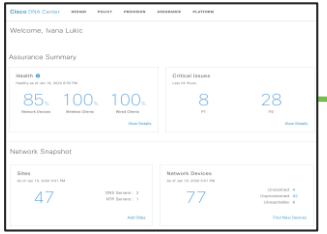
EULA Acceptance



Final confirmation

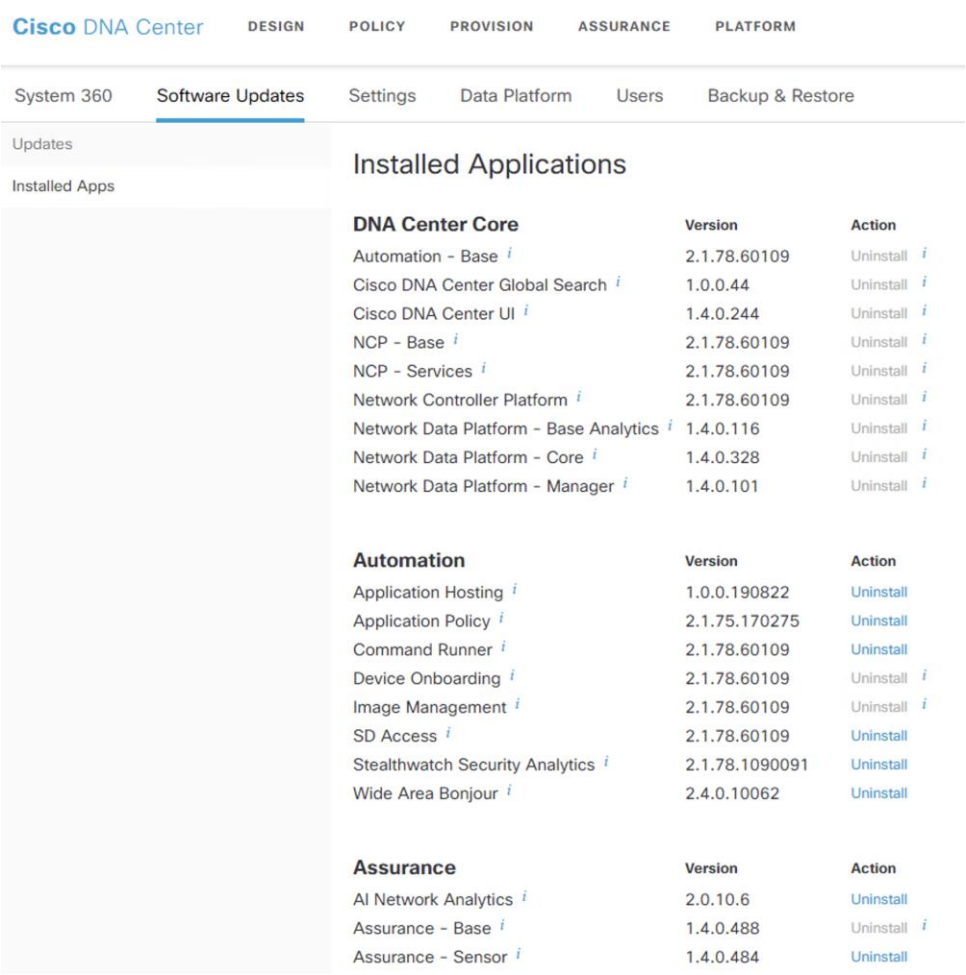


Login to DNAC Homepage



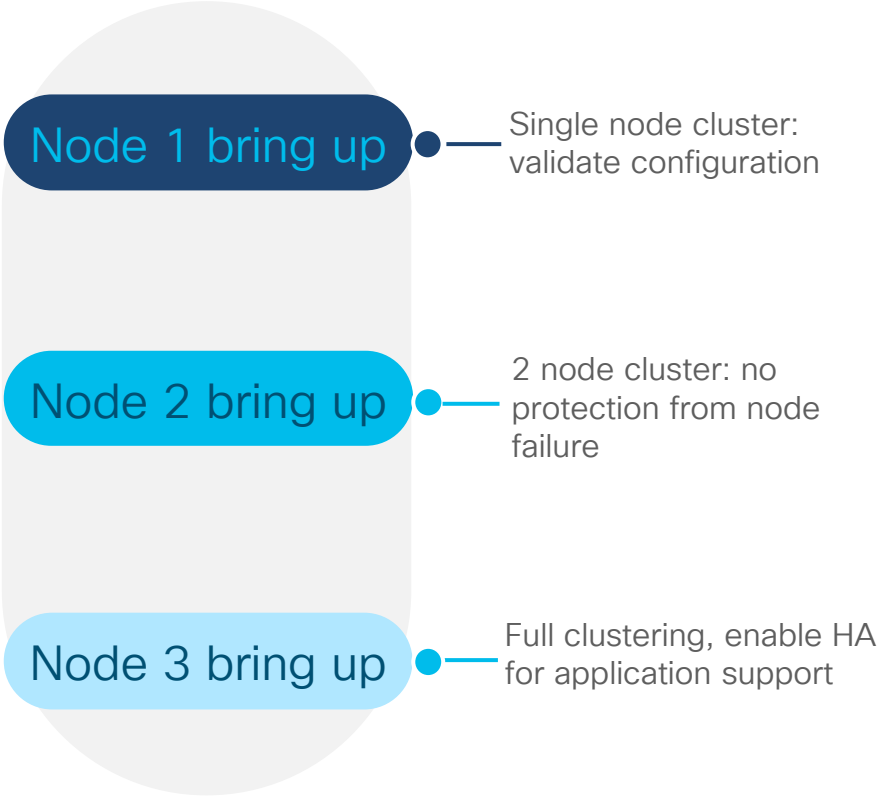
Installation = DONE

- On 1.3.1, 13 packages are not directly installed
  - SD-Access
  - Assurance – Sensor
  - Automation – Sensor
  - Application Policy
  - Command Runner
  - Cisco DNA Center Platform
  - etc.

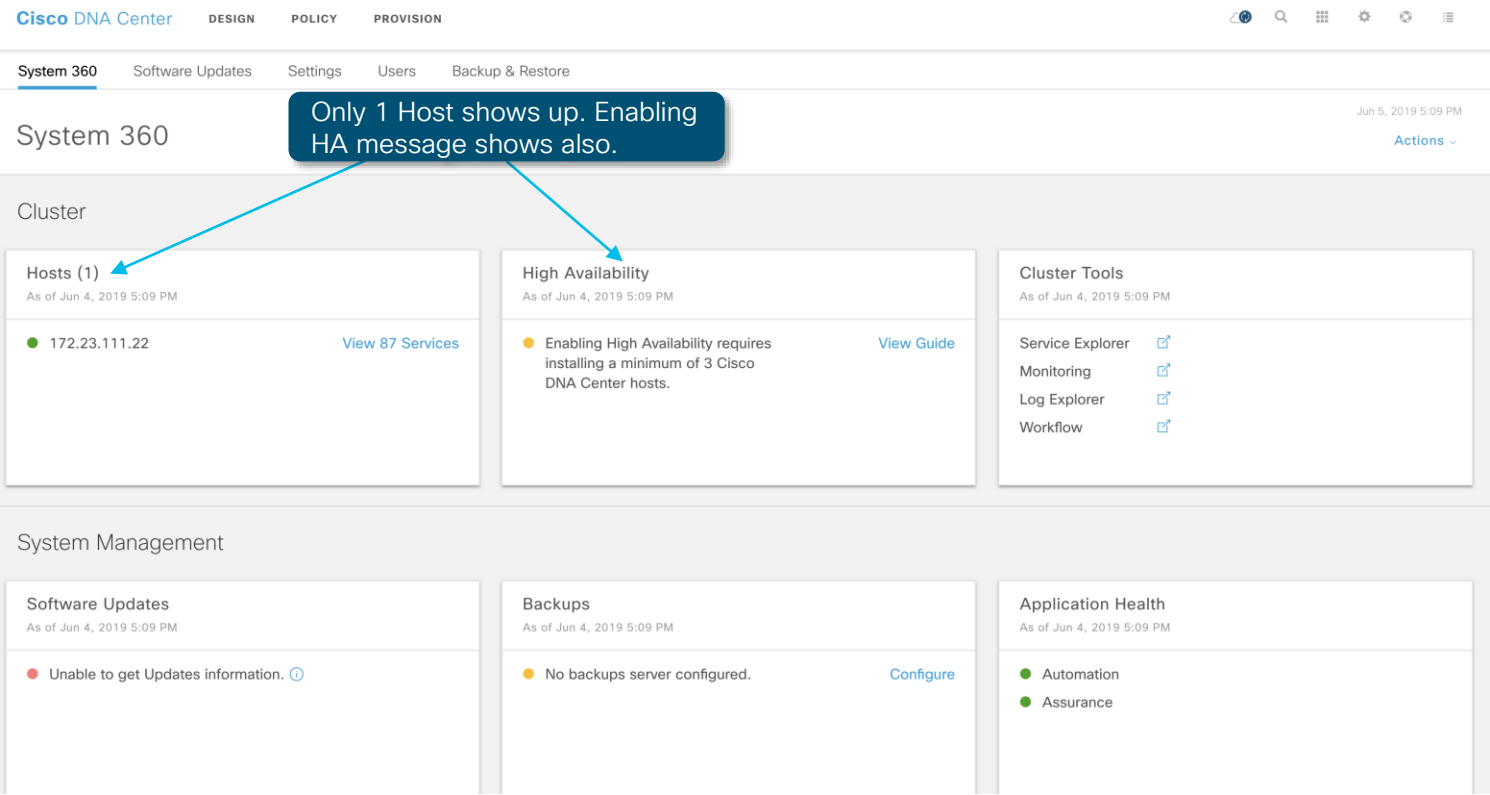


Installation – 3 Node Cluster

- Bring up first node: choose “create a cluster”
- Bring up the second node: Choose “join cluster”
- Afterwards bring up the third node the same way
- Remember 2-node Cisco DNA Center cluster cannot withstand a node failure (One node crash will lead to stall of the other node)



Cisco DNA Center settings without HA



Cisco DNA Center settings without HA

Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

System 360 | Software Updates | Settings | Data Platform | Users | Backup & Restore

System 360

Cluster

Hosts (3)
As of Jun 4, 2019 5:00 PM

- 192.192.192.222 — View 120 Services
- 192.192.192.224 — View 5 Services
- 192.192.192.226 — View 5 Services

High Availability
As of Jun 4, 2019 5:00 PM

- Your system meets the requirements for High Availability. — Activate HA

Cluster Tools
As of Jun 4, 2019 5:00 PM

- Service Explorer
- Monitoring
- Log Explorer
- Workflow

System Management

Software Updates
As of Jun 4, 2019 5:01 PM

- Connected to Cisco's software server.
- 3 Application Updates available. — View

Backups
As of Jun 4, 2019 5:01 PM

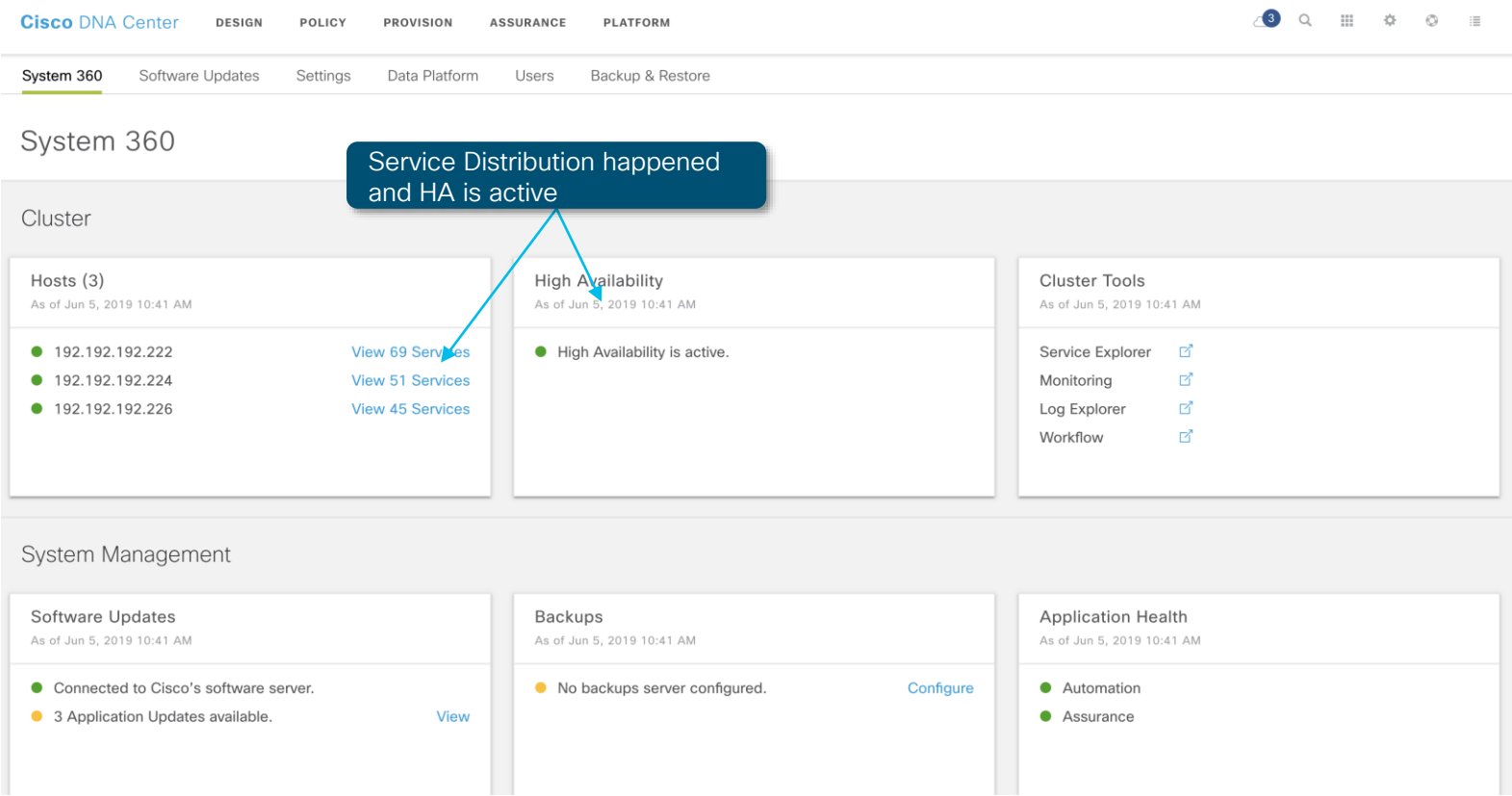
- No backups server configured. — Configure

Application Health
As of Jun 4, 2019 5:01 PM

- Automation
- Assurance

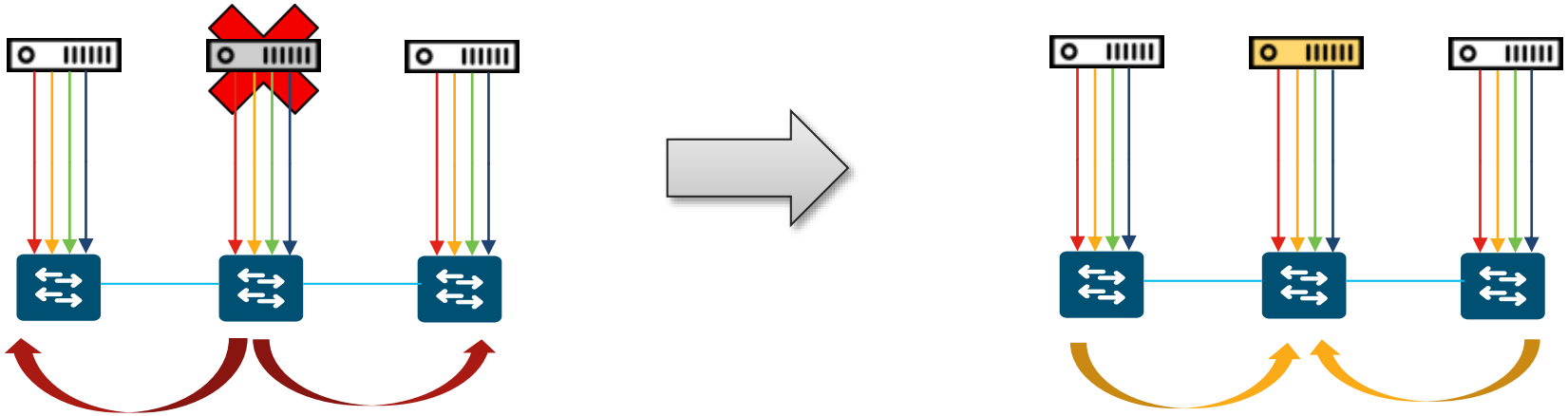
Activate HA shows up after the three nodes are installed

Cisco DNA Center settings with HA



Cisco DNA Center behavior on node failure

For Your Reference



Node fails, automation services are automatically distributed	Current re-distribution takes 15 minutes	Node failure restore (RMA) will require re-distribution of services. Needs 15 minutes – can be planned outage	Link failure - no significant delay in redistribution of services when link comes back up	Failure of two nodes will bring the cluster down

External Connectivity Requirements

For Your Reference

The following URLs need to be accessible from the Cisco DNA Center for various operations

External Connections	URLs
Cisco DNA Center Update package downloads	https://*.ciscoconnectdna.com/*
Smart Account and SWIM Software Downloads	https://*.cisco.com/*
Rendering Geo-Maps on the Cisco DNA Center UI	https://*.tiles.mapbox.com/*
Meraki Integration	https://*.meraki.com/
IPAM Integration	URL for the IPAM-server
User feedback	https://dnacenter.uservoice.com/

Internal Connectivity Requirements

For Your Reference

Ports to be open on Firewalls

For IPs connected to your Enterprise Network:

SFTP: in TCP 22

NTP: in UDP 123, out the same

SNMP: in UDP 162, out UDP 161

SCEP: in TCP 16026

DNS: out UDP 53

Telnet: out TCP 23

For IPs connected to your Management Network:

SSH: in TCP 2222, out TCP 22

HTTP: in TCP 80

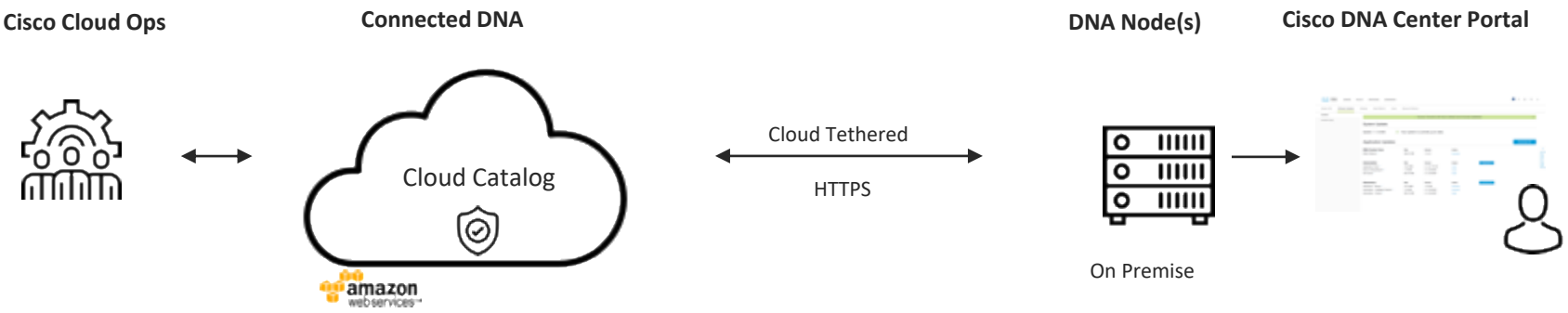
For IPs connected to your Internet Access:

HTTPS: in TCP 443, out the same

- Ensure that these ports are open for traffic flows to and from the appliances.
- Additional ports, protocols, and types of traffic must be accommodated if you are deploying the appliance in a network that employs SDA infrastructure.

Note:
For the detailed list of the required ports/protocols visit:
http://cs.co/dnac_required_ports

Cisco DNA Center Software Updates Workflow



Cisco Cloud Ops pushes packages to cloud catalog

Packages available in cloud catalog. Push Notification to users.

Secure connection from Cisco DNA Center on-premise to Connect DNA Cloud [via Https (Port 443)]

Available updates are displayed in the Cisco DNA Center Packages & Updates page. User downloads the packages to upgrade

Dedicated Cisco cloud ops team for continuous monitoring

Approved by Cisco Security and Trust Organization and Ongoing penetration testing and remediation process in place

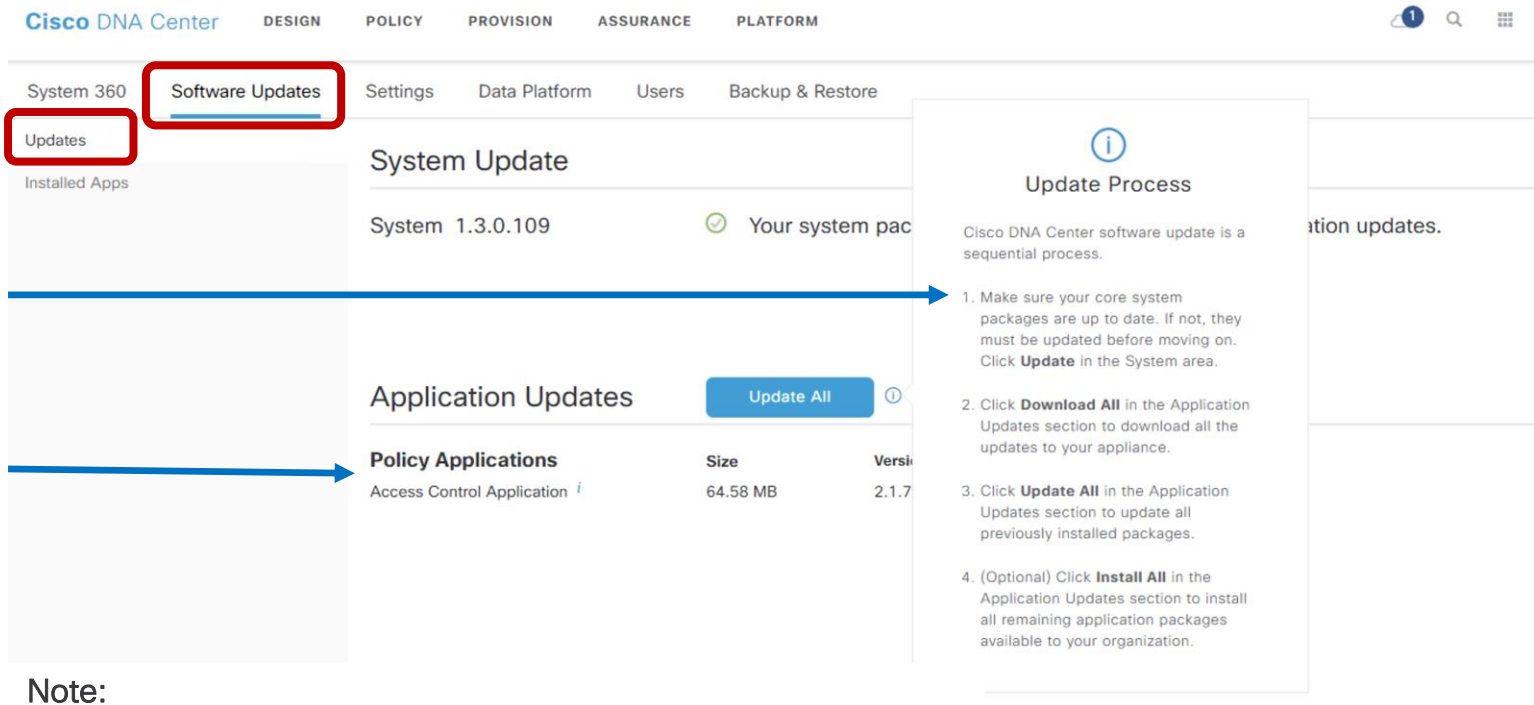
Integrated with CDN service for faster downloads geographically

Connectivity to the Cisco Cloud is required for DNA Center software updates. New releases are available approximately once in 2-4 weeks

Update Management

Update Process

Available Update



Note:

Subsequent upgrades done via cloud tethering

Proxy configuration available

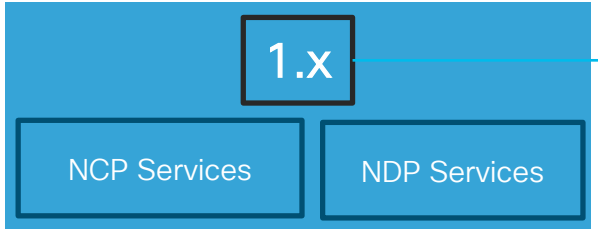
Cisco DNA Center – Release Versioning

Cloud Tethering for ease of adoption of Patch and Minor Releases

Cisco DNA Center App version

- App Numbering can be independent of the platform
- Dependent apps will be automatically updated

Cisco DNA Center version



- Shown in **About screen** and used in **marketing collateral**
- Cisco DNA Center components will share first two version identifiers
- Visible in App/ Services management page

Full version format

1.x.y.build#

Major version — Minor release — Patch release

NCP: Network Controller Platform Service
NDP: Network Data Platform Service

Role Based Access Control – RBAC

Telemetry	Internal use only
Observer Admin	Provides primarily read-only privileges to all Cisco® DNA Center resources
Network Admin	Similar to System Admin Role but with no access to DNA Center Admin settings (add/delete users etc.)
Super Admin	Provides full administrative privileges to all Cisco® DNA Center resources

RBAC – Roles and Privileges

For Your Reference

Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

System 360 | Software Updates | Settings | Data Platform | Users | Backup & Restore

Users - Role Based Access Control

- Change Password
- User Management
- Role Based Access Control
- External Authentication

Role based access control

NETWORK-ADMIN-ROLE See details >

NETWORK-ADMIN-ROLE

12 user(s) have this role in your network

OBSERVER-ROLE See details >

OBSERVER-ROLE

10 user(s) have this role in your network

SUPER-ADMIN-ROLE See details >

SUPER-ADMIN-ROLE

4 user(s) have this role in your network

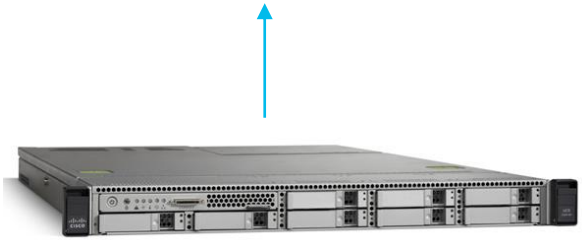
TELEMETRY-ADMIN-ROLE See details >

TELEMETRY-ADMIN-ROLE

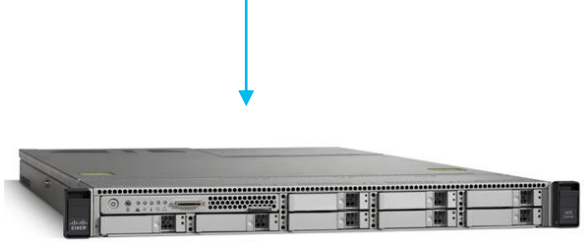
0 user(s) have this role in your network

Backup and Restore Procedure

Backup from Master



Restore to Standby



- Backup and restore Automation data using UI
- Backup and restore Assurance data using UI

Note: The backup and restore node/ cluster should be running ***the same software version***

Backup and Restore Procedure

For Your Reference

Scenarios for backup and restore procedures for Cisco DNA Center:

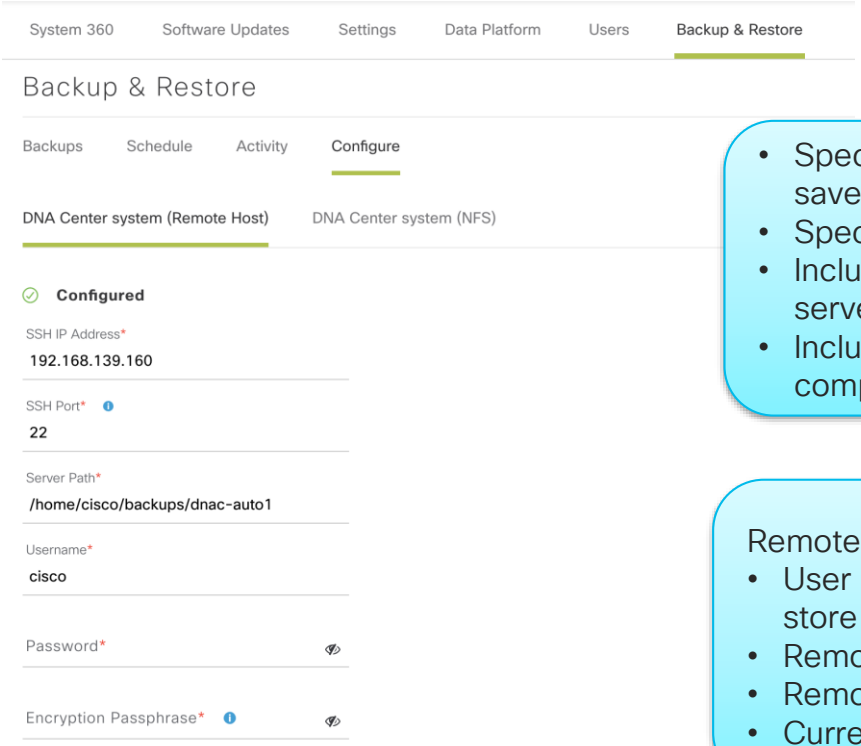
- To create backup files for disaster recovery for the appliance
- To create backup files to restore to a different appliance (if required for your network configuration)

- During backup, Cisco DNA Center creates a copy of the following files and exports the files to a specific location on a remote server:
  - Cisco DNA Center databases
  - Cisco DNA Center credentials
  - Cisco DNA Center file system and files

- During restore, Cisco DNA Center removes and replaces the existing database and files with the backup files.
- Cisco DNA Center is unavailable during restore
- You can restore a backup to a Cisco DNA Center system with a different IP address. This could happen if for any reason the IP address is changed on Cisco DNA Center and you need to backup from an older system

Configuring Backup

For Your Reference



- Specify the address and port to the server you wish to save the backup file to.
- Specify the path on the server to save the backup.
- Include the username and password to SSH into your server.
- Include an encryption passphrase to encrypt sensitive components of your backup.

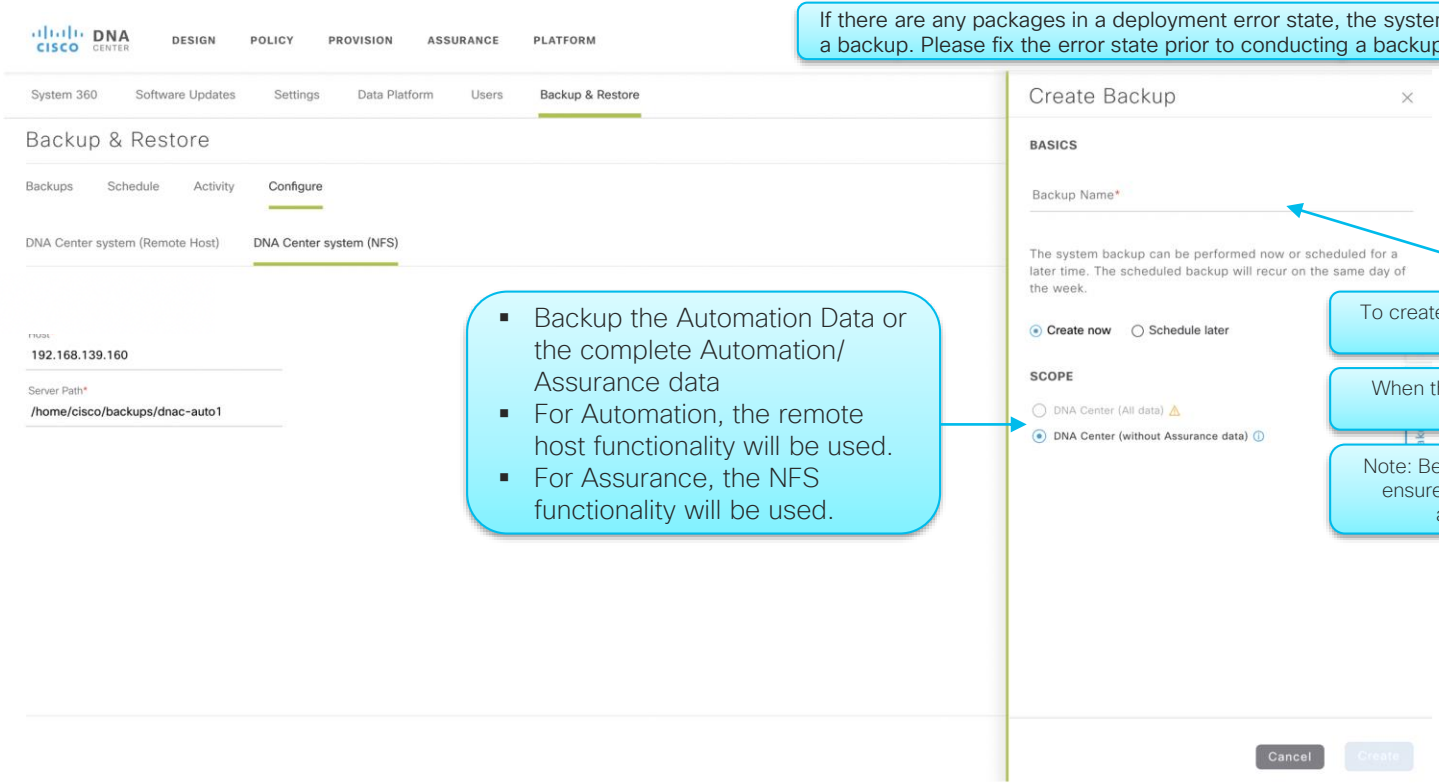
Remote Server Requirements:

- User must have their own external remote server to store backup files.
- Remote server must have ssh and sftp enabled.
- Remote server must have rsync installed.
- Currently must be Linux based remote server.

Create a backup using UI

For Your Reference

If there are any packages in a deployment error state, the system will not allow to start a backup. Please fix the error state prior to conducting a backup.



- Backup the Automation Data or the complete Automation/ Assurance data
- For Automation, the remote host functionality will be used.
- For Assurance, the NFS functionality will be used.

To create a backup now, enter in a backup name.

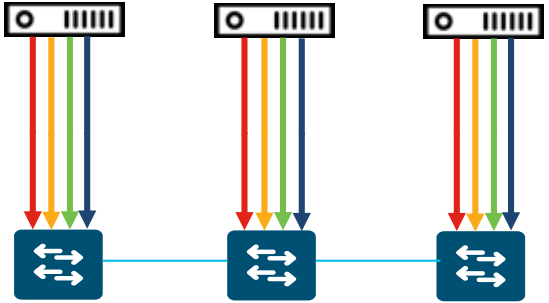
When the name is entered, the "Create" button will fill.

Note: Before conducting a backup, please ensure you have adequate disk space allocated for your backup.

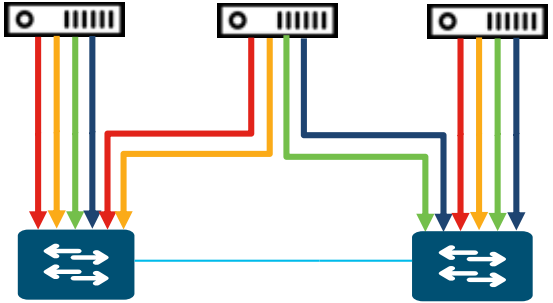
Design Considerations

High Availability Deployment Scenarios

Cabling up Cisco DNAC clusters to Top of Rack or Access Switches



Recommended



Two Switches: Single point of failure for Cisco DNAC

Enterprise Interface

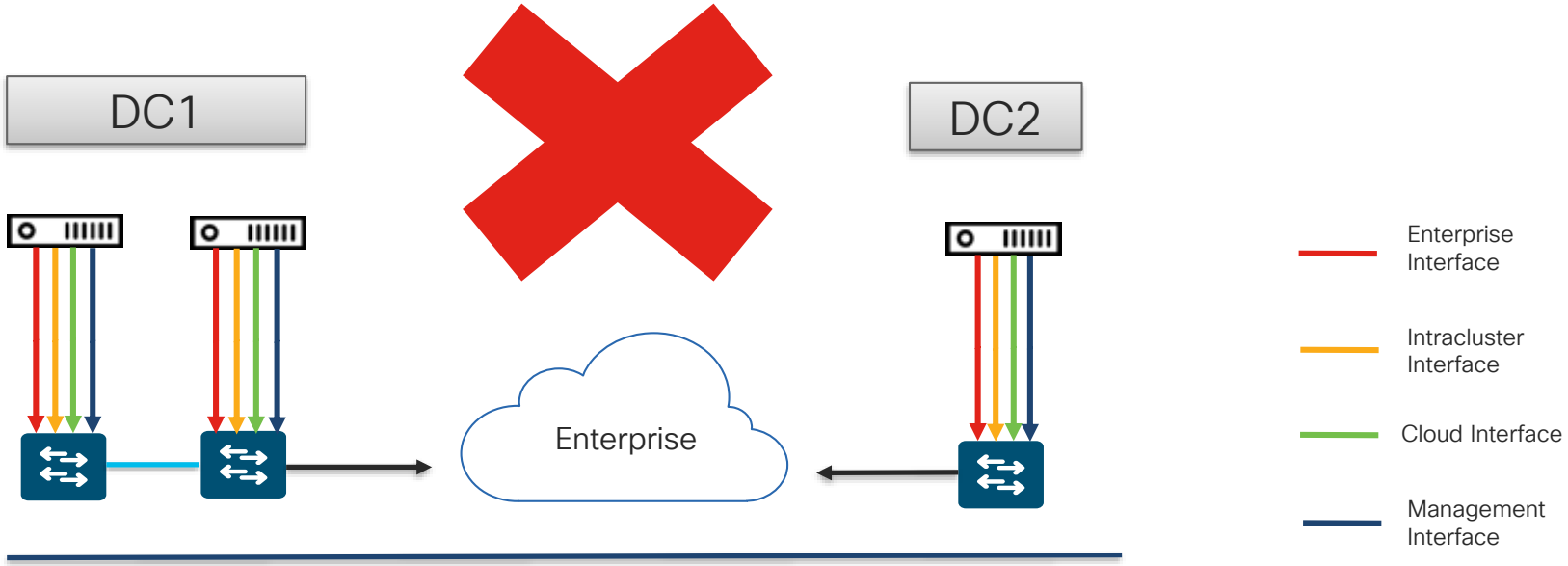
Intracluster Interface

Cloud Interface

Management Interface

High Availability Deployment Scenarios

Multi DC



Cisco DNA Center Design Considerations

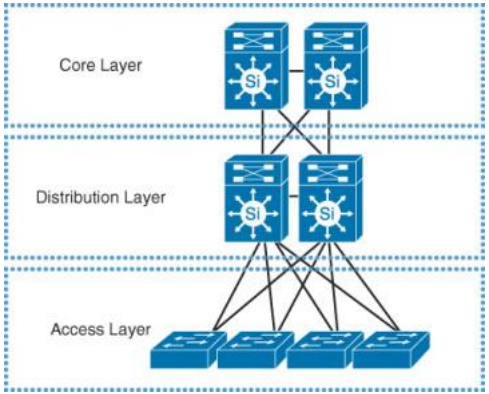
- Number of devices / APs (see the scaling guide)
- One Cisco DNA Center can manage several sites
  - Maybe more than 1 cluster is needed
- Latency
  - <10ms Cisco DNA Center Cluster Links
  - No support of physically distributing the cluster
  - Same subnet for all appliances
  - 200ms RTT to the Network Devices
- Check about
  - SD-A requirements
  - Applications used
  - Number of users
  - Number of config changes / IOS Updates

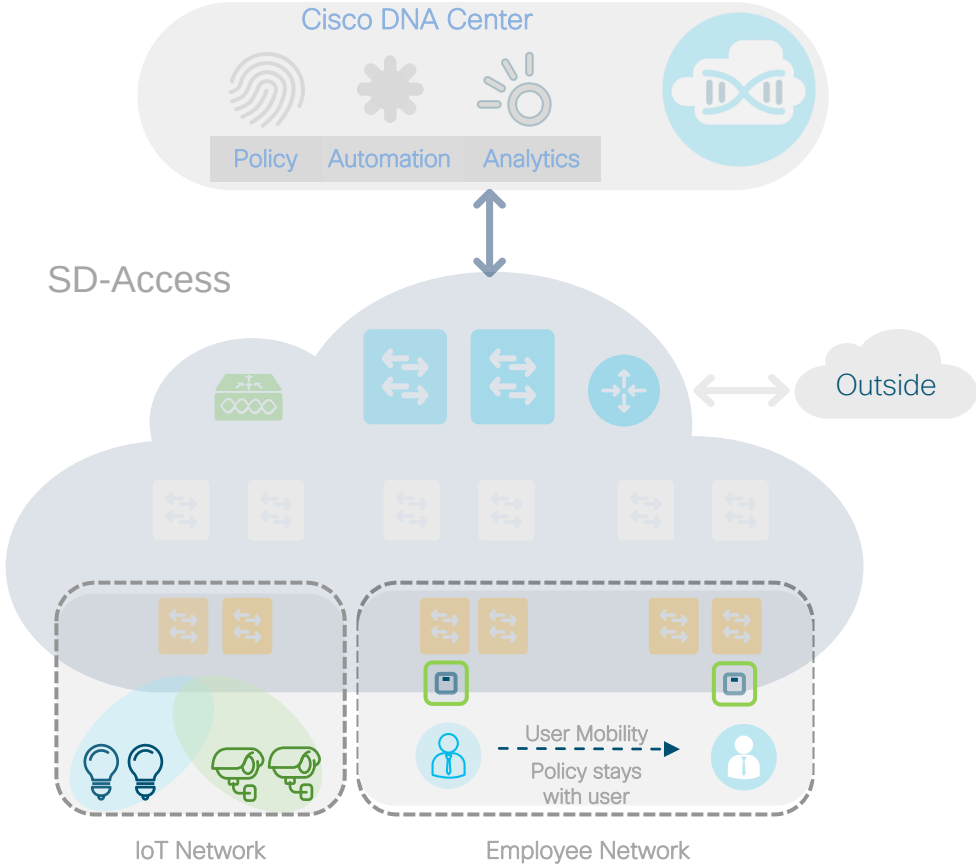
Agenda

- Cisco DNA Center 10 minutes overview
- Before you deploy – purchase and design considerations
- **Base automation for wired and wireless**
- Getting started with Cisco SD-Access
- Assurance and application policies
- Key takeaways

What can I do with Cisco DNA Center to automate a traditional wired network?

