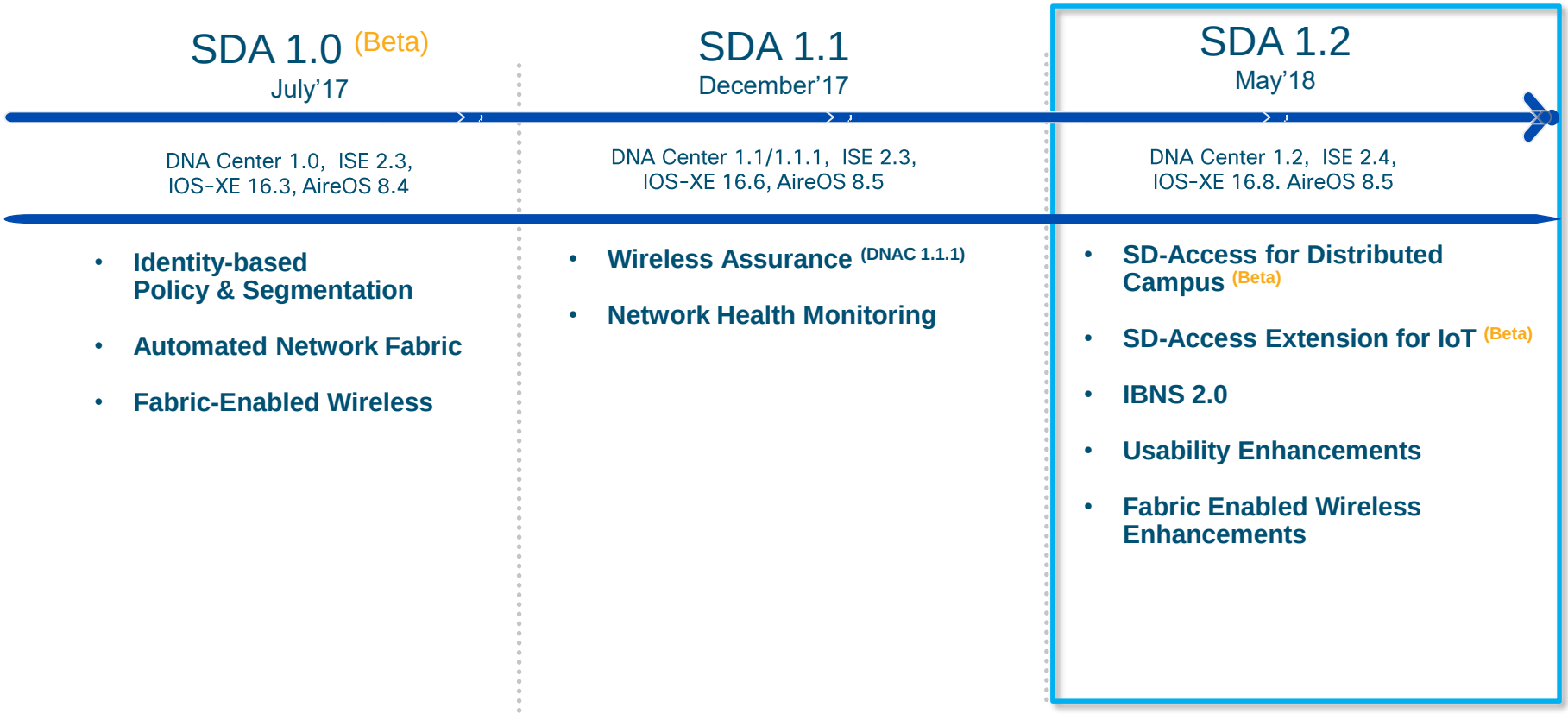
SD-Access 1.2 Update

Rene Andersen
Version 1.0

29/05/2018

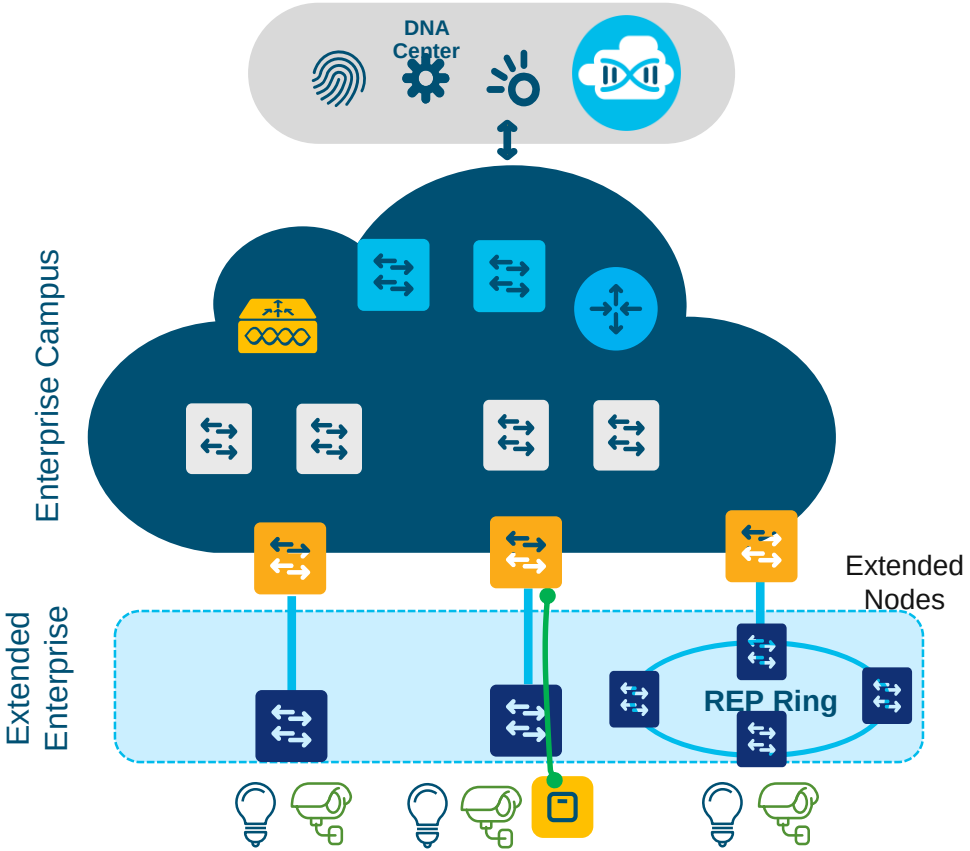
SD-Access Roadmap



SD-Access Extension for IoT

Securely Consolidate IT and OT to One Network

SD-Access Extension for IoT



- Operational simplicity for IT designed and managed and IT designed and OT managed
- Greater visibility to broad set of IoT devices
- Improved threat detection and containment

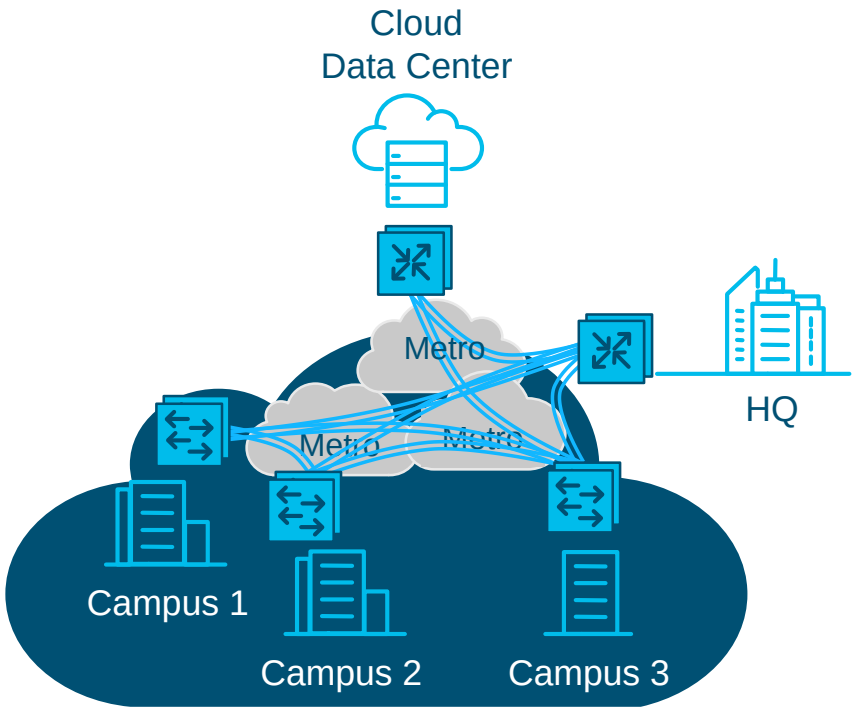
Extended Node Portfolio

IE4000 IE4010 IE5000

Catalyst Digital Building

3560-CX Compact

SD-Access for Distributed Campus

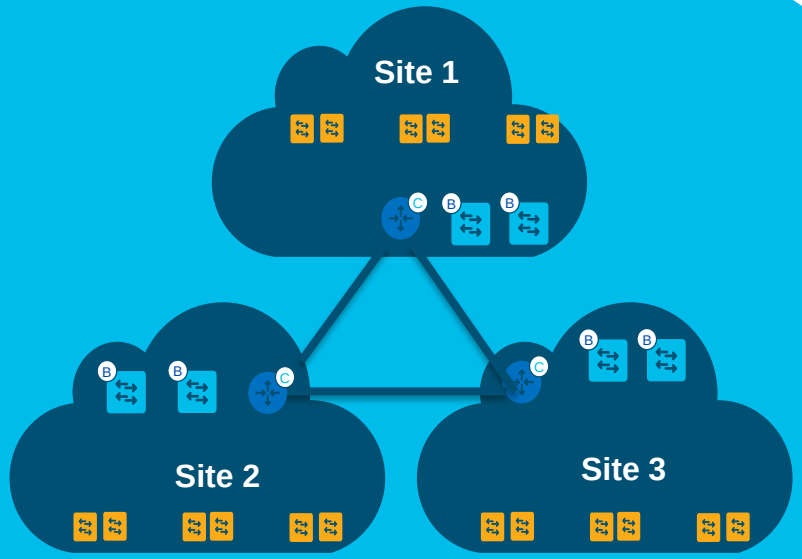


SD-Access Policy-Based Access for **Distributed Campus**

- End-to-end segmentation
- Centralized Automation & Assurance
- Future Proof for SD-WAN
  (Viptela SD-WAN Integration on Roadmap)

Introducing SD-Access Distributed Campus

Enhanced Resiliency and Scale for Large Deployments



Extend SD-Access Benefits Campus-wide

- End-to-End Policy and Segmentation
- Enhanced Resiliency & Local Isolation
- Direct Internet Access per Site
- Automated Inter-Site Connectivity
- Scalable to 100+ sites
- Flexible: 50-100,000 Users/Site

Automation and Assurance managed through DNA Center

SD-Access 1.2 Software Compatibility

DNA Center	DNAC 1.2
ISE	TBD
Catalyst 3K/9K	IOS-XE 16.8.1s
Catalyst 4500	IOS 3.10.2 es
Catalyst 6800	15.5(1)SY1 es
Nexus 7700	8.2(1) SMU's, CSCvg39911, CSCvh87828, CSCvg09282, CSCvh32898
ASR1K/ISR4K/CSR	IOS-XE 16.8.1s
Wireless LAN	AireOS 8.5 MR3

* **Minimum SW version needed for new features in SDA 1.2**

SD-Access 1.2.X Backward Compatibility

DNA Center	DNAC 1.1.x	
ISE	ISE 2.3 Patch 2	ISE 2.3 Patch 1
Catalyst 3K/9K	IOS-XE 16.6.3	IOS-XE 16.6.2s
Catalyst 4500	IOS 3.10.0e	IOS 3.10.0c
Catalyst 6800	15.4(1)SY4	
Nexus 7700	8.2(1) SMU	
ASR1K/ISR4K/CSR	IOS-XE 16.6.3	IOS-XE 16.6.2s
Wireless LAN	AireOS 8.5 MR2	AireOS 8.5 MR1