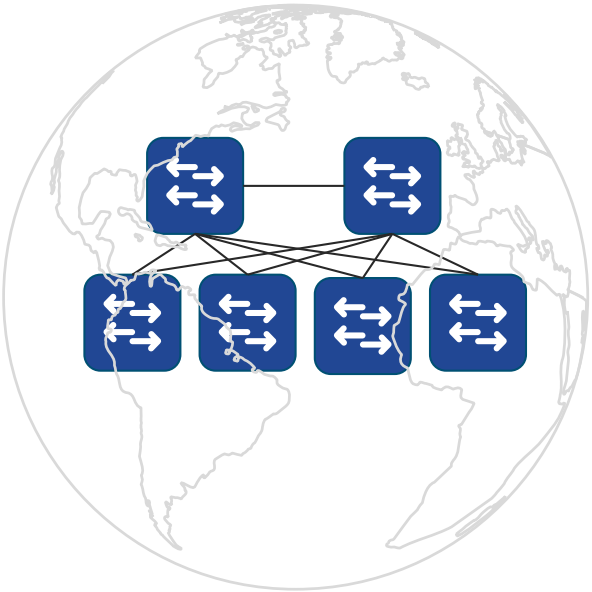
Classic Design





Base Automation

- Design
  - Network Hierarchy
  - Network Settings
  - Network Profiles
- Populate device inventory
- Provision



Design matches network management BCP

Facts

Network Managed by Regions / Areas

Multiple Network Operations Team

Collocated Network Services

Differences in Network Designs

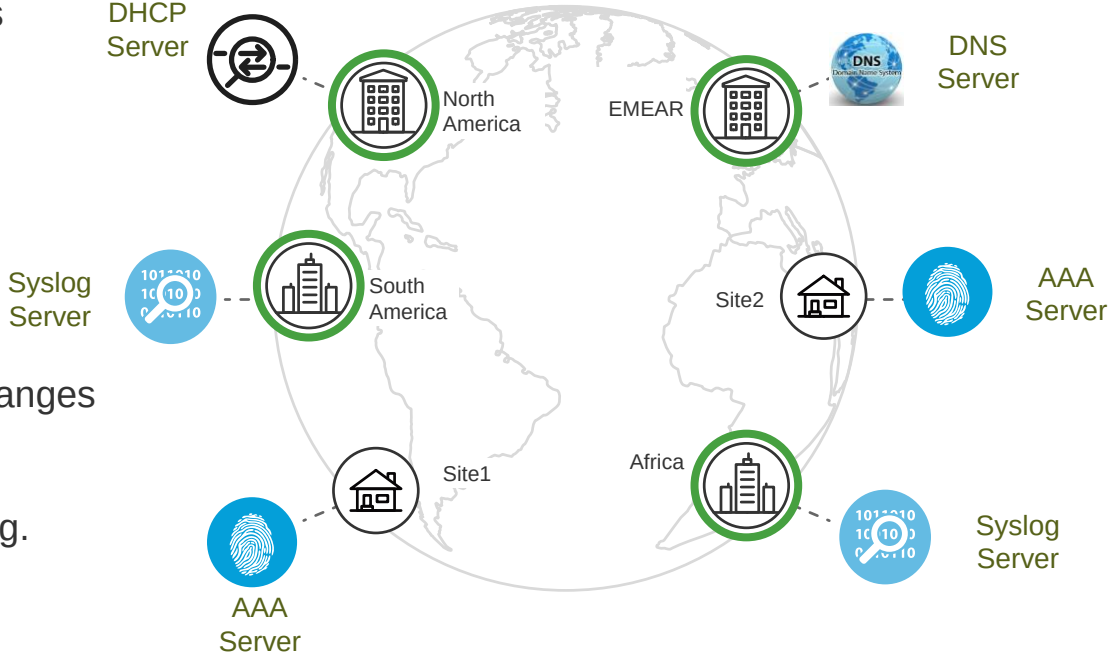
Key Challenges

Minimize error prone configuration changes

Automate roll out of regional changes

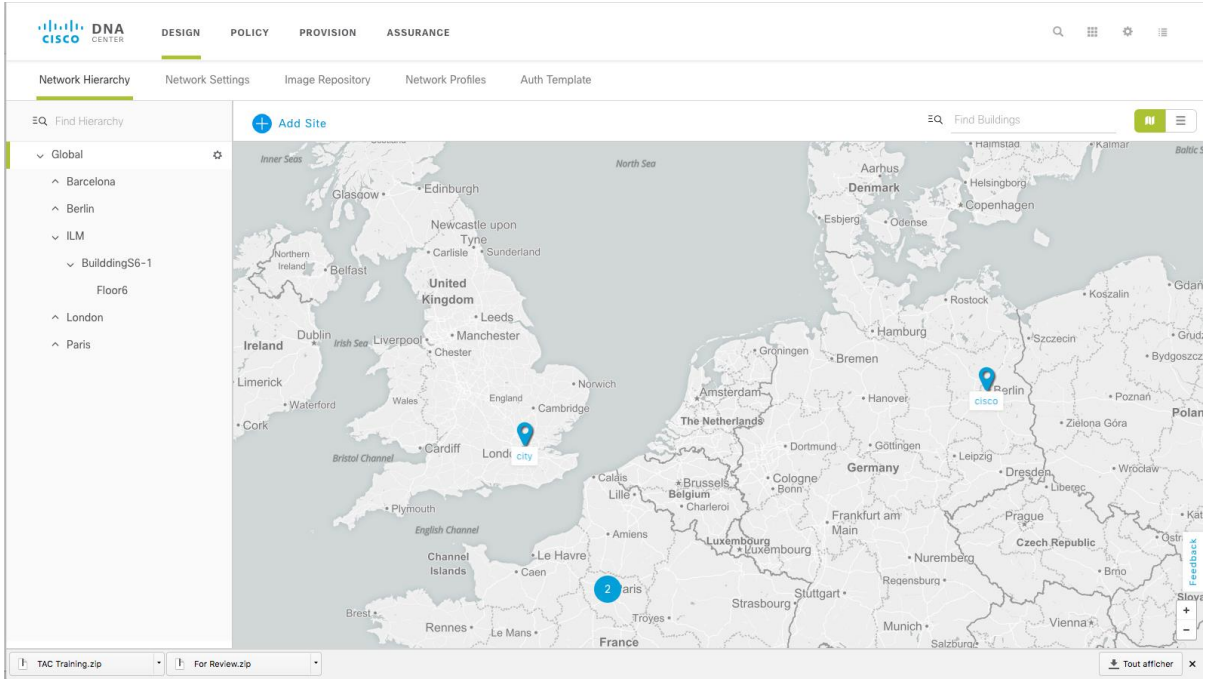
Adhere to compliance standards for eg. password changes

Allocation of IP address pools



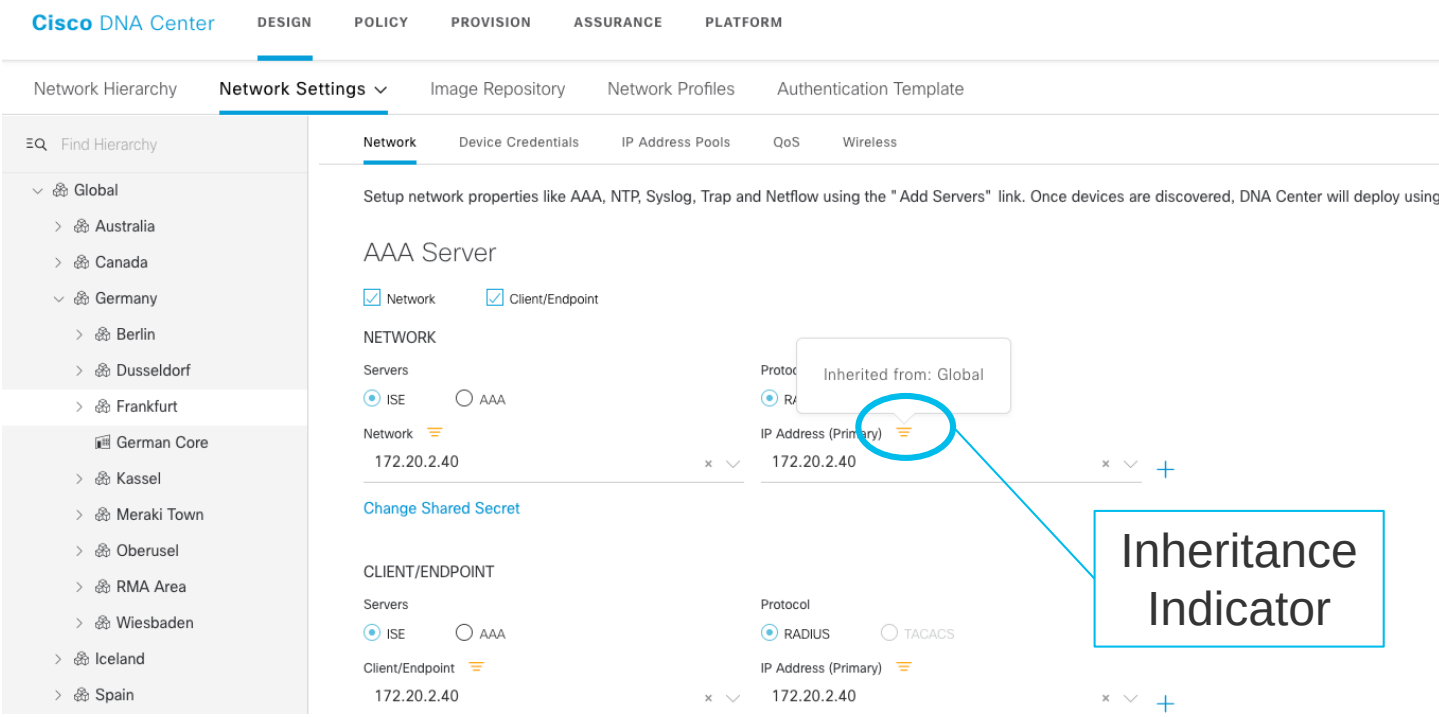
Design Network Hierarchy

- Hierarchy consists of areas, buildings, and floors
- “Global” area on top of hierarchy
- Areas can contain other areas or buildings
- Buildings have geo-location (based on [www.mapbox.com)](http://www.mapbox.com)
- No need to enter GPS coordinate, only postal address
- Buildings can contain floors (mandatory for wireless / see later)



Automate Roll Out of Regional Changes

- AAA/ISE servers for network and client endpoints
- DHCP, DNS, NTP servers
- Syslog, Netflow & Trap collectors
- Message of the Day
- TimeZone
- Device Credentials
- All Properties Inherited and can be Overridden at Sites/Building



Cisco DNA Center – ISE pxGrid client

Edit AAA/ISE server

Device re-provision required to get the edited changes reflected on to the devices.

1

Server IP Address*
172.20.2.40

Shared Secret*
••••

Cisco ISE server

Username*
admin

Password*
••••

FQDN*
ISESDA-1a.fra-lab.net

Subscriber Name*
dnacr3

SSH Key

Virtual IP Address(es)

View Advanced Settings

Cancel | Apply

2

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | Threat Centric NAC

Click here to do wireless setup a

All Clients | Web Clients | Capabilities | Live Log | Settings | Certificates

Enable | Disable | Approve | Group | Decline | Delete | Refresh | Total Pending Approval(1)

1 selected item 1 - 5 of 5

Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
ise-mnt-ise-sda-pod7		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Administrator	Certificate	View
ise-admin-ise-sda-pod7		Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Administrator	Certificate	View
ise-bridge-ise-sda-pod7		Capabilities(0 Pub, 5 Sub)	Online (XMPP)	Administrator	Certificate	View
					Certificate	View
dnac-pod7		Capabilities(0 Pub, 0 Sub)	Pending	Session	Certificate	View

3

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | Threat Centric NAC

All Clients | Web Clients | Capabilities | Live Log | Settings | Certificates

Enable | Disable | Approve | Group | Decline | Delete | Refresh | Total Pending Approval(0)

Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method
ise-mnt-ise-sda-pod7		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Administrator	Certificate
ise-admin-ise-sda-pod7		Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Administrator	Certificate
ise-bridge-ise-sda-pod7		Capabilities(0 Pub, 5 Sub)	Online (XMPP)	Administrator	Certificate
ise-pubsub-ise-sda-pod7		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate
dnac-pod7		Capabilities(0 Pub, 3 Sub)	Online (XMPP)	Session	Certificate

Authentication and Policy Servers

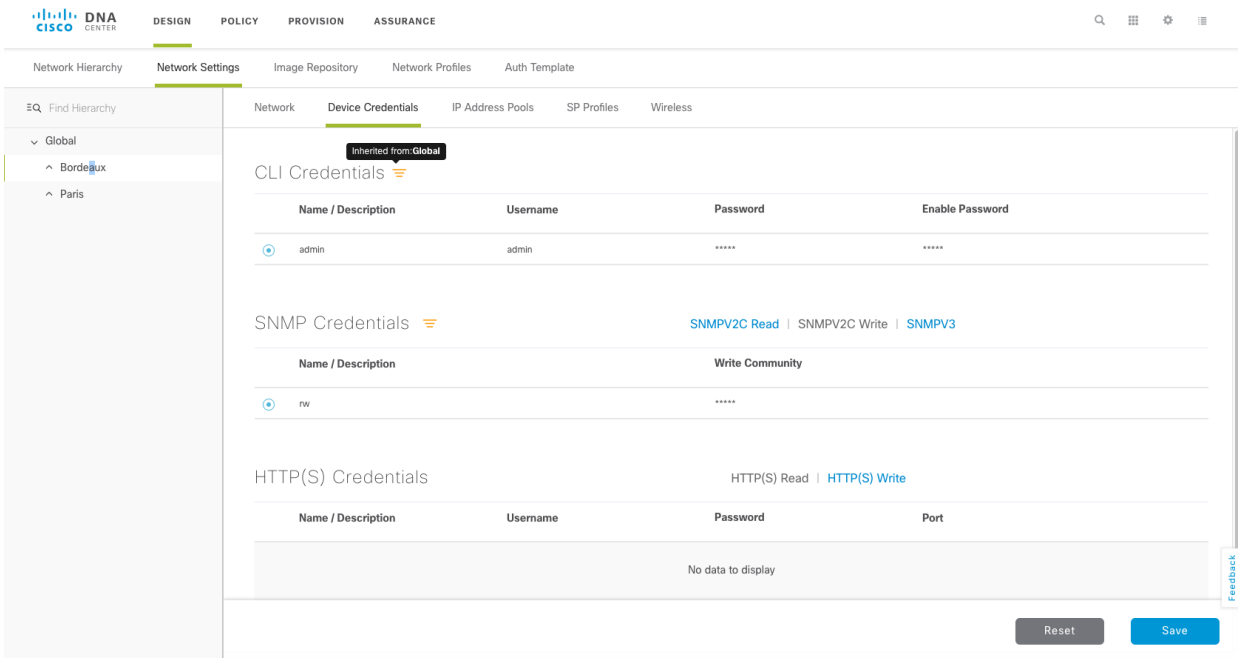
Use this page to specify the servers that authenticate DNA Center users. ISE servers can also supply policy and user information.

Last updated: 1:04 pm | Refresh | Export | Add

IP Address	Protocol	Type	Status
192.168.40.177	RADIUS	ISE	ACTIVE

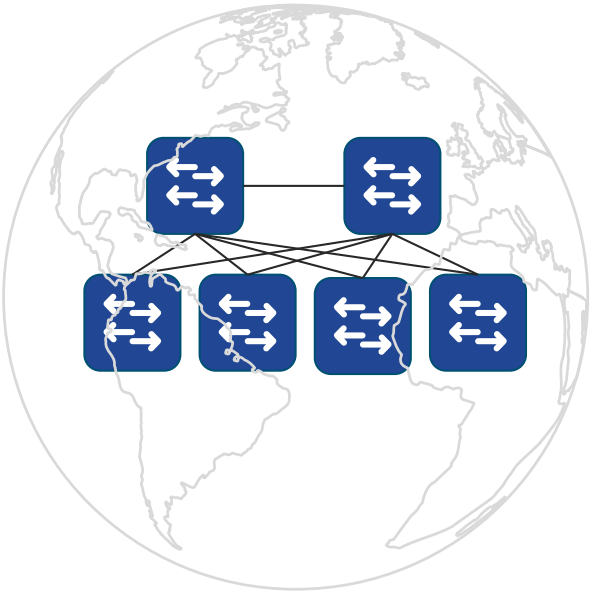
Device Credentials

- Defined Globally and Inherited
- CLI credentials
- SNMP V3 and V2C
- HTTP(S) Credentials. Mandatory for Enterprise NFV



Base Automation

- Design
- Populate device inventory
  - Device Discovery
  - Device Addition
  - Inventory Data Collection
- Provision



Network Discovery

Tools

Discovery

Automate addition of devices to controller inventory

Inventory

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

Visualize how device

Command Runner

Allows you to run diagnostic CLIs against one or more devices

License Manager

Visualize and manage license usage

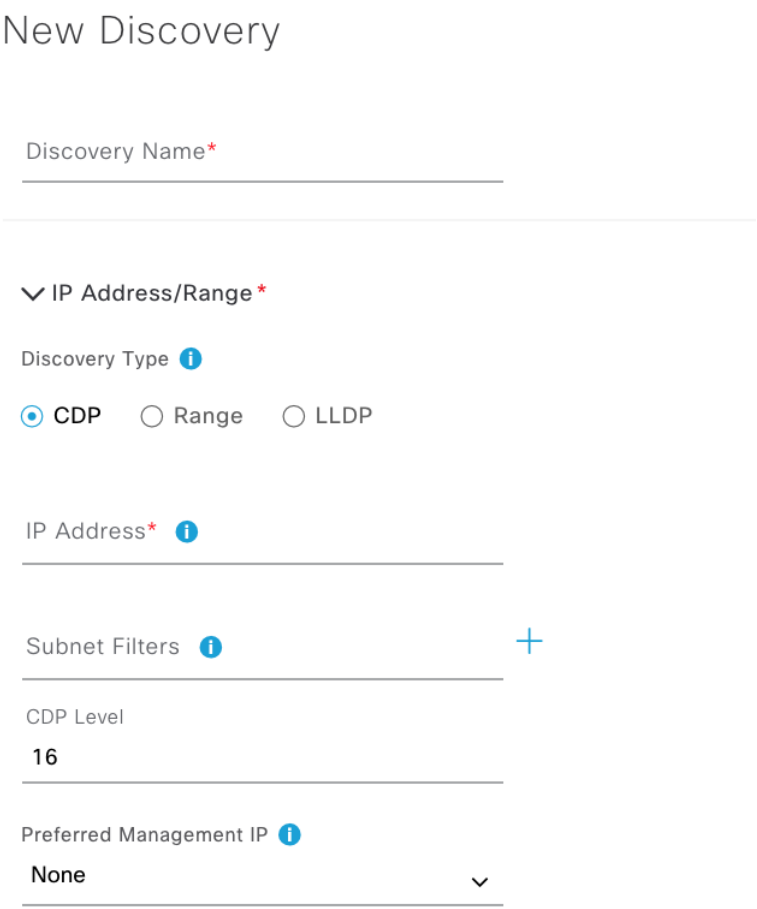
T

An interactive

Network Discovery

- Discover and manage your existing network
- CDP / LLDP (Using a seed Device) or IP Range Based Discovery
- Option to choose the “Loopback IP” as the Management IP
- Successfully discovered device is added to inventory for data collection

** Device can also be added via Bulk Import using CSV directly from Inventory tool*



Discoveries

Search by Device IP

MasterEN
Range 10.0.255.1-10.0.255.9 ..
10

MasterEN

Delete | Clone | Edit | Start

Complete 10

DISCOVERY DETAILS

CDP LEVEL	PROTOCOL ORDER	RETRY COUNT
None	ssh	3
TIMEOUT	**IP RANGE**	**IP FILTER LIST**
5	10.0.255.1-10.0.255.9 10.0.192.1-10.0.192.1	None
PREFERRED MANAGEMENT IP		
Use LoopBack		

CREDENTIALS

HISTORY

Showing last 1 run

#	Status	Devices	Start Time	Duration
1	Completed		Today at 1:41 PM	00:00:32

Devices

LIST | CHART

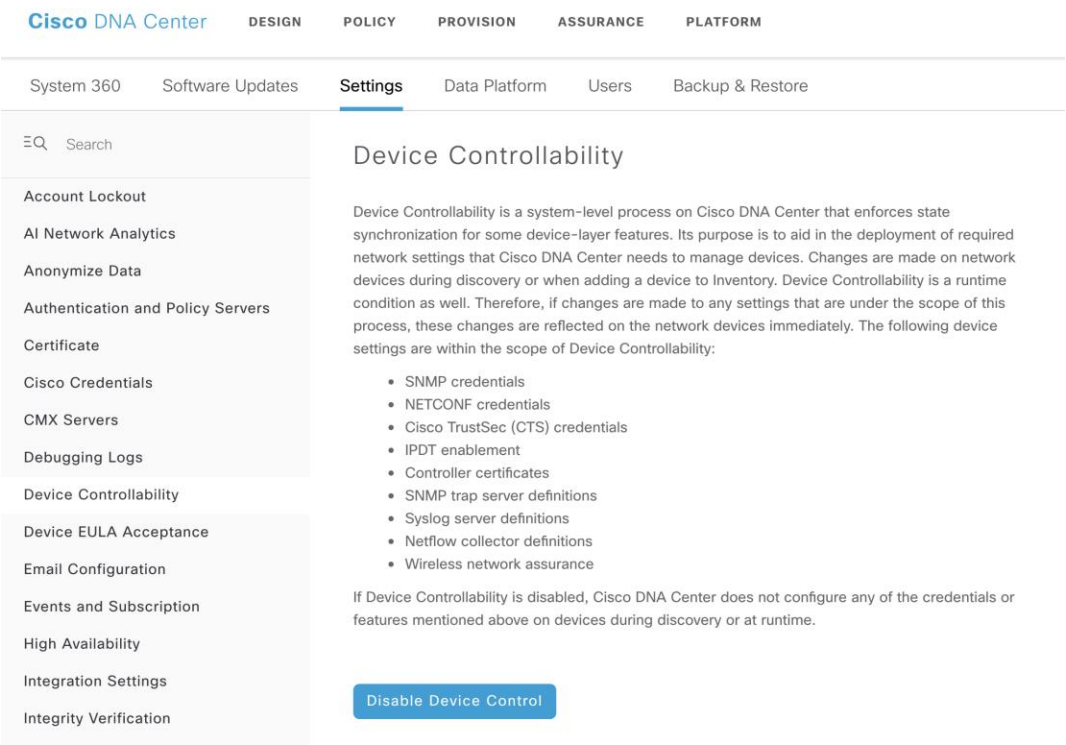
Filter | SUCCESS | UNREACHABLE | FAILURE | NOT TRIED | UNAVAILABLE

IP Address	Device Name	Status	ICMP	SNMP	CLI	HTTP(S)	NETCONF
10.0.255.9	SW-MCU	✓	✓	✓	✓	●	●
10.0.255.5	SW-SP-East	✓	✓	✓	✓	●	●
10.0.255.1	N7K-CORE1	✓	✓	✓	✓	●	●
10.0.255.2	N7K-CORE2	✓	✓	✓	✓	●	●
10.14.200.1	RTR-IWAN-MPLS.prime.ciscofrance.com	✓	✓	✓	✓	●	●
10.0.255.4	RTR-IWAN-INET.prime.ciscofrance.com	✓	✓	✓	✓	●	●
10.0.255.8	DC-2	✓	✓	✓	✓	●	●
10.0.255.7	DC-1.prime.ciscofrance.com	✓	✓	✓	✓	●	●
172.17.254.205	CT5508	✓	✓	✓	✓	●	●
10.0.255.6	SW-SP-West	✓	✓	✓	✓	●	●

Show 25 | Showing 1 to 10 of 10 | Page 1 of 1

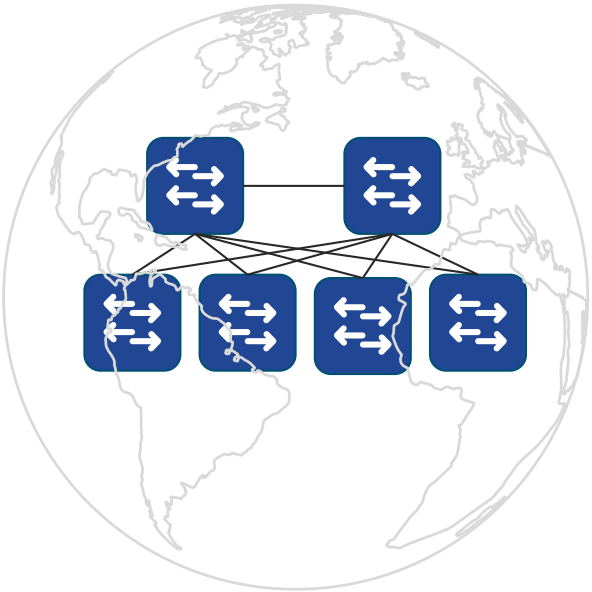
Device controllability and discovery

- Enabled by default
- Configures features on the device: SNMP trap receiver, IP Device Tracking, Cisco DNAC certificates…
- Configures SNMP credential on device if missing and provided in network setting



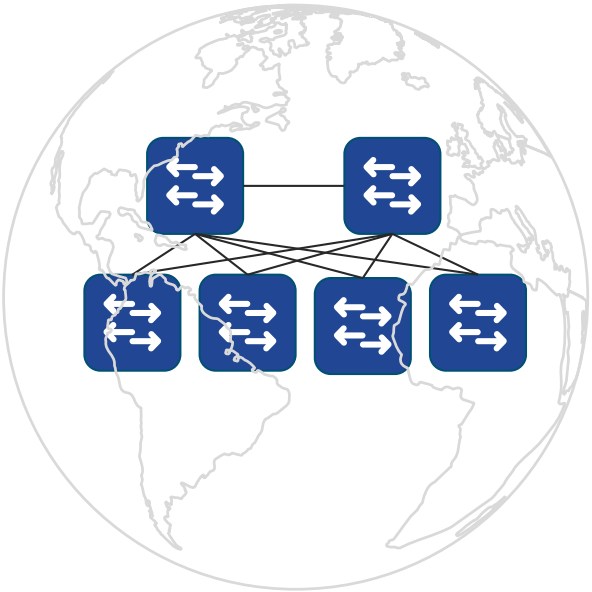
Base Automation

- Design
- Populate device inventory
- Provision
  - Assign Devices to Sites
  - Deploy Network Settings
  - Deploy Configuration Template
  - Upgrade Device
  - New Device Onboarding



Base Automation

- Design
- Populate device inventory
- **Provision**
  - Assign Devices to Sites
  - Deploy Network Settings
  - Deploy Configuration Template
  - Upgrade Device
  - New Device Onboarding

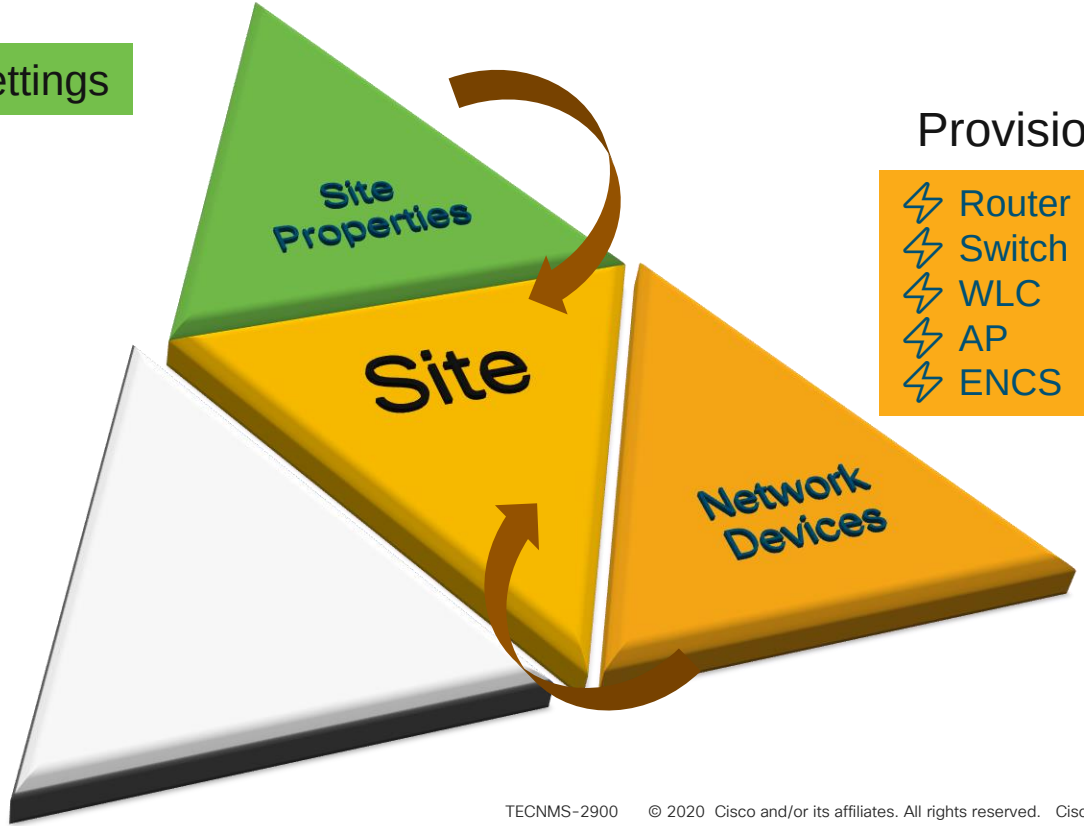


How Device Deployment comes together

Site – “glues” Design Properties

Design

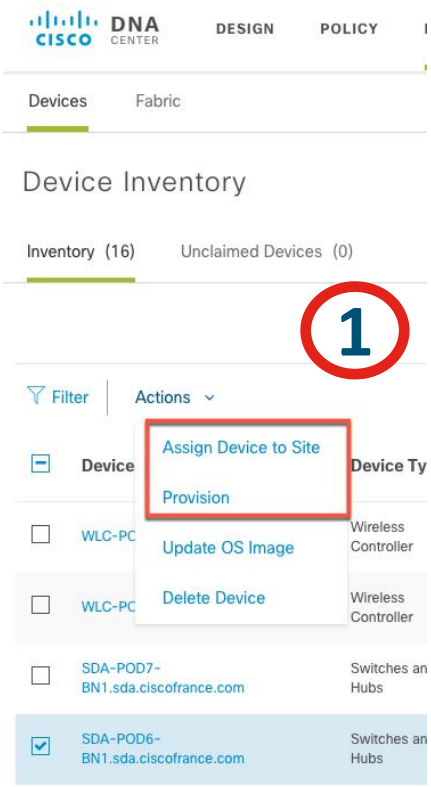
- Network Settings

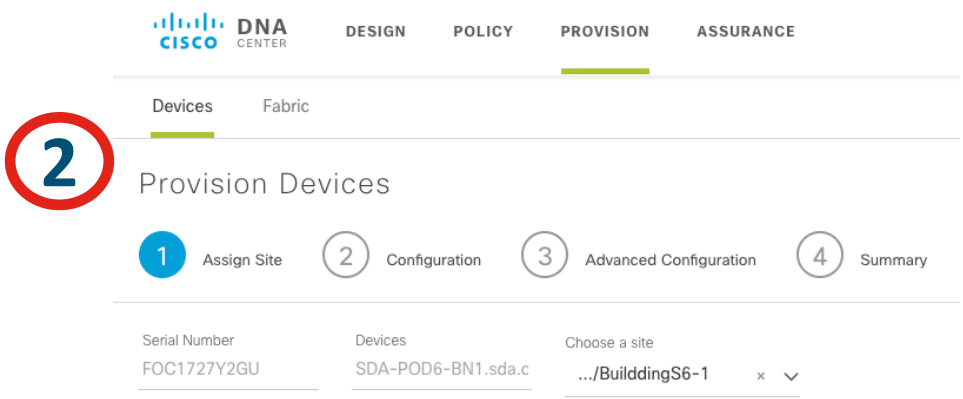


Provision

- Router
- Switch
- WLC
- AP
- ENCS

Provision device: assign devices to site





Provision device: deploy network settings on devices

3 Advanced Configuration 4 Summary

Device Details

Device Name:	POD6-EN_2.sda.ciscofrance.com
Platform Id:	WS-C3850-24P-E
Device IP:	172.106.100.98
Device Location:	BuilddingS6-1

3

Network Settings

NTP Server:	10.0.255.3
AAA Network Primary Server:	192.168.40.177
AAA Client Primary Server:	192.168.40.177
	WARNING: Do not use "admin" as the username ISE as your AAA server. If you do, this can result i
SYSLOG Server:	192.168.40.91
SNMP Trap Server:	192.168.40.91
DNS Domain Name:	sda.ciscofrance.com
DNS Primary Server:	192.168.40.1
DNS Secondary Server:	Not Configured

4

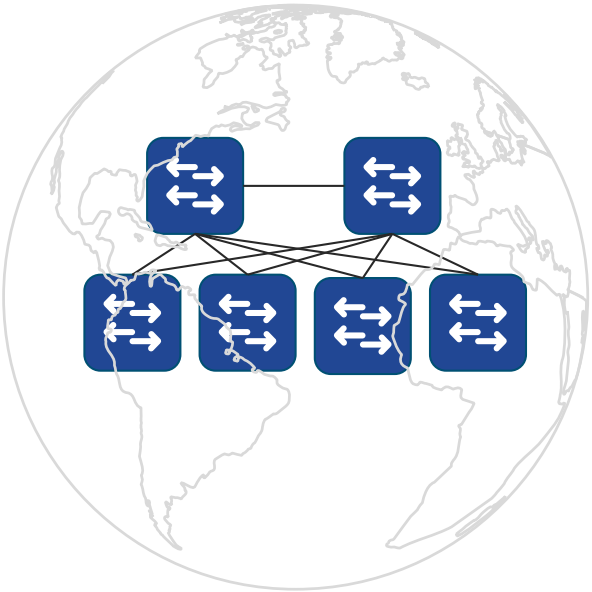
Provision Device

Run Now Schedule Later

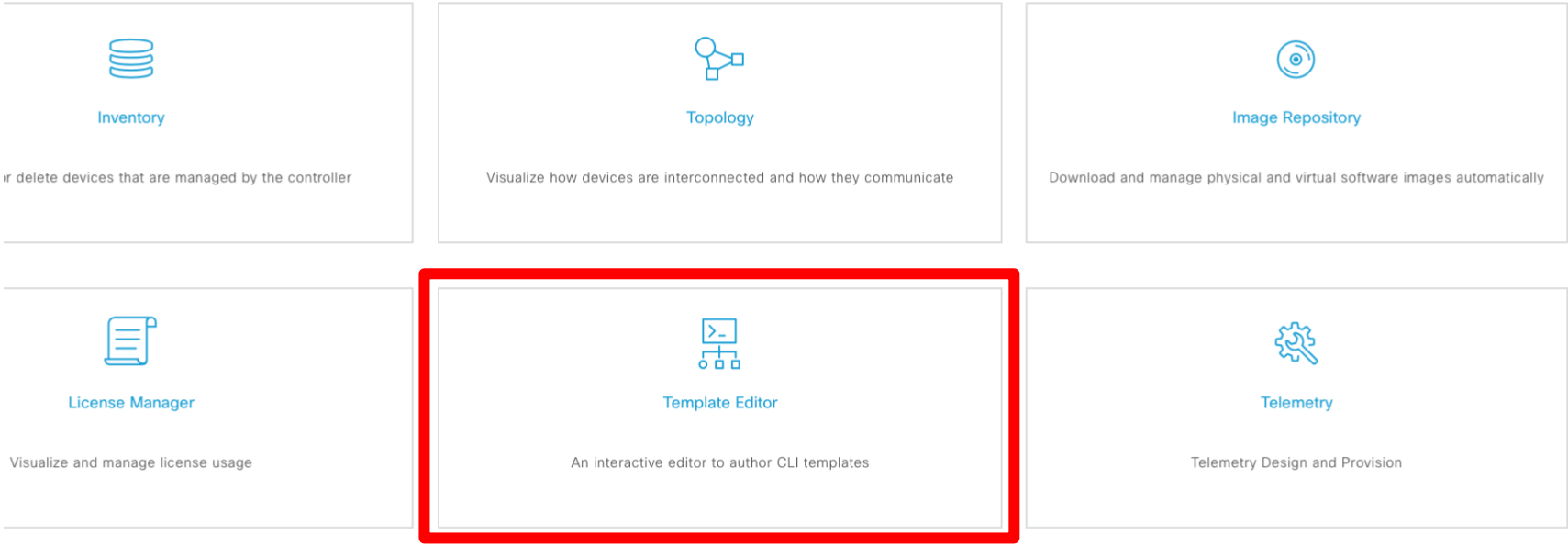
Cancel Apply

Base Automation

- Design
- Populate device inventory
- Provision
  - Assign Devices to Sites
  - Deploy Network Settings
  - Deploy Configuration Template
  - Upgrade Device
  - New Device Onboarding

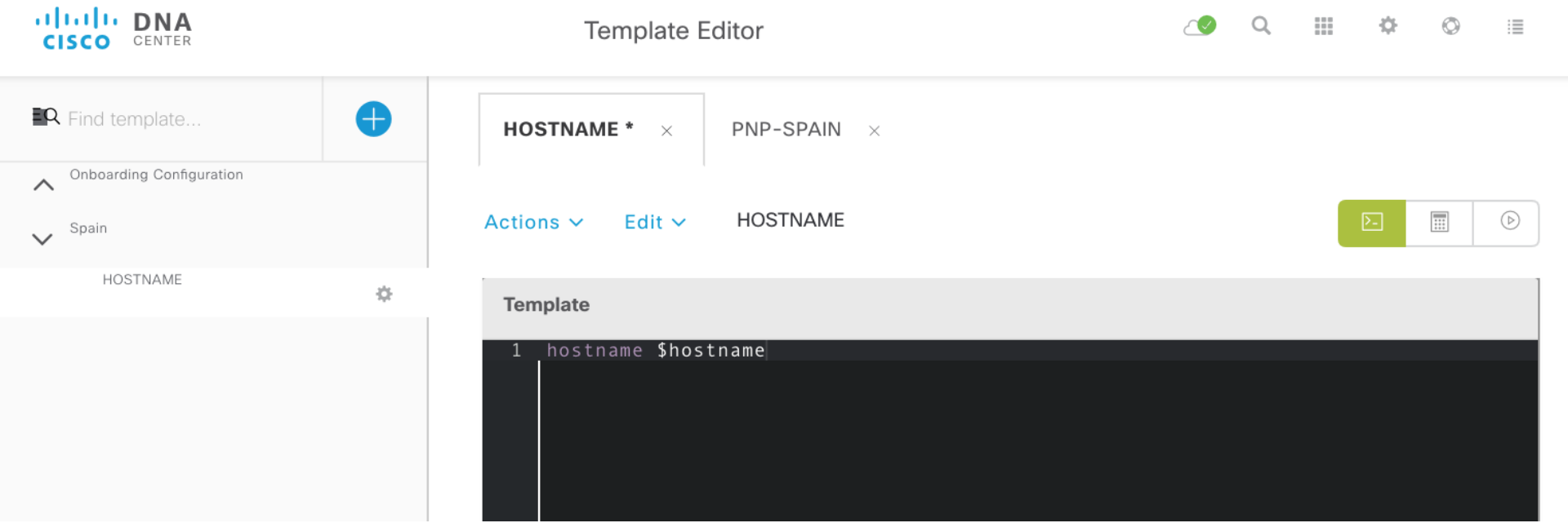


CLI Template Editor



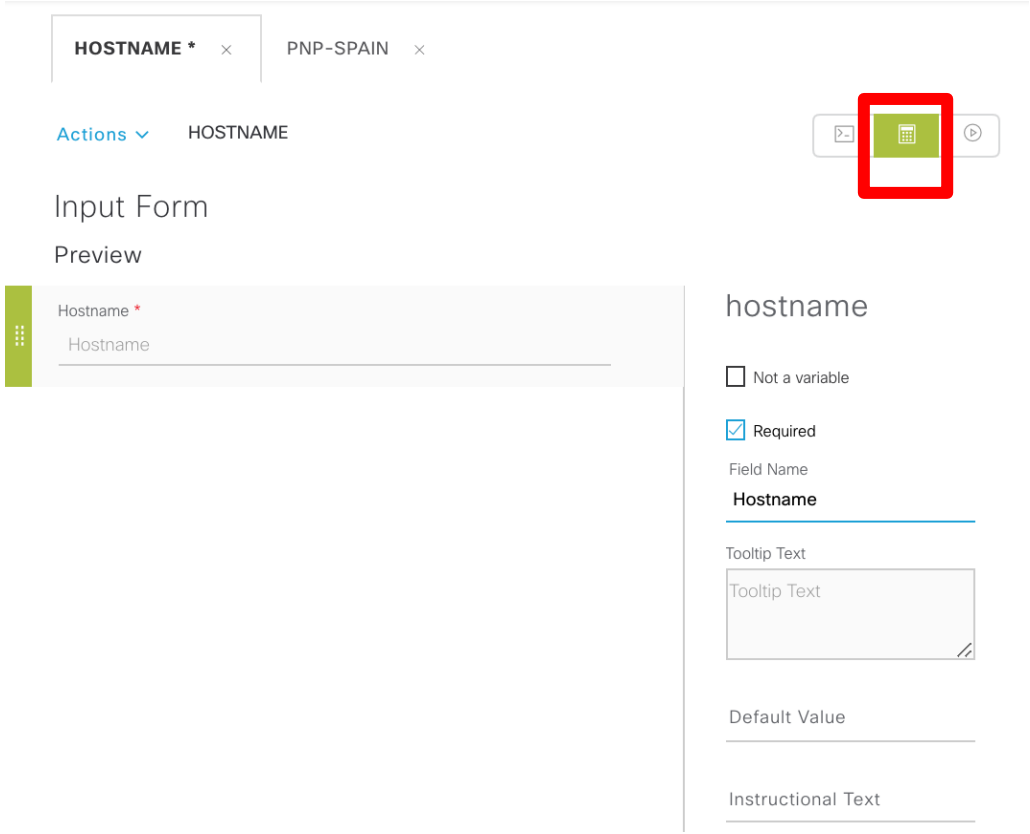
Template Editor

Template Engine is VTL (Velocity Template) like in Prime infrastructure

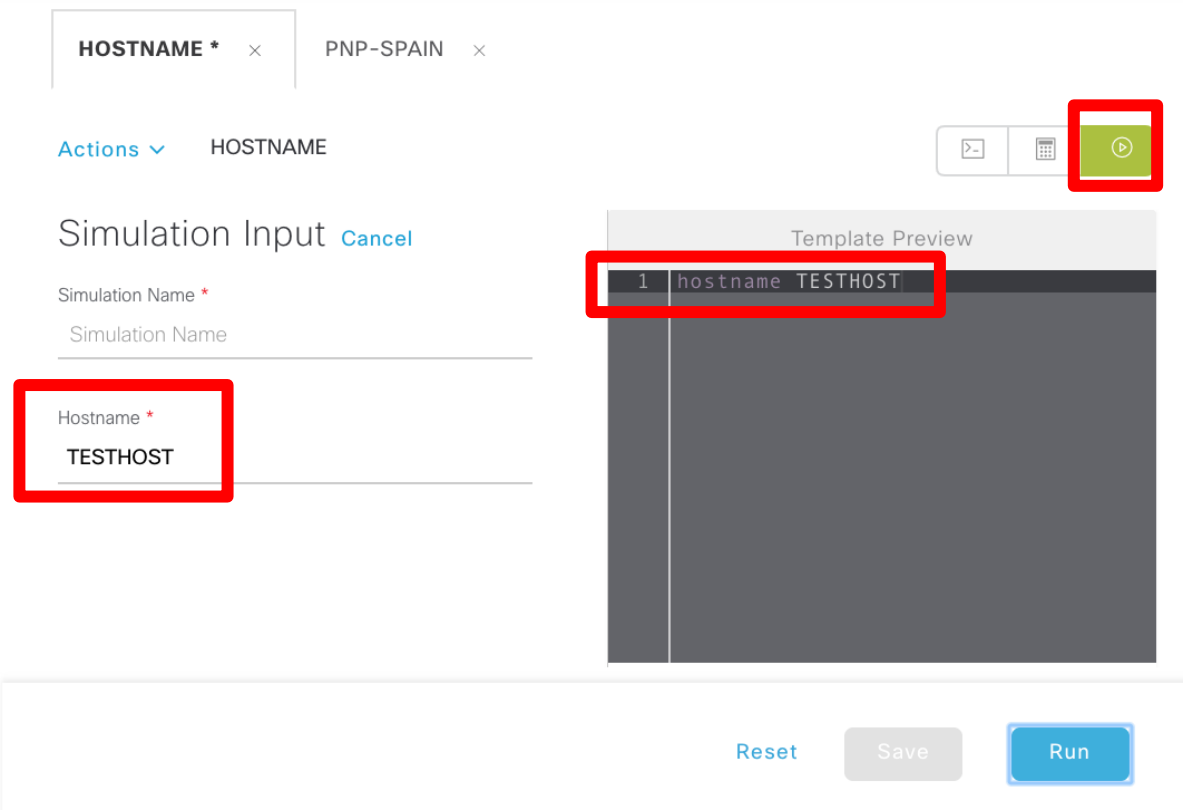


Parameter definition

- Different parameter types
  - Integer
  - String
  - IPv4 address
  - Mac Address
- Input validation
- Default value…