* **DNAC's releases will support backward compatibility In terms of device code versions**

SD-Access 1.2 Scale

SD-Access1.2 Scale

Fabric Constructs	Maximum Supported on Single DNAC Cluster
No of Fabric Domains per DNA Cluster	10
No of Fabric Sites across the Fabric Domains*	200
Total Endpoints (including APs) per DNA Cluster* APs (Counted as Endpoints) per DNA Cluster *	25K 4000
Number of Virtual Networks	64
Fabric Nodes (Edge, Border, WLC) per DNA cluster *	500**
Non-Fabric Nodes(Intermediate, Subtended, Routers) per DNA Cluster *	1000
Control Plane Nodes Per Fabric Site	2
Default Border Nodes Per Fabric Site	4

- Above scale is split across all the configurable fabric domains (10) or can be in one fabric domain

** A Stack of switches is considered as one Fabric Node

Single DNAC cluster = 3 DNAC appliances (2+1 in HA)

*** These are 1D Platform numbers**

SD-Access 1.2 – Edge Scale

Fabric Constructs	Catalyst 3650	Catalyst 3850	Catalyst 9300	Catalyst 4K (Sup8E)	Catalyst 9400	Catalyst 9500
Virtual Networks	64	64	256	64	256	256
Local End Points/Hosts	2K	4K	4K	4K	4K	4K
SGT/DGT Table	4K	4K	8K	2K	8K	8K
SGACLs (Security ACEs)	1350	1350	5K	1350	18K	18K

*** These are 1D Platform numbers**

SD-Access – Border Scale

Scale	Catalyst 3850(XS)	Catalyst 9300	Catalyst 9400 (*SUP1 XL)	Catalyst 9500	Catalyst 9500H	Catalyst 6800	Nexus N7700	ASR1K/ ISR4K	CSR1Kv
Virtual Networks	64	256	256	256	256	500	500	4K	n.a.
SGT/DGT Table	4K	8K	8K	8K	8K	30K	16K	62K	n.a.
SGACLs (Security ACEs)	1500	5K	18K	18K	18K	30K(XL) 12K(non XL)	16K	64K	n.a.
Fabric Control Plane Entries with Border Co-Located on Same Device	3K	16K	80K	80K	80K	25K	Not Supported	200K/100K (16GB) 100K/50K (8GB)	200K
IPv4 Fabric Routes	8K	4K	20K	48K	48K	1M (XL)/ 256K	500K	4M (16GB) 1M (8GB)	n.a.
IPv4 Fabric Host Entries	16K	16K	80K	96K	96K		32K		

* SUP1 XL is only supported as Border node

SD-Access 1.2 Features

SDA 1.2 Features

Below are the new features that are being introduced with DNAC/SD-Access 1.2

- SD-Access Extension for IOT (Requires IOS-XE 16.8.1s)
- SD-Access for Distributed Campus (Requires IOS-XE 16.8.1s)
- Host On-Boarding Enhancements including IBNS 2.0
- Lan Automation Enhancements
- Wireless Enhancements

SD-Access Extension for IOT

Introducing SD-Access Extension

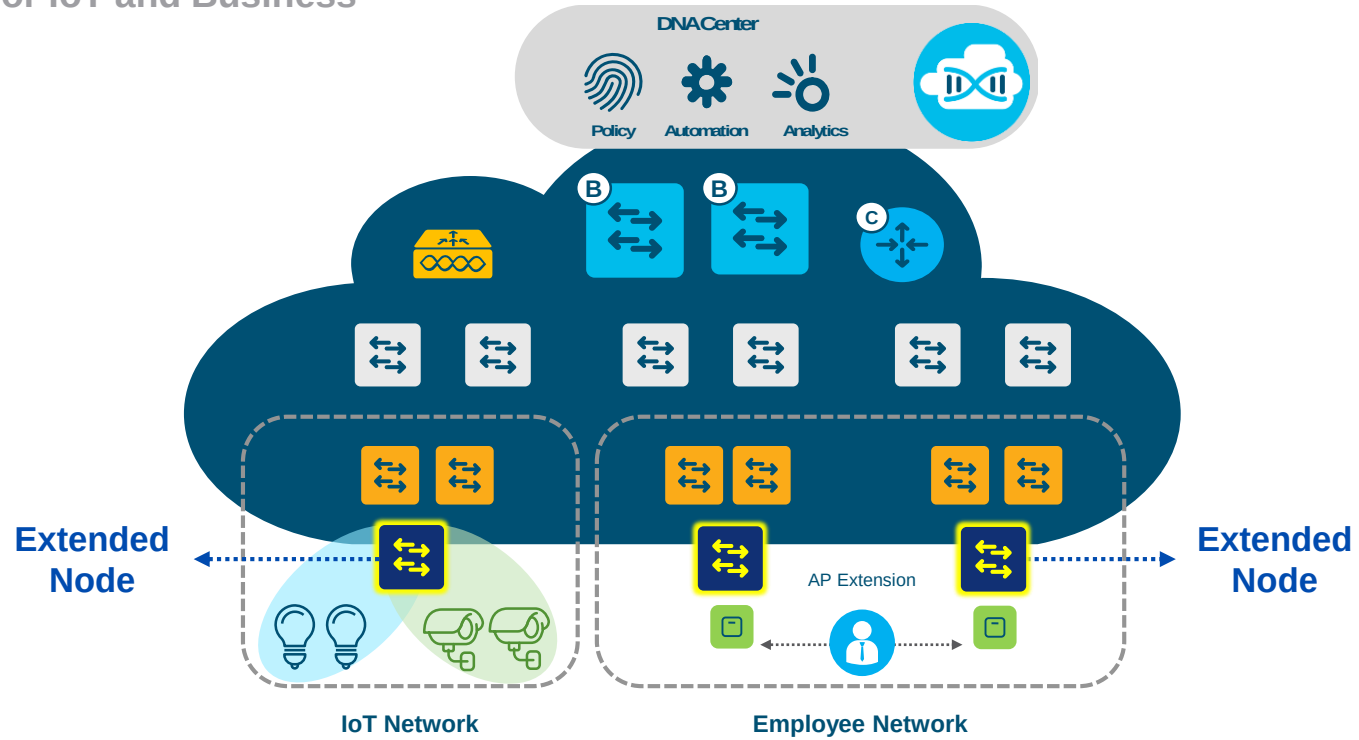
Extending the Fabric Edge for IoT and Business