Test your form with simulation tool



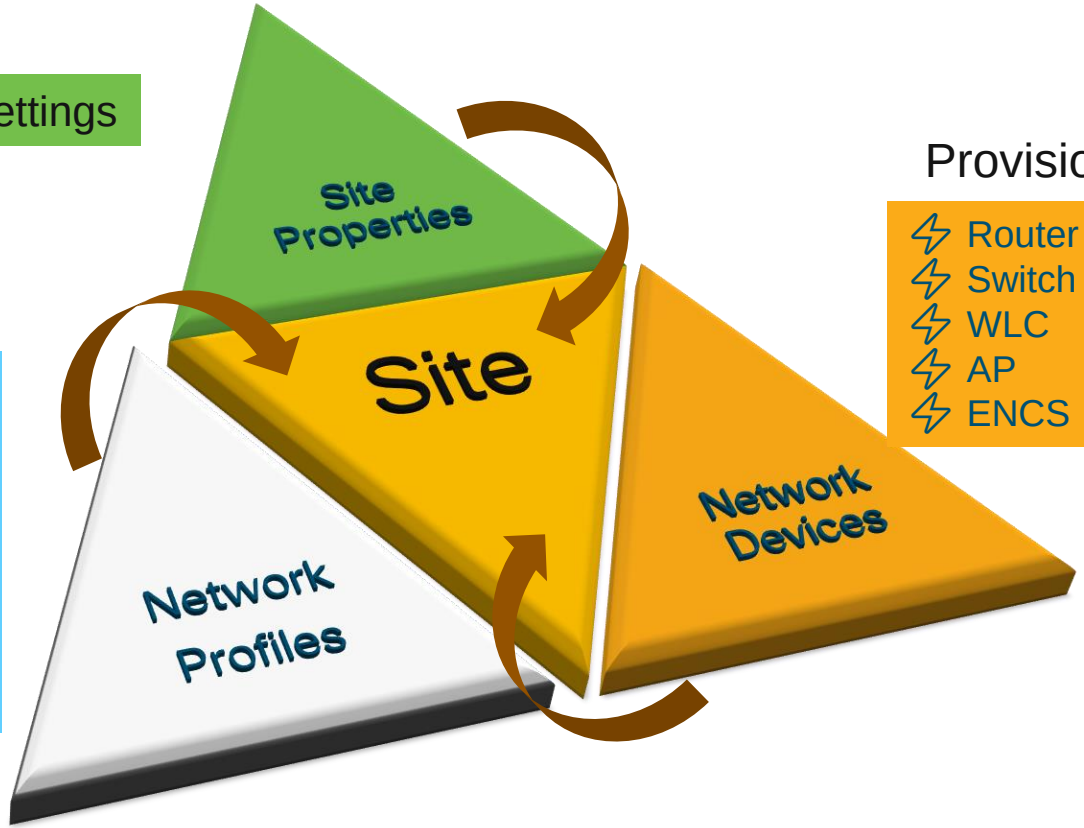
How Device Deployment comes together
Site – “glues” Design Properties

Design

- Network Settings

Design

- Switch network Profile
  - Templates
- Wireless network profiles
  - SSID’s
  - Interfaces
  - RF Profiles
  - Templates
- Router/NFV network Profiles



Provision

- Router
- Switch
- WLC
- AP
- ENCS

Base Automation

- Design
- Populate device inventory
- Provision
  - Assign Devices to Sites
  - Deploy Network Settings
  - Deploy Configuration Template
  - Upgrade Device
  - New Device Onboarding

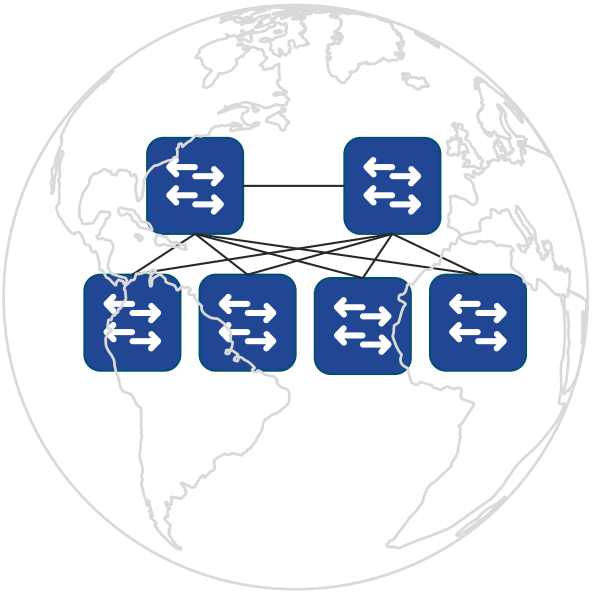
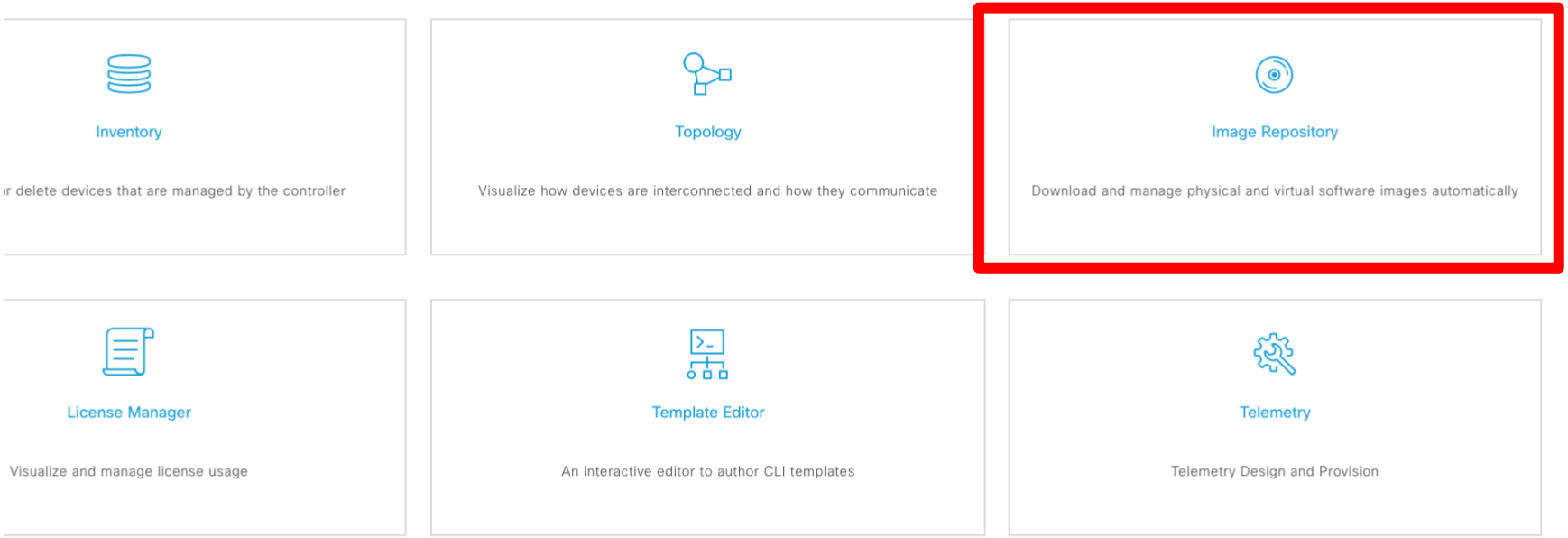


Image management



Managing Software Image

Goals:

- Ensure Consistency of Software for all network devices (by platform type)
- React to PSIRT and bugs fast
- Deploy software with confidence

Benefits:

- Golden Image based workflows drive software consistency
- Pre/Post check ensures that software updates do not have side effects on the network
- Patching provides small updates to react quickly to security fixes

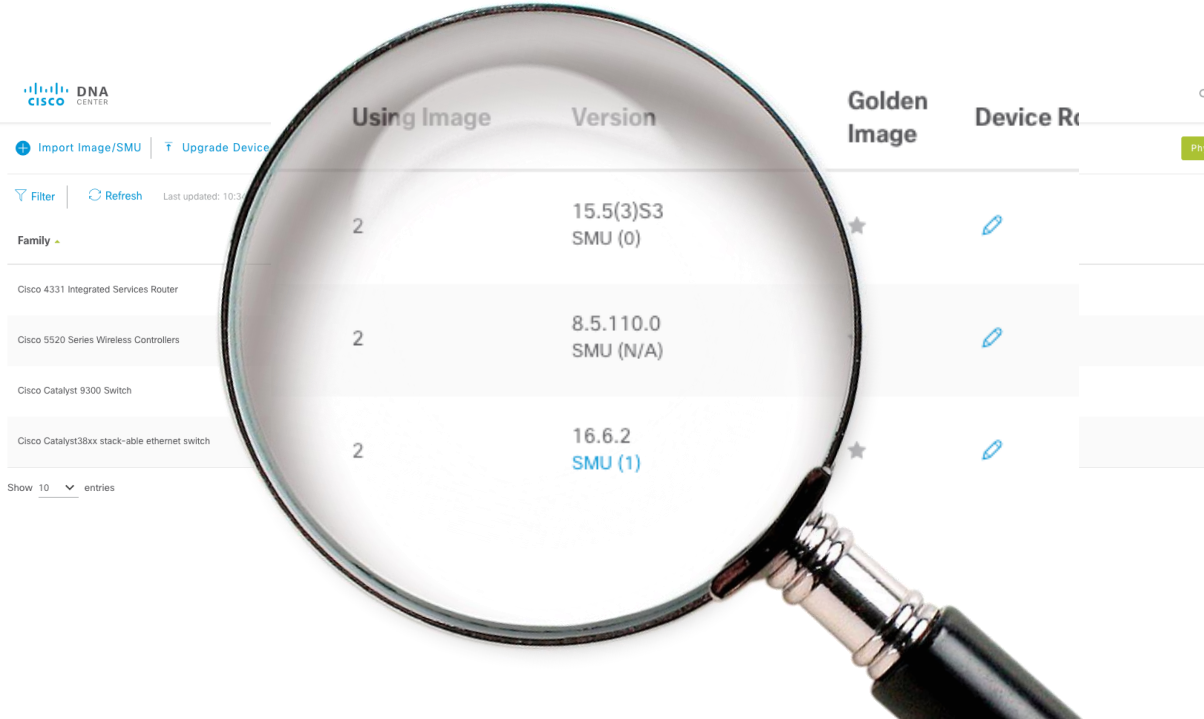
*What is SMU ?

- Point Fixes for the IOS-XE images (16.x onwards)
- Provides the ability to just update what is needed

Visualize Software Images

Image Repository centrally stores Software Images and VNF Images

- For a given Device Family, view :
  - All images
  - Image Version
  - Number of Devices using a particular image



Manage Software Images

- Import Images/SMU from :
  - Local PC
  - URL(http/ftp)
  - CCO
  - Another managed network device

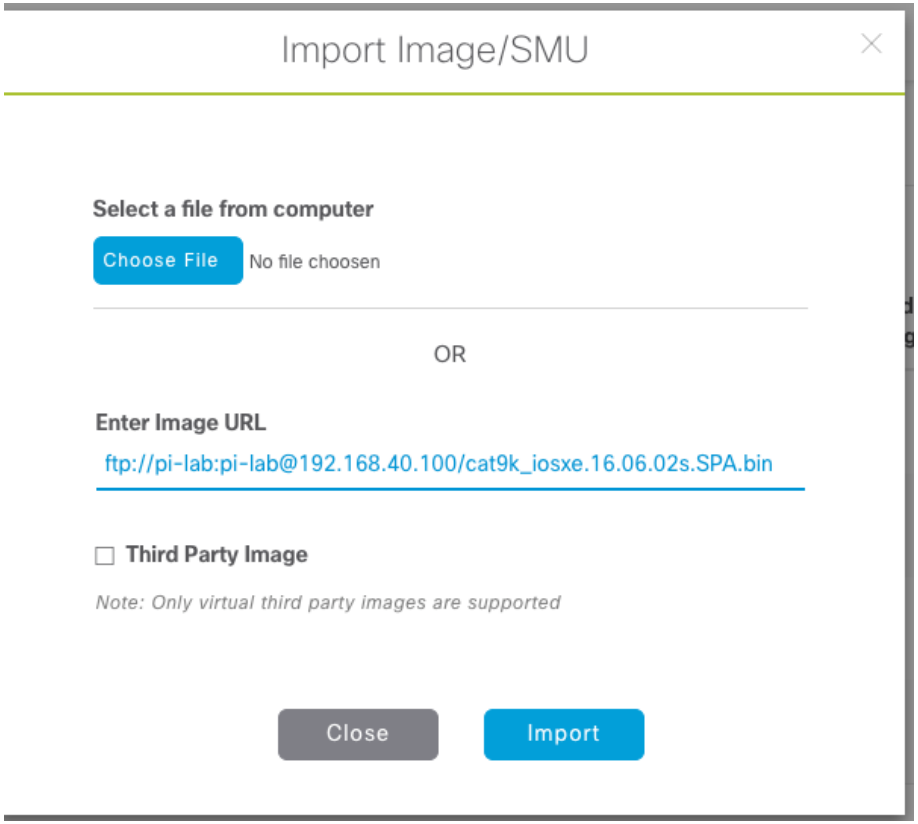


Image Standardization – “Golden Images”

Device Type

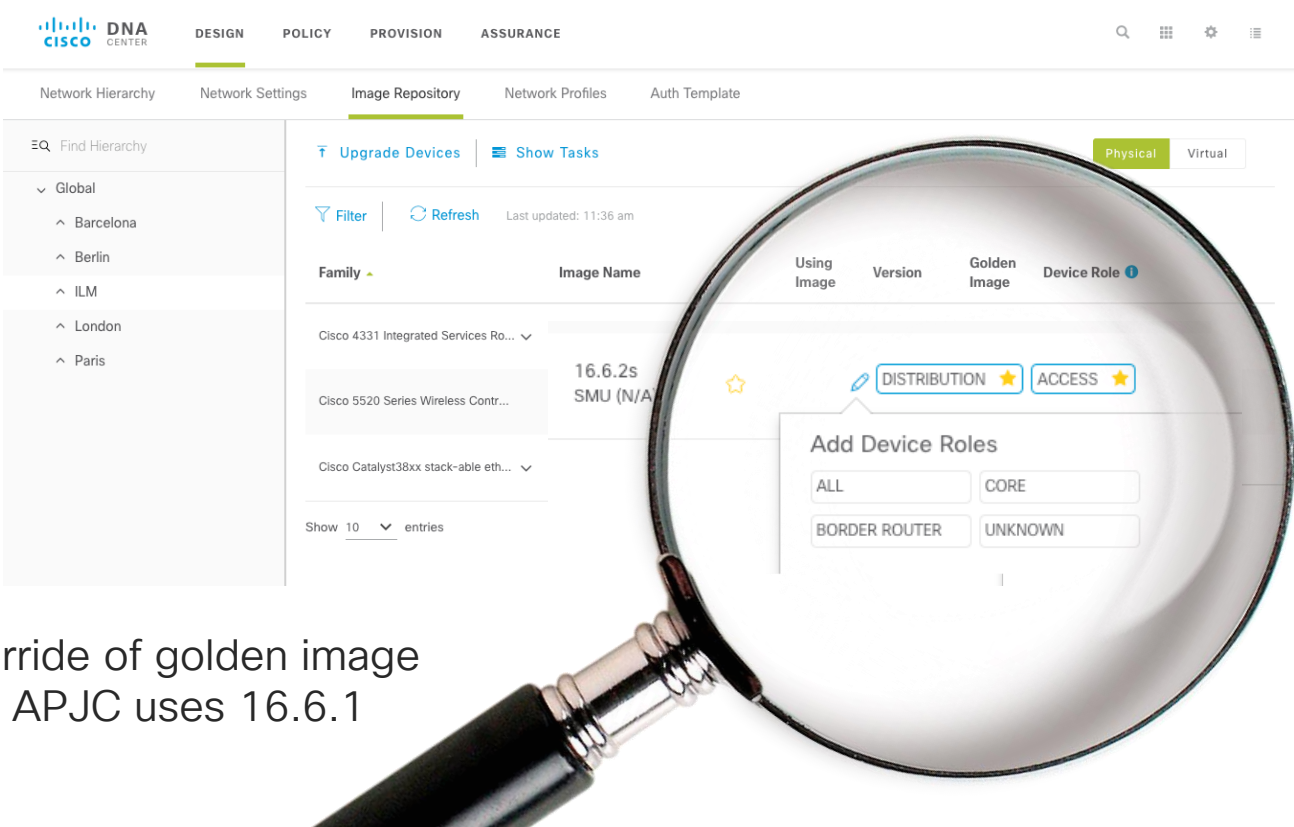
- Golden image per device type

Device Role

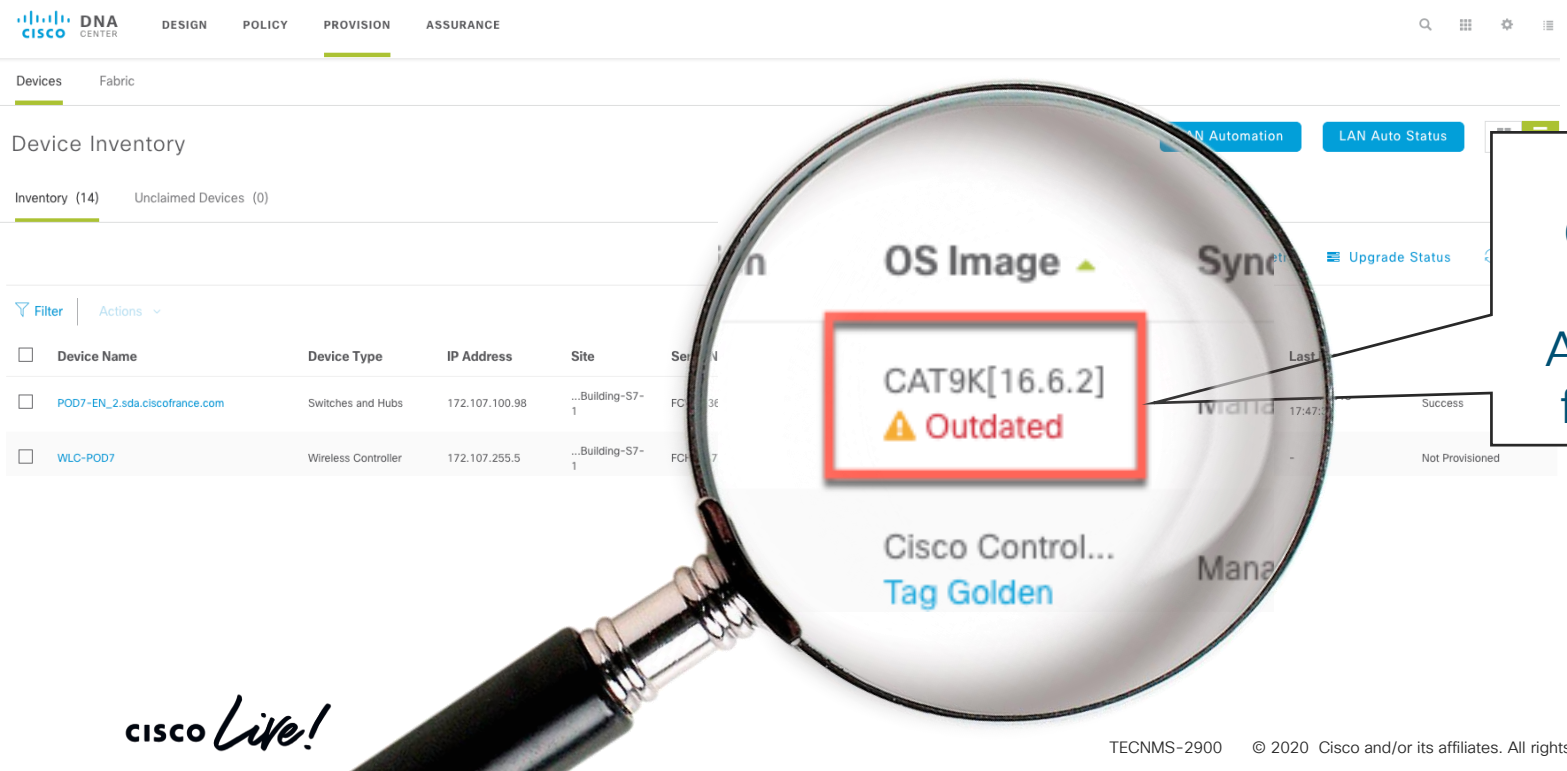
- Devices in the same family classified by role (core, distribution, access …)

Site Mapping

- Site hierarchy provides override of golden image
- Ex: EMEA uses v16.6.2s vs APJC uses 16.6.1



Devices not Compliant with Golden Image



Built-in Compliancy checks to Automatically flag devices

SWIM/SMU Workflow Experience with Cisco DNA Center

1

Fabric

Device Inventory

LAN Automation | LAN Auto Status

Inventory (14) | Unclaimed Devices (0)

Network Telemetry | Upgrade Status | Refresh

Filter | Actions

- Assign Device to Site
- Provision
- Update OS Image
- Delete Device

Device		IP Address	Site	Serial Number	Uptime	OS Version	OS Image	Sync Status	Last Provision	Provision Status
SDA-PO BN1.sda		172.107.255.1	...Building-S7-1	FOC1727Z25S	11 days, 20:03:49.39	16.6.2s	CAT3K_CAA[16....	Managed	Jan 04 2018 17:47:40	Success
SDA-PO BN1.sda.ciscofrance.com	and Hubs	172.106.255.1	...BuilddingS6-1	FOC1727Y2GU	11 days, 21:06:52.10	16.6.2s	CAT3K_CAA[16....	Managed	-	Not Provisioned
POD7-EN_1.sda.ciscofrance.com	Switches and Hubs	172.107.100.97	...Building-S7-1	FOC1704V0LQ	11 days, 19:56:03.41	16.6.2	CAT3K_CAA[16.... ⚠ Outdated	Managed	Jan 04 2018 19:07:38	Success

Upd

1

- Select device/(s) to update Image/SMU

2

- Automatic Pre-Checks done for RAM & Flash
- Abort if Pre-Check Fails

2

Device	Device Type	Target Image	Target Version	Target Image Size	Flash	RAM	Reboot
POD7-EN_2.sda.ciscofrance.com	Switches and Hubs	cat9k_iosxe.16.06.02s...	16.6.2s	569 MB	●	●	Yes

Note: 1. System will not update the devices if no image is available or tagged in the repository.
2. Ensure that the target image is the right image for the selected device.
3. Upgrade of Unified AP is not allowed.

Run Now | Schedule Later

Cancel | Apply

SWIM/SMU Workflow Experience with Cisco DNA Center

3

Recent Tasks (Last 50)

All

Image Upgrade for 172.107.100.98

cat9k_iosxe.16.06.02s.SPA.bin

Duration : 0h: 16m: 40s Start Time : Jan15 2018 10:44:05 Successful

1. Distribute Operation ✔ Show Scripts

Distribution of image : cat9k_iosxe.16.06.02s.SPA.bin on device : 172.107.100.98 completed successfully.

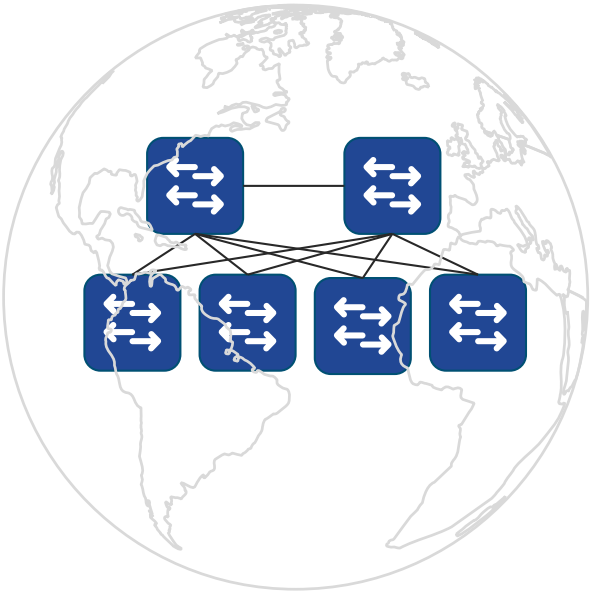
2. Activate Operation ✔

Activation of image : cat9k_iosxe.16.06.02s.SPA.bin on device : 172.107.100.98 completed successfully

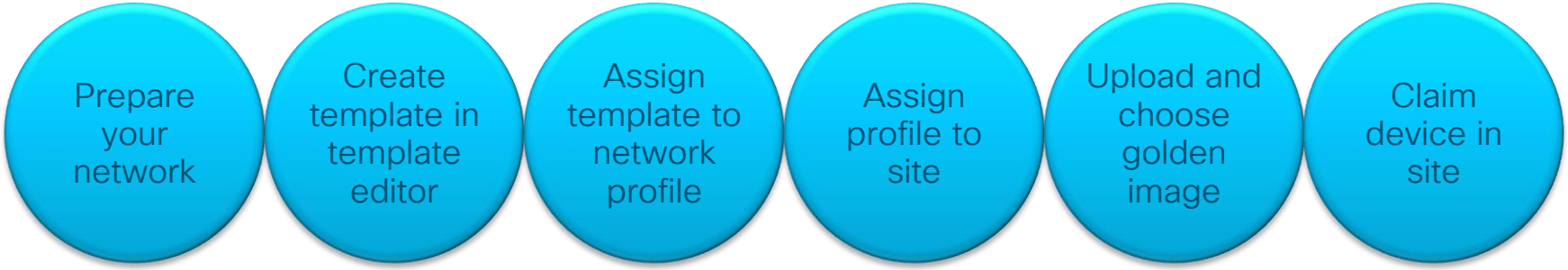
- Detailed status information regarding the Upgrade Process
- In case of failure during Image upgrade or Pre & Post checks, provide reason for failure and automatically Rollback

Base Automation

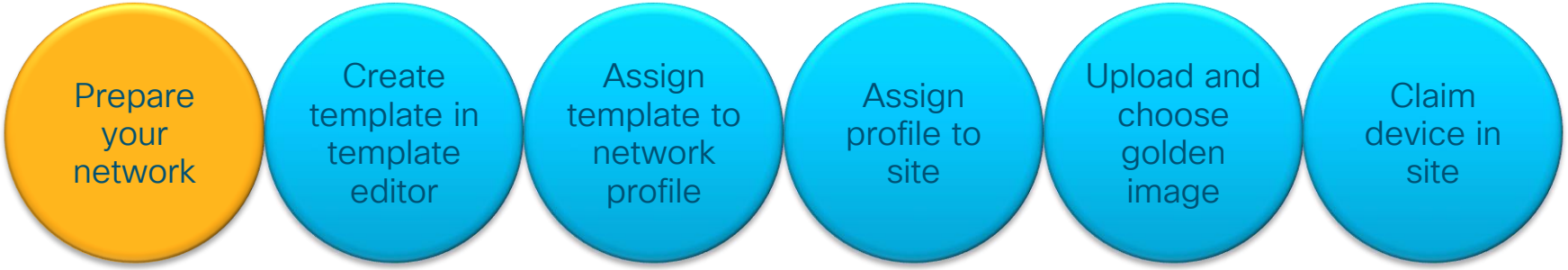
- Design
- Populate device inventory
- Provision
  - Assign Devices to Sites
  - Deploy Network Settings
  - Deploy Configuration Template
  - Upgrade Device
  - New Device Onboarding



Router and Switch workflow for Plug and Play



Router and Switch workflow for Plug and Play



PnP Server Discovery Options

	Switches (Catalyst®)	Routers (ISR, ASR)	Wireless Access Points
1	DHCP Server	**DHCP options 43** PnP string: 5A1D;B2;K4;I172.19.45.222;J80 added to DHCP Server	
2	DNS Server	**DNS lookup** pnpserver.localdomain resolves to Cisco DNAC IP Address	
3	cisco	**PnP Connect** https://devicehelper.cisco.com/device-helper re-directs to Cisco DNAC IP Address	
4		**USB-based bootstrapping** USB drive with bootstrap config file - router-confg / router.cfg / ciscortr.cfg	
5		**Manual - using the Cisco® Installer App** iPhone, iPad, Android, (roadmap - Windows mobile and PC)	

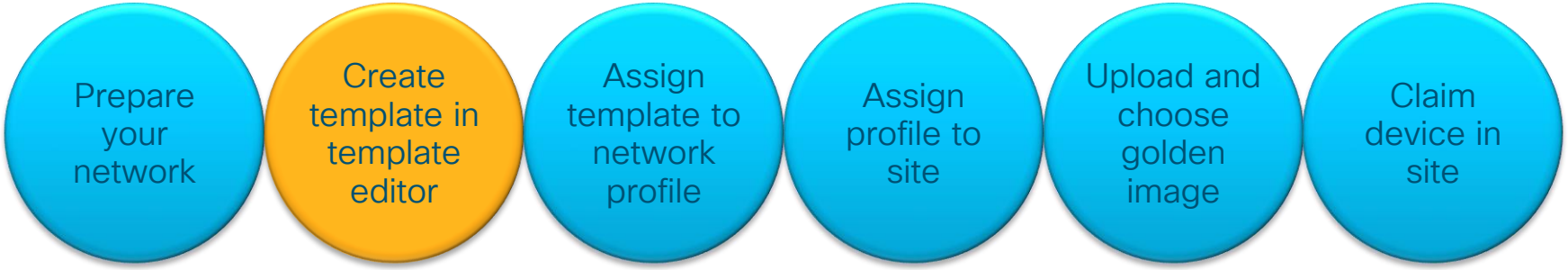
PnP Server Discovery Options

	Switches (Catalyst®)	Routers (ISR, ASR)	Wireless Access Points
1	DHCP Server	Typical LAN use cases	
2	DNS Server		
3	cisco	PnP Connect https://devicehelper.cisco.com/device-helper re-directs to Cisco DNAC IP Address	
4		USB-based bootstrapping USB drive with bootstrap config file - router-confg / router.cfg / ciscortr.cfg	
5		Manual - using the Cisco® Installer App iPhone, iPad, Android, (roadmap - Windows mobile and PC)	

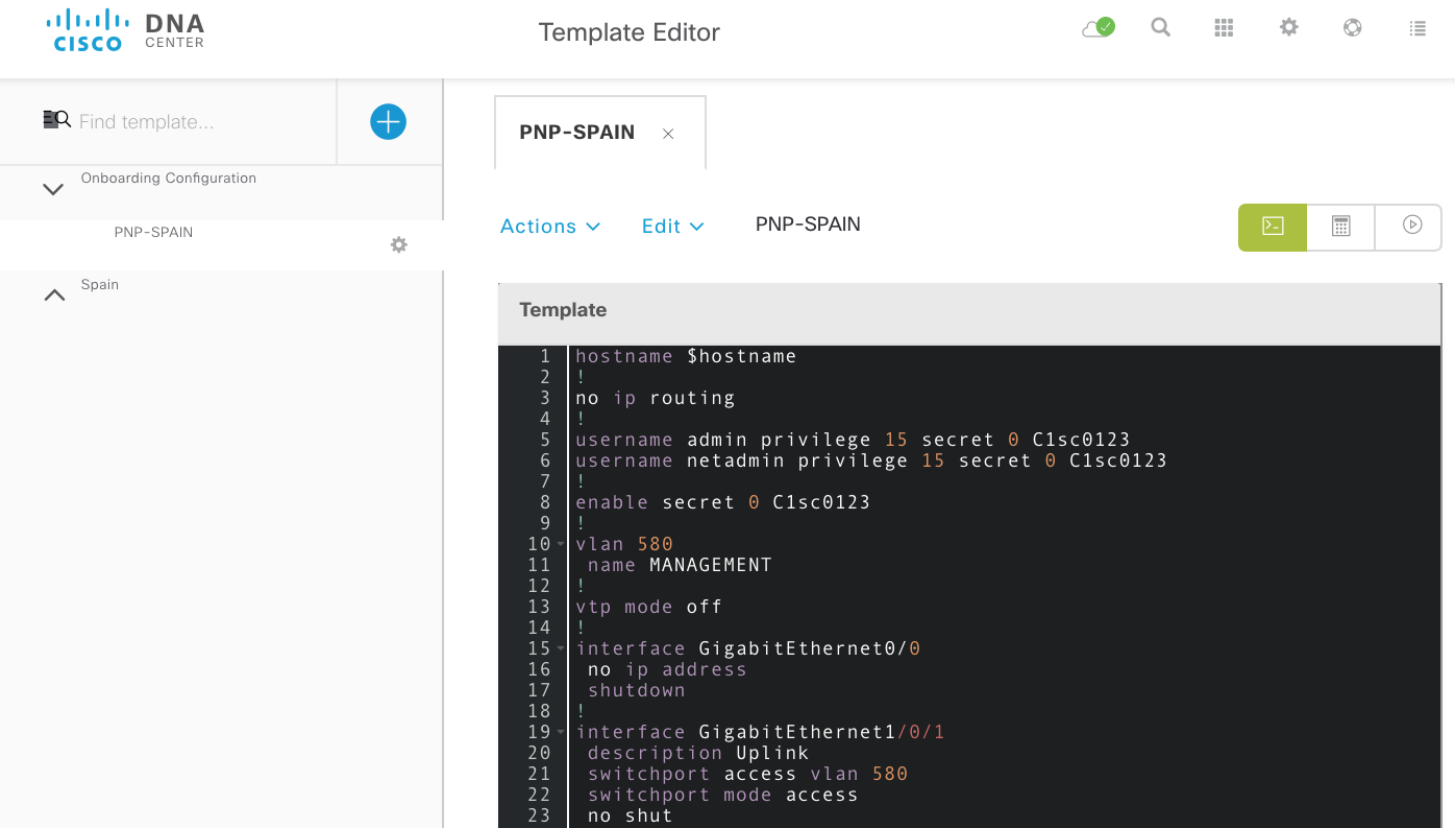
PnP Server Discovery Options

	Switches (Catalyst®)	Routers (ISR, ASR)	Wireless Access Points
1	DHCP Server	Typical LAN use cases	
2	DNS Server		
3	cisco	Typical WAN use cases	
4			
5			

Router and Switch workflow for Plug and Play



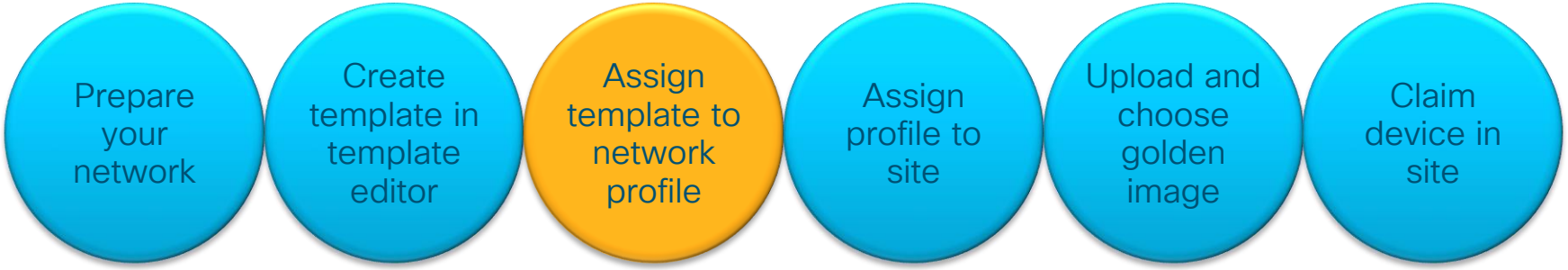
Create template in onboarding configuration project



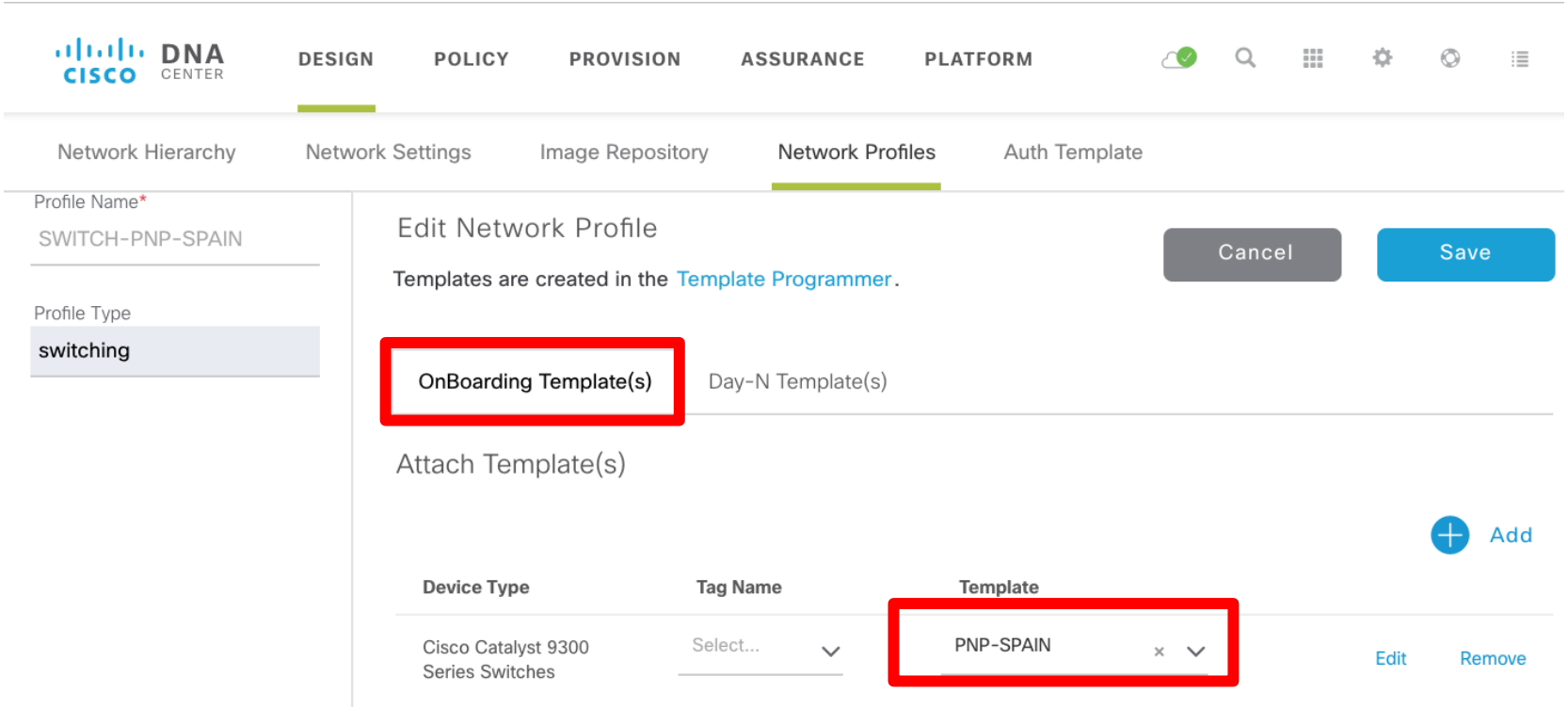
Important Tips

- #1 issue is that device is not reachable by Cisco DNA Center after PNP
- Make sure your configuration gives Cisco DNA Center connectivity to your network device (routing, username, SNMP, vty login, trunk, etherchannel)
- Try it before on a test setup before using massively in production

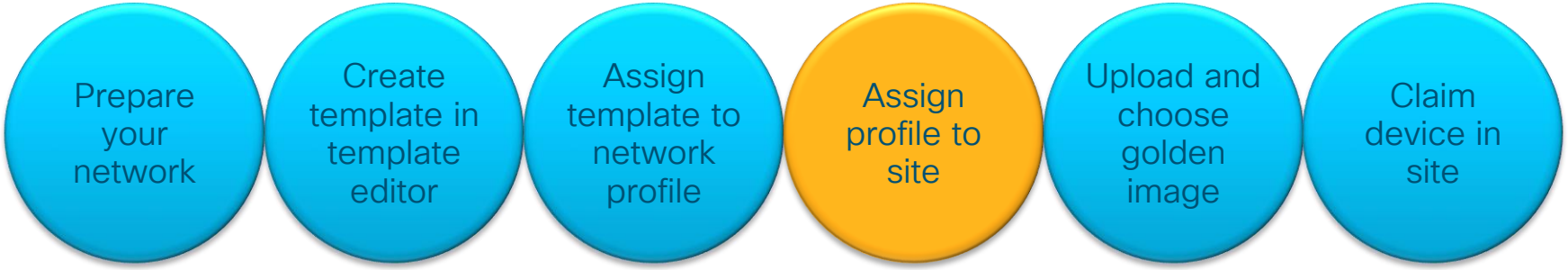
Router and Switch workflow for Plug and Play



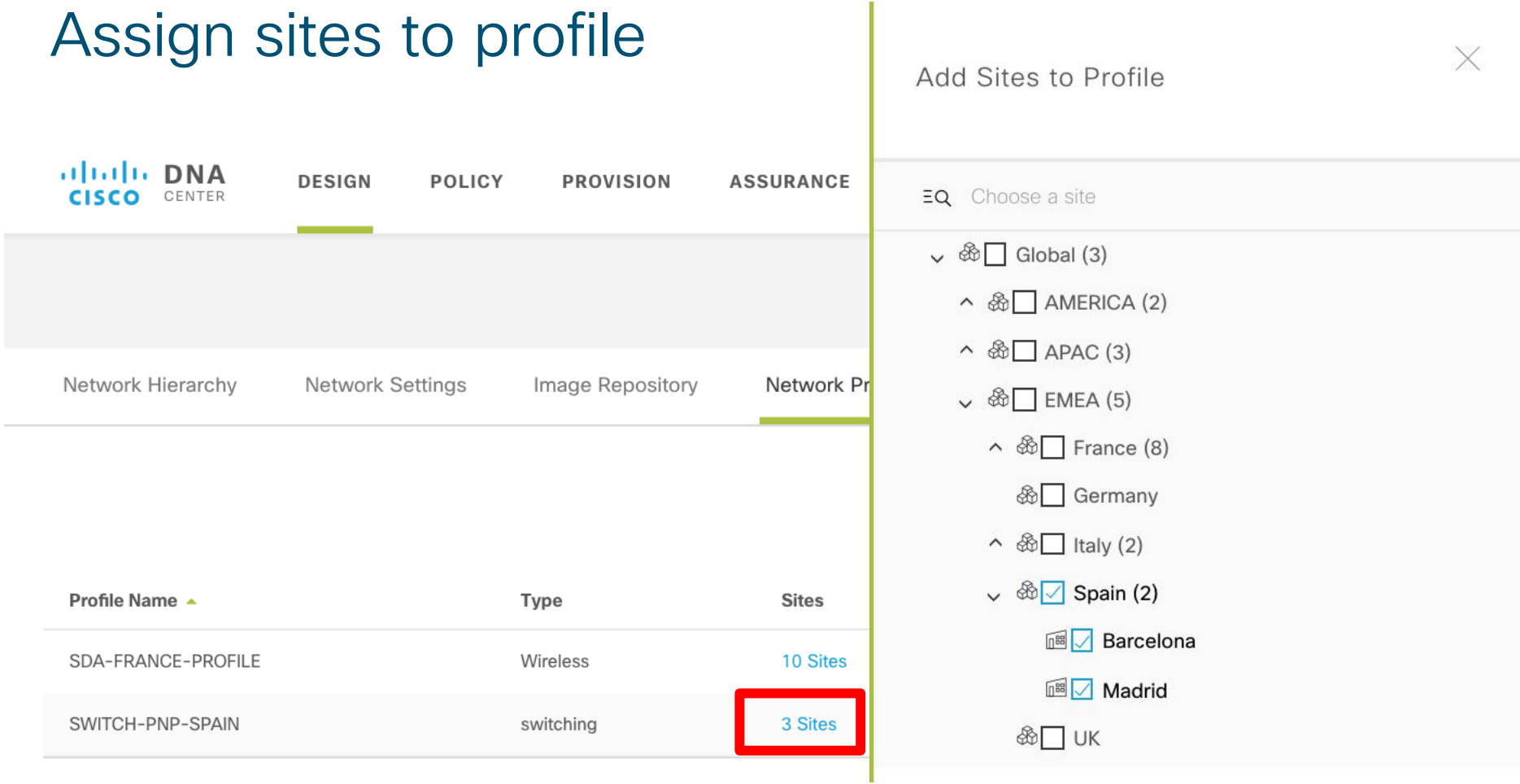
Add Onboarding Template to network profile



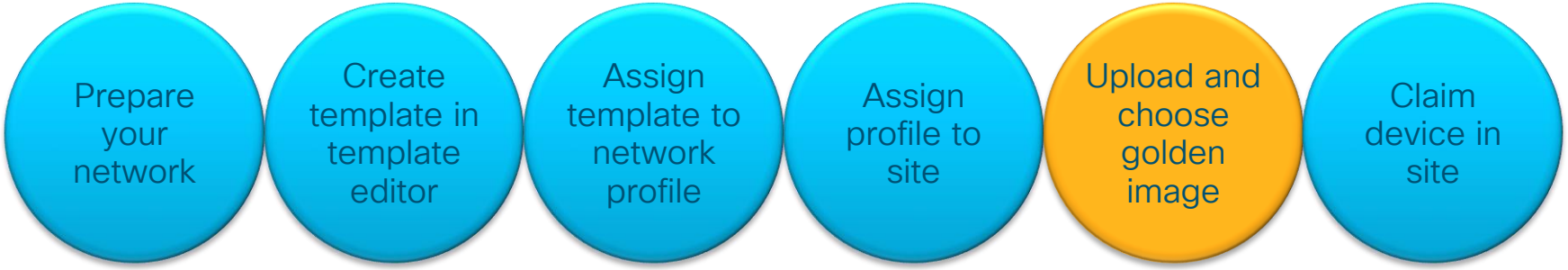
Router and Switch workflow for Plug and Play



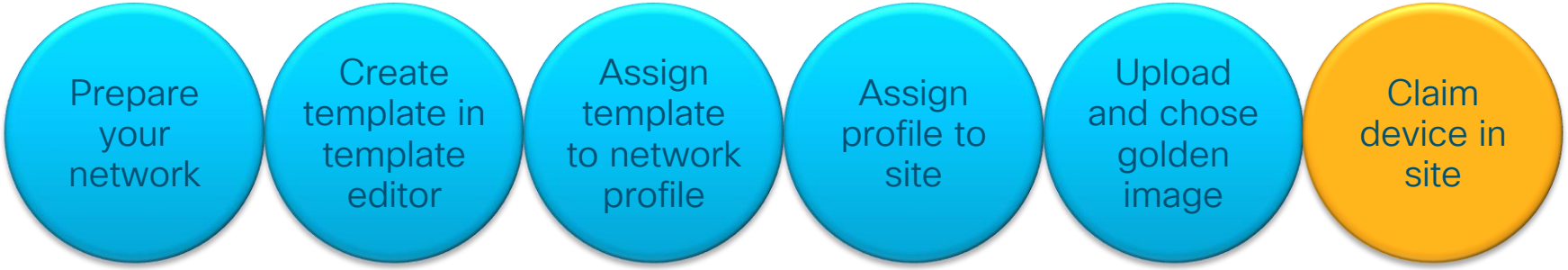
Assign sites to profile



Router and Switch workflow for Plug and Play



Router and Switch workflow for Plug and Play



Demo
PnP Workflow

Nicht sicher | fra-dnac-r3.cisco.com/dna/home

Apps

Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

13

Welcome, Eure Hohheit

Take a Tour Learn More

Assurance Summary

Health

Healthy as of Jan 25, 2020 6:06 PM

85% Network Devices

--% Wireless Clients

100% Wired Clients

View Details

Critical Issues

Last 24 Hours

13 P1

19 P2

View Details

Trends and Insights

Last 7 Days

0 Throughput

0 Coverage

0 Capacity

View Details

Network Snapshot

Sites

As of Jan 25, 2020 6:07 PM

46

DNS Servers : 2
NTP Servers : 1

Add Sites

Network Devices

As of Jan 25, 2020 6:07 PM

77

Unclaimed: 3
Unprovisioned: 36
Unreachable: 8

Find New Devices

Application Policies

As of Jan 25, 2020 6:08 PM

1

Successful Deploys: 1
Errored Deploys: 0
Stale Policies: 1

Add New Policy

Network Profiles

As of Jan 25, 2020 6:07 PM

Images

As of Jan 25, 2020 6

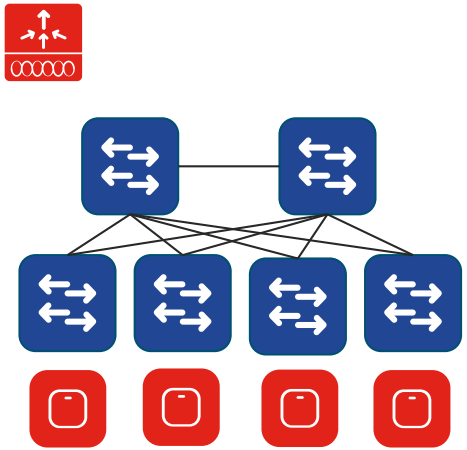
Cisco DNA Licensed Devices

As of Jan 25, 2020 6:07 PM

SecureCRT

1

What can I do with Cisco DNA Center to automate a traditional wireless network?



Legacy network

SD-Access Fabric

Automation and Assurance

Wireless Workflow with Cisco DNA-Center

Create Site Hierarchy

→

Design Wireless settings:
Wireless interface
SSIDs
RF Profiles

→

Create wireless Network Profile and associate to Sites

↓

Provision WLC and APs

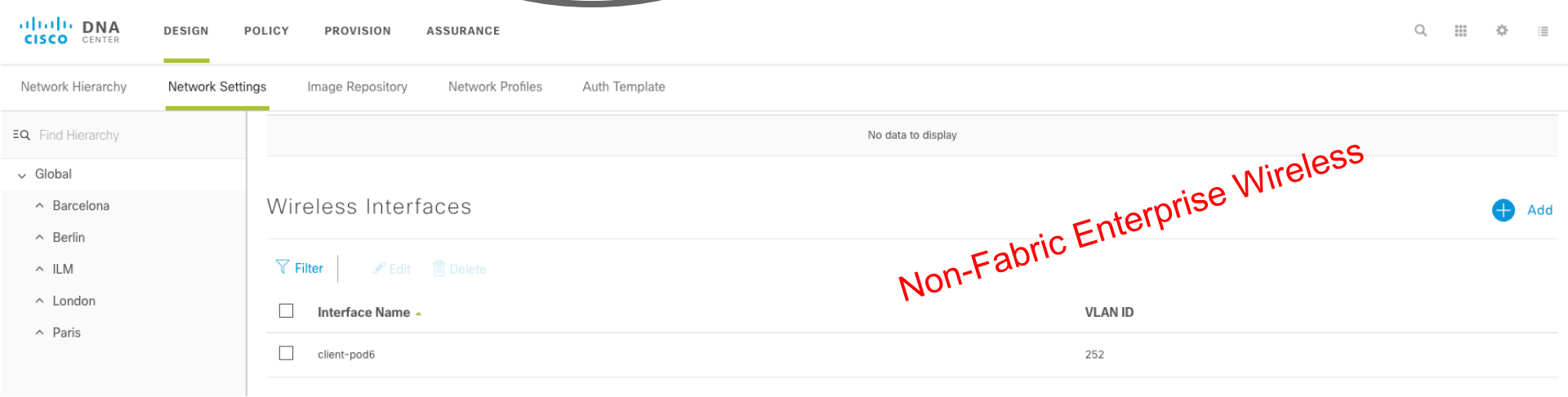
Design Wireless settings

Standard Network Settings
Create and inherit settings

→ **Wireless Interfaces**
Map dynamic interface to VLAN

→ **SSIDs**
Based on best practices

→ **RF Profiles**
Based on best Practices



Non-Fabric Enterprise Wireless

Design Wireless settings

Standard Network Settings
Create and inherit settings

→

Wireless Interfaces
Map dynamic interface to VLAN

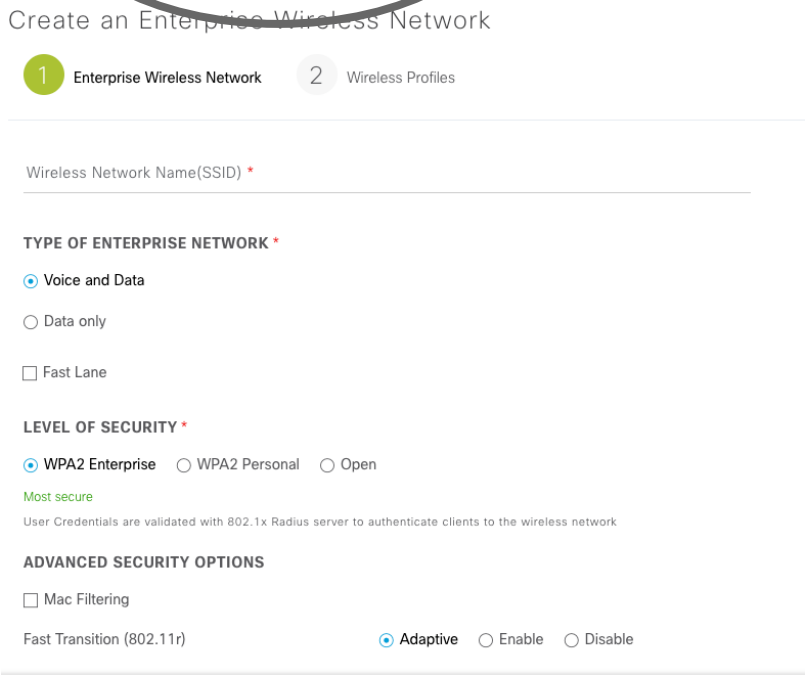
→

SSIDs
Based on best practices

→

RF Profiles
Based on best Practices

- Enterprise/Guest SSID
- Enable Apple Fast Lane
- Simplified Security Options
- Enable QoS for Data/Voice+Data
- Fabric or non Fabric



Design Wireless settings

Standard Network Settings
Create and inherit settings

→

Wireless Interfaces
Map dynamic interface to VLAN

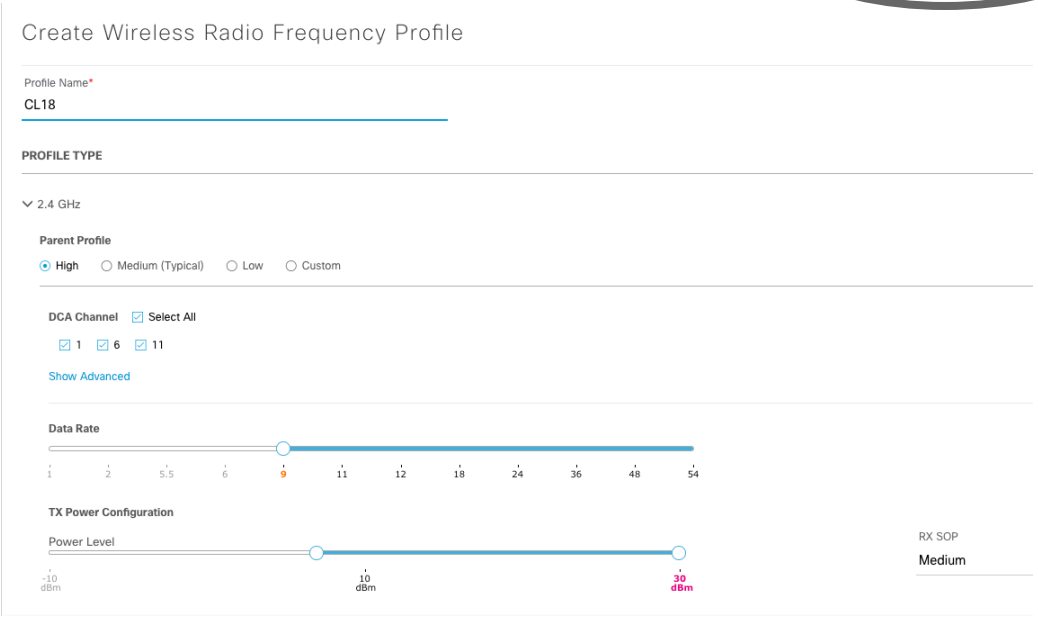
→

SSIDs
Based on best practices

→

RF Profiles
Based on best Practices

- Out-of-the-box RF Profiles available - High,Medium(Typical),Low
- Ability to customize RF Profiles for 2.4 and 5GHz clients: DCA Channels for 2.4 and 5Ghz clients, Data Rates, TX power, RX SOP



How Wireless Deployment comes together

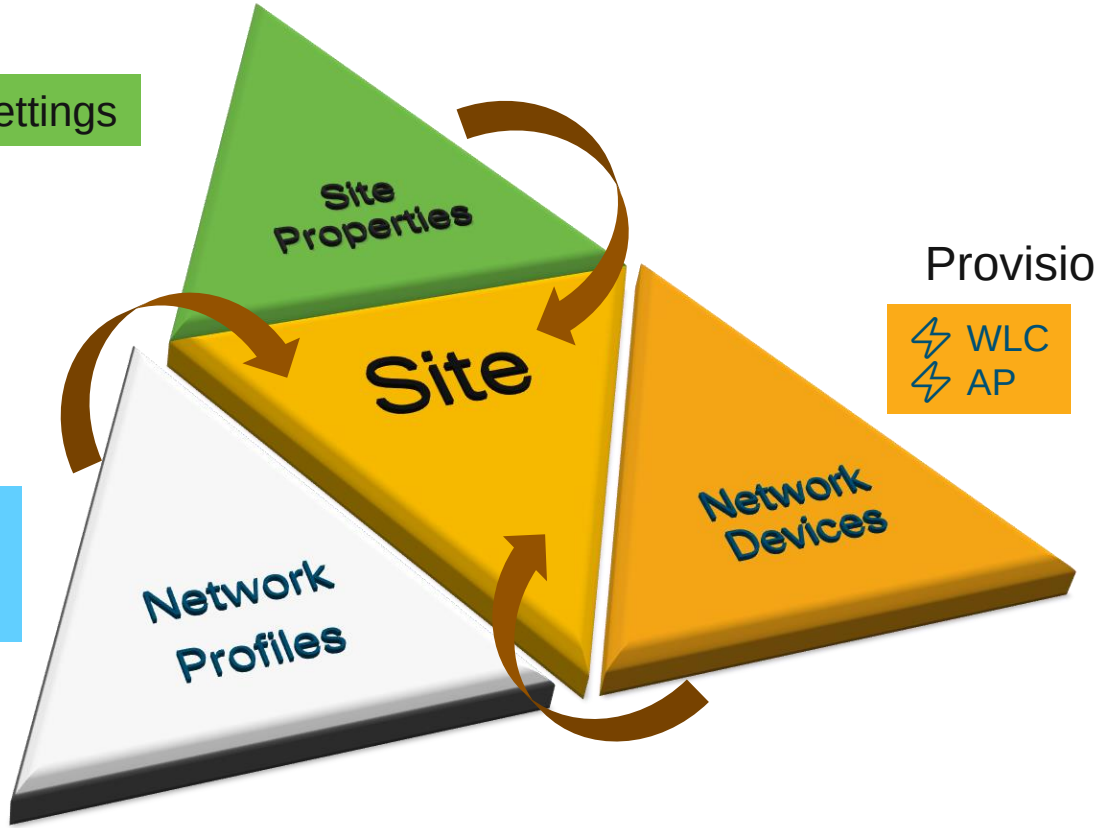
Site – “glues” Design & Provision Properties

Design

- Network Settings

Design

- SSID’s
- Interfaces
- RF Profiles

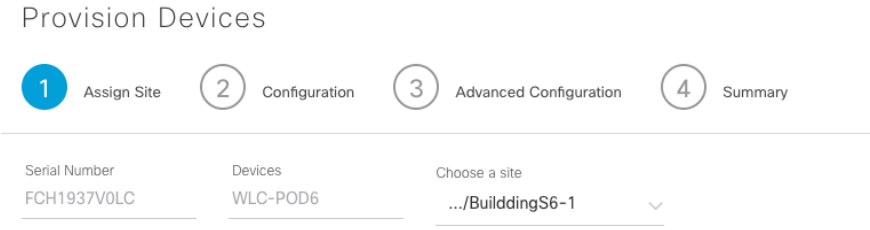


Provision

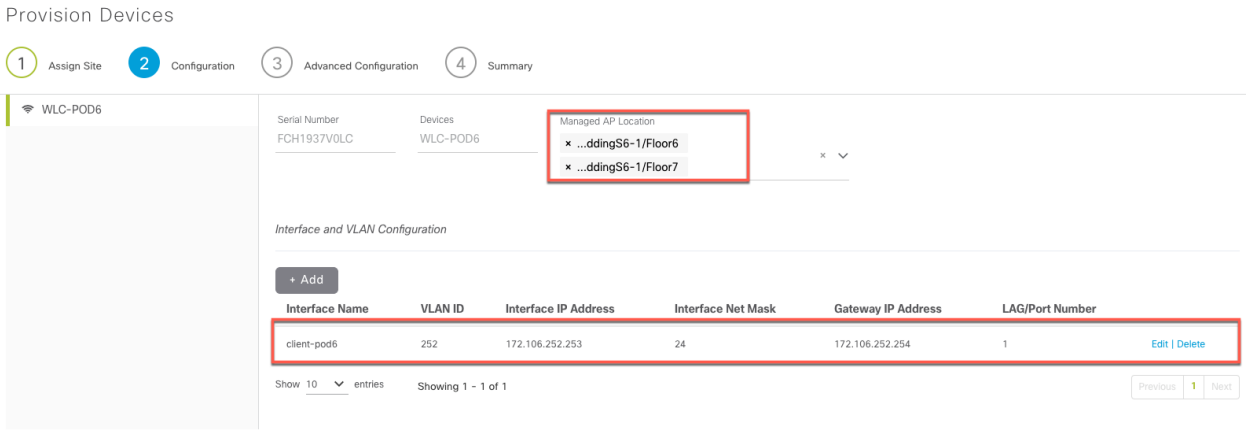
- WLC
- AP

WLC provisioning

- Assign controller to a site ➔ selection of site properties and network profiles



- Which floors are managed by the controller ➔ AP group per floor with appropriate WLANs
- Interface parameters (non fabric) to associate with WLAN



WLC provisioning

Provision Devices

1 Assign Site 2 Configuration 3 Advanced Configuration 4 Summary

3 Advanced Configuration 4 Summary

Device Details

Device Name:	WLC-POD6
Platform Id:	AIR-CT5520-K9
Device IP:	172.106.255.5
Device Location:	BuilddingS6-1

Network Setting

NTP Server:	10.0.255.3
AAA Network Primary Server:	192.168.40.177
AAA Client Primary Server:	192.168.40.177
	WARNING: Do not use "admin" a ISE as your AAA server. If you do
DHCP Server:	192.168.40.215
SYSLOG Server:	192.168.40.91
SNMP Trap Server:	192.168.40.91

NTP Servers

NTP Polling Interval seconds 3600

Server Index	Server Address(Ipv4/Ipv6)	Key Index	NTP Msg Auth Status
1	10.0.255.3	0	AUTH DISABLED

RADIUS Authentication Servers

Auth Called Station ID Type AP MAC Address:SSID

Use AES Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter Hyphen

Framed MTU 1300

Network User	Management	Tunnel Proxy	Server Index		Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
☑	☑	☐	1	*	192.168.40.177	1812	Disabled	Enabled

Syslog Configuration

Syslog Server IP Address(Ipv4/Ipv6) Add

Syslog Server	
192.168.40.91	Remove

WLC provisioning

Provision Devices

1 Assign Site 2 Configuration 3 Advanced Configuration 4 Summary

SSID

Name:	DNAC-POD6
Type:	Enterprise
Security:	wpa2_enterprise
Fast Transition:	ADAPTIVE
Traffic Type:	Voice + Data
Fabric Enabled:	No
Fast Lane Enabled:	No
Mac Filtering Enabled:	No
Flex Connect Enabled:	No

Managed Sites

As Primary:	Floor6
	Floor7

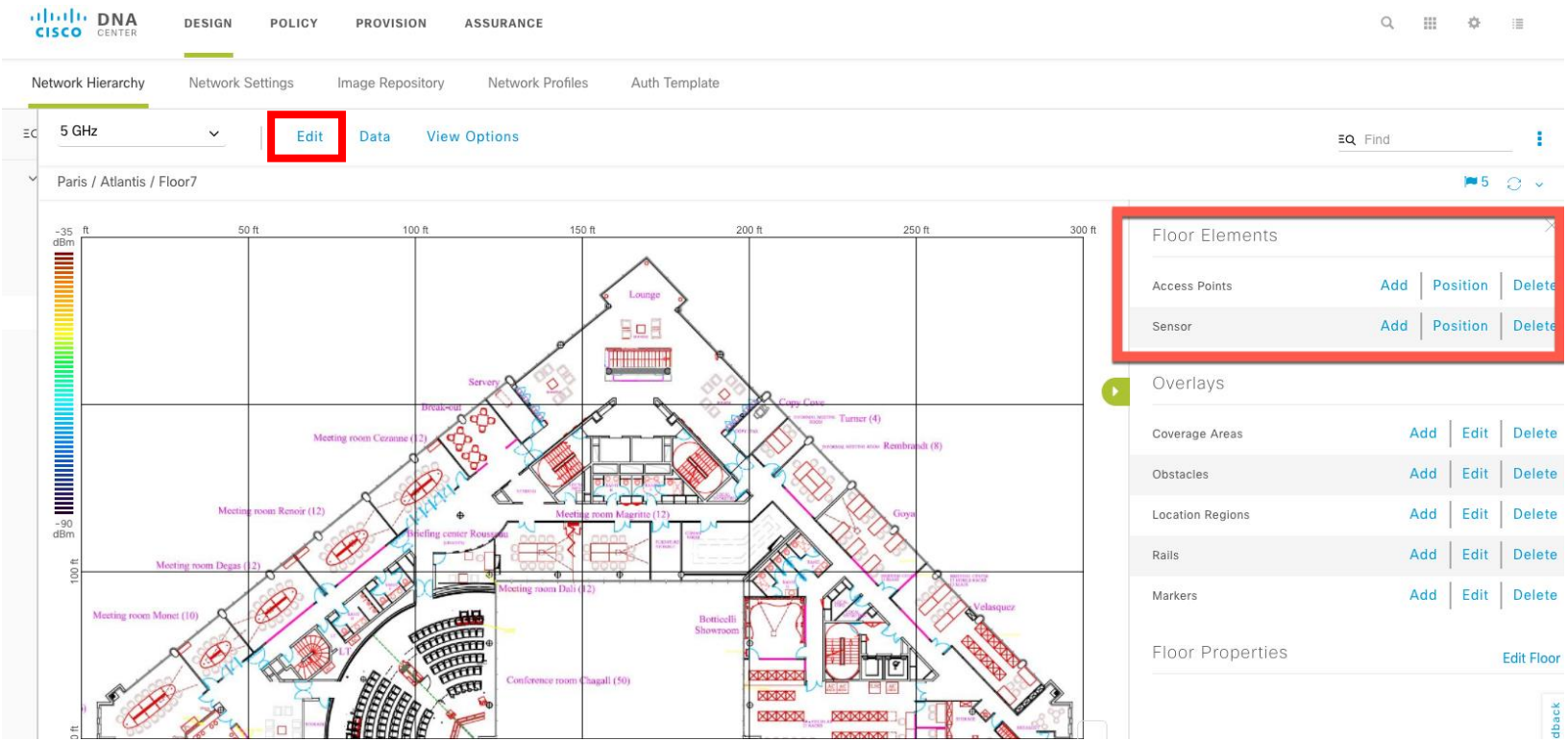
Interfaces

Name:	client-pod6
VLAN ID:	252
IP Address:	172.106.252.253
Net Mask (in bits):	24
Gateway IP Address:	172.106.252.254

General | Security | QoS | Policy-Mapping | Advanced

Profile Name	DNAC-POD6_NF_50219
Type	WLAN
SSID	DNAC-POD6
Status	☑ Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appe
Radio Policy	All
Interface/Interface Group(G)	client-pod6
Multicast Vlan Feature	☐ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	none

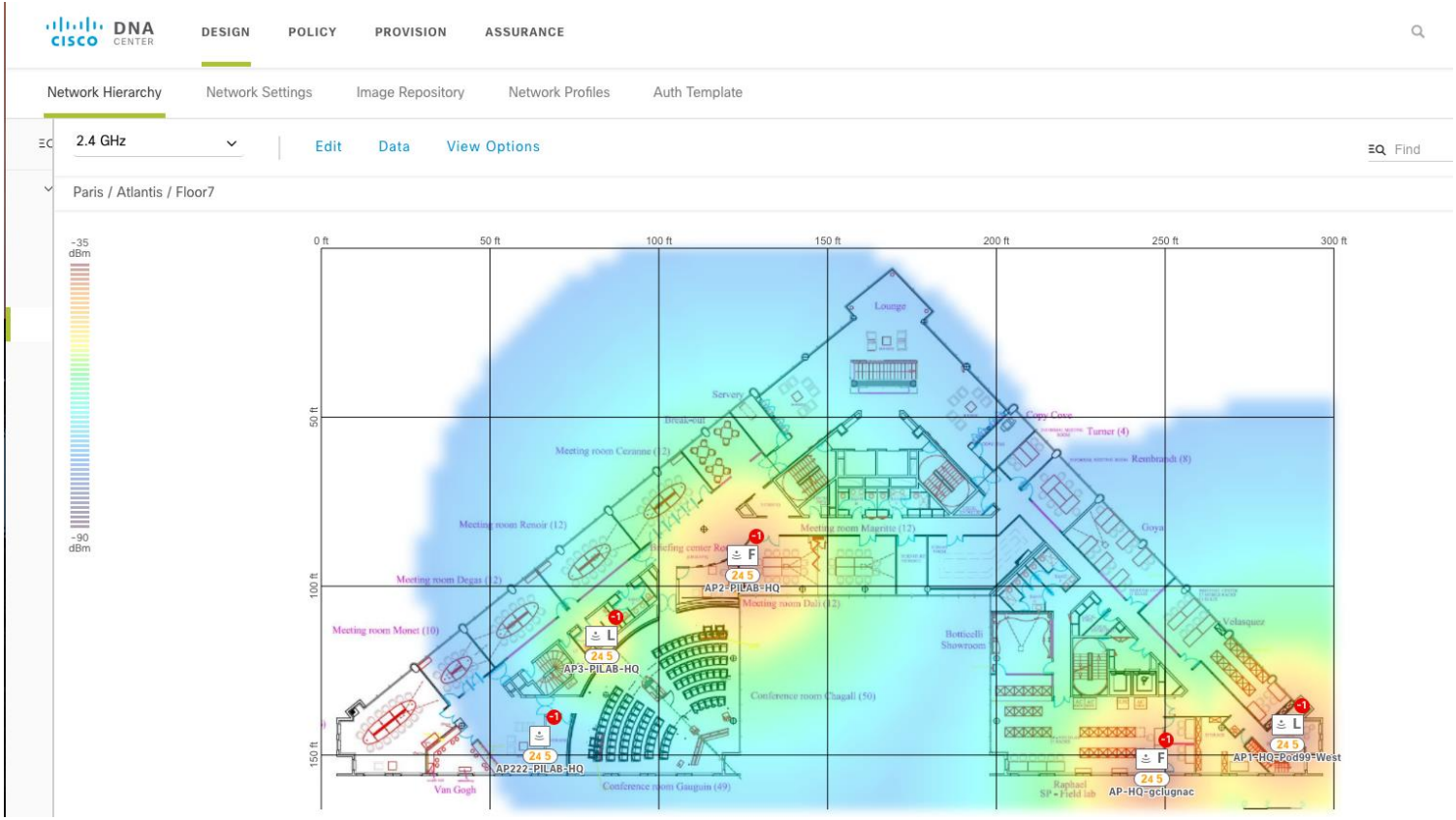
AP positioning (like Prime Infrastructure)



Map editing, AP positioning

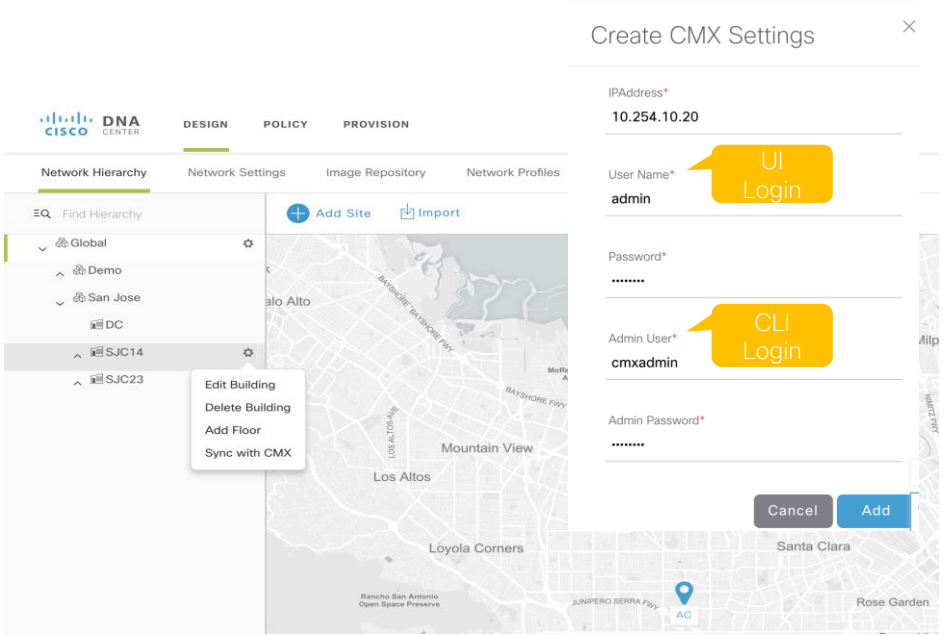
- Just like Prime Infrastructure
- Position AP: Drag and Drop, by coordinates, by 2 walls, by 3 points
- Draw overlay elements (Obstacles, Markers ...)

AP Heatmap



CMX Integration

- Simplified CMX integration via Cisco DNA Center for automation of the following manual tasks:
  - Import maps to CMX
  - Add WLCs to CMX
- The minimum supported CMX version is 10.4.1.12



Useful tools

Command Runner – A Debugging App

Tools

Discovery

Automate addition of devices to controller inventory

Inventory

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

Topolc

Visualize how devices are inte
commun

Command Runner

Allows you to run diagnostic CLIs against one or more devices

License Manager

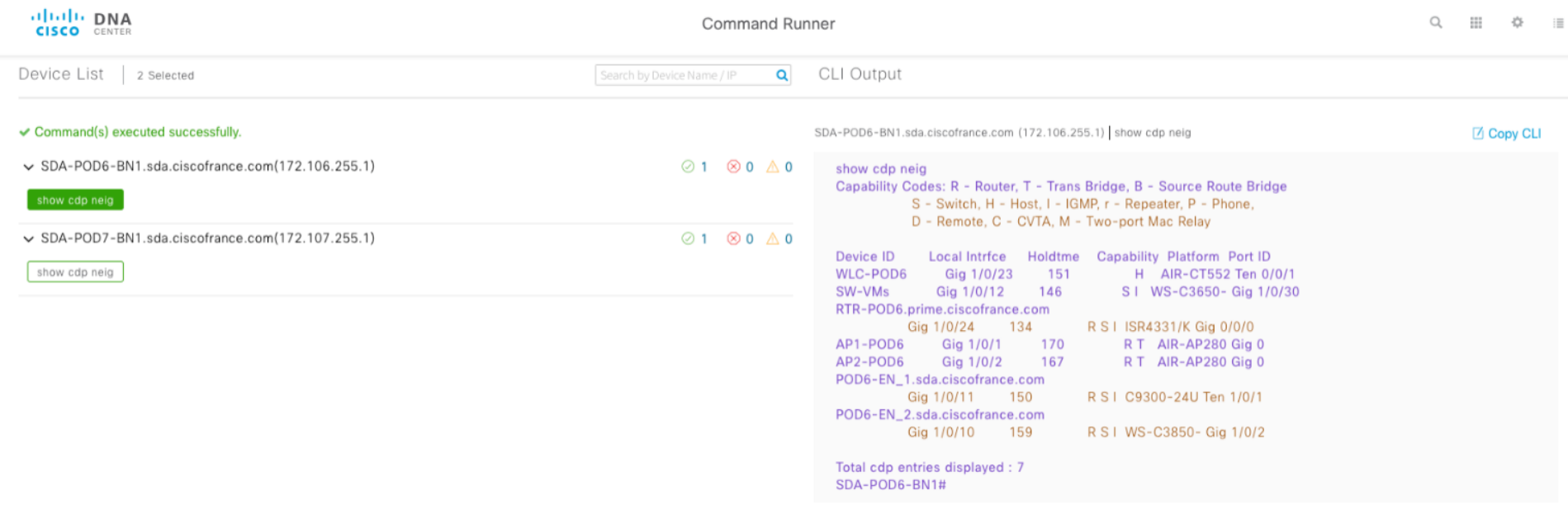
Visualize and manage license usage

Template

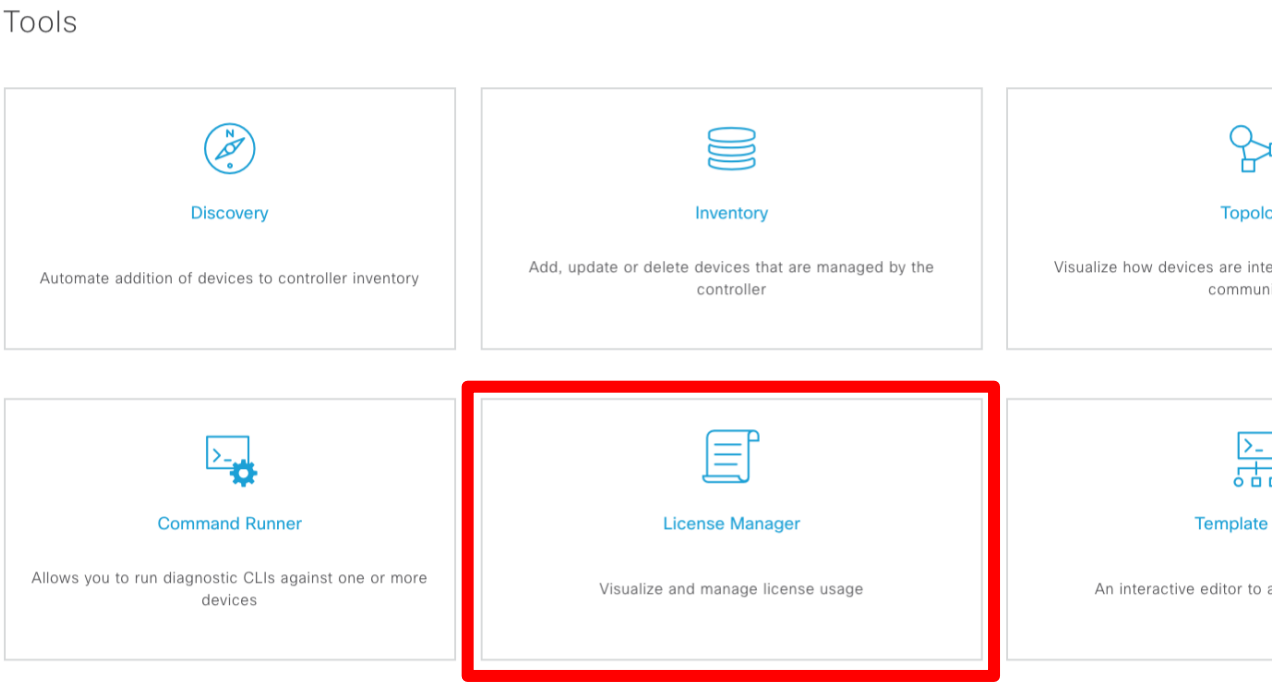
An interactive editor to a

Command Runner – A Debugging App

Command runner is Cisco DNA Center package which facilitates users to execute many read-only commands on one or more devices

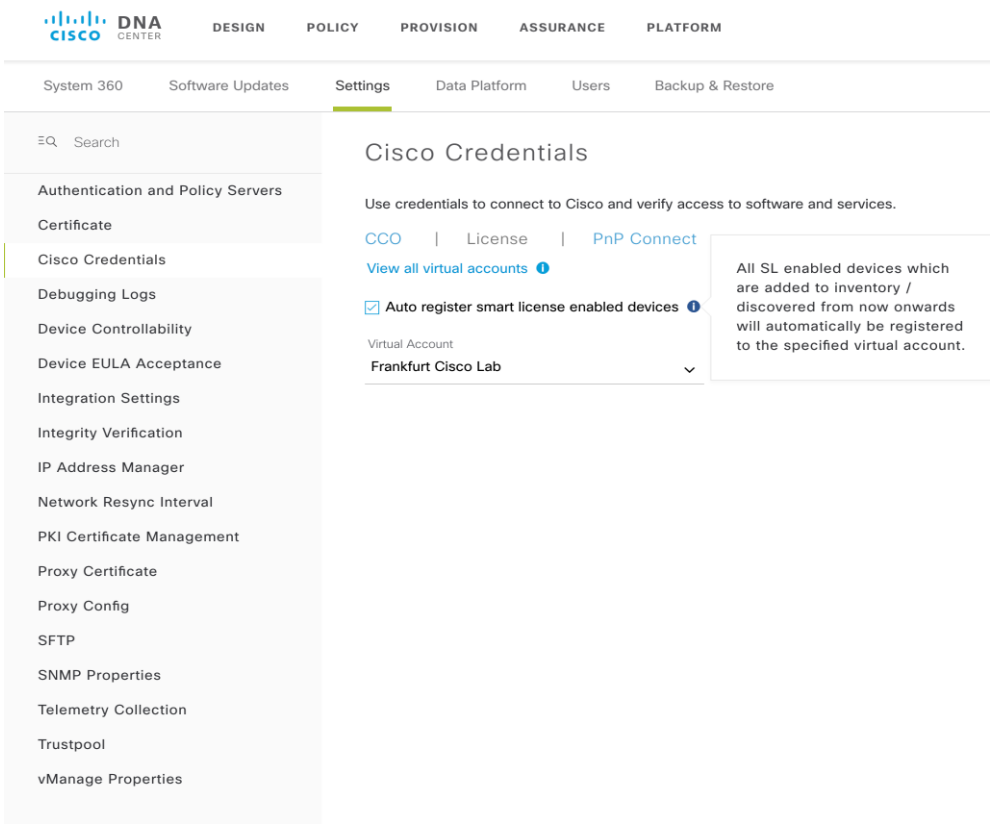


License manager – Smart licensing made easier



Manage licensing with Cisco DNA Center

- Remember Smart Licensing is now mandatory for switches starting 16.9
  - ➔ Cisco DNA Center can help !
- Cisco DNA Center allows you to register newly added devices directly into your Smart Account
- Just check the box and select the correct virtual account



Smart Account

- Cisco DNA Center creates the token using the provided credentials
- Token is used to register devices into your Smart Account

Cisco Software Central > Smart Software Licensing

English [Change] Hello, Marcel Rothstein Cisco Sales Enablement

Smart Software Licensing

Feedback Support Help

Alerts | Inventory | Convert to Smart Licensing | Reports | Preferences | Satellites | Activity

Questions About Licensing? Try our Virtual Assistant

Virtual Account: Frankfurt Cisco Lab

4 Major | Hide Alerts

General | Licenses | Product Instances | Event Log

Virtual Account

Description: Frankfurt Cisco Lab VA requested by Marcel Rothstein

Default Virtual Account: No

Product Instance Registration Tokens

The tokens are used to register product instances so they can use licenses from this virtual account.

New Token...

Token	Expiration Date	Uses	Export-Controlled	Description	Created By	Actions
YWM[redacted]	2020-Jan-15 10:09:57 (in 36…		Allowed	CL-Demo-Direct-CLI	m[redacted]	Actions
MTAz[redacted]	2020-Jan-09 16:12:59 (in 35…		Not Allowed	Token created by DNA Center	m[redacted]	Actions
ZDZj[redacted]	2020-Jan-02 09:49:55 (in 35…		Not Allowed	Token created by DNA Center	m[redacted]	Actions

The token will be expired when either the expiration or the maximum uses is reached

Showing All 3 Records

Licensing

- License comes with the device, not with Cisco DNA Center
- Cisco DNA Center licenses are term based (3/5/7 years)
- Cisco DNA Center requires a minimum of Cisco DNA Essentials licenses on the infrastructure to use "NMS" capabilities
- Cat 9k has built-in license for minimum of 3 years
- Other switches can buy add-on Cisco DNA license
  - E.g. C3850-DNA-E-24=, C2960X-DNA-E-48=, C6807-DNA-A=
- Cisco DNA license already includes service for Cisco DNA
  - Includes 24x7 TAC access, knowledge base access, software downloads for Cisco DNA only, TAC access for Perpetual stack will require SNTC or Partner Support or Solution Support

Security Advisories

Cisco DNA Center

Security Advisories

This page shows security advisories published by Cisco that may affect devices on your network based on the software image currently installed. At this time, further analysis of the configuration, platform details, or other criteria may be required to determine if a vulnerability is actually present.