Platform Support

Catalyst Digital Building

Catalyst 3560-CX

IE Series (4K/5K)



Purpose Built Switches for IoT

Users, Device and IoT Segmentation

Policy based Automation

Beta in SDA 1.2

SD-Access Extension

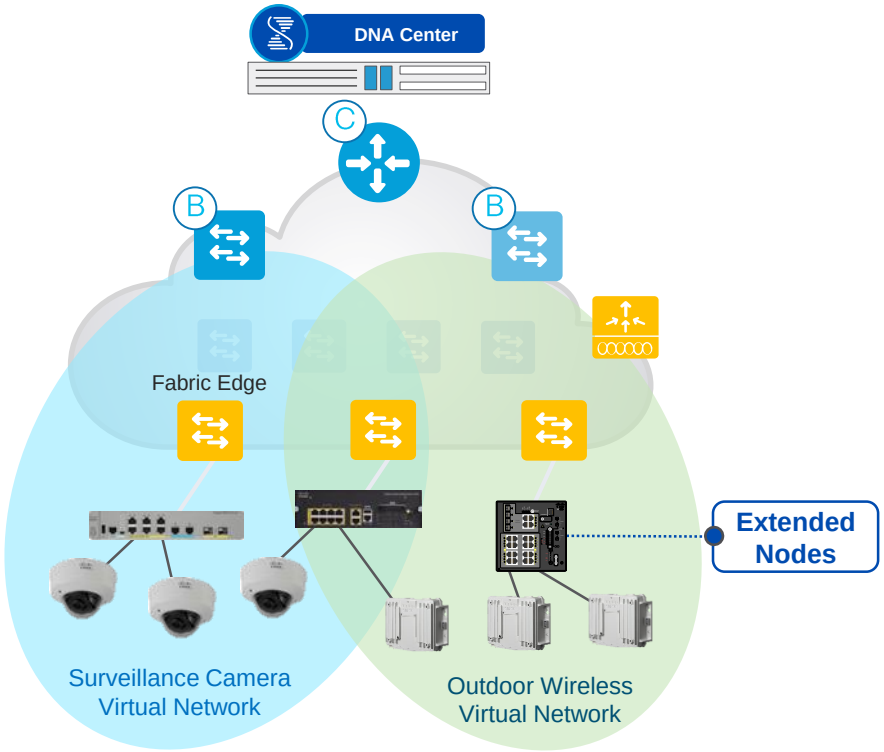
Key Benefits for IoT and Business

SD-Access Capabilities

- Easy automated Device install and setup
- Stretched subnets for ease of endpoint connections
- Workflow based policy automation
- Segment Applications with separate Virtual Networks

DNA Center Solution Benefits

- Single pane of glass for management
- Inventory, Topology, Image management
- Automate Day 1 Installation
- Network Assurance – Device 360



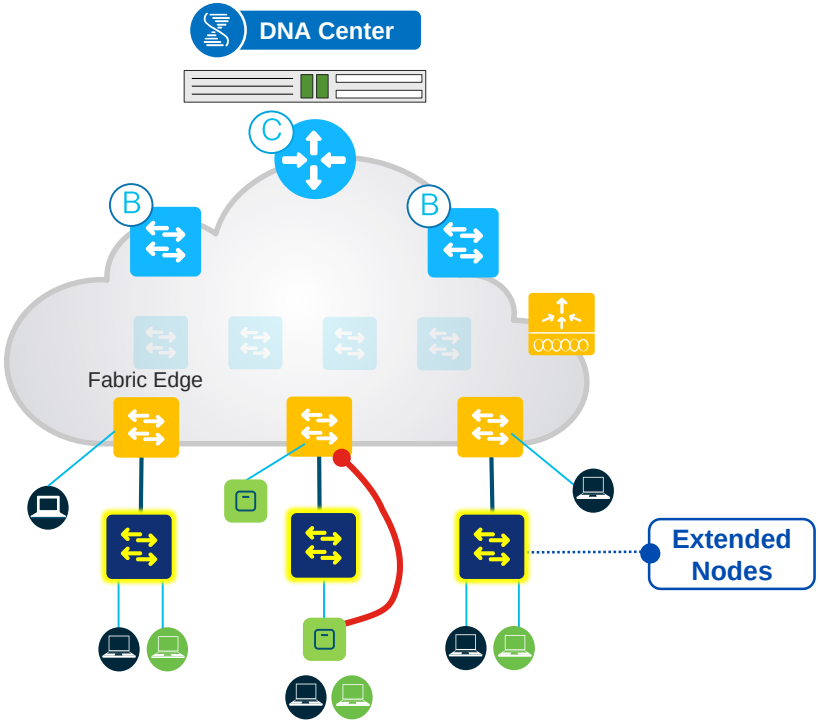
Extended Nodes extend SD-Access beyond the Fabric edge

Traditional vs SD-Access Extension

	Traditional	SD-Access Extended Node
Day 1 – Design and Installation	• Manual “box by box” configuration • Networking expertise required to provision and deploy devices	• Automated device deployment decreases time to operation • Zero touch configuration enables non-networking personnel to install
Day N – Operations and Updates	• Network additions are complex • No automated workflows • Changes / Adds require manual configuration of multiple devices • Operation monitoring limited	• Deployment flexibility with fabric enabled technologies – i.e. Stretched Subnets • Intent-based workflow uses automation for fabric and service configuration removes complexity of new service additions • Intent drives network updates are centrally administered, removing manual reconfiguration and reducing downtime • Network operational assurance with device 360 shows performance and pin points operational issues
Security	• Static L2 – L4 ACLs • Address based segmentation • Changes / Adds require manual configurations of multiple devices • Continuous auditing required to maintain security rule sets	• Group based security policy auto configured in the fabric – separating policy from addressing simplifies security enforcement and maintenance • Fabric provides site-wide segmentation enables intent-based security • Integrated threat defense, with suspicious users or devices easily quarantined

SD-Access Extended Node

- **Extended node** connects to a single **Edge node** using an **802.1Q Trunk port** (single or multiple VLANs) using static assignment
- Switchports on the Extended node can then be **statically assigned** to an **appropriate IP Pool** (in DNA Center)
- **SGT tagging** (or mapping) is accomplished by **Pool to Group mapping** (in DNA Center) on the connected Edge node
- Traffic **policy enforcement** based on SGTs (SGACLs) is **performed at the Edge node**



Beta in SDA 1.2

SD-Access Extension

Fabric Edge Support Matrix

SDA Extended Node	C3850	C4500	C9300/9400/9500
3560CX	No	No	Yes
IE switches	No	No	Yes
CDB	No	No	Yes

Beta in SDA 1.2

SD-Access Extension

Minimum Extended Node Version

Platform Support

Catalyst Digital Building

15.2(6)E1 Link to CDB SW download page

Catalyst 3560-CX

15.2(6)E1 Link to Cat 3560-CX SW download page

IE Series (4K/5K)

15.2(6)E1 Link to IE4000 SW Download page

Beta in SDA 1.2

SD-Access Extension

DNA Licensing

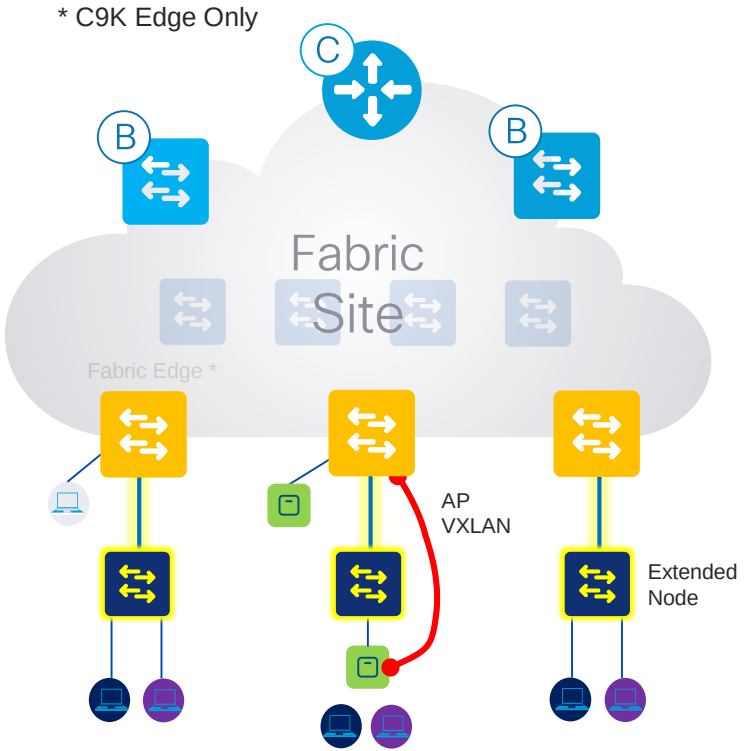
- **2 DNA license (Advantage, Essentials)**
  - Essentials is for basic networking buyers
  - **Advantage required for SDA + Extension**
- DNA license purchased for 3,5,7 year terms

License Type	IE2000	IE3000	IE4000	IE4010	IE5000	C3560-CX	CDB
DNA Essentials	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DNA Advantage	No	No	Yes	Yes	Yes	Yes	Yes

SD-Access Extended Nodes Deployment Models

SD-Access Extended Node

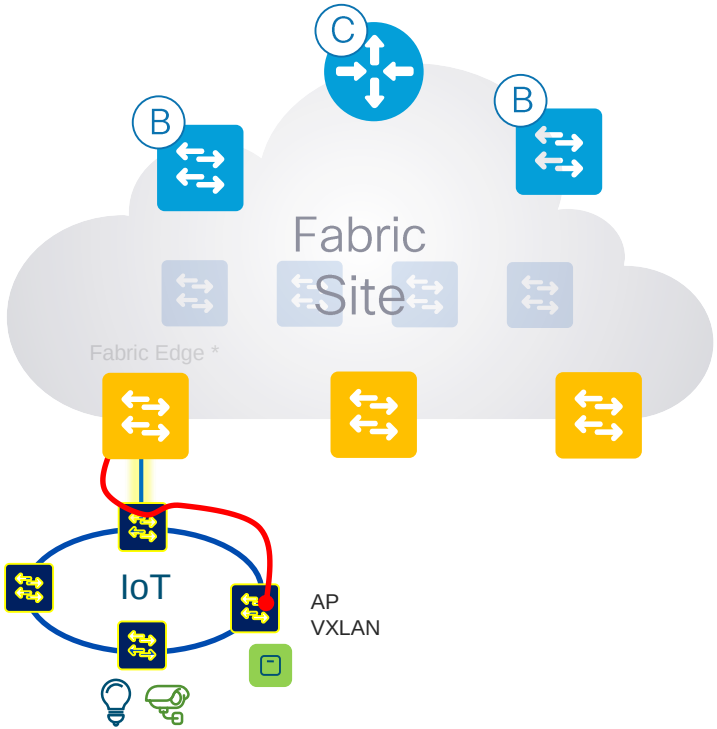
Point to Point Connection's



- Extended node connects to a single Edge node using an 802.1Q Trunk port .
- Extended node is connected to fabric edge nodes using zero touch plug & play (PNP).
- Switch ports on the Extended node can then be statically assigned to an appropriate IP Pool or dynamically assigned using authentication via DNA Center.
- Policy tagging is done on the fabric edge nodes when using IP subnet to SGT mapping.
- Traffic policy enforcement based on SGTs (SGACLs) is performed at the Edge node