Note: The information shown here is subject to the Cisco Security Vulnerability Policy.

Security Advisories Focus: Advisories

Last scanned: Jan 26, 2020 2:18 PM Scan

Advisories (66)

Filter

Advisory ID	Advisory Title	CVSS Score	Impact	CVE	Devices	Known Since (days)	Last Updated
cisco-sa-20190828-iosxe-rest-auth-bypass	Cisco REST API Container for IOS XE Software Authentication Bypass Vulnerability	10	CRITICAL	CVE-2019-12643	7	151	10/19/2019
cisco-sa-20180328-xesc	Cisco IOS XE Software Static Credential Vulnerability	9.8	CRITICAL	CVE-2018-0150	1	669	09/20/2018
cisco-sa-20170317-cmp	Cisco IOS and IOS XE Software Cluster Management Protocol Remote Code Execution Vulnerability	9.8	CRITICAL	CVE-2017-3881	1	1045	04/18/2019
cisco-sa-20180328-smi2	Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability	9.8	CRITICAL	CVE-2018-0171	1	669	05/04/2018
cisco-sa-20200108-ios-csrf	Cisco IOS and Cisco IOS XE Software Web UI Cross-Site Request Forgery Vulnerability	8.8	HIGH	CVE-2019-16009	2	18	01/09/2020
cisco-sa-20170629-snmp	SNMP Remote Code Execution Vulnerabilities in Cisco IOS and IOS XE Software	8.8	HIGH	CVE-2017-6740,CVE-2017-6743,CVE-2017-6744,CVE-2017-6741,CVE-2017-6742,CVE-2017-6736,CVE-2017-6737,CVE-2017-6738,CVE-2017-6739	1	941	04/18/2019

RMA workflow – replace faulty devices

DEVICES (1)
FOCUS: Inventory

Global > Germany > RMA Area > ALZ1

DEVICE TYPE: All | Routers | Switches | APs | WLCs

REACHABILITY: All | Reachable | Unreachable

Filter | Add Device | Tag Device | Actions | 1 Selected

- Inventory
- Software Image
- Provision
- Device Replacement
  - Replace Device
  - Unmark for Replacement
  - Mark for Replacement
- Others

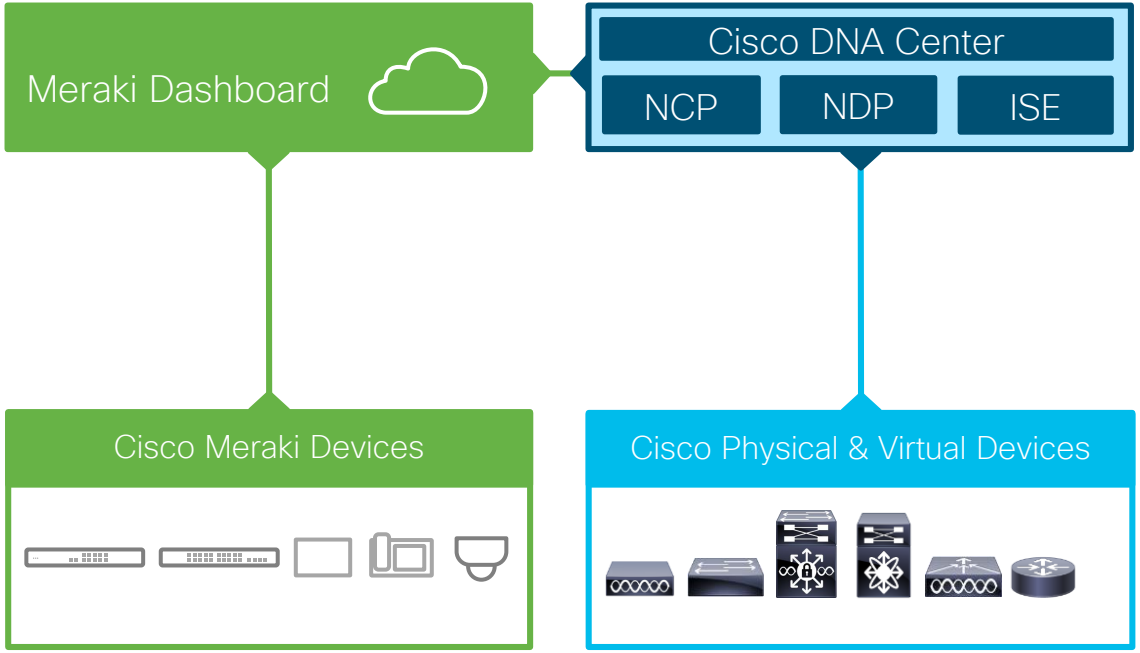
	Device Name	IP Address		Site	Reachability	MAC Address	Device Role	Image Version
☑	RMA-Switch	172.20.11.100	Hubs	.../RMA Area/ALZ1	Reachable	08:ec:f5:bd:6b:80	ACCESS	16.12.1

Demo
RMA Workflow

RMA – good to know

- 1:1 replacement only (same HW)
- PnP supported (zero touch)
- SDA supported with manual work (no PnP within SDA today)
- No support for stacked switches, dual SUP devices, Nexus, WLC today
- Licensed is not removed from CSSM
- SW (IOS) update is supported
  - Config sync (daily at 11pm archieved)
  - Vlan.dat sync

Meraki Visibility in Cisco DNA Center



Why does it matter?

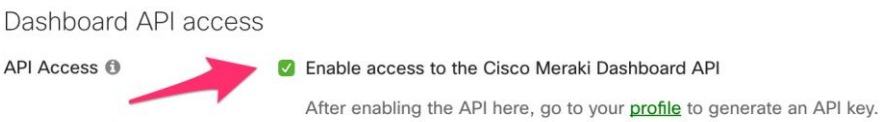
- Starting point of integration between Cisco's access platforms
- Provides hybrid (Cisco DNA + Meraki) customers a single management pane of glass

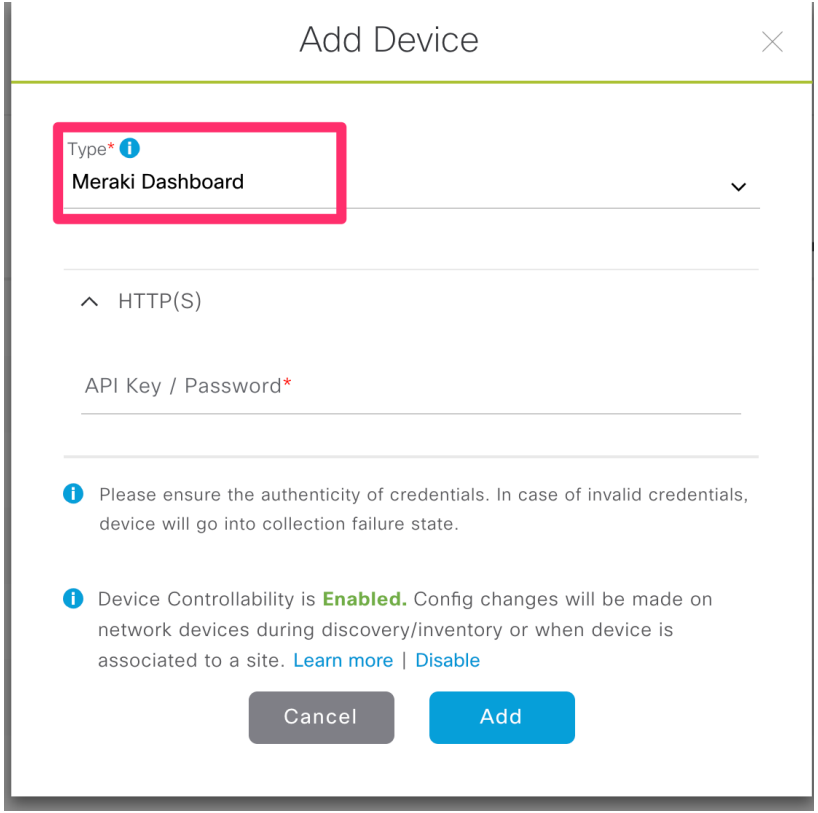
Target Use Case:

- Customer is an existing Meraki branch customer but exploring/installing Cisco DNA-C and Cat9K
- Customer has a mixed branch environment

Adding Meraki Devices

- Click on: „Add device“ in inventory
- Select Meraki Dashboard as type
- Add your token from Meraki Dashboard (Organization –> Settings)





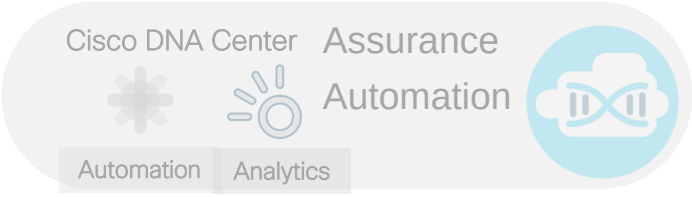
BREAK !
15 minutes

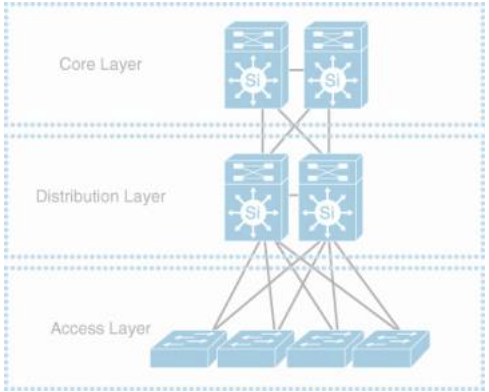
Agenda

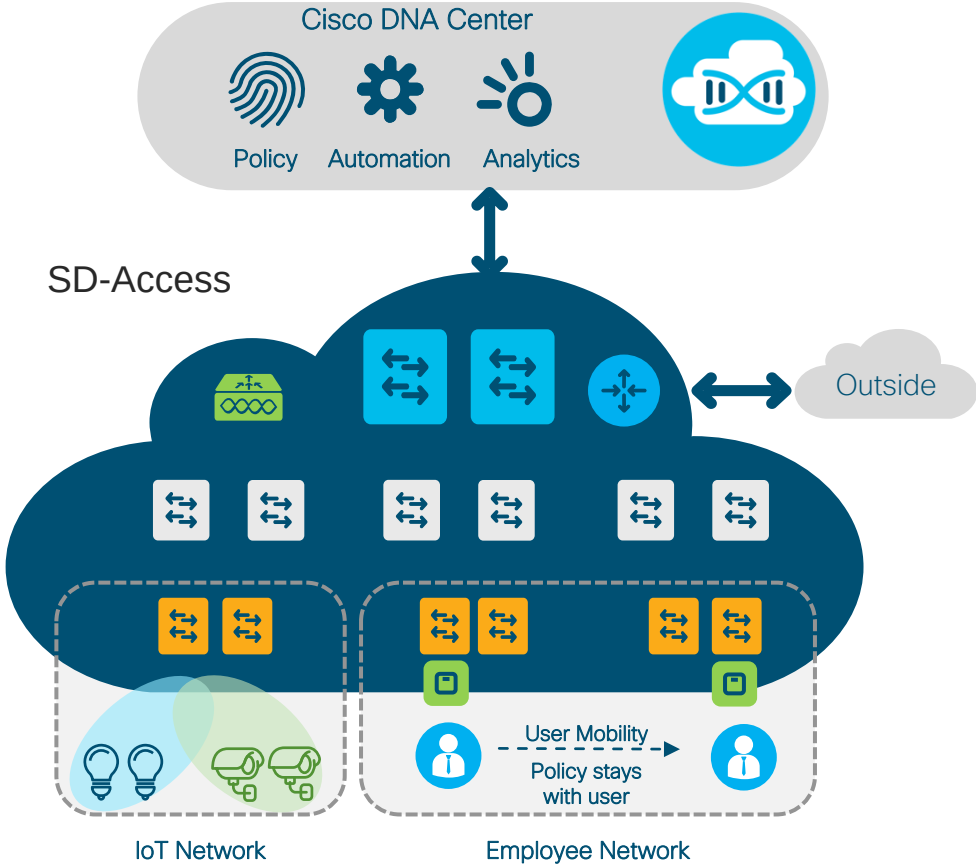
- Cisco DNA Center 10 minutes overview
- Before you deploy – purchase and design considerations
- Base automation for wired and wireless
- **Getting started with Cisco SD-Access**
- Assurance and application policies
- Key takeaways

What can I do with Cisco DNA Center to automate SD-Access ?

Classic Design

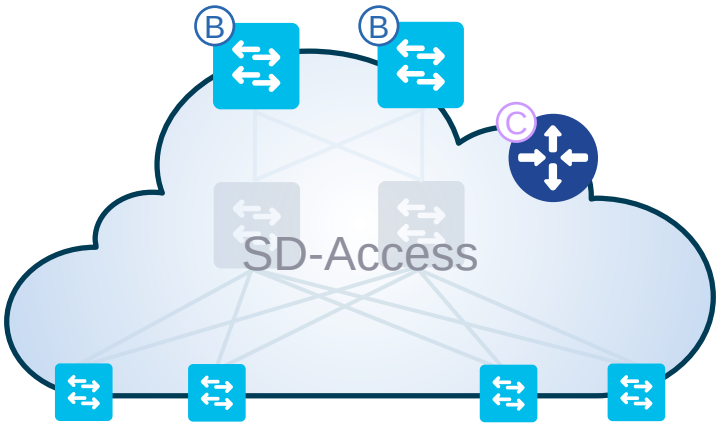






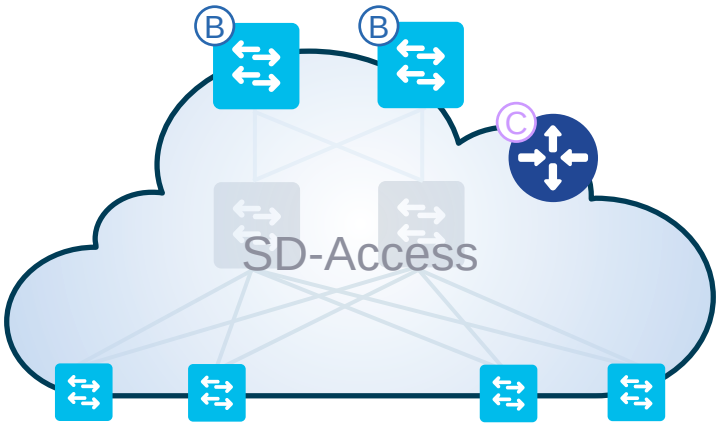
SD-Access agenda

- Introduction to SD-Access
- Underlay automation
- Fabric provisioning
- Policy definition
- Host onboarding



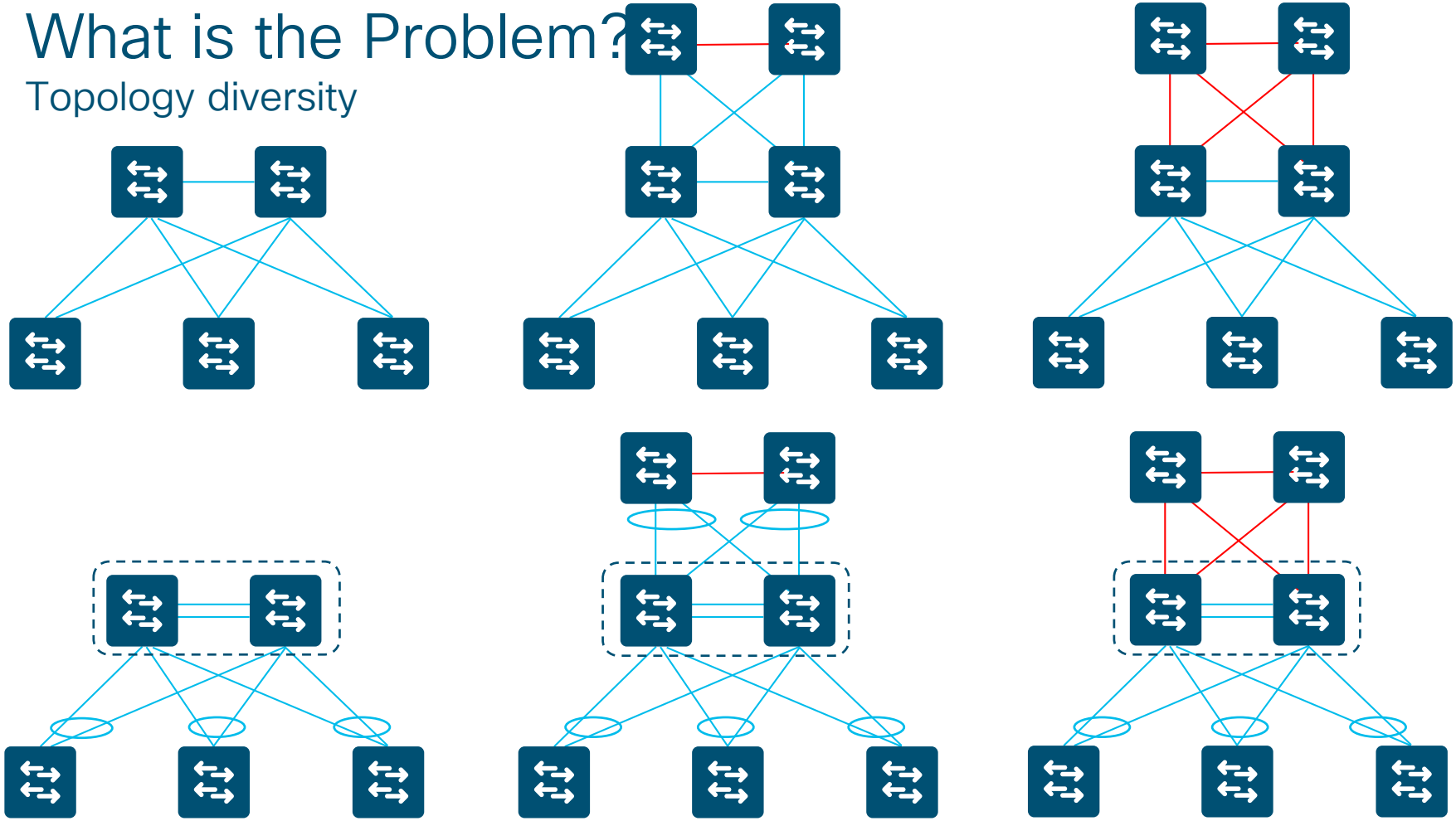
SD-Access agenda

- Introduction to SD-Access
- Underlay automation
- Fabric provisioning
- Policy definition
- Host onboarding



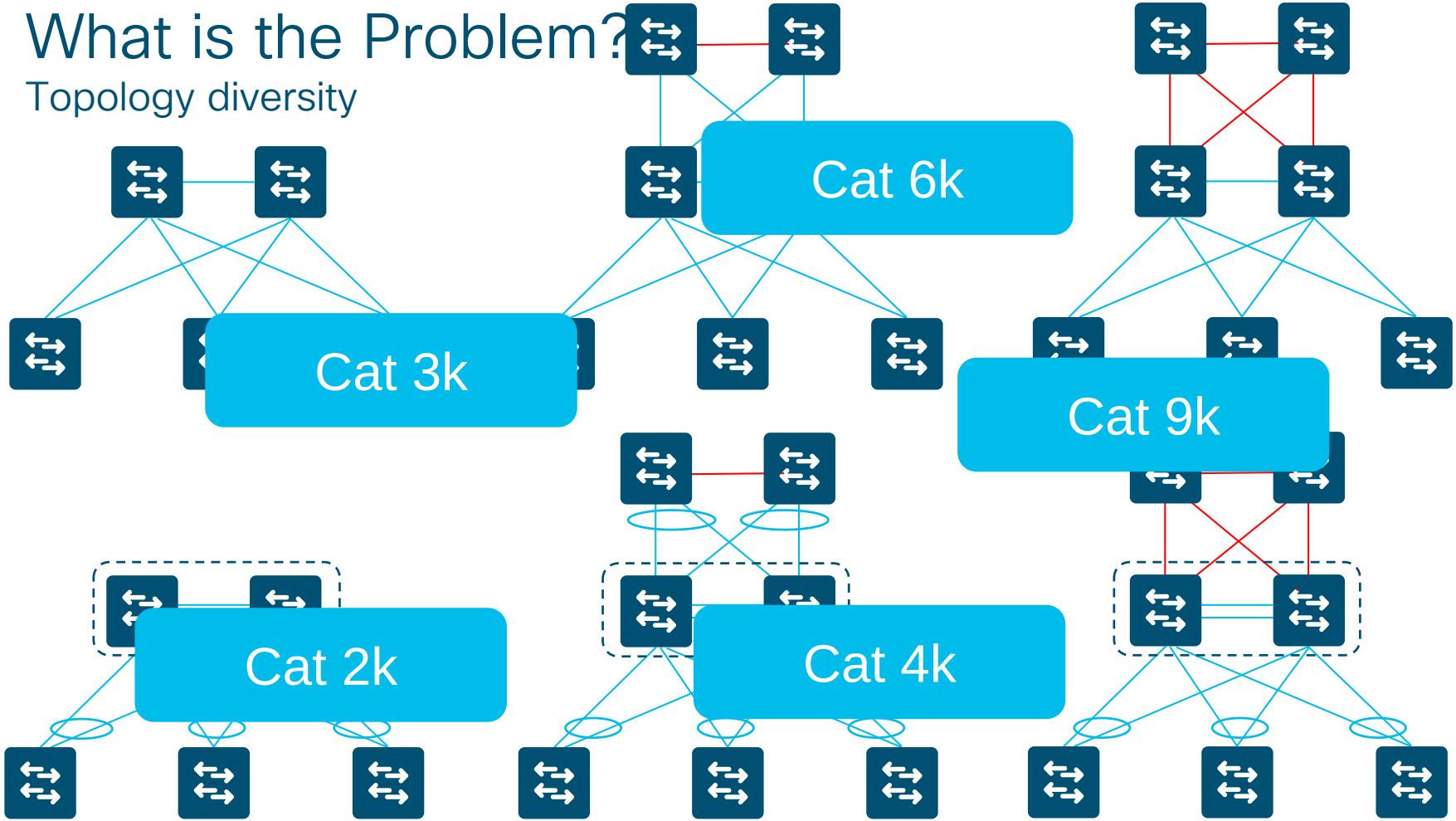
What is the Problem?

Topology diversity



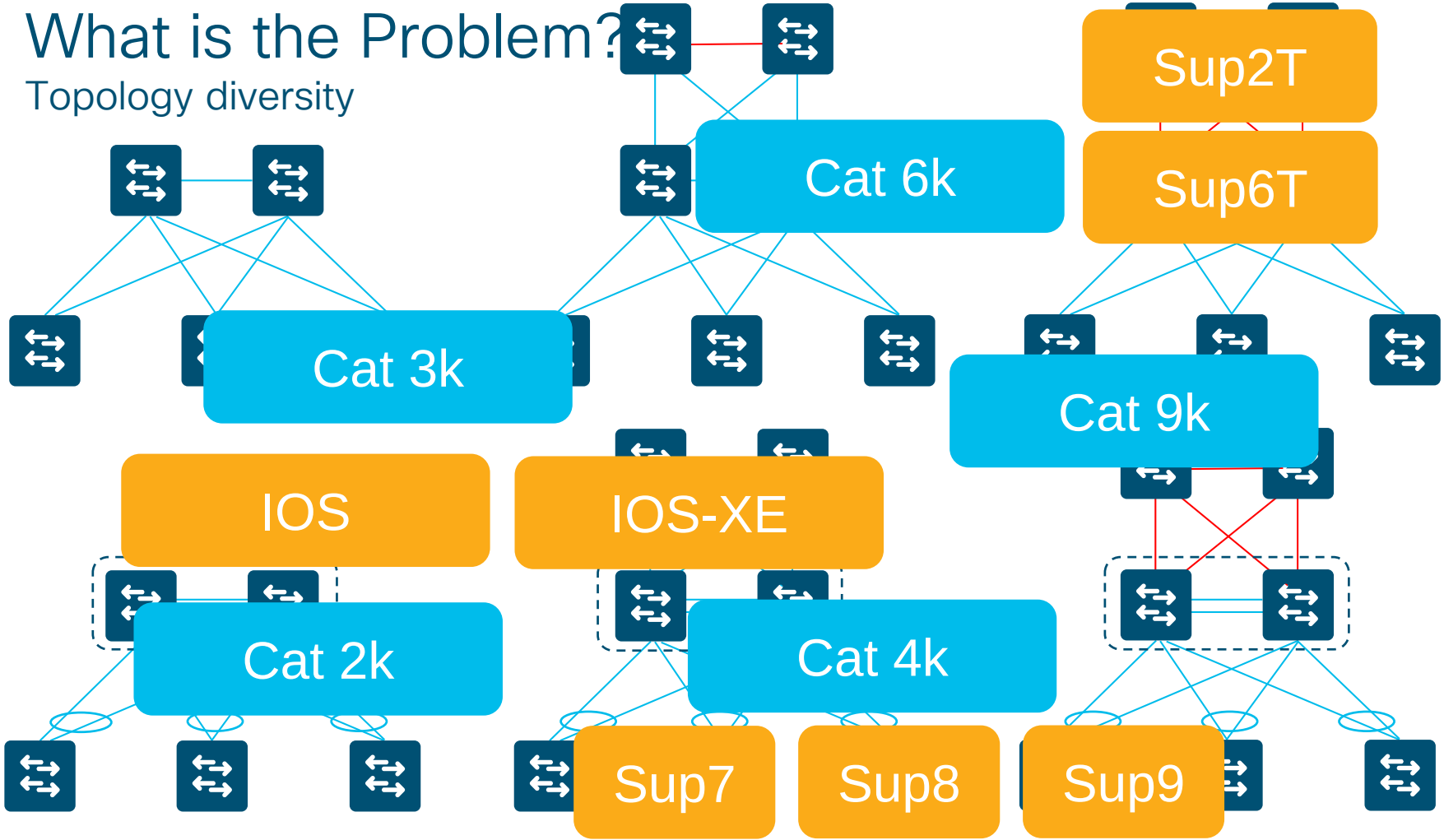
What is the Problem?

Topology diversity



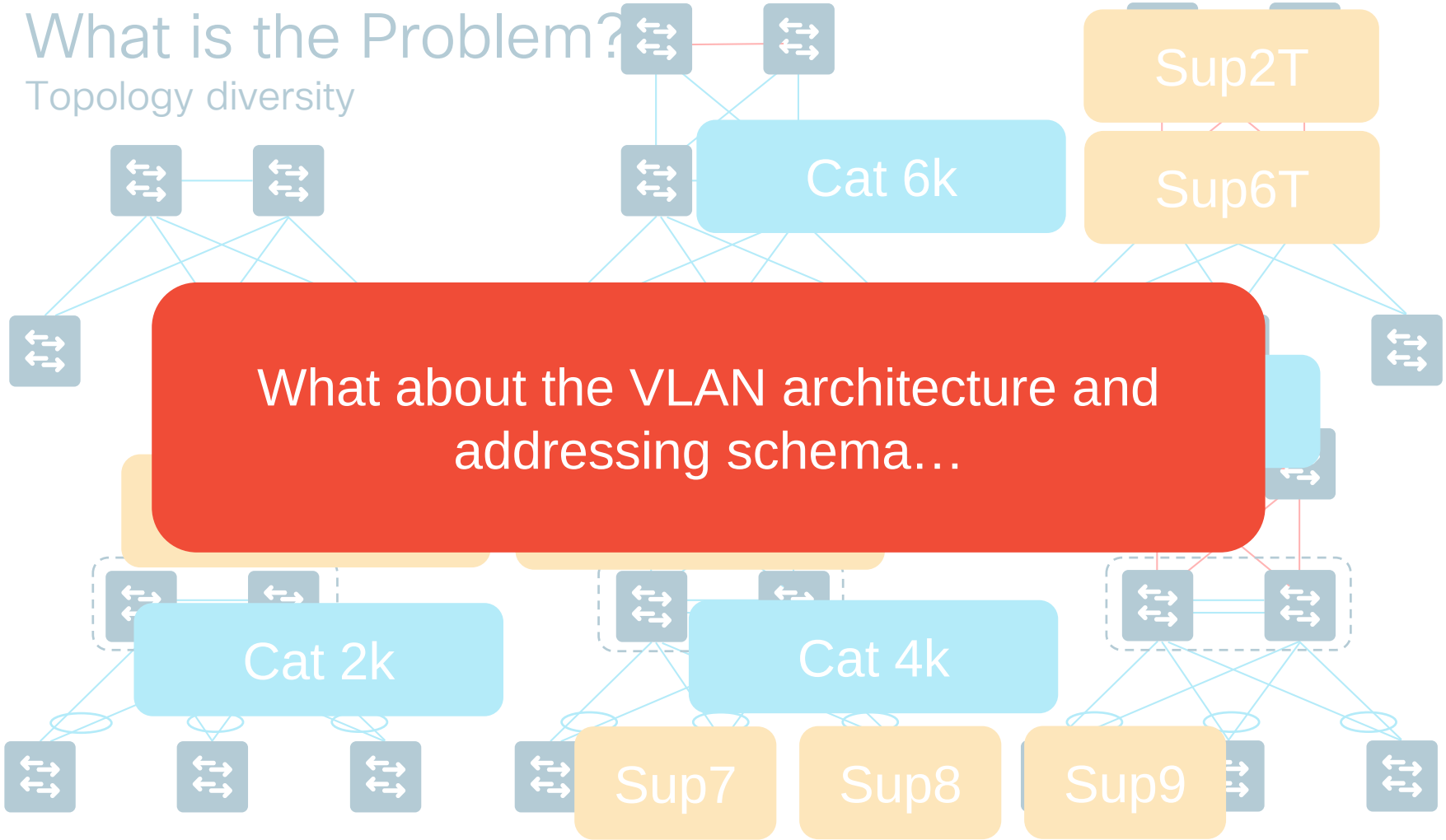
What is the Problem?

Topology diversity



What is the Problem?

Topology diversity



What about the VLAN architecture and addressing schema…

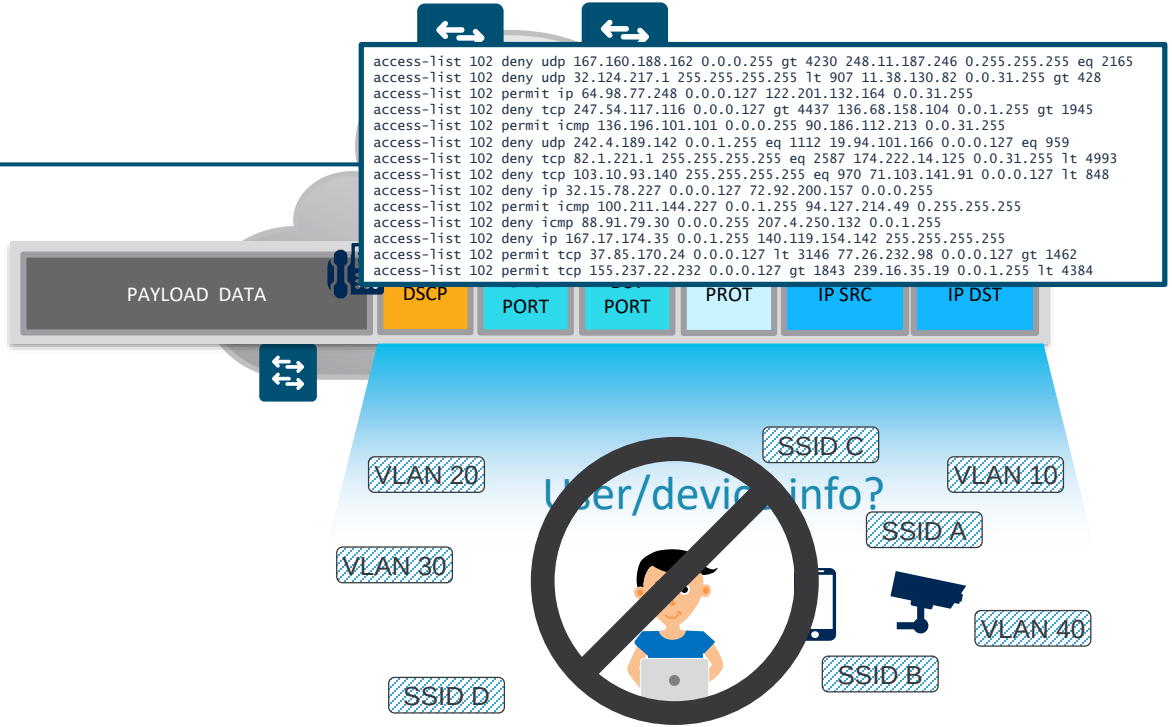
What is the Problem?

Policy Model has an impact on topology

Network Policy

IP ADDRESSES

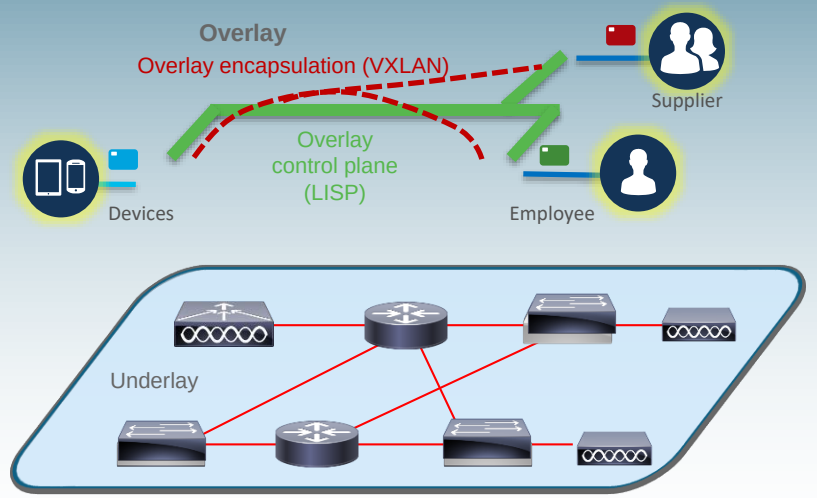
- **Locate you**
- **Identify you**
- **Drive "treatment"**
- **Constrain you**



Solution? – Create a FABRIC that separates "Forwarding Plane" from the "Services Plane"

Fabric brings Policy Simplification

Fabric breaks dependency between IP and Policy. Separation of Forwarding and Services planes. In Fabric Polices are tied to User/Device Identity



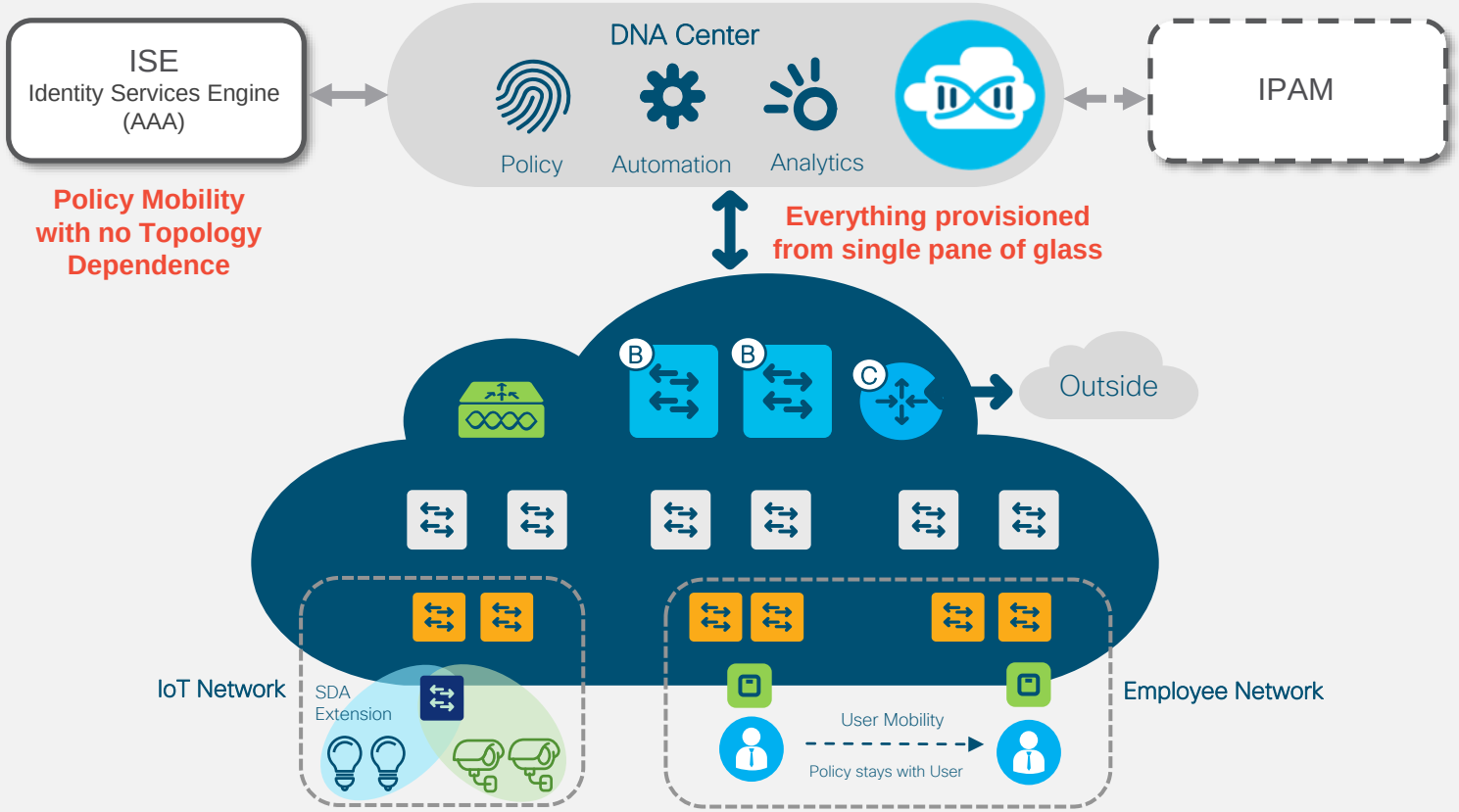
Fabric Overlay – Services plane

- Dynamically connects Users/Devices/Things
- End to End Policies and Segmentation
- **Homogeneous – Easy to automate**

Fabric Underlay – Forwarding plane

- Connects the network elements to each other
- Optimized for traffic forwarding (resiliency, performance)
- **Homogeneous – Easy to automate**

SD-Access overall architecture



Fabric Enables any Service or Policy on any Port

Before you start - SD-Access CVDs

For Your Reference

Software-Defined Access

Solution Design Guide

October, 2019

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/sda-sdg-2019oct.pdf

Software-Defined Access Medium and Large Site Fabric Provisioning

Solution Adoption Prescriptive Reference Deployment Guide

October 2019

https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/sda-fabric-deploy-2019oct.pdf

Software-Defined Access & Cisco DNA Center Management Infrastructure

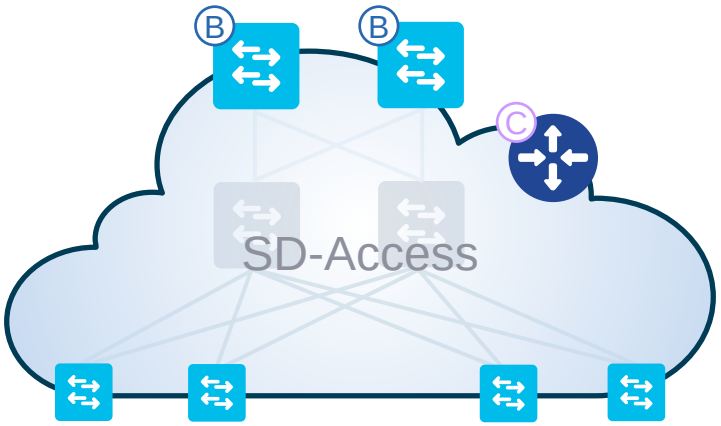
Solution Adoption Prescriptive Reference Deployment Guide

October, 2019

https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/sda-infra-deploy-2019oct.pdf

SD-Access agenda

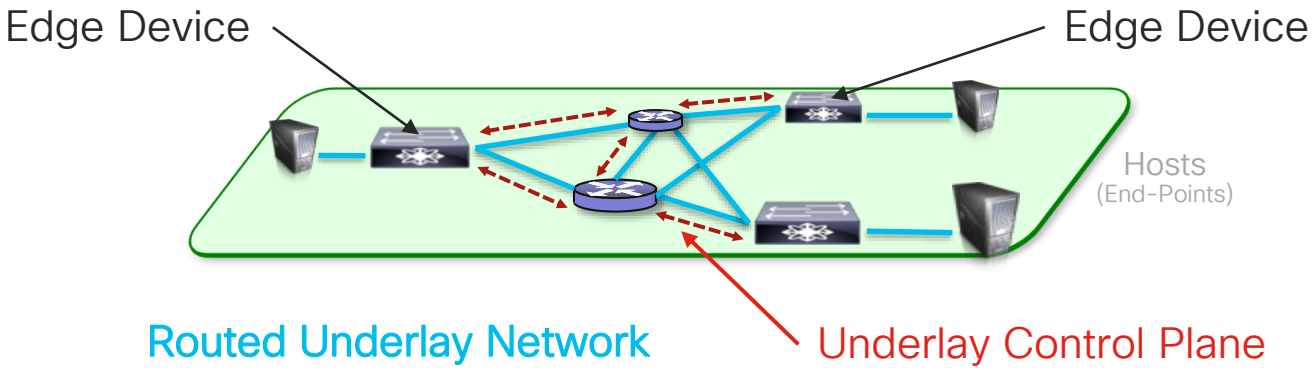
- Introduction to SD-Access
- Underlay automation
- Fabric provisioning
- Policy definition
- Host onboarding