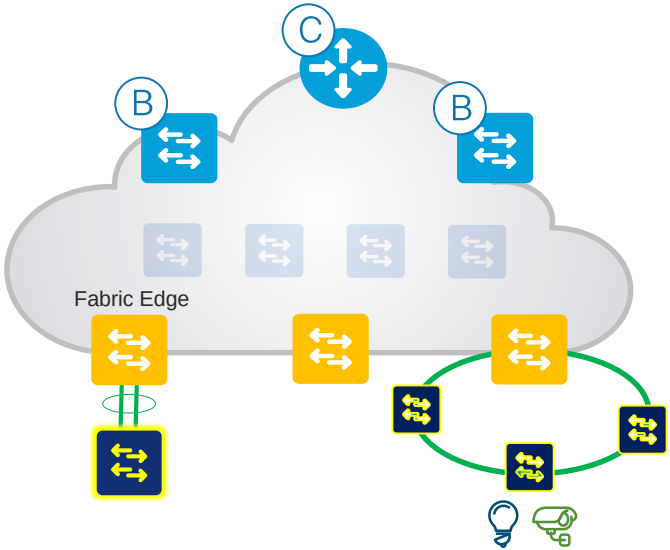
SD-Access Extended Node

Ring Connection's



- Extended node connects to a single Edge node using an 802.1Q Trunk port .
- Extended node is connected to fabric edge nodes using zero touch plug & play (PNP).
- This deployment model is not fully automated with DNAC
- The extended node that connects to the Edge node can be in a ring.
- The entire ring needs to be manually provisioned. DNAC will not automate it.
- The host facing ports on the extended nodes in the ring are also manually configured.

Not Supported in SDA 1.2



- No REP or STP starting from FE
- No Ether Channel links from FE to Extended node

Zero Touch Provisioning for Extended Nodes

Zero Touch Provisioning Overview

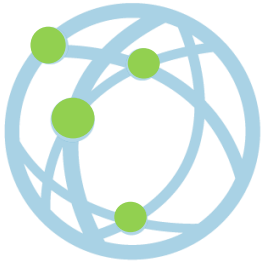
Plan

Verify Network Design

Verify System support

Prepare Extended Nodes

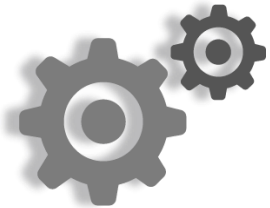
Design



Design IP Address Pools

Assign IP address Pools to the right site

Provision



Dynamic discovery & automation

Static Discovery & automation

Host Onboarding settings

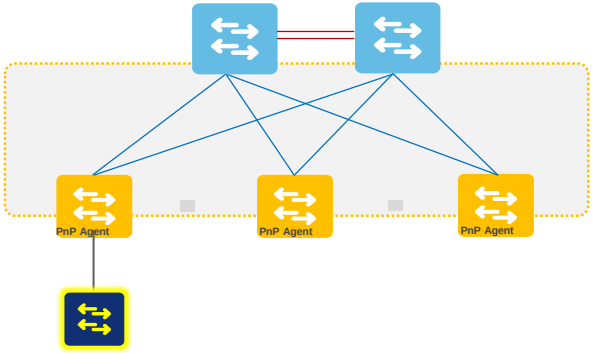
3 Step Process

IoT Ready Network

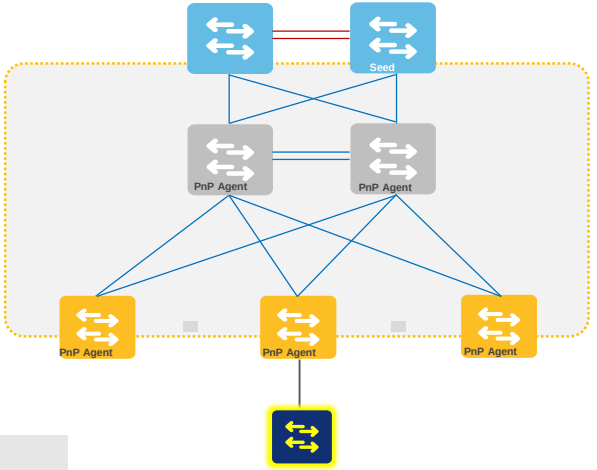
Plan – Network Design

Cisco DNA Center

2 Tier – Collapsed Core Design



3 Tier – Campus Design



Network Discovery

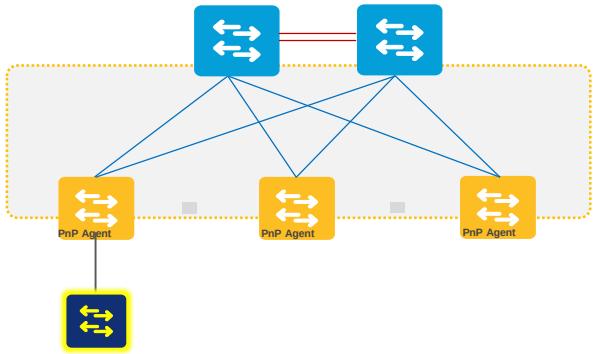
Dynamic and on-demand network discovery process

Fabric edge node programmed to on-board new Extended node switches with zero configurations