Start building SD-Access fabric underlay

Do it manually

Use
LAN Automation



Start building SD-Access fabric underlay

Do it manually considerations

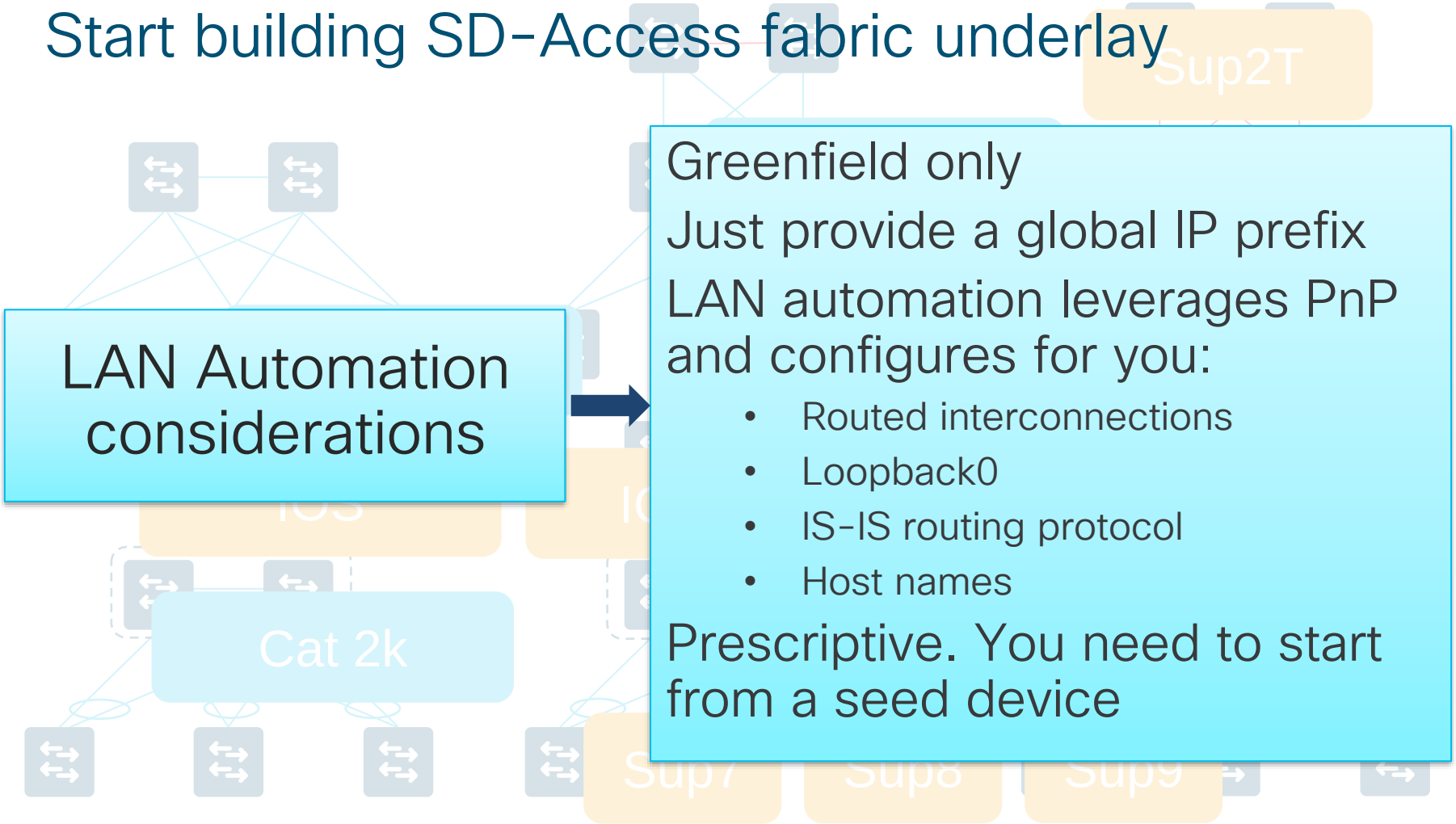
Greenfield or Brownfield

Configure via CLI

- Routed interconnections
- Loopback0
- Routing protocol for Loopback reachability

Not very complex but you have to do it

Start building SD-Access fabric underlay



LAN Automation considerations

Greenfield only

Just provide a global IP prefix

LAN automation leverages PnP and configures for you:

- Routed interconnections
- Loopback0
- IS-IS routing protocol
- Host names

Prescriptive. You need to start from a seed device

Prepare your seed devices – interface configuration

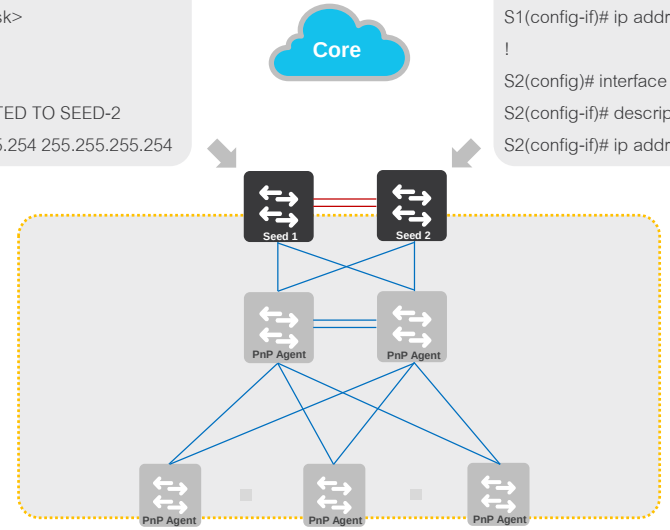
For Your Reference

Seed-1

```
S1(config)# interface Loopback 0
S1(config-if)# ip address <ip> <mask>
!
S1(config)# interface <id>
S1(config-if)# description CONNECTED TO SEED-2
S1(config-if)# ip address 10.128.255.254 255.255.255.254
```

Seed-2

```
S1(config)# interface Loopback 0
S1(config-if)# ip address <ip> <mask>
!
S2(config)# interface <id>
S2(config-if)# description CONNECTED TO SEED-1
S2(config-if)# ip address 10.128.255.255 255.255.255.254
```



IP Address Plan

Plan and identify Network Address range for Underlay Automation network

Manually configure IP subnet on inter-seed switch interfaces from Underlay network address range if there is interconnection

Loopback Interface

Leverage existing Loopback interface or create new if required

Loopback IP could be outside of domain Network address range, but must be reachable to Cisco DNA Center

Prepare your seed devices – routing configuration

Global approach

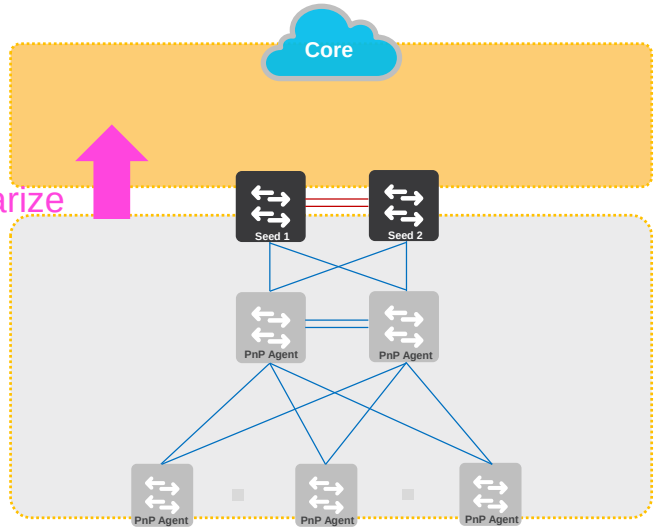
For Your Reference

Use routing protocol of your choice

Summarize

Redistribute

IS-IS deployed by LAN automation



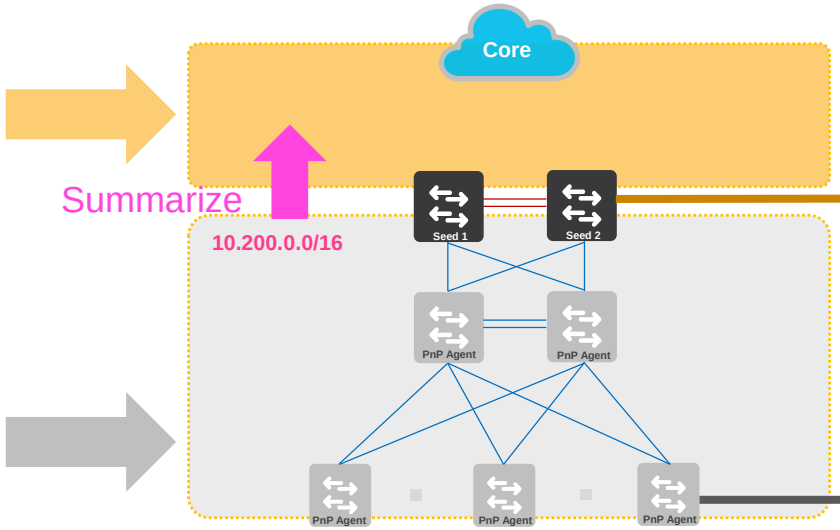
Prepare your seed devices - routing configuration

For Your Reference

Example in case you use OSPF in the core

OSPF deployed manually

IS-IS deployed by LAN automation



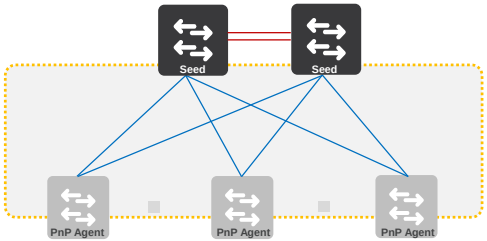

```
router isis
 redistribute ospf 1

router ospf 1
 redistribute connected
 summary-address
10.200.0.0 255.255.0.0
```

Automated

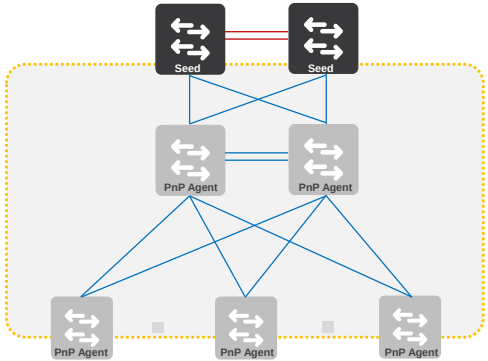
```
router isis
 net <AUTO>
 domain-password cisco
 metric-style wide
 log-adjacency-changes
 nsf ietf
 bfd all-interfaces
```

Supported topologies for a single LAN automation process

2 Tier – Collapsed Core Design



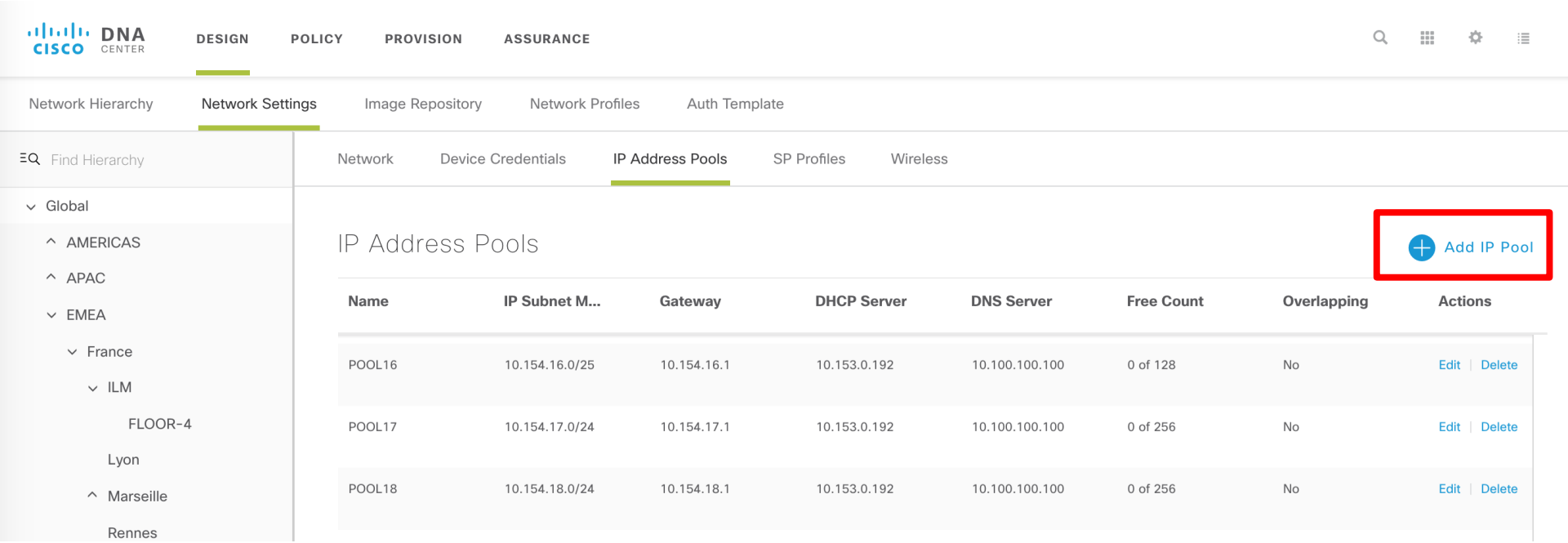
3 Tier – Campus Design



Have different topology ?

Remember you can do underlay manually or do LAN automation several times!

Specify IP address pool that will be used for LAN automation



Specify IP address pool that will be used for LAN automation

Add IP Pool

IP Pool Name *
GLOBAL-UNDERLAY

IP Subnet *
10.200.0.0

CIDR Prefix
/16 (255.255.0.0)

Gateway IP Address *
10.200.0.1

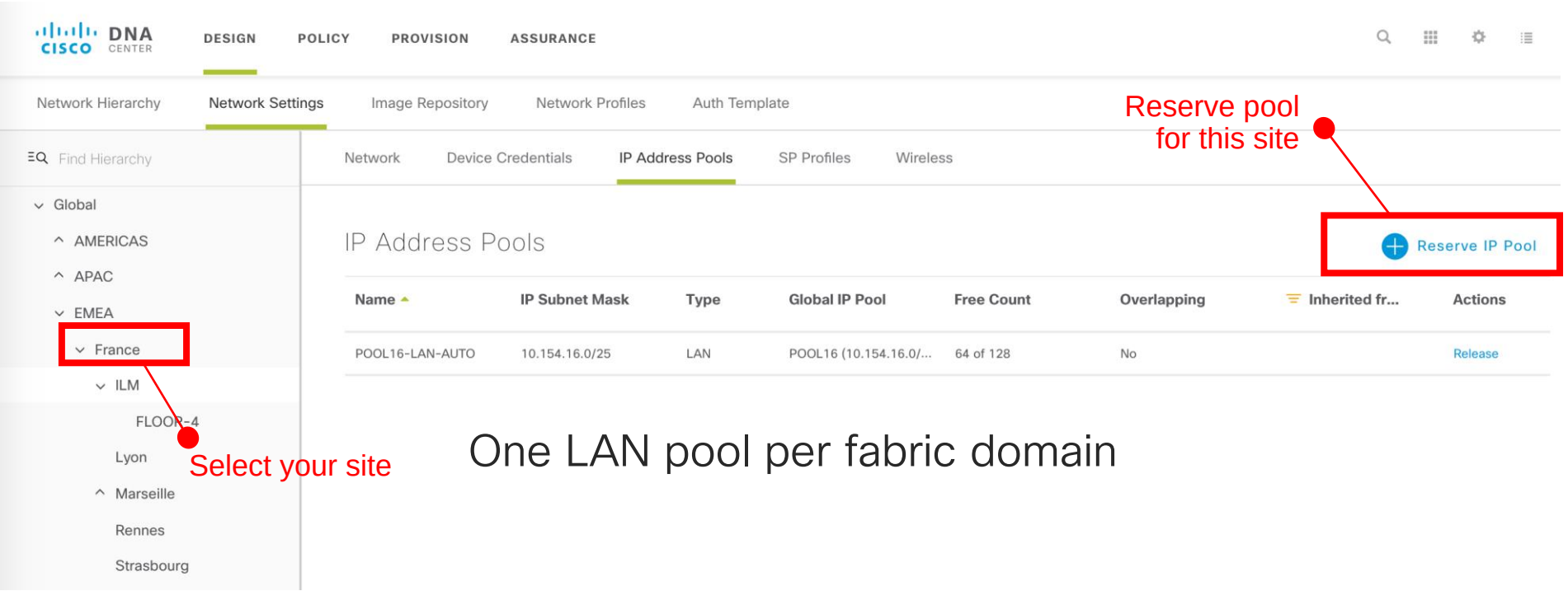
DHCP Server(s)

DNS Server(s)

☐ Overlapping

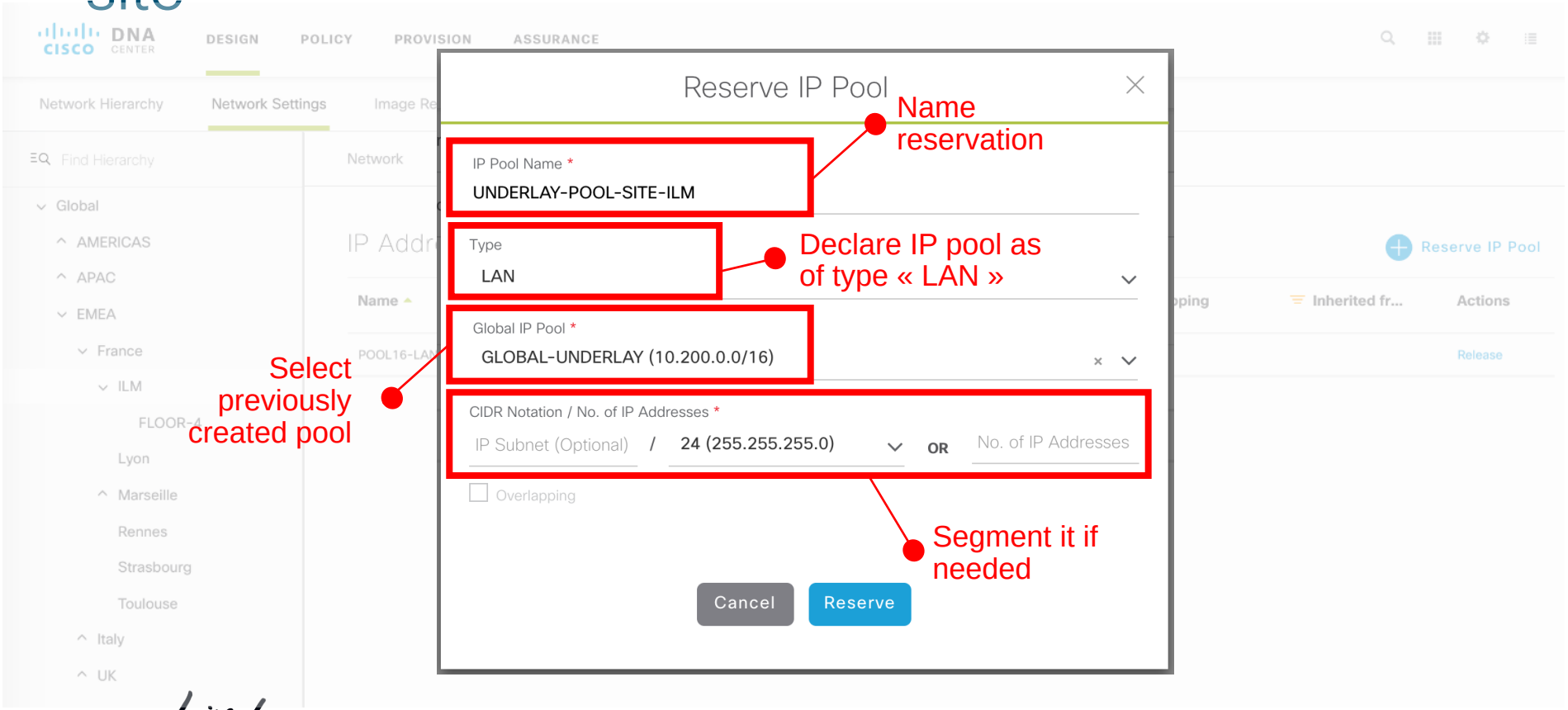
Cancel Save

Reserve the pool for LAN automation on desired site



One LAN pool per fabric domain

Reserve the pool for LAN automation on desired site



LAN automation overall process

For Your Reference

- Define site with characteristics (includes credentials)
- Reserve an IP address pool for your LAN addressing (P2P links / loopbacks)
- Select your seed devices for automation (usually the core/distribution switches)
  - These ones will be configured manually
- Ensure the configuration is compatible with LAN automation
  - Check existing routing protocols and redistribution
- Discover manually seed devices
- Enable LAN automation
  - Choose interfaces where you want to discover downstream switches
  - Choose prefix to be configured in hostname of discovered switches
- LAN automation does it all (discover devices, allocate host names and addresses, give credentials, add them in Cisco DNA Center)
- Stop LAN automation
- Newly discovered switches are now ready for fabric provisioning

Repeat as many times as needed (for example if you add a new switch)

Demo
LAN Automation

QuickTime Player File Edit View Window Help 100% Tue 11:04 ilukic

Home - Cisco DNA Center

Not Secure | fra-dnac-r3.cisco.com/dna/home

Incognito

Edge1-3650-48T - SecureCRT

Connect Change State Print Configuration

Enter host

Connect Bar

Edge1-3650-48T | Edge2-3650-48P | Intermediate1-3850-12XS | Intermediate2-3850-12S | Border1 | Border2

Session Manager

```
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]:
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]:
```

Ready

Telnet: 172.20.12.254 5, 69 26 Rows, 100 Cols Xterm

Cisco DESIGN POLICY PROVISION ASSURANCE PLATFORM

Welcome, Ivana Lukic

Take a Tour

Learn More

Assurance

Health

Healthy as of Jan 21, 2020 10:58 AM

82% Network Devices | 80% Wireless Clients | 100% Wired Clients

View Details

Critical Issues

Last 24 Hours

11 P1 | 19 P2

View Details

Trends and Insights

Last 7 Days

0 Throughput | 0 Coverage | 0 Capacity

View Details

Network Snapshot

Sites

As of Jan 21, 2020 10:59 AM

46

DNS Servers : 2

NTP Servers : 1

Add Sites

Network Devices

As of Jan 21, 2020 10:59 AM

74

Unclaimed: 4

Unprovisioned: 39

Unreachable: 9

Find New Devices

Application Policies

As of Jan 21, 2020 11:03 AM

1

Successful Deploys: 1

Errored Deploys: 0

Stale Policies: 1

Add New Policy

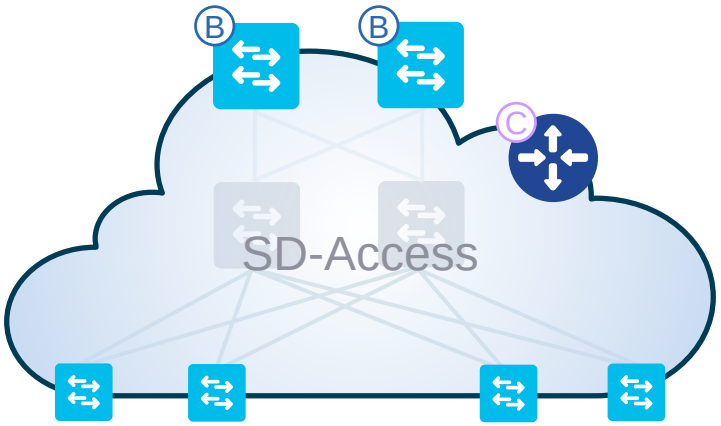
Network Profiles

Images

Cisco DNA Licensed Devices

SD-Access agenda

- Introduction to SD-Access
- Underlay automation
- Fabric provisioning
- Policy definition
- Host onboarding



SD-Access Fabric technologies

LISP based Control-Plane

RFC6830 – RFC6831 – RFC6832 – RFC6833 – RFC6834 – RFC6835 – RFC6836 – RFC7052 – RFC 7215
RFC7834 – RFC7835 – RFC7954 – RFC7955 – RFC8060 – RFC8061 – RFC8011 – RFC8013

VXLAN based Data-Plane

RFC7348

Integrated Cisco TrustSec

IETF draft-smith-vxlan-group-policy-05 - draft-smith-kandula-sxp-06

SD-Access Fabric technologies

VXLAN = Ethernet in UDP

Means routed underlay (from access)

Say goodbye to spanning-tree issues !!!

LISP based

RFC6830 – RFC6831 – RFC6832 – RFC6833 – RFC6834 – RFC6835 – RFC6836 – RFC7052 – RFC 7215
RFC7834 – RFC7835 – RFC7954 – RFC7955 – RFC8060 – RFC8061 – RFC8011 – RFC8013

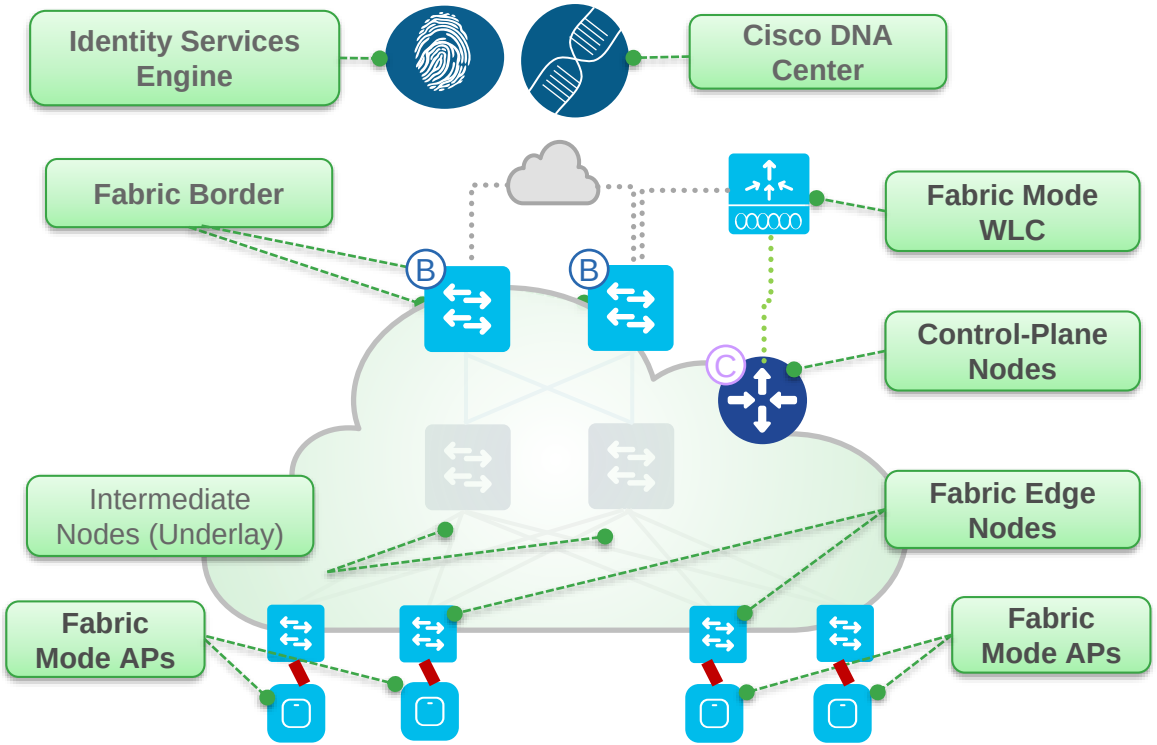
VXLAN based Data-Plane

RFC7348

Integrated Cisco TrustSec

draft-smith-vxlan-group-policy-05 - draft-smith-kandula-sxp-06

SD-A roles and terminology

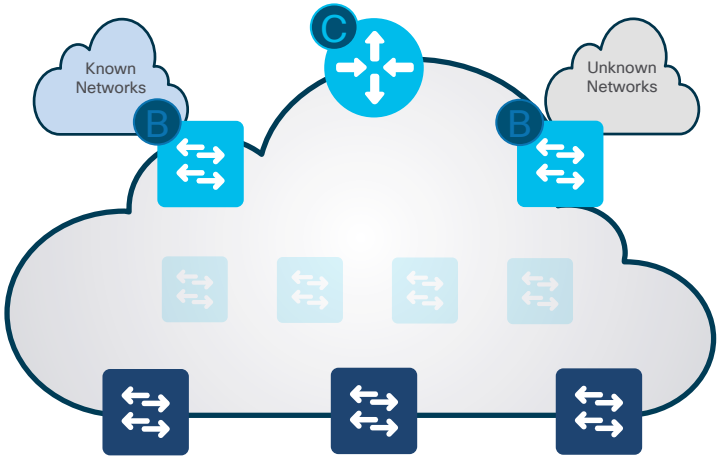


- **Cisco DNA Center** – Automation appliance for fabric automation, policy and assurance
- **ISE – Identity Service Engine** – advanced AAA solution, implements segmentation using trustsec
- **Control-Plane Nodes** – Map System that manages Endpoint ID to Device relationships. Can be collocated with Border Node
- **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** – Wireless Controller (WLC) that is fabric-enabled
- **Fabric Mode APs** – Access Points that are fabric-enabled.

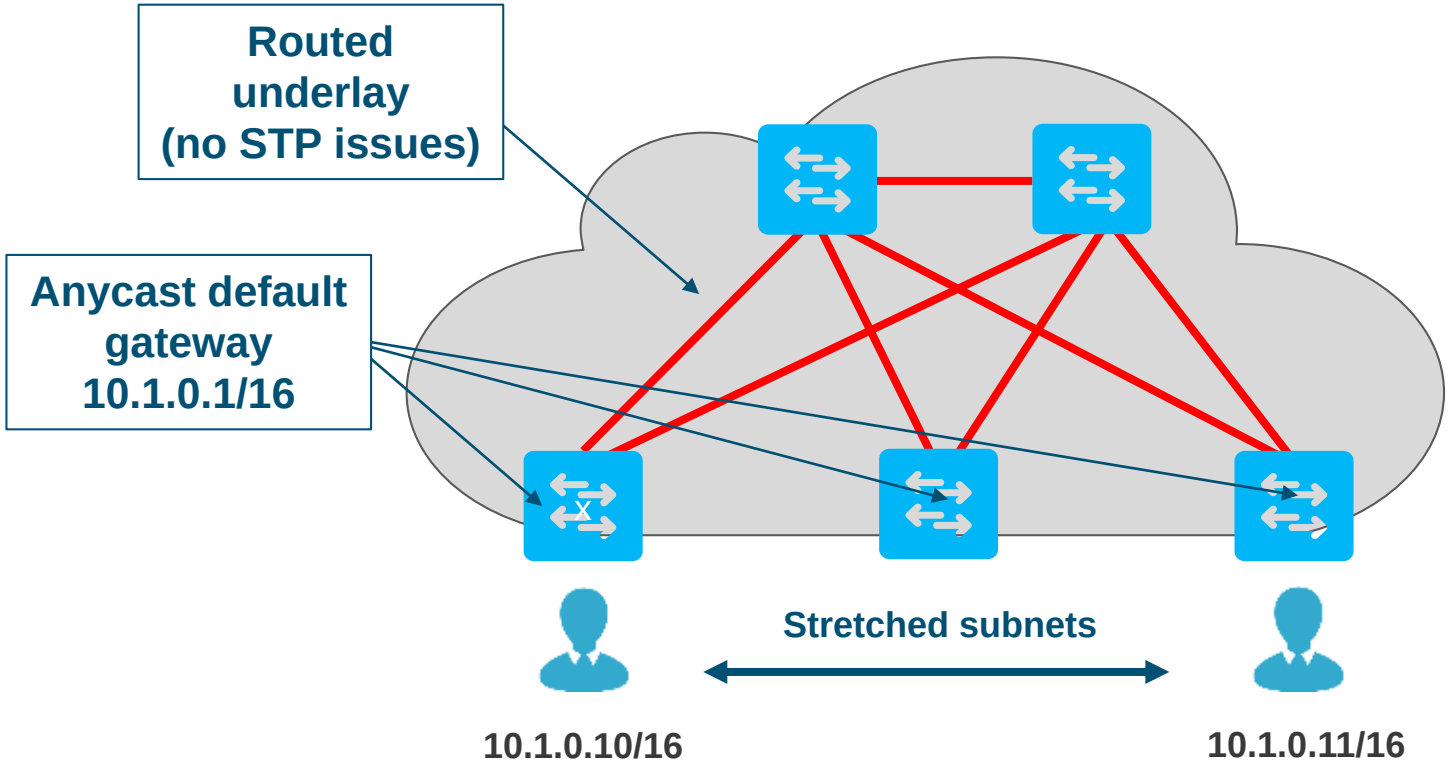
SD-Access - Edge Nodes

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



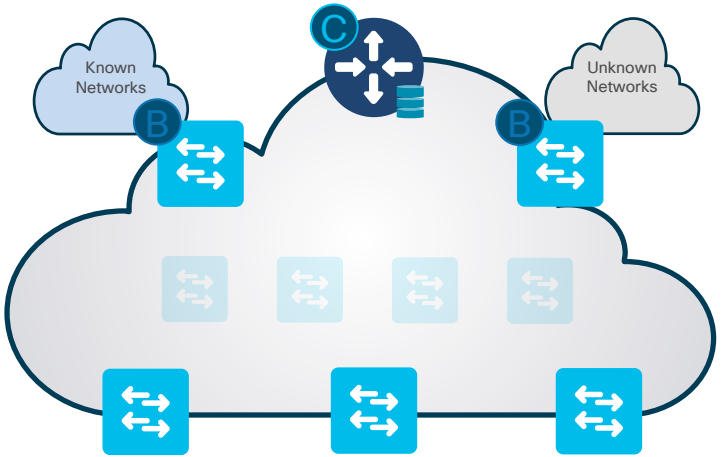
Fabric Enables any subnet anywhere



SD-Access – Control Plane Nodes

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

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

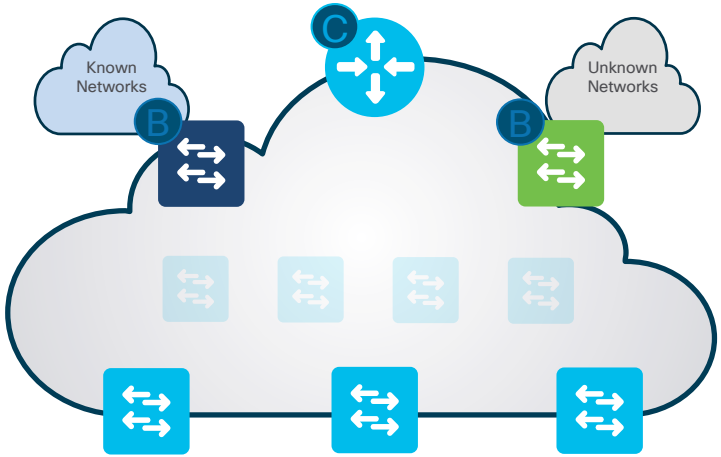


SD-Access - Border Nodes

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

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

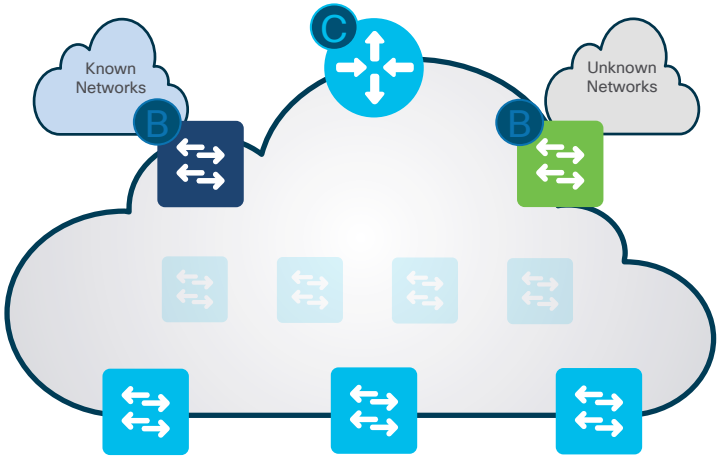
- **Internal Border**
  - Used for “Known” Routes inside your company
- **External Border** (or Default)
  - Used for “Unknown” Routes outside your company



SD-Access - Border Nodes

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

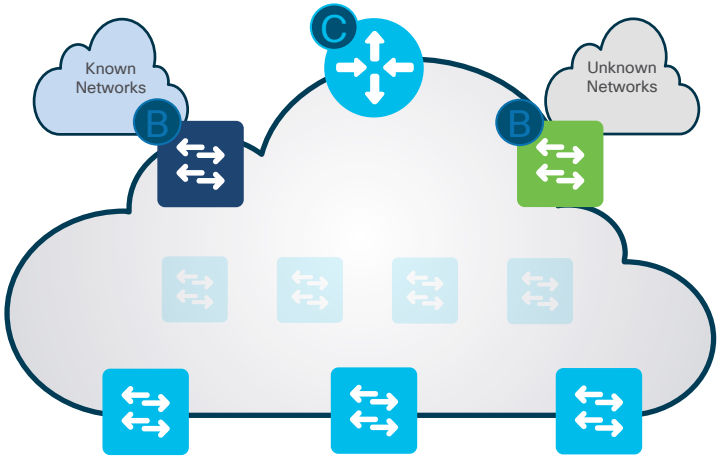
- Connects to any “known” IP subnets available from the outside network (e.g. DC, WLC, FW, etc.)
- Exports all internal IP Pools to outside (as aggregate), using a traditional IP routing protocol(s).
- **Imports and registers (known) IP subnets** from outside, into the Control-Plane Map System
- Hand-off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



SD-Access - Border Nodes

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 - Border Nodes

CI9500-SD12-BN.fra-lab.net

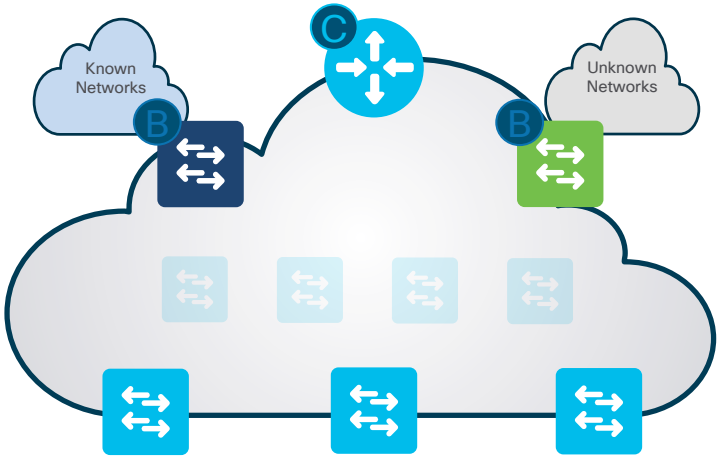
Border Information

Border Type	INTERNAL & EXTERNAL
Internal Domain Protocol Number	65123
Border Handoff	
External Connectivity IP Pool	FS1-borderpool
> TenGigabitEthernet1/0/1	

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

There is also a **Combined Border Node**

- **Internal + External Border**
  - Enables External Border and Imports All Routes except for 0.0.0.0/0
  - Best option for areas will limited Borders, and for SDA Transit Borders



Fabric provisioning overall process

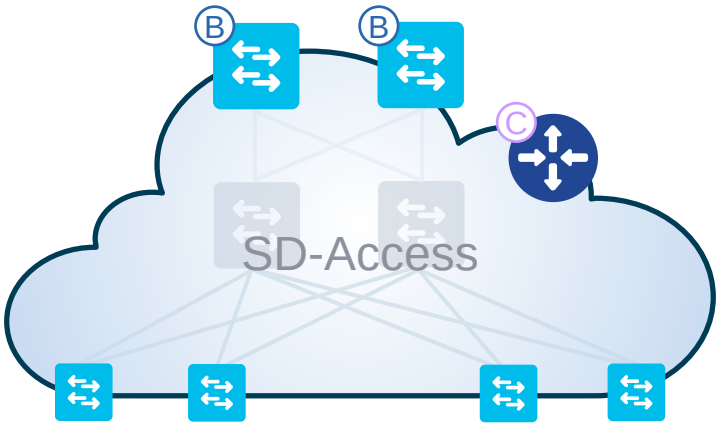
For Your Reference

- Before you start
  - Routing underlay must be configured (manually or using LAN Automation)
  - Assign devices to your fabric site and provision devices (DNS, radius, …)
- Create your fabric (one Cisco DNA Center can manage many fabrics)
- Select your fabric borders and control plane nodes (co-located on site cores / seed devices in most of the case)
  - Need to assign BGP ASN (BGP is used for VN connection to the outside world)
  - Select border type (internal, external or internal & external)
- Select your Edge nodes

Repeat as many times as needed (for example if you add a new switch)

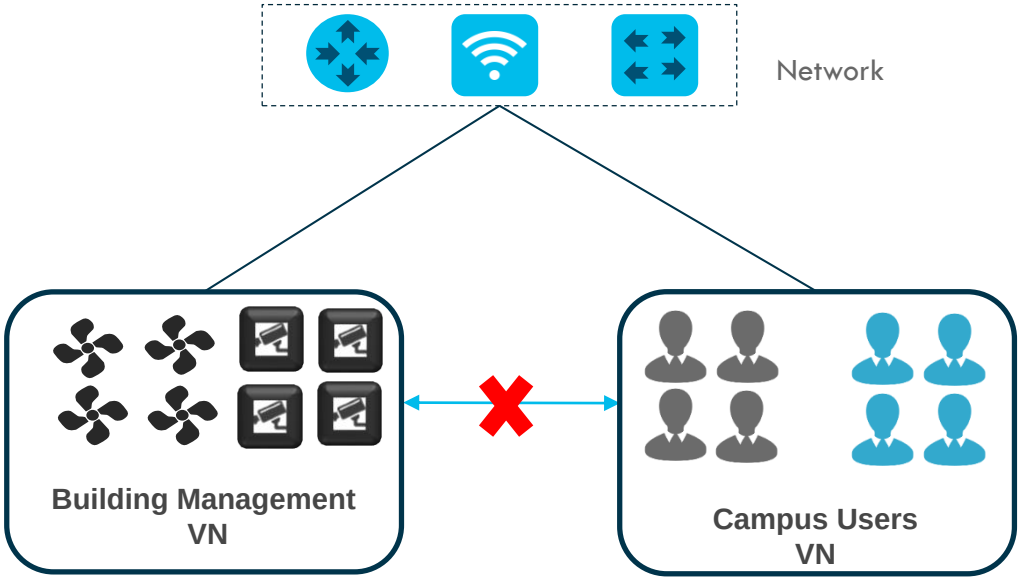
SD-Access agenda

- Introduction to SD-Access
- Underlay automation
- Fabric provisioning
- Policy definition
- Host onboarding



SD-Access - Two Level segmentation

Macro-segmentation

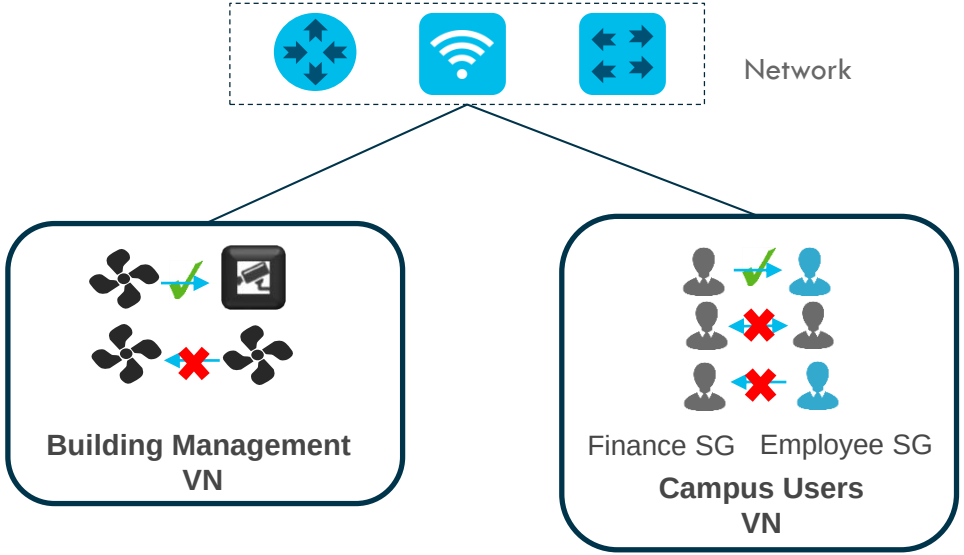


Virtual Network (VN)

First level Segmentation that ensures **zero** communication between specific groups. Ability to consolidate multiple networks into one management plane.