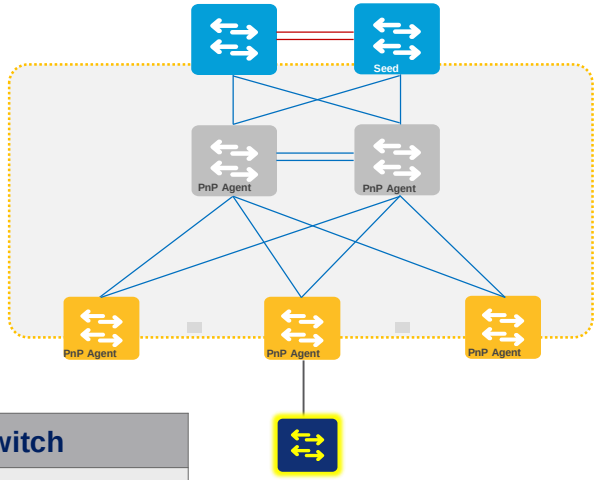
Plan – Catalyst Switch Role support

Cisco DNA Center

2 Tier – Collapsed Core Design

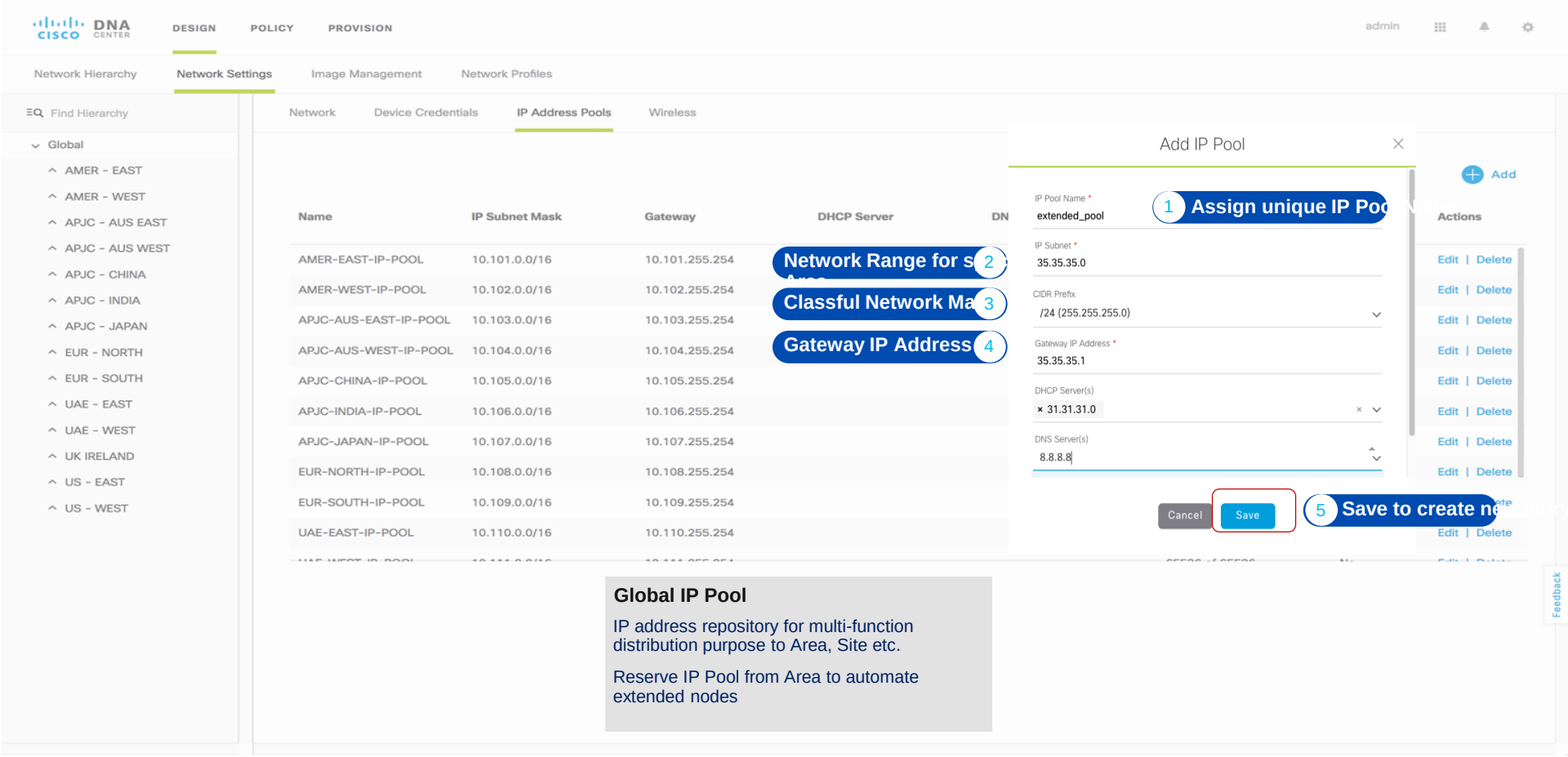


3 Tier – Campus Design



Layer	Role	Supported Switch
Fabric Edge	PnP Agent	Catalyst 9K
Extended Nodes		3560CX, CDB,IE4K/5K