SD-Access - Two Level segmentation

Micro-segmentation (inside a Virtual Network)

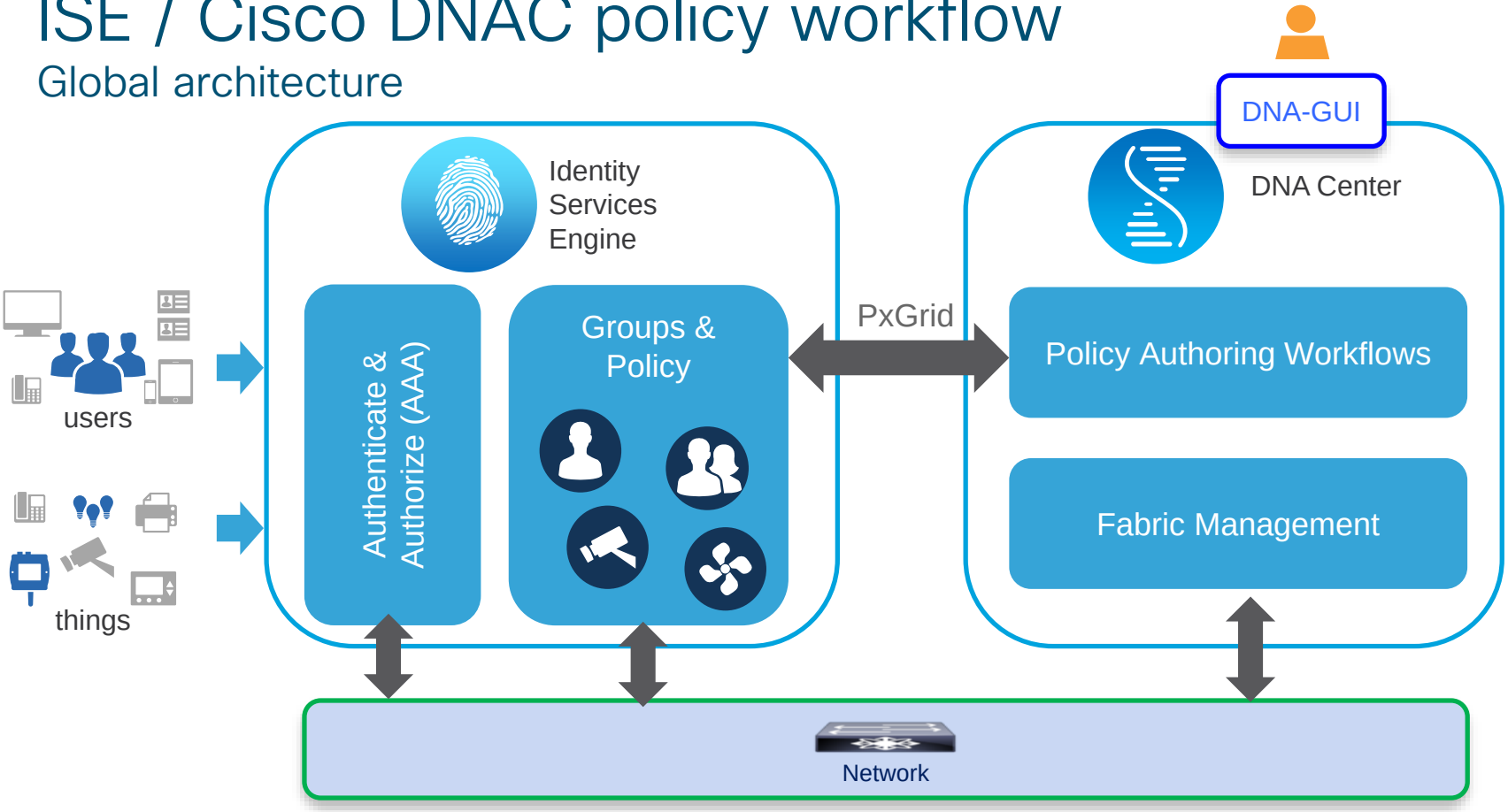


Groups

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.

ISE / Cisco DNAC policy workflow

Global architecture



SDA – Macro segmentation

DNA-C (UI)

DNAC

Create Fabric

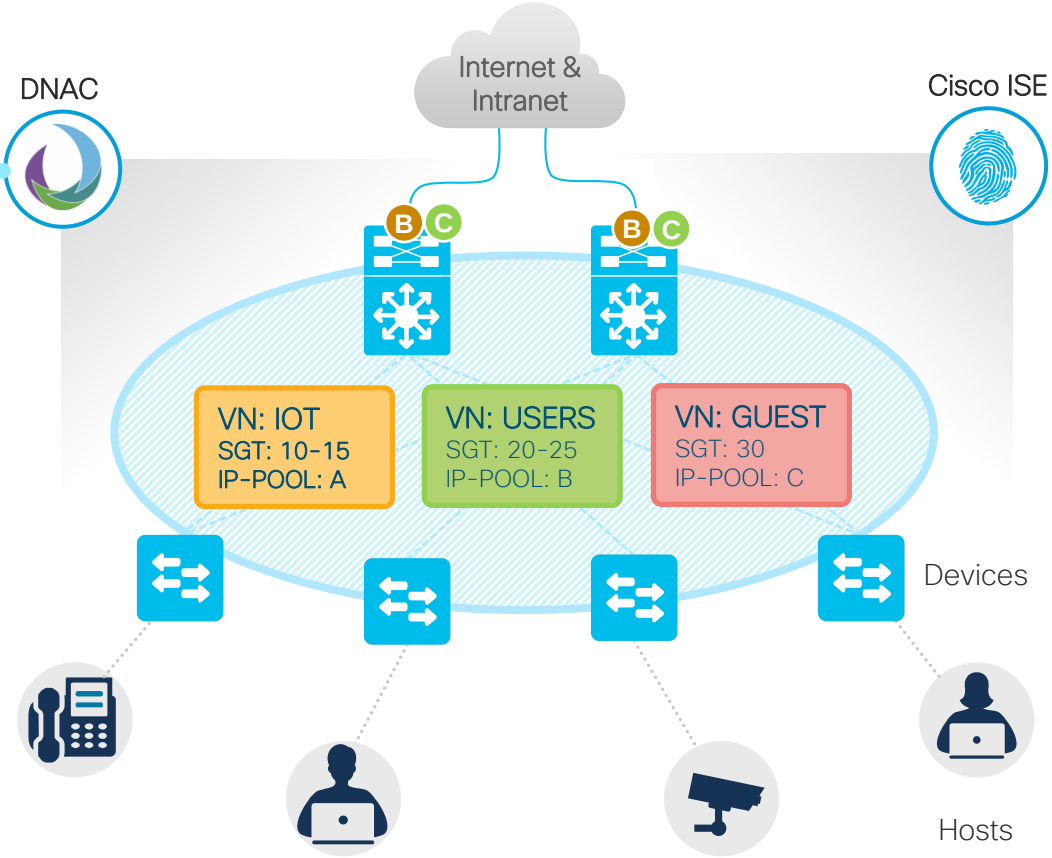
SJC-19-Fabric

Add Nodes to Fabric

Select **Control Plane** Node

Select **Border** Node

Add **'Virtual Network(s)'**



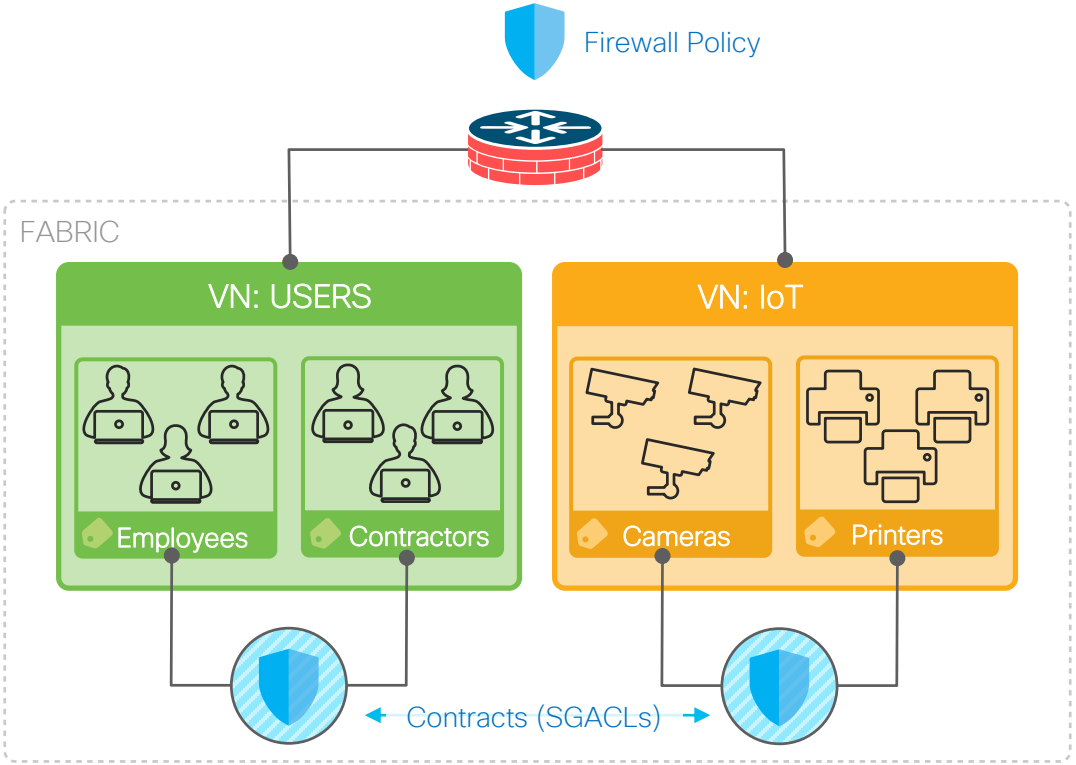
SDA enables Macro and Micro-segmentation

Inter-VN routing and policy enforcement on 'Fusion Router'

Macro segmentation with 'Virtual Networks'

Micro segmentation with 'Scalable Groups'

Contracts control access between SGTs



VN to SGT binding

For Your Reference

Cisco DNA Center | DESIGN | POLICY | PROVISION | ASSURANCE | PLATFORM

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

Find Virtual Network

DEFAULT_VN (18)

INFRA_VN (0)

Guest (1)

Create or Modify Virtual Network by selecting Available Scalable Groups.

Virtual Network Name*

Guest

Guest Virtual Network

Available Scalable Groups

Find Scalable Group

Show Unselected

AU Auditors
BY BYOD
CO Contractors
DE Developers
DS Development_S ...
EM Employees
EX Extranet
IN Intranet
NS Network_Servic ...
PC PCI_Servers
PO Point_of_Sale_S ...
PS Production_Serv ...
PU Production_User ...
QS Quarantined_Sy ...
TS Test_Servers
TS TrustSec_Devic ...
UN Unknown

Groups in the Virtual Network

Find Scalable Group

GU Guests

Cisco DNAC / ISE Creating a Policy

For Your Reference

Cisco DNA Center | DESIGN | POLICY | PROVISION | ASSURANCE | PLATFORM

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

Policies (10) Enter full screen

GBAC Configuration | Default: Permit IP | Create Policies

Filter | Deploy | Refresh

Permit | Deny | Custom | Default

Destination: Auditors, BYOD, CompanyA, Contractors, Developers, Development_..., Employees, Faculty, Guests, Network_Servi..., PCI_Servers, Point_of_Sale_..., Production_Se..., Production_Us..., Quarantined_S..., R13_Admins, R13_Drucker, R13_Gast, R13_Mitarbeiter, R13_Server, Student, test1, Test_Servers, tlx11, tlx13, TrustSec_Devi..., Unknown

Source: Auditors, BYOD, CompanyA, Contractors, Developers, Development_S..., Employees, Faculty, Guests

Developers > **Default Policy** > Production_Users
Production_Users > **Default Policy** > Developers

Expand Minimap

Cisco DNAC / ISE Creating a Policy

Cisco DNA Center | DESIGN | POLICY | PROVISION | ASSURANCE | PLATFORM

Group-Based Access Control | IP Based Access Control

Policies (10) Enter full screen

Filter | Deploy | Refresh

Permit | Deny | Custom | Default

Source \ Destination	Auditors	BYOD	CompanyA	Contractors	Developers	Development_...	Employees	Faculty	Guests	Network_Servi...	PCI_Servers
Auditors											
BYOD											
CompanyA											
Contractors											
Developers											
Development_S...											
Employees											
Faculty											
Guests											
Network_Services											
PCI_Servers											
Point_of_Sale_S...											

Create Policy

Development_Servers → R13_Drucker Custom

Policy Status

Enabled

Contract:

Change Contract

Name	Description	Policies Referencing
ks		1

#	Action	Application	Protocol	Source / Destination	Port	Logging
1	PERMIT	http	TCP	Destination	80	OFF
2	PERMIT	https	UDP/TCP	Destination	443	OFF

Expand Minimap

Default Action DENY **Logging** OFF

Cancel | Save

Contracts = SGACL

Configuration made in Cisco DNA-C reflected in ISE

For Your Reference

Cisco DNA-C

ISE

Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

Group-Based Access Control | IP Based Access Control

Access Contracts (12)

Filter | Actions | Deploy

Name	Description
Deny IP	Deny IP SGACL
Deny_IP_Log	Deny IP with log
erertef	
ks	
lht	
nur_https	

View Access Contract

Name: ks

Description

CONTRACT CONTENT (2)

#	Action	Application	Transport Protocol	Source / Destination	Port	Logging
1	Permit	http	TCP	Destination	80	OFF
2	Permit	https	TCP/UDP	Destination	443/443	OFF

Default Action Deny Logging OFF

Security Groups ACLs List > ks

Security Group ACLs

* Name: ks

Description:

IP Version: IPv4 IPv6 Agnostic

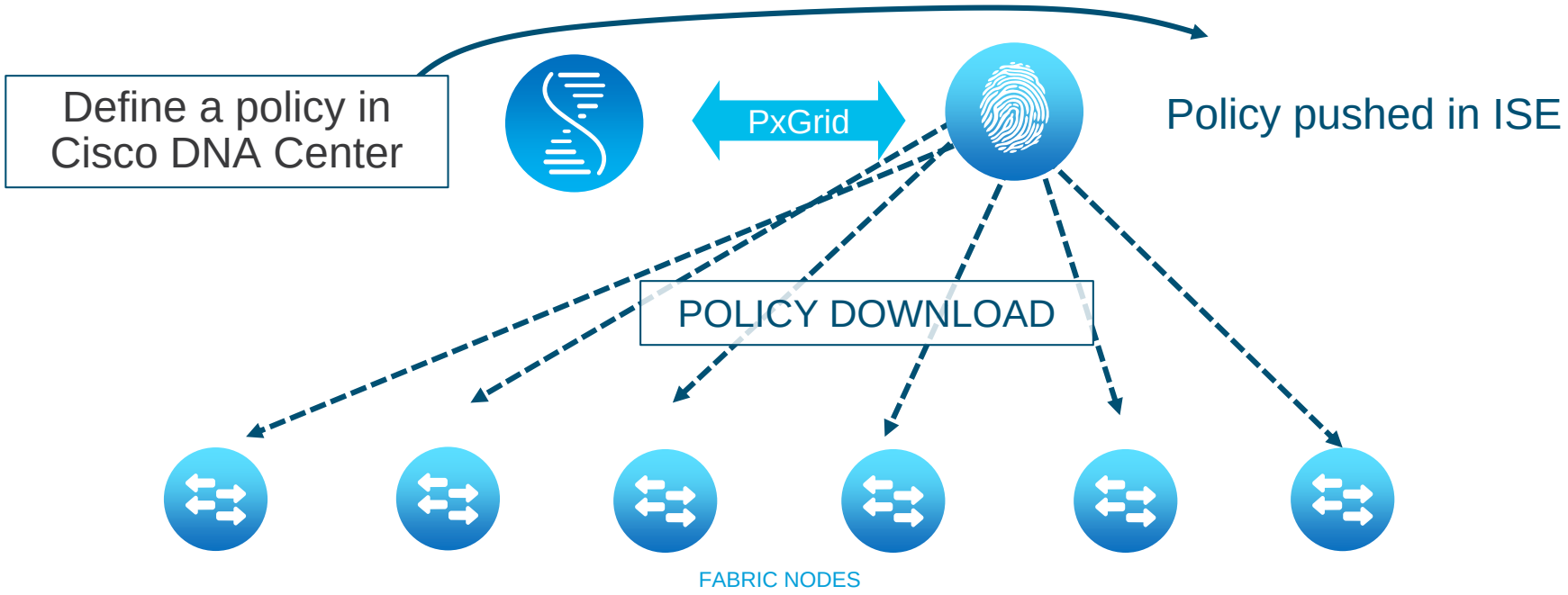
* Security Group ACL content:

```
permit tcp dst eq 80
permit udp dst eq 443
permit tcp dst eq 443
deny ip
```

ISE / Cisco DNAC policy workflow

Define Group Based policies

For Your Reference



Policy definition overall process

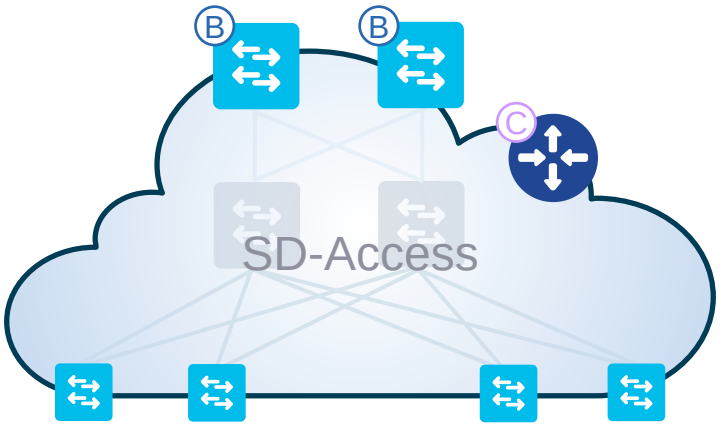
For Your Reference

- Before you start
  - ISE must be associated with Cisco DNA Center
- Note well
  - You can change policies at any time (before or after a fabric is provisioned)
  - Policies are global accross all your fabrics
- Define your Groups
- Define your Virtual Networks in Cisco DNA Center
- Define your Group Based Policies in Cisco DNA Center
- Define host Authentication policies in ISE and assign dynamically Groups to hosts

Repeat as many times as needed (for example if you add a new VN or group)

SD-Access agenda

- Introduction to SD-Access
- Underlay automation
- Fabric provisioning
- Policy definition
- Host onboarding



Select your default Authentication template

For Your Reference

Cisco DNA Center | DESIGN | POLICY | PROVISION | ASSURANCE | PLATFORM

Devices | Fabric | Services

Fabric-Enabled Sites

Find Hierarchy

- Rack2
  - Germany
    - Berlin
      - Cisco BER
    - Dusseldorf
      - DLF1
    - Frankfurt
      - Cisco FRA

All Fabrics > Cisco FRA

Rack2

Fabric Infrastructure | Host Onboarding

Authentication Template

Select Authentication Template

Settings will be applied to all Fabric Edge host ports, unless overridden by a static port assignment.

○	Open Authentication	Edit
◉	Closed Authentication	Edit
○	Low Impact	Edit
○	No Authentication	

Set as Default

Associate IP pools to VN and use (Data or Voice)

All Fabrics > Cisco FRA
Rack2

Fabric Infrastru

Virtual Netw

Select a Virtua

Critical Pool:

DEFAULT_V

demodus

Edit Virtual Network: demo1

Advanced View

Reset Export Add

Actions

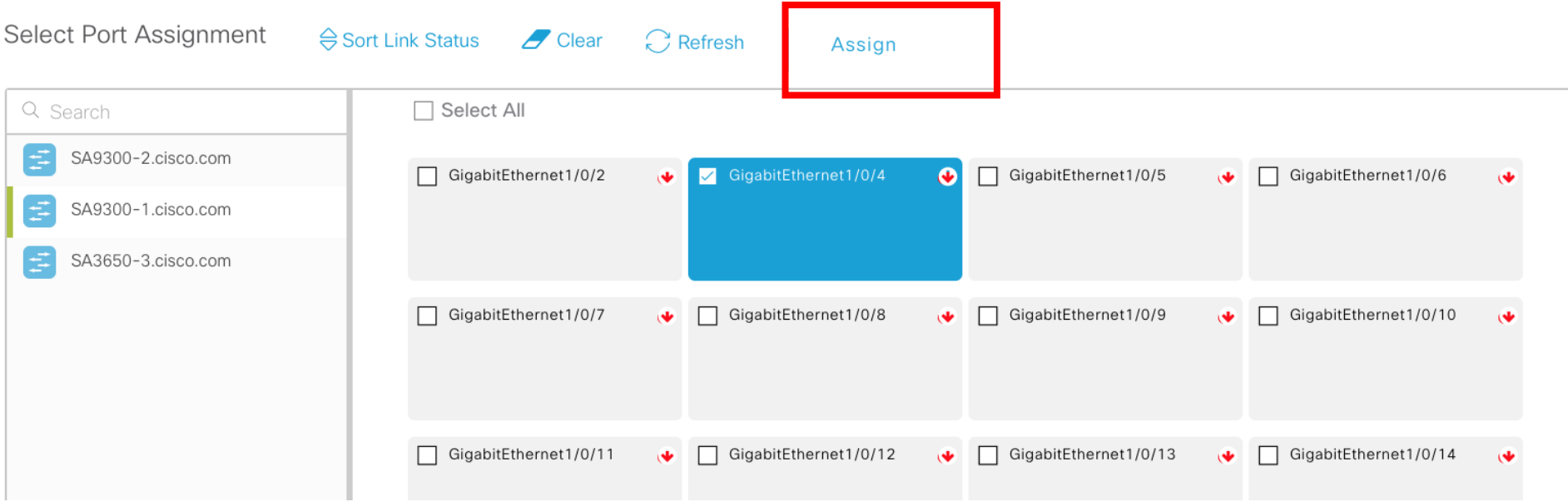
Find

IP Address Pool	Authentication Policy	Traffic Type	Layer-2 Flooding
FS1-VN-demo1	172_2...demo1	Data	Disabled
FS1-VN-demo1-voice	172_2...demo1	Voice	Disabled
FS1-WLAN-SSID-demo1	172_2...demo1	Data	Disabled

Showing 3 of 3

Configure ports individually when needed

For Your Reference



Host onboarding overall process

For Your Reference

- Before you start
  - Your fabric must be provisioned
  - L3 communication to the outside world MUST be configured
- Define IP pools to be used in the fabric
- Define the default fabric access authentication template (Closed Authentication, Easy Connect, No Authentication, Open Authentication)
- Associate IP pools to VN and use (Data or Voice). This creates « segments ».
- If needed, configure desired ports with authentication schema. Provide segment and group if no authentication on port

Repeat as many times as needed (for example if you add a new VN or group)

Demo
Fabric workflow

QuickTime Player File Edit View Window Help 100% Tue 17:26 ilukic

Cisco DNA Center | Cisco Catalyst 9200 Series Switc | Cisco Catalyst 9300 Series Switc

Not Secure | fra-dnac-r3.cisco.com/dna/provision/devices/inventory?devices-view=inventoryView&selectedSite=ec520076-96c2-4fae-89c2-6634b8f8fbd1

Incognito

Cisco DNA Center

DESIGN POLICY PROVISION ASSURANCE PLATFORM

Devices Fabric Services

Find Hierarchy

- Global
  - Unassigned Devices (10)
  - Australia
  - Canada
  - Germany
    - Berlin
    - Dusseldorf
    - Frankfurt
    - German Core
    - Kassel
    - Meraki Town
    - Oberusel
      - Brauhaus
      - Eschborn
      - Feldberg
    - RMA Area
    - Wiesbaden
  - Iceland
  - Spain
  - US

DEVICES (6)

FOCUS: Inventory

Global > Germany > Oberusel > Brauhaus

Take a Tour

DEVICE TYPE: All | Routers | Switches | APs | WLCs

REACHABILITY: All | Reachable | Unreachable

Filter | Add Device | Tag Device | Actions

Last updated: 5:25 PM

Device Name	IP Address	Support Type	Device Family	Site	Reachability	MAC Address	Device Role	Image Version	Uptime
borderNode1.fra-lab.net	172.20.31.254	Supported	Switches and Hubs	.../Oberusel/Brauhaus	Reachable	00:87:31:a0:3d:80	CORE	16.12.1s	7 hrs 1
borderNode2.fra-lab.net	172.20.31.253	Supported	Switches and Hubs	.../Oberusel/Brauhaus	Reachable	00:76:86:3d:83:80	CORE	16.12.1s	7 hrs 4
edgeNode1.fra-lab.net	172.20.106.78	Supported	Switches and Hubs	.../Oberusel/Brauhaus	Reachable	00:c8:8b:f0:07:80	ACCESS	16.12.1s	1 day 0
edgeNode2.fra-lab.net	172.20.106.73	Supported	Switches and Hubs	.../Oberusel/Brauhaus	Reachable	88:5a:92:27:54:80	ACCESS	16.12.1s	1 day 0
intermediateNode1.fra-lab.net	172.20.106.72	Supported	Switches and Hubs	.../Oberusel/Brauhaus	Reachable	9c:57:ad:e0:02:00	ACCESS	16.12.1s	1 day 0
intermediateNode2.fra-lab.net	172.20.106.67	Supported	Switches and Hubs	.../Oberusel/Brauhaus	Reachable	9c:57:ad:54:28:00	ACCESS	16.8.1a	1 day 0

Showing 6 of 6

And for Wi-Fi ? It’s the same !!!

Design

Enterprise Wireless

Filter | Edit Delete

	Network Name (SSID)
☐	SDA-LAB

Provision

Actions

- Assign Device to Site
- Provision
- Update OS Image
- Delete Device

☑ WLC5520-1

Add to fabric

Add to Fabric
View Info
Device Role

WLC5520-1

Policies

Policies for Wired AND Wireless

Wireless SSID's

☐ Enable Wireless Multicast

SSID Name	Type	Security	Traffic Type	Address Pool
SDA-LAB	Enterprise	WPA2 Enterprise	Voice + Data	IT:10.154.20.0

Show 10 entries

Showing 1 - 1 of 1

Host onboarding

You should get prepared for Cisco SD-Access

- SD-Access offers maximum benefits
  - Full automation
  - Software-defined Policies
  - Assurance

➔ You should prepare for it NOW to be ready for future network upgrades

Agenda

- Cisco DNA Center 10 minutes overview
- Before you deploy – purchase and design considerations
- Base automation for wired and wireless
- Getting started with Cisco SD-Access
- **Assurance and application policies**
- Key takeaways

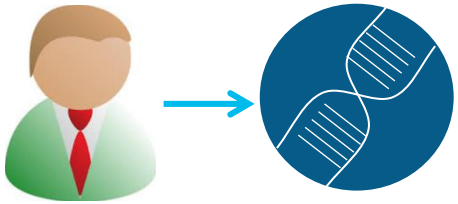
Application policies

Easy-QoS configures your network to deliver best performance for business relevant applications

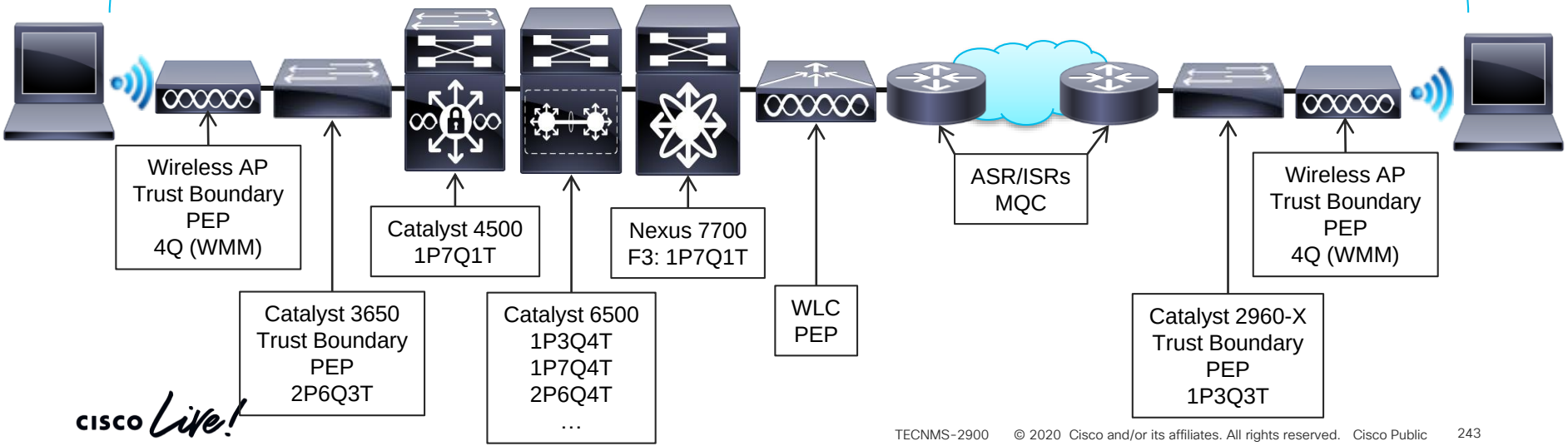
Application policies

EasyQoS

Network Operators express high-level business-intent to EasyQoS



Southbound APIs translate business-intent to platform-specific configurations

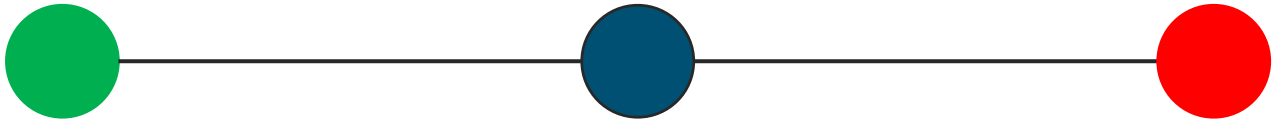


Mapping Traffic Class to QoS treatments

Apply RFC 4594/2474/3662-based Marking / Queuing / Dropping Treatments

Traffic Class	Per-Hop Behavior	Queuing & Dropping	Application Examples
VoIP Telephony	EF	Priority Queue (PQ)	Cisco IP Phones (G.711, G.729)
Broadcast Video	CS5	(Optional) PQ	Cisco IP Video Surveillance / Cisco Enterprise TV
Real-Time Interactive	CS4	(Optional) PQ	Cisco TelePresence
Multimedia Conferencing	AF4	BW Queue + DSCP WRED	Cisco Jabber, Cisco WebEx
Multimedia Streaming	AF3	BW Queue + DSCP WRED	Cisco Digital Media System (VoDs)
Network Control	CS6	BW Queue	EIGRP, OSPF, BGP, HSRP, IKE
Signaling	CS3	BW Queue	SCCP, SIP, H.323
Ops / Admin / Mgmt (OAM)	CS2	BW Queue	SNMP, SSH, Syslog
Transactional Data	AF2	BW Queue + DSCP WRED	ERP Apps, CRM Apps, Database Apps
Bulk Data	AF1	BW Queue + DSCP WRED	E-mail, FTP, Backup Apps, Content Distribution
Default Forwarding	DF	Default Queue + RED	Default Class
Scavenger	CS1	Min BW Queue (Deferential)	YouTube, Netflix, iTunes, BitTorrent, Xbox Live

Determining Applications Business-Relevance



Relevant

- These applications directly supports business objectives

Default

- These applications may/may not support business objectives
  - E.g. HTTP/HTTPS
- Alternatively, administrator may not know the application (or how its being used in the org)

Irrelevant

- These applications are known and do not directly support any business objectives; this class includes ***all personal/consumer applications***

- Same Application can be relevant or irrelevant depending on your organization.

EasyQoS workflow with Cisco DNA-Center

Create Application set(s) (Optional)

Create/Use Application(s) and associate to Application Set (Optional)

Create Application Policy

Deploy

Application policy Creation

Provide a Name → Choose Wired or Wireless → Chose a Scope (Sites)

↓

Drag and drop application sets to appropriate business relevance

Create your own QoS – Policy Set

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

Application Policy Name
cl-demo1

Wired | Wireless

Site Scope 1 Sites | Queuing Profiles CVD_QUEUING_PROFILE | SP Profiles 2 Profiles | Host Tracking

Business Relevant (1)

Markus1
1 applications | 1

Find Application

Markus-1

Default (2)

file-sharing
32 applications

general-browsing
9 applications

Markus-1

Details | QoS Settings

Markus-1

Edit Details

Details:

Port Classifiers:

IP Address	Protocol	Ports
10.1.1.5	TCP_OR_UDP	N/A

Traffic Class: Multimedia Streaming

Application Set: Markus1

Policies associated through consumer or bi-directional settings

Use the pre-check

Policy Preview Configurations

Find device

Device Name	Device Type	Device Role	Configuration Changes
C9k-u-13.fra-lab.net	Cisco Catalyst 9300 Switch	ACCESS	View
C9k-u-4.fra-lab.net	Cisco Catalyst 9300 Switch	ACCESS	Generate
CBC-WLAN-Edge-12.fra-lab.net	Cisco Catalyst 3650 Switch Stack	ACCESS	Generate
CI9500-SD11-BN.fra-lab.net	Cisco Catalyst 9500 Switch	DISTRIBUTION	Generate
SN-FOC1938W2KV.fra-lab.net	Cisco Catalyst 35xx Stackable Ethernet Switch	ACCESS	Generate

Check your settings and deploy

Back to all devices

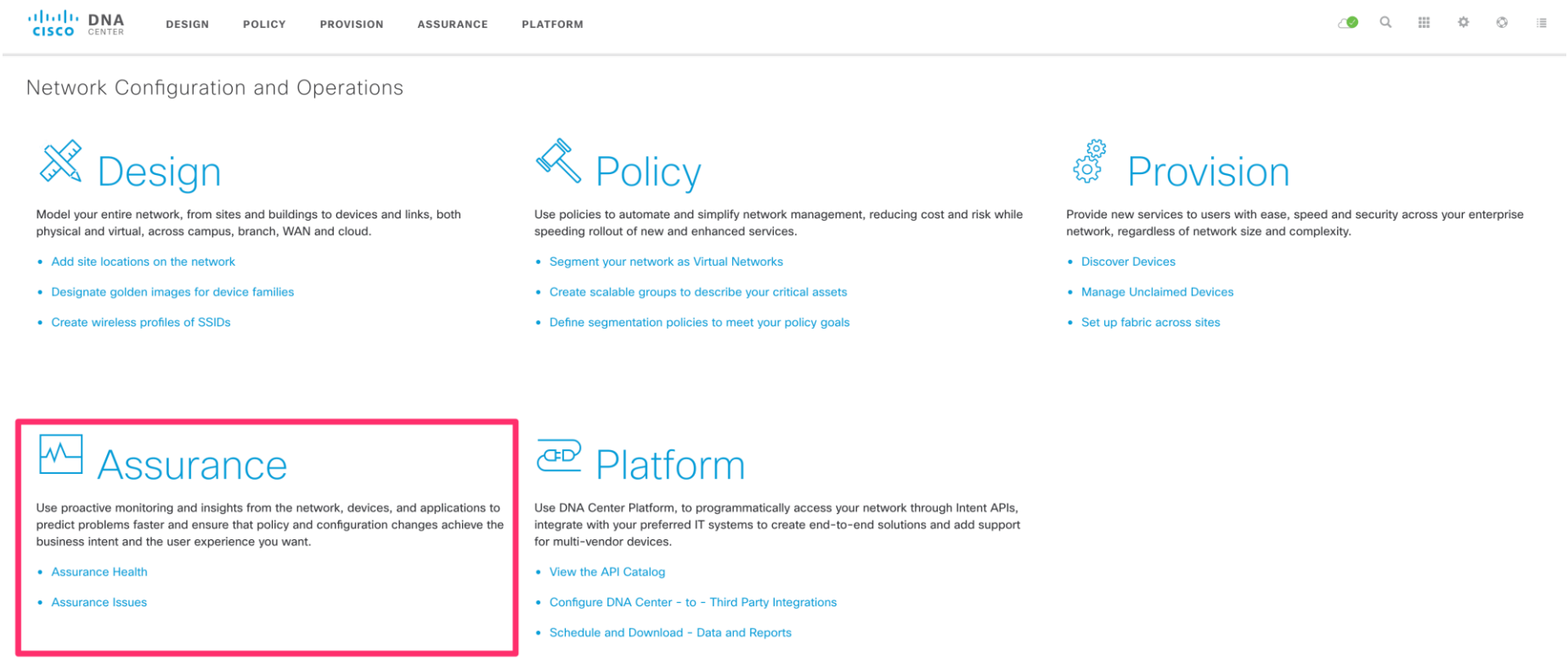
Configuration changes to C9k-u-13.fra-lab.net

```
ip nbar custom Markus-1 transport udp-tcp id 28486
ip address 10.1.1.5
port range 1234 1235
exit
ip nbar attribute-map BR2
attribute business-relevance default
exit
class-map match-any DNA-EZQOS_2P6Q3T_9K#VOICE-PQ1
match dscp EF
class-map match-any DNA-EZQOS_2P6Q3T_9K#VIDEO-PQ2
match dscp CS5
match dscp CS4
class-map match-any DNA-EZQOS_2P6Q3T_9K#CONTROL-PLANE
match dscp CS3
match dscp CS2
match dscp CS7
match dscp CS6
```

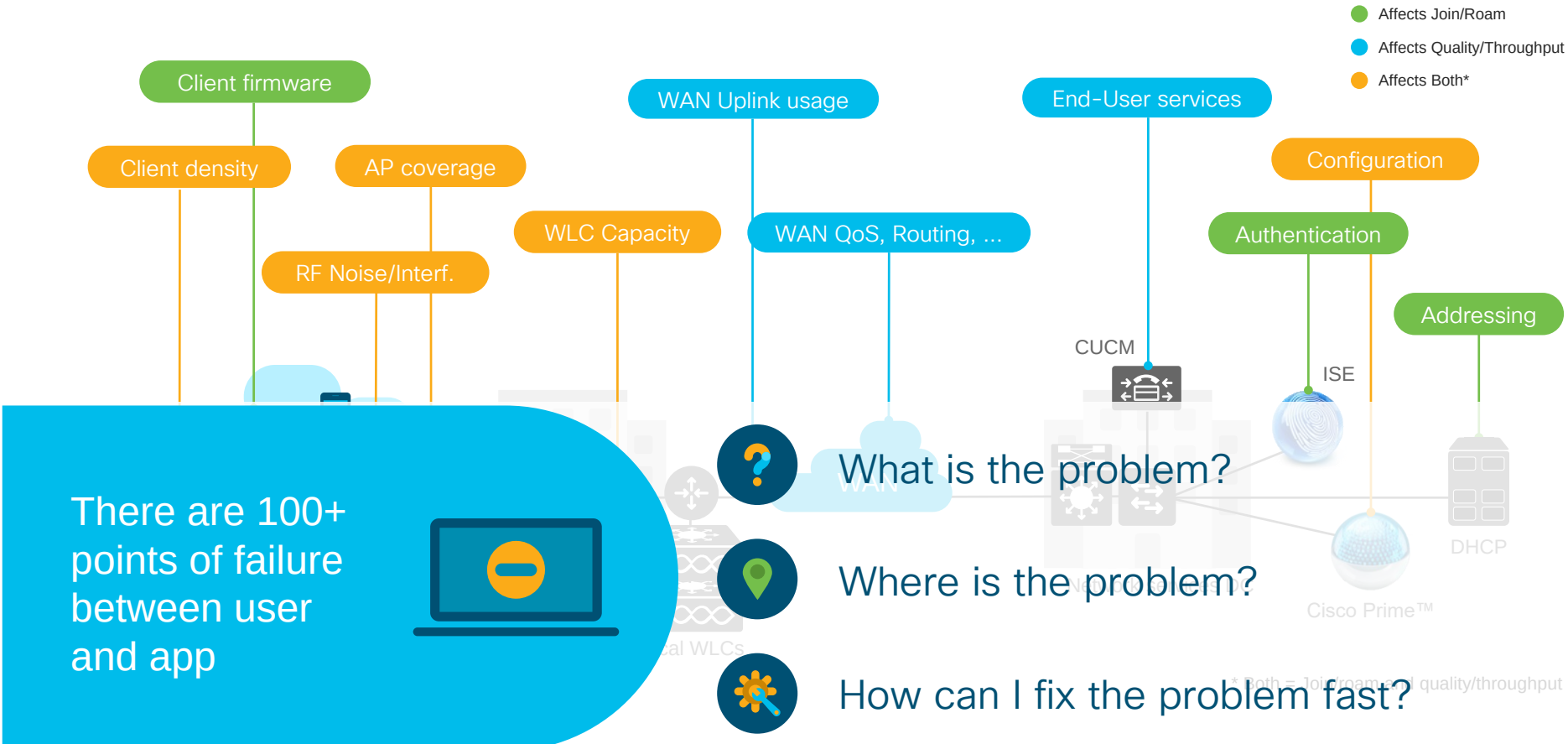
Assurance

Gain visibility in your network and solve performance issues faster

Assurance – how to use it



Network Quality is a Complex, End-to-End Problem

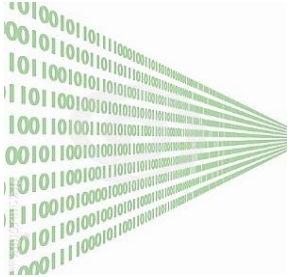


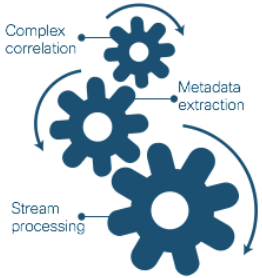
Cisco DNA Assurance and Analytics – What's New

Existing Approach	Cisco DNA Approach
Reactive: Traditional monitoring based on network element KPIs	Proactive: True Assurance based on deeper correlation across all entities
Network Unaware	Network and Context Aware - deeper insights through Analytics
Closed Interfaces & Developer Inefficiencies	Open interfaces with adaptive APIs and ITSM Integration framework
Use case specific monolithic architecture	Hyper-distributed multi-tenant & cloud first secure architecture
Rigid Network Telemetry	Micro services based agile modern network telemetry collection capabilities

DNA-C Assurance
From Network Data to Business Insights

Unified Network Telemetry Contextual Data → Correlation Complex Event Processing → Issues Insights → Guided Remediation - Now → Auto Fix It - Future





✓ 140 Actionable Insights

Client Onboarding
- Association failures
- Authentication failures
- IP address failures

Client RF Experience
- Sticky client, Ping pong
- Coverage Hole
- Client Capacity

App Experience
- Throughput analysis
- App Performance – Packet Loss, Latency and Jitter
- DNS Issues

Network Device
- CPU, Mem utilization
- Crash, AP Join Failure, Flapping AP
- Power supply failure
- Radio Utilization

Supported Issues: Wired Use Cases

For Your Reference

Client Onboarding

- ✓ Client/Device DHCP
- ✓ Client/Device DNS
- ✓ Client authentication / authorization

Control Plane

- ✓ Control plane reachability
- ✓ Edge reachability
- ✓ Border reachability
- ✓ MAP server
- ✓ BGP AS mismatch, Flaps
- ✓ OSPF adjacency failure
- ✓ EIGRP adjacency failure

Data Plane

- ✓ Border and edge connectivity
- ✓ Border node health
- ✓ Access node health
- ✓ Network Services DHCP, DNS, AAA
- ✓ Interface High Utilization
- ✓ Interface Flaps
- ✓ Gateway Connectivity
- ✓ Application Performance (Packet Loss, Latency, Jitter)

Policy Plane

- ✓ ISE/PxGrid connectivity
- ✓ Border Node policy
- ✓ Edge Node policy
- ✓ SGACL validation

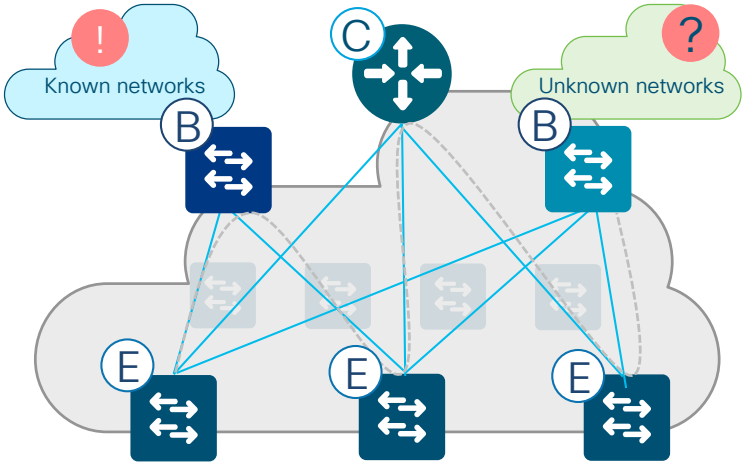
Network Device Monitoring

- ✓ High CPU
- ✓ High Mem
- ✓ High Temp
- ✓ Line-card
- ✓ Modules
- ✓ POE power
- ✓ TCAM Table

Proactive Connectivity Assessment for Wired

Test your network anywhere at any time

- IPSLA analyzes IP service levels for services to increase productivity, lower operational costs, and reduce downtime
- IPSLA tests are run in the **fabric network** to verify connectivity to **control plane, fabric border, fabric edge nodes, and fabric network services such as** DHCP, DNS, AAA servers
- This provides **predictive performance** capability before issue happens
- This configuration is done by Cisco DNA-C



Example

```
ip sla 1
icmp-echo 192.168.110.1
frequency 300
```

E Fabric edge

C Fabric control

B Fabric border and default border

Supported Issues: Wireless Use Cases

For Your Reference

Client Onboarding

- ✓ Association failures
- ✓ Authentication failures
- ✓ IP address failure
- ✓ Client Exclusion
- ✓ Excessive on-boarding time
- ✓ Excessive authentication time
- ✓ Excessive IP addressing time
- ✓ AAA, DHCP reachability
- ✓ Client Side Analytics (Apple / Samsung Insights)

Client Experience

- ✓ Throughput analysis
- ✓ Roaming pattern analysis
- ✓ Sticky client
- ✓ Slow roaming
- ✓ Excessive roaming
- ✓ RF, Roaming pattern
- ✓ Dual band clients prefer 2.4GHz
- ✓ Excessive interference

Network Coverage & Capacity

- ✓ Coverage hole
- ✓ AP License Utilization
- ✓ Client Capacity
- ✓ Radio Utilization

Network Device Monitoring

- ✓ Availability
- ✓ Crash, AP Join Failure
- ✓ High Availability
- ✓ CPU, Memory
- ✓ Flapping AP, Hung Radio
- ✓ Power supply failures

Application Performance

- ✓ Sensor Tests:
  - Web: HTTP & HTTPS
  - Email: POP3, IMAP, Outlook Web Access
  - File Transfer: FTP & TFTP
- ✓ Application Experience (Packet Loss, Latency, Jitter)

Wireless Sensors Proactively Assess Performance

Test your network anywhere at any time

- On-Boarding Tests
  - 802.11 Association
  - 802.11 Authentication & Key Exchange
  - IP Addressing DHCP (IPv4)
- Network tests
  - DNS (IPv4)
  - RADIUS (IPv4)
  - First Hop Router/Default gateway (IPv4)
  - Intranet Host
  - External Host (IPv4)
- Application tests
  - Email: POP3, IMAP, Outlook Web Access (IPv4)
  - File Transfer: FTP (IPv4)
  - Web: HTTP & HTTPS (IPv4)

Sensors act as clients

Access point

Dedicated Sensor AP1800

Active Sensor AP1800S

- HTTPS for Automation and reporting
- PnP-based Provisioning
- Fully Managed by DNAC

Full Stack Visibility Use Cases

Network Experience

Network Health: Monitor and troubleshoot the overall health of network devices

Device 360: Comprehensive view to troubleshoot device issues

Time Travel: Contextual Analysis of historical problems going back up to 14 days in time

Client Experience

Client Health: Provide visibility into clients connected to the network and their experience

Client 360: Comprehensive view of client issues, onboarding, event viewer and connectivity status

Intelligent Capture: Provide packet capture data, AP and Client statistics, and spectrum data

Sensor based SLA Monitoring

1800s Active Sensor: Proactively test the network and end user experience

Active Testing: 12+ types to onboarding and network performance tests

SLA Dashboard: Onboarding, Network Services and App Connectivity

Application Experience

Health Score Dashboard: Monitor App Health score of business critical apps

App 360: Troubleshoot App issues with a view on performance metrics

Client 360: Troubleshoot specific clients facing app experience issues

Overall Health

Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

Dashboards Insights And Trends Manage

Network Devices

LATEST 80% Healthy TOTAL: 45

Router	Core	Distribution	Access	Wireless Controller	Access Point
6/8	1/1	7/7	15/17	1/4	6/8

40%

5p

View Network Health

Wired Clients

LATEST 97% Healthy CONNECTED: 36

40%

5p

Wireless Clients

LATEST — —% Healthy ACTIVE: 0

40%

5p

View Client Health

Top 10 Issue Types

Priority	Issue Type	Device Role	Category	Issue Count	Site Count (Area)	Device Count	Last
P1	Switch unreachable	ACCESS	Availability	50	0	2	Dec 22, 2019 4:33 pm
P1	Router unreachable	BORDER ROUTER	Availability	50	1	2	Dec 22, 2019 4:33 pm
P1	Interface Connecting Network Devices is Down	ACCESS	Connectivity	6	1	1	Dec 22, 2019 3:51 pm
P2	Network Device Interface Connectivity - OSPF Adjacency Failure	DISTRIBUTION	Connectivity	13	1	1	Dec 22, 2019 3:10 pm
P2	Switch power failure	UNKNOWN	Device	4	0	1	Dec 22, 2019 12:10 pm

Network Health

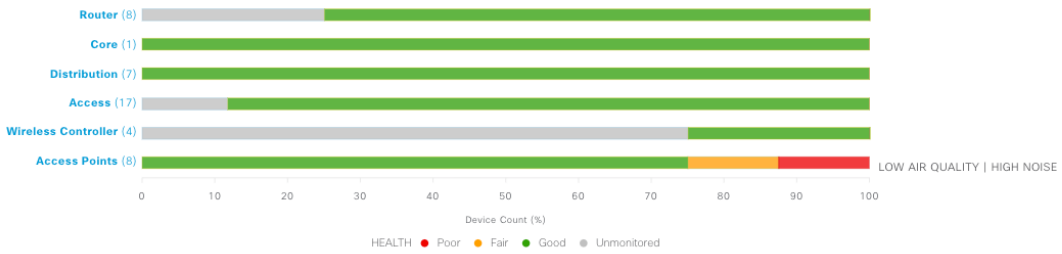
LATEST TREND

Network Devices

80 %

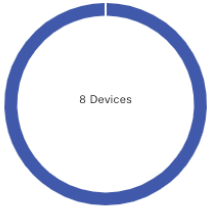
Healthy Network Devices

TOTAL DEVICES	45
Monitored	38
Healthy	36
Unhealthy	2
Unmonitored	7



Total APs Up/Down

LATEST TREND

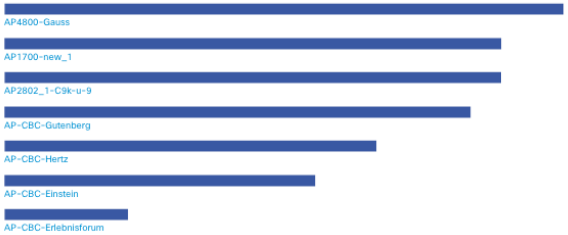


Up (8) Down (0) No Data (0)

View Details

Top N APs by High Interference

LATEST TREND 2.4 GHz



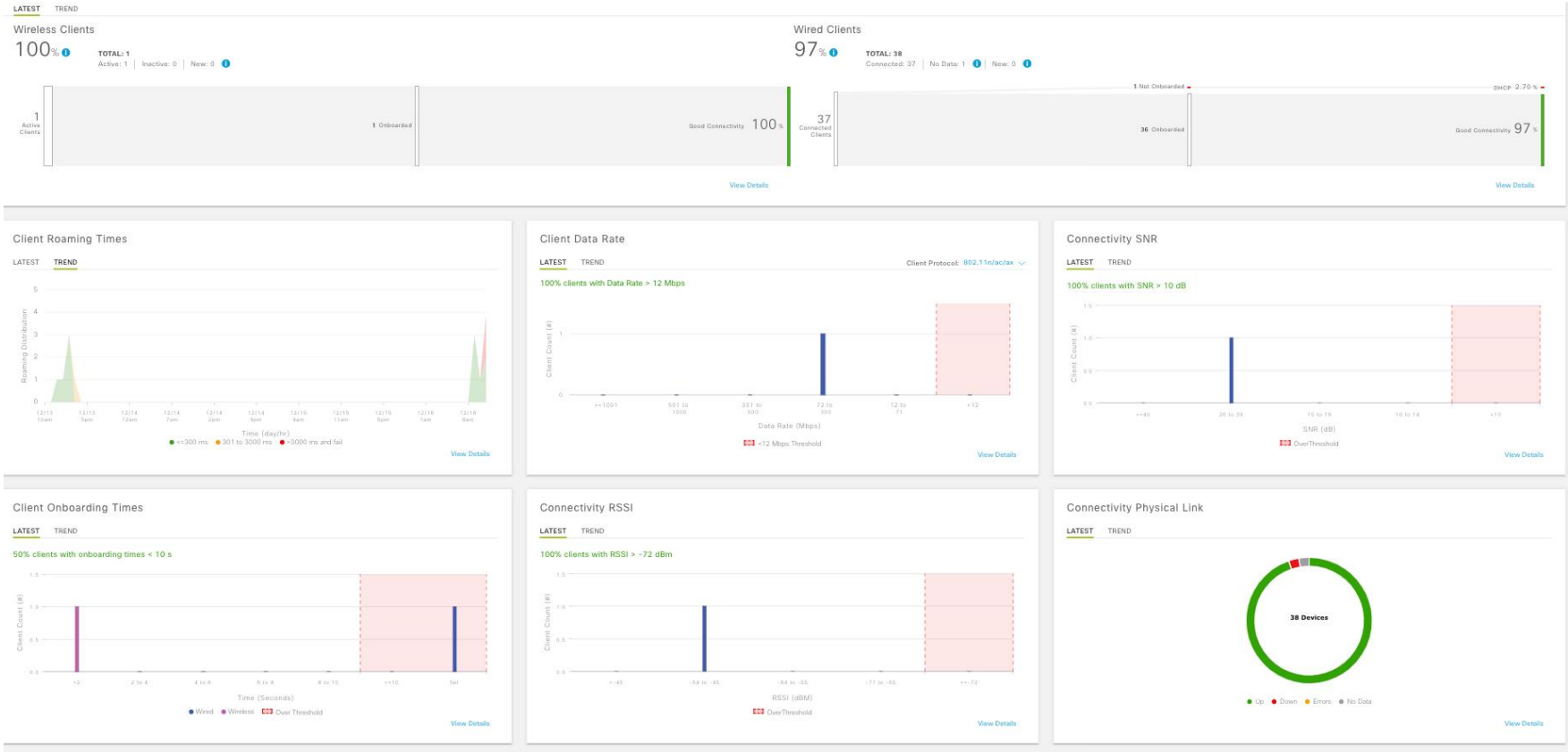
View Details

Top N APs by Client Count

LATEST TREND

No data to display

Client Health



Device 360

Network Health

Device 360

10/10 Switch C3k-R3U-3.fra-lab.net

Device Model: WS-C3650-48TD-E | IP Address: 172.20.197.66 | Location: Global / Germany / Berlin / Cisco BER / 12OG | Software Version: 16.12.1s | Role: ACCESS | HA Status: Non-redundant | Uptime: 102 days 19:44:37

Jan 26, 2020 12:25 am

Device Health: 10

Device Health is the minimum of all KPI Health Score.

* - The KPI is not included for Health Score

System Resources		
Memory Utilization	10	58%
CPU Utilization	--	--

Data Plane		
Inter-device Link Availability	10	--
Link Errors	10	--

Control Plane		
Fabric Reachability	10	Reachable

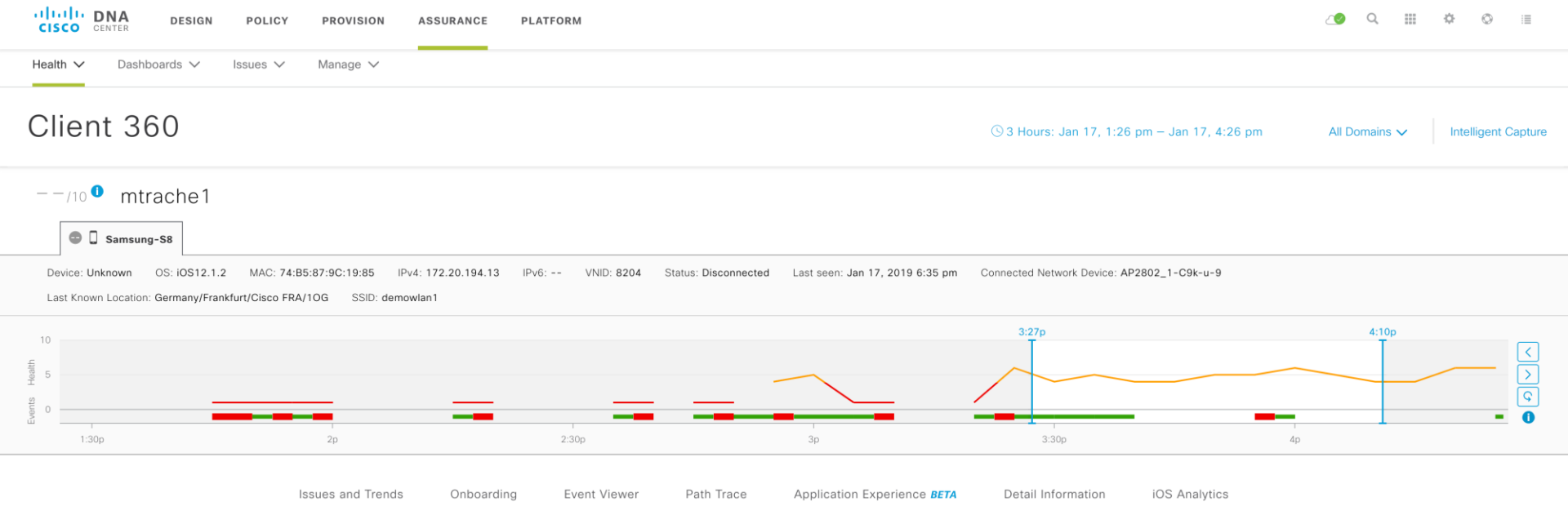
Events

See Full List (0

Issues (0) Jan 26, 2020 12:19 pm

Physical Neighbor Topology

Client 360



Client 360 Issues & Onboarding

Issues (3)

P3	Application Network Latency for Application 'ssl' is Above the Threshold Value of 262ms. Total occurrences: 1	Jan 17, 2019 4:00 pm
P3	Application Network Latency for Application 'cisco-spark' is Above the Threshold Value of 150ms. Total occurrences: 1	Jan 17, 2019 3:45 pm
P3	Connected Wireless client exhibiting sticky behavior on SSID "demowlan1" on AP "AP2802_1-C9k-u-9" (5.0 GHz). Total occurrences: 1	Jan 17, 2019 3:41 pm

Resolved Issues

Onboarding

Jan 17, 2019 4:10 pm

AAA DHCP

Client 360 Events

Event Viewer

Find

Jan 17, 2019		
DHCP	AP:AP2802_1-C9k-u-9 | WLC:WLC5520 | WLAN:demowla...	3:57:06.300 PM - 3:57:06.300 PM
Onboarding	AP:AP2802_1-C9k-u-9 | WLC:WLC5520 | WLAN:demowla...	3:57:06.164 PM - 3:57:06.277 PM
Run	Client Onboarded	3:57:06.277 PM
KeyExchange		3:57:06.277 PM
Authentication Done	Dot1x Full Auth	3:57:06.272 PM
Authentication Start		3:57:06.168 PM
Association Done		3:57:06.165 PM
Association Start	Client Association with AP	3:57:06.164 PM
Re-Authentication	EAP ID Timeout | AP:AP2802_1-C9k-u-9 | WLC:WLC5520 ...	3:55:26.184 PM - 3:56:58.032 PM

Onboarding

Jan 17, 2019 3:57:06 PM

Detailed Information

Status: Success

Details:

ROLE	LOCAL
AP_MAC	00:F2:8B:26:EF:30
AP_Name	AP2802_1-C9k-u-9
AUTH-Server	172.20.2.40
User Name	mtrache1
Frequency(GHz)	5.0
IPv4	172.20.194.13
WLC_Name	WLC5520
WLAN	demowlan1

Path Trace

To find the location of an issue, perform a path trace between two nodes in your network – a source device and a destination device.

Run New Path Trace

Client 360 Application Experience

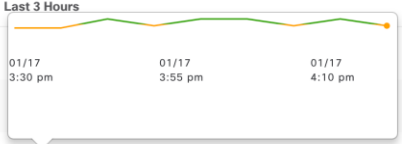
Application Experience *BETA* As of Jan 17, 2019 4:10 pm Refresh

Business Relevant | **Business Irrelevant** | Default

Application (14) Export

Filter Find

Name	Health		Usage Bytes	Average Throughput	DSCP		Packet Loss (%)		Network Latency	
	Last 10 Minutes	Last 3 Hours			Marking	Preservation	Max	Average	Max	Average
netflix	--			143.56 Kbps	DF	No	1	0.3	65 ms	37 ms
dropbox	--			164 bps	DF	No	5	2	92 ms	52 ms
icloud	9	View	231.18 KB	141 bps	AF11	No	100	3	28 ms	11 ms
itunes	--	View	76.18 KB	121 bps	DF	No	0	0	98 ms	41 ms
apple-services	10	View	95.95 KB	83 bps	DF	No	0.44	0.02	82 ms	25 ms



Show 5 entries

Showing 1 - 5 of 14

Previous 1 2 3 Next

Client 360 Device Information

Detail Information

Jan 17, 2019 4:10 pm

Device Info | Connectivity | RF

Information	
User Name	mtrache1
Host Name	Samsung-S8
MAC Address	74:B5:87:9C:19:85
IPv4 Address	172.20.194.13
IPv6 Address	--
Device Type	iPhone11,8
Operating System	iOS12.1.2
Status	CONNECTED
VNID	8204

Connection Information	
Band	5 GHz
Spatial Streams	2
Channel Width	20 MHz
WMM	Supported
U-APSD	Disabled

Client 360 Apple Insights

Device Info | Connectivity | RF | iOS Analytics

Neighbor APs (4)

Export

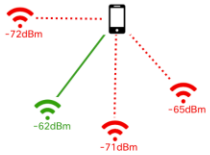
Filter

BSSID	AP Name	Channel	RSSI (dBm)	Location
00:F2:8B:26:EF:3F	AP2802_1-C9k-u-9	112	-62	Global/Germany/Frankfurt/Cisco FRA/1OG
00:F2:8B:26:EF:30	AP2802_1-C9k-u-9	11	-72	Global/Germany/Frankfurt/Cisco FRA/1OG
00:81:C4:41:2A:AF	AP3800-C9k-u-5	64	-65	Global/Germany/Frankfurt/Cisco FRA/EG
00:81:C4:41:2A:A0	AP3800-C9k-u-5	1	-71	Global/Germany/Frankfurt/Cisco FRA/EG

Show 10 entries

Showing 1 - 4 of 4

Previous 1 Next



Client Disassociation Details (12)

Export

Filter

Time	Disassociation Reason	Disassociated AP	Session Duration	AP Location
Thursday, January 17, 2019 3:21 PM	DHCP failure	AP2802_1-C9k-u-9		1OG
Thursday, January 17, 2019 3:05 PM	DHCP failure	AP2802_1-C9k-u-9		1OG
Thursday, January 17, 2019 3:04 PM	DHCP failure	AP2802_1-C9k-u-9		1OG
Thursday, January 17, 2019 2:58 PM	DHCP failure	AP2802_1-C9k-u-9		1OG
Thursday, January 17, 2019 2:57 PM	DHCP failure	AP2802_1-C9k-u-9		1OG
Thursday, January 17, 2019 2:47 PM	DHCP failure	AP2802_1-C9k-u-9		1OG
Thursday, January 17, 2019 2:36 PM	DHCP failure	AP2802_1-C9k-u-9		1OG
Thursday, January 17, 2019 2:18 PM	DHCP failure	AP2802_1-C9k-u-9		1OG
Thursday, January 17, 2019 1:55 PM	DHCP failure	AP2802_1-C9k-u-9		1OG
Thursday, January 17, 2019 1:51 PM	DHCP failure	AP2802_1-C9k-u-9		1OG

Show 10 entries

Showing 1 - 10 of 12

Previous 1 2 Next

Cisco DNA Center Assurance Apple Insights

1 Device Profile

Client shares these details
1. iPhone 7, iPad Pro
2. iOS 11

Support per device-group Policies and Analytics

2 Wi-Fi Analytics

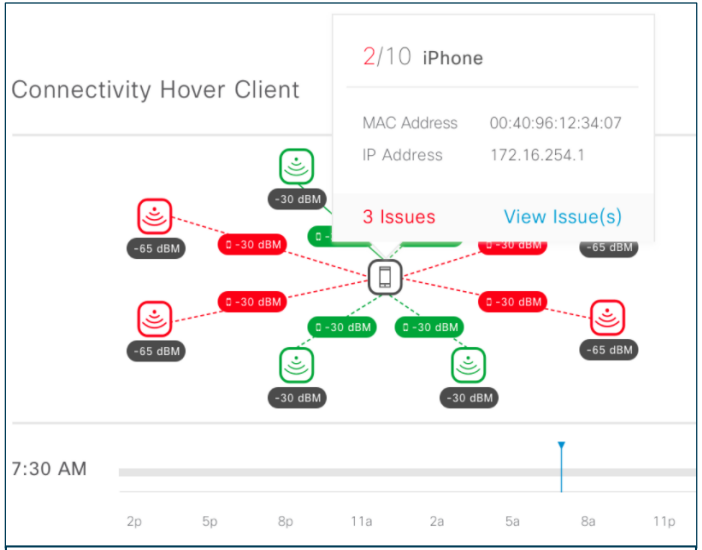
Client shares these details
1. BSSID
2. RSSI
3. Channel #

Insights into the clients view of the network

3 Assurance

Client shares these details
Error code for why did it previously disconnected

Provide clarity into the reliability of connectivity



Disassociation Events

Filter

Find

Disassociation Reason	Disassociated from AP	Time	Location Building
cl_ST_USER_TRIGGERED	LA1-AP3802-31	Sun Oct 22 2017 21:47:01 GMT-0700 (Pacific Standard Time)	Los Angeles
cl_ST_USER_TRIGGERED	LA1-AP3802-31	Sun Oct 22 2017 21:28:01 GMT-0700 (Pacific Standard Time)	Los Angeles
cl_ST_DEVICE_IDLE	LA1-AP3802-31	Sun Oct 22 2017 21:33:01 GMT-0700 (Pacific Standard Time)	Los Angeles
cl_ST_DEVICE_IDLE	LA1-AP3802-31	Sun Oct 22 2017 21:19:01 GMT-0700 (Pacific Standard Time)	Los Angeles
cl_ST_DEVICE_IDLE	LA1-AP3802-31	Sun Oct 22 2017 21:11:01 GMT-0700 (Pacific Standard Time)	Los Angeles

Start troubleshooting

Top 10 Issues (5) Jan 15, 2018 9:05:00 to Jan 16, 2018 9:05:00

Connectivity OSPF Adjacency Failed on Device " 172.20.1.255" Interface TenGigabitEthernet5/13 with Neighbor 172.20.1.116 Total occurrences: 105	Jan 16, 2018 8:35 am
Onboarding Clients Failing DHCP Attempts Because DHCP IP Addressing Timed Out at " Global/Germany/Frankfurt/Cisco FRA/EG" Total occurrences: 40	Jan 16, 2018 8:30 am
Connectivity OSPF Adjacency Failed on Device " 172.20.2.244" Interface GigabitEthernet0/0/2 with Neighbor 172.20.2.252 Total occurrences: 26	Jan 16, 2018 8:09 am
Connectivity OSPF Adjacency Failed on Device " 172.20.2.254" Interface GigabitEthernet0/1 with Neighbor 172.20.2.253 Total occurrences: 20	Jan 16, 2018 8:09 am
Connectivity Interface Virtual-Access2 State Changed to Down on Device " 172.20.2.254" Total occurrences: 2	Jan 15, 2018 3:11 pm

Onboarding issues – details

Clients Failing DHCP Attempts Because DHCP IP Addressing Timed Out at " Global/Germany/Frankfurt/Cisco FRA/EG"

Status: Open

Last Occurred: Jan 15, 2018 8:00 PM

Description

Clients located in " Global/Germany/Frankfurt/Cisco FRA/EG" timed out and have not been assigned an IP address from the DHCP server.

Impact

Location:
1 Building

Clients
3 Wireless Clients

Client DHCP Attempts (AP Group: bab060da-58bd-476d-b639-7ea297005870)

Jan 14, 2018 8:00 pm to Jan 15, 2018 8:00 pm

Impacted Client... Impacted Client...

Suggested Actions (6)

Onboarding issues – how many clients are affected?

Clients Failing DHCP Attempts Because DHCP IP Addressing Timed Out at " Global/Germany/Frankfurt/Cisco FRA/EG"

Status: Open

Last Occurred: Jan 15, 2018 8:00 PM

Description

Clients located in " Global/Germany/Frankfurt/Cisco FRA/EG" timed out and have not been assigned an IP address from the DHCP server.

Impact

Location:
1 Building

Clients
3 Wireless Clients

Impacted Wireless Clients | Impacted Locations

Find

Hostname	Mac Address	Device Type	AP	SSID / VLAN	WLC
Unknown	00:13:EF:80:0E:31	WIRELESS	AP3802i_1	demowlan1 / 30	CT5520_1
mhgrisu4	80:1F:02:F6:F5:0C	WIRELESS	AP3802i_1	demowlan1 / 30	CT5520_1
mhgrisu1	00:13:EF:90:0B:BB	WIRELESS	AP3802i_1	demowlan1 / 30	CT5520_1

Authentication ...

Troubleshoot OSPF issue

Top 10 Issue Types

Priority	Issue Type	Device Role	Category	Issue Count	Site Count (Area)	Device Count	Last Occurred Time
P2	Network Device Interface Connectivity - OSPF Adjacency Failure	CORE	Connectivity	5	1	1	Jan 21, 2020 10:19 am
P2	Network Device Interface Connectivity - OSPF Adjacency Failure	DISTRIBUTION	Connectivity	13	1	1	Jan 21, 2020 10:02 am
P2	Switch power failure	DISTRIBUTION	Device	1	1	1	Jan 21, 2020 1:43 am
P3	Device time has drifted from DNAC	ACCESS	Device	5	1	2	Jan 21, 2020 10:03 am
P3	Device time has drifted from DNAC	WLC	Device	8	1	2	Jan 21, 2020 5:48 am
P3	High input/output error on Switch interfaces	CORE	Connected	3	1	1	Jan 20, 2020 4:11 pm
P3	Device time has drifted from DNAC	CORE	Device	1	1	1	Jan 20, 2020 1:47 pm

View All Open Issues

OSPF issue - details

OSPF Adjacency Failed on Device "L3-Rack13" Interface GigabitEthernet1/0/37 with Neighbor 192.168.1.2

Open

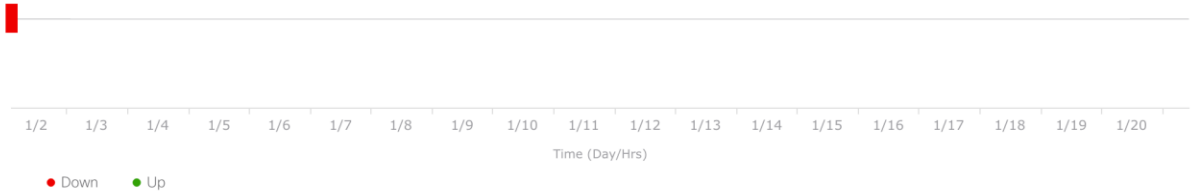
Description

OSPF adjacency failed on device name:'L3-Rack13', interface:'GigabitEthernet1/0/37' at site:'Cisco FRA' with neighbor '192.168.1.2'
Go to L3-Rack13

Last Occurred: Jan 21, 2020 10:02 AM

Syslog Events

Jan 20, 2020 10:02 am to Jan 21, 2020 10:32 am



OSPF issue – suggestions

Suggested Actions (6)

1	Ping the neighbor IP to verify connectivity.	Run
2	Check OSPF neighbors.	Run
3	If the Neighbor is in "Init" state. Check if there is authentication configured using "show run | sec OSPF". Authentication type and keys should match on both routers	Run
4	If the Neighbor is in "Exstart" state. Check if the MTU settings are same on the interface connecting the routers.	Run
5	Check interface GigabitEthernet1/0/37 has any incrementing errors	Run
6	If you are unable to resolve the issue, contact Cisco TAC for support.	

OSPF issue – step by step

Suggested Actions (6)

1 Ping the neighbor IP to verify connectivity.

ping neighbor IP

ping 192.168.1.2

Success

```
ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/13 ms
L3-Rack13#
```

2 Check OSPF neighbors.

Check OSPF neighbors

show ip ospf neighbor

Success

```
show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.20.1.255      1   FULL/BDR        00:00:39    172.20.1.49     TenGigabitEthernet1/1/4
192.168.1.2       1   EXSTART/DR      00:00:38    192.168.1.2     GigabitEthernet1/0/37
L3-Rack13#
```

OSPF issue – solution

3 If the Neighbor is in "Init" state. Check if there is authentication configured using "show run | sec OSPF". Authentication type and keys should match on both routers

Run

4 If the Neighbor is in "Exstart" state. Check if the MTU settings are same on the interface connecting the routers.

Check the interface MTU

show ip interface GigabitEthernet1/0/37 | in MTU

Success

```
show ip interface GigabitEthernet1/0/37 | in MTU
  MTU is 1500 bytes
L3-Rack13#
```

5 Check interface GigabitEthernet1/0/37 has any incrementing errors

Run

Agenda

- Cisco DNA Center 10 minutes overview
- Before you deploy – purchase and design considerations
- Base automation for wired and wireless
- Getting started with Cisco SD-Access
- Assurance and application policies
- **Key takeaways**

Why to start with Cisco DNA Center today?

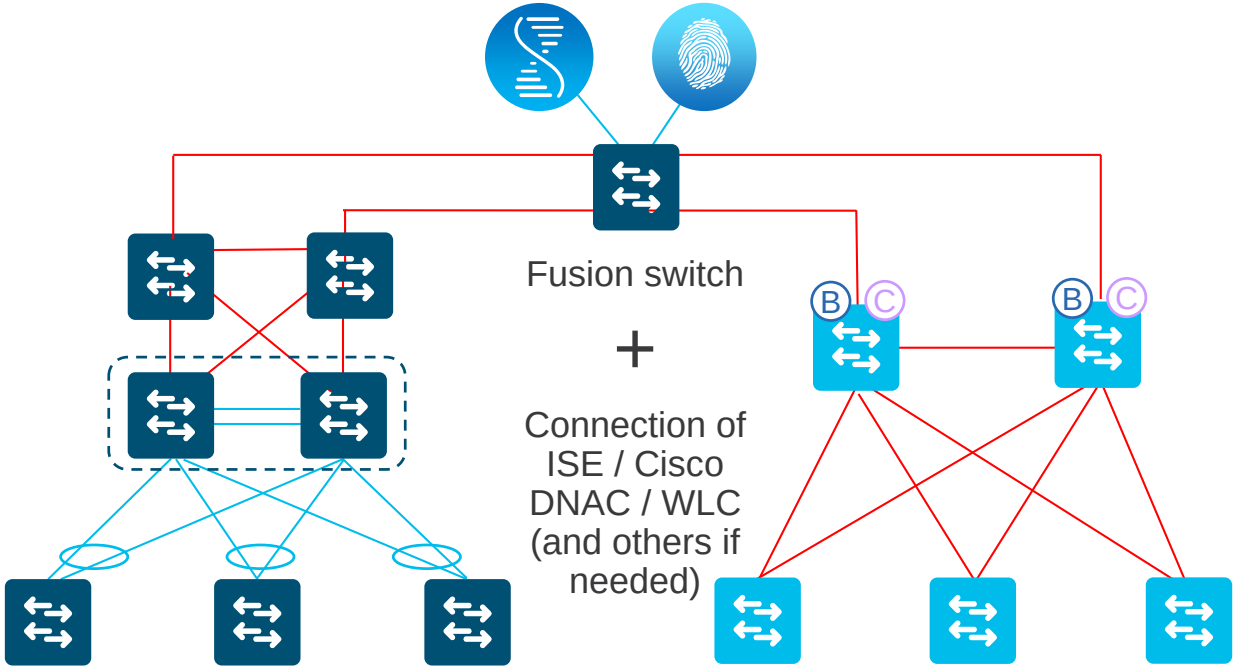
Monitoring	Use Cisco DNA Center just for Analytics & Assurance (Read Only)
Analytics	Even without SD-Access you get great insight & visibility
Troubleshooting	Active support for troubleshooting (suggested troubleshooting steps)
Operations management	Prove the value of Cisco DNA Center and later move to an SDA deployment

Why to start with Cisco DNA Center today?

Automation	Easy roll-out of new devices Use Cisco DNA Center in the LAB to see automation in action
Software Defined Access	Follow the SD-Access sessions at Cisco Live
Get Hands-on	1) Improve your understanding with dCloud demo (ask your account team for a pod) 2) Deploy an SD-Access pilot somewhere
Automate your Policies	Use Cisco DNA Center to easily segment your networks and automate your Polices

Simple Cisco SD-Access pilot architecture

Option 1 – Pilot fabric dissociated from current network



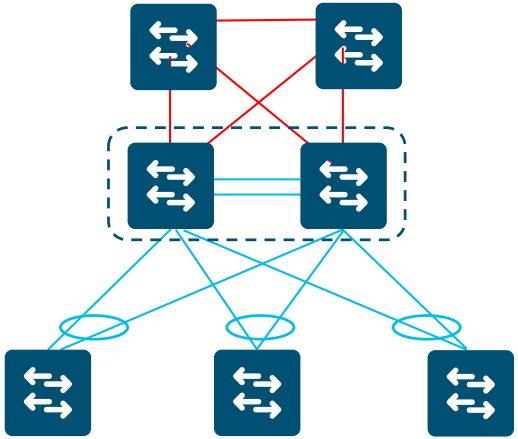
Underlay automation testing

Very close to production site

No requirement on existing infrastructure

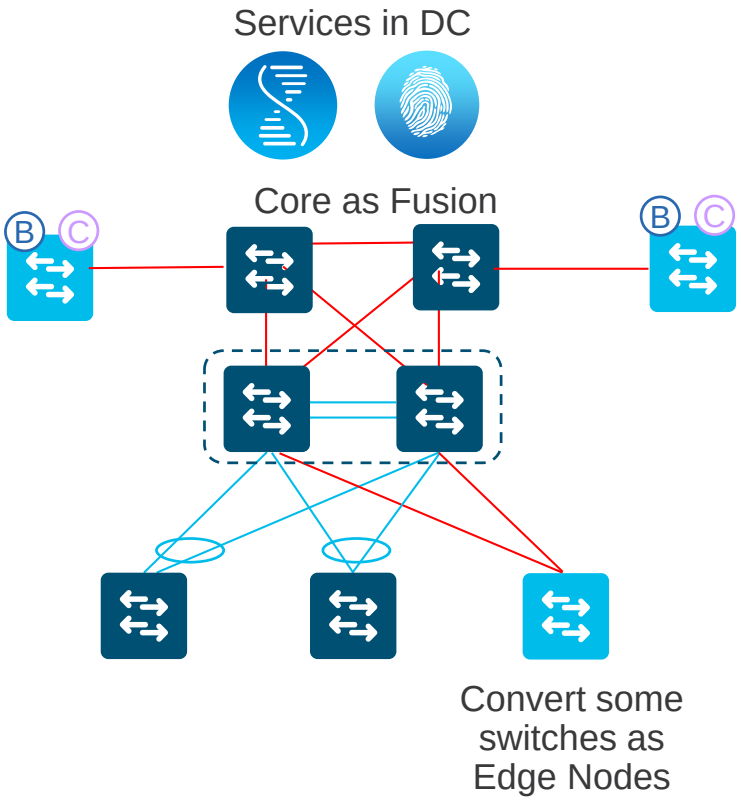
Simple Cisco SD-Access pilot architecture

Option 2 – Pilot fabric on top of current network



Simple Cisco SD-Access pilot architecture

Option 2 – Pilot fabric on top of current network



No Underlay automation testing

Interesting for validation of the migration process for large sites

Beware of MTU on intermediate nodes

Traffic between fabric and non-fabric switches always passes through Border Nodes

OPS

Operations Track

www.ciscolive.com/emea/learn/technology-tracks/operations.html

Opening Keynote 09:00

LTRNMS-2500
Lab: A Practical Look at Cisco DNA Center 09:30

BRKNMS-2285
How to be a hero with Cisco DNA Center Platform APIs 14:30

BRKSDN-2497
Build Your API-Based NW Troubleshooting Kit 17:00

BRKNMS-2426
Cisco DNA Center - From 0 to 100 How to get the network up and running from scratch 08:30

PSOOPS-2236
Unlocking the power of open platform with Cisco DNA Center Platform 11:00

TCRNMS-2100
TechCircle: Cisco DNA Center Innovations 13:15

BRKOPS-2150
Deploying Advanced Network Services using Cisco DNA Center 14:45

BRKOPS-2024
Wireless Automation & Assurance with Cisco DNA Center using APIs 16:45

BRKNMS-2031
Cisco DNA Center: The evolution from traditional Management to Intent-Based Automation & Assurance 11:15

Guest Keynote 17:00

Cisco Live Celebration 18:30

BRKSDN-2295
Controlling the wild wild west of applications in your network using Cisco DNAC QoS Policies 09:00

BRKOPS-2826
Cisco DNA Center Maintenance and Troubleshooting 11:30

DNA Automation

GURU

OPS

Operations Track

www.ciscolive.com/emea/learn/technology-tracks/operations.html

Opening Keynote 09:00

LTRNMS-2500
Lab: A Practical Look at Cisco DNA Center 09:30

BRKOPS-2131
Cisco DNA Analytics and Assurance - The Shortest Path to Network Innocence 14:30

BRKOPS-2562
Data is the new Oil: The Nuts & Bolts of leveraging Cisco DNA Assurance data for creating value added services 17:00

LTRNMS-2043
Cisco DNA Assurance and Analytics Lab 09:00

BRKOPS-2991
Machine Learning in Network Operations: Lessons Learned 11:00

TCRNMS-2100
TechCircle: Cisco DNA Center Innovations 13:15

BRKOPS-2024
Wireless Automation & Assurance with Cisco DNA Center using APIs 16:45

BRKOPS-3825
Interpreting streaming telemetry data using ML/AI 11:15

BRKNMS-2031
Cisco DNA Center: The evolution from traditional Management to Intent-Based Automation & Assurance

BRKOPS-2100
Resolving Network Faults Faster through Automating Entire Fault Management Process. 14:45

Guest Keynote 17:00

Cisco Live Celebration 18:30

BRKSDN-2295
Controlling the wild wild west of applications in your network using Cisco DNAC QoS Policies 09:00

BRKOPS-2826
Cisco DNA Center Maintenance and Troubleshooting 11:30

DNA Assurance

GURU

Cisco SD-Access

SD-Access Breakouts

TUE

- Keynote — 09:00
- **BRKCRS-2810** — Cisco SD-Access - A Look Under the Hood — 11:00
- **BRKCRS-1400** — Recipe for transforming Enterprise Networks with IBN — 14:30
- **BRKCRS-2811** — Cisco SD-Access – Connecting the Fabric to External Networks — 17:00

WED

- **BRKCRS-2815** — Cisco SD-Access – Connecting Multiple Sites in a Single Fabric — 08:30
- **BRKCRS-2821** — Cisco SD-Access – Connecting to the DC, FW, WAN and more! — 11:00
- **BRKCRS-2832** — Extending Cisco SD-Access beyond Enterprise walls — 11:00
- **BRKCRS-2823** — Cisco SD-Access – Firewall Integration — 16:45

THU

- **BRKCRS-2818** — Build a Software Defined Enterprise with Cisco SDWAN & SD-Access — 08:30
- **BRKCRS-2830** — Cisco SD-Access – Lessons learned from Design & Deployment. — 09:45
- **BRKCRS-2502** — Best Practices for Design and Deployment of Cisco SD-Access — 11:15
- **BRKCRS-2825** — Cisco SD-Access - Scaling the Fabric to 100s of Sites — 11:15
- **BRKCRS-2823** — Cisco SD-Access deep dive — 14:45
- Keynote — 17:00
- Customer Appreciation — 18:30

FRI

- **BRKCRS-2819** — Creating multi-domain architecture using Cisco SD-Access — 09:00
- **BRKCRS-3811** — Cisco SD-Access – Policy Driven Manageability — 09:00
- **BRKCRS-2812** — Cisco SD-Access – Integrating with your existing network — 11:30
- **BRKARC-2020** — Cisco SD Access - Troubleshooting the fabric — 11:30
- **BRKCRS-2824** — Intuitive Zero-Trust Design, Migration When Securing the SD-Access Workplace — 11:30

GURU

OPS

Operations Track

www.ciscolive.com/emea/learn/technology-tracks/operations.html

Opening Keynote 09:00

BRKNMS-2573 11:00
From Prime Infrastructure to Software Defined Network (SDN) Management with Cisco DNA Center

BRKOPS-2131 14:30
Cisco DNA Analytics and Assurance - The Shortest Path to Network Innocence

BRKNMS-2426 08:30
Cisco DNA Center - From 0 to 100 How to get the network up and running from scratch

BRKOPS-2110 11:00
End-2-end policy from the Campus to the DC and back, a packet journey with SDA to ACI

TCRNMS-2100 13:15
TechCircle: Cisco DNA Center Innovations

BRKSDN-2500 14:45
Real World Use Cases for Deploying and Operating Cisco SD-Access Using Cisco DNA Center

BRKNMS-2031 11:15
Cisco DNA Center: The evolution from traditional Management to Intent-Based Automation & Assurance

Guest Keynote 17:00

Cisco Live Celebration 18:30

BRKSDN-2295 09:00
Controlling the wild wild west of applications in your network using Cisco DNAC QoS Policies

BRKOPS-2859 11:30
Towards operating a multi-domain network

Operating Cisco SDA

GURU

Complete your online session survey

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

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

Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

Thank you

CISCO

You make **possible**