Design – Configure Network Range for Extended Nodes

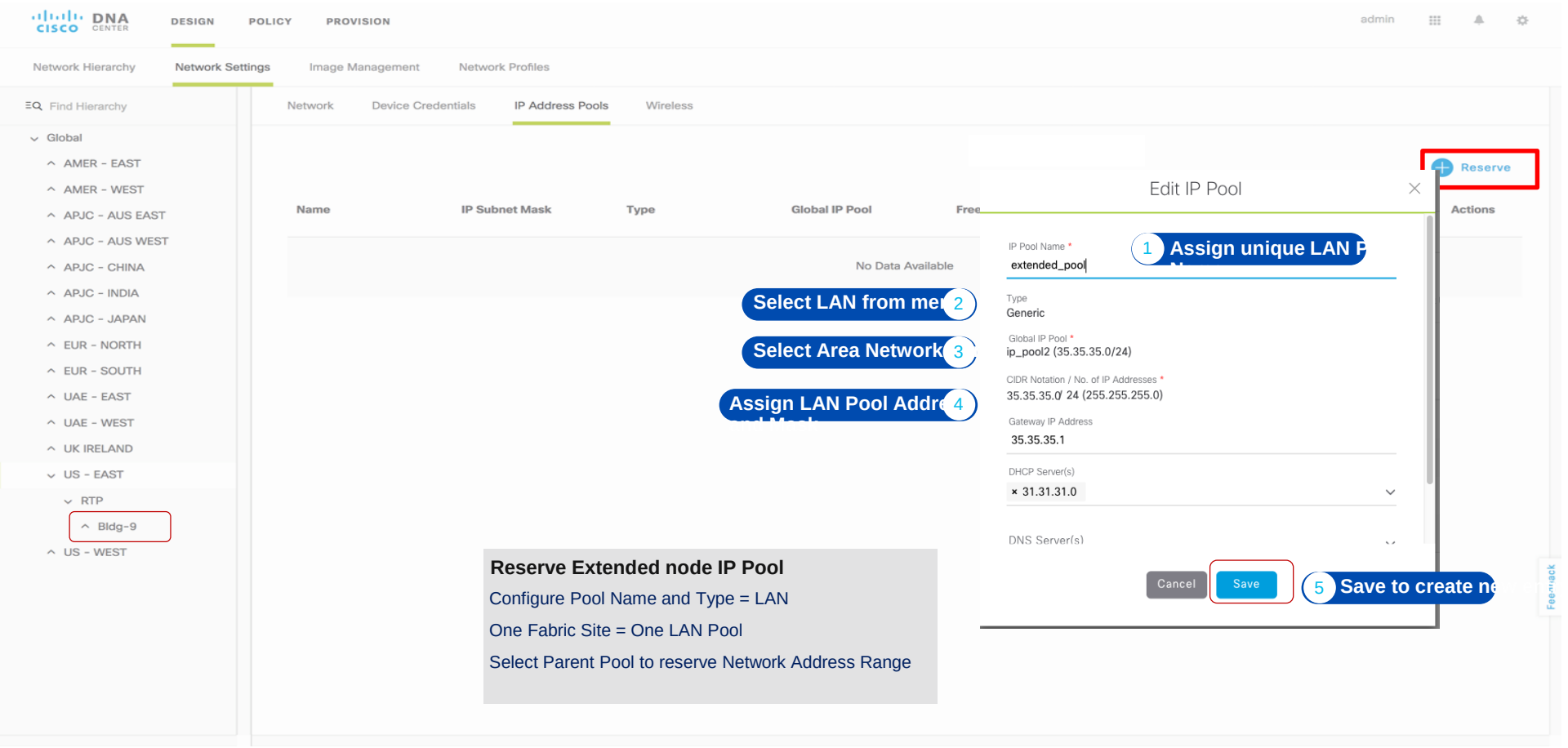


Global IP Pool

IP address repository for multi-function distribution purpose to Area, Site etc.

Reserve IP Pool from Area to automate extended nodes

Design – Configure Extended Node Pool at Site



Reserve Extended node IP Pool

Configure Pool Name and Type = LAN

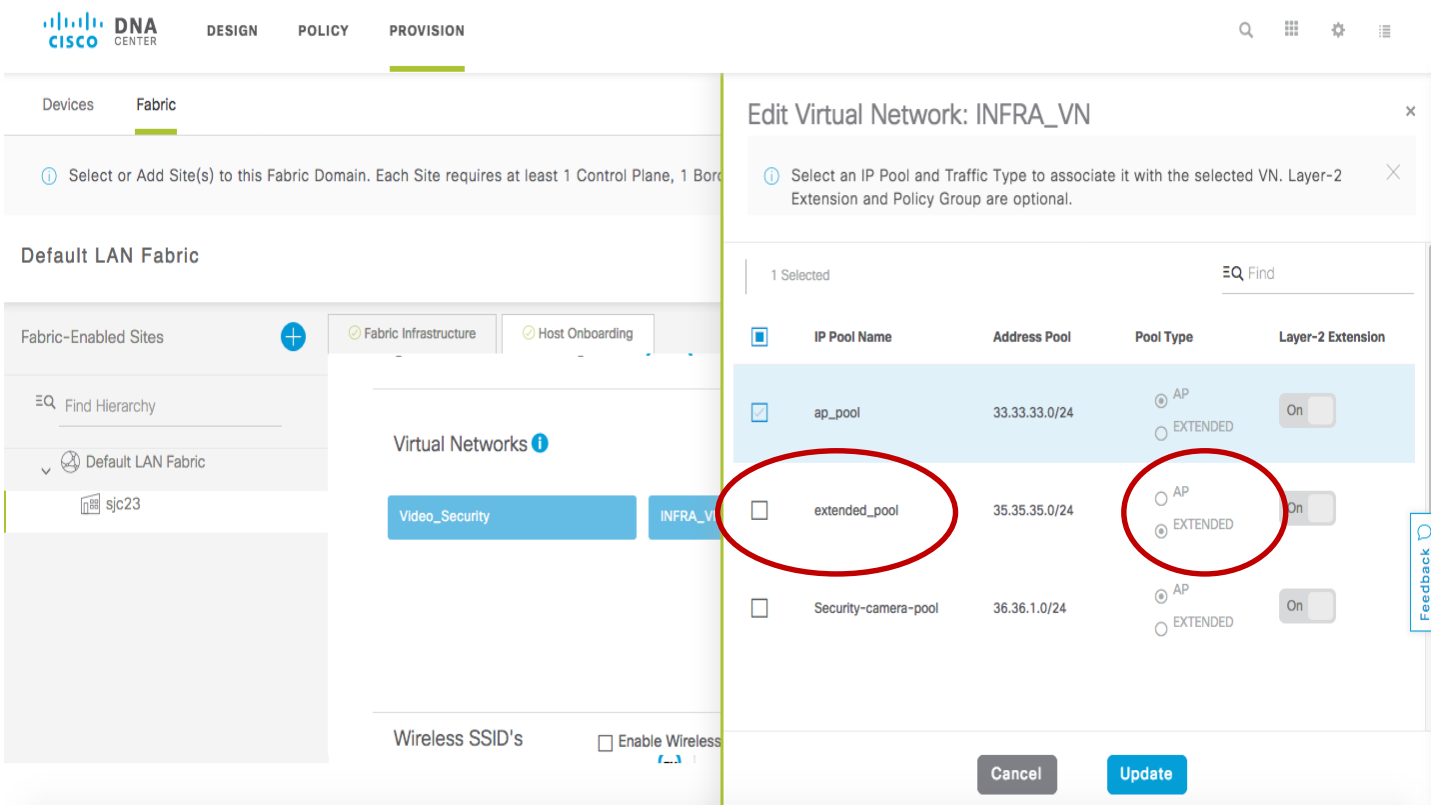
One Fabric Site = One LAN Pool

Select Parent Pool to reserve Network Address Range

SD-Access @ DNA Center

Enabling Fabric Extension (method 1)

* Automated provision of Extended nodes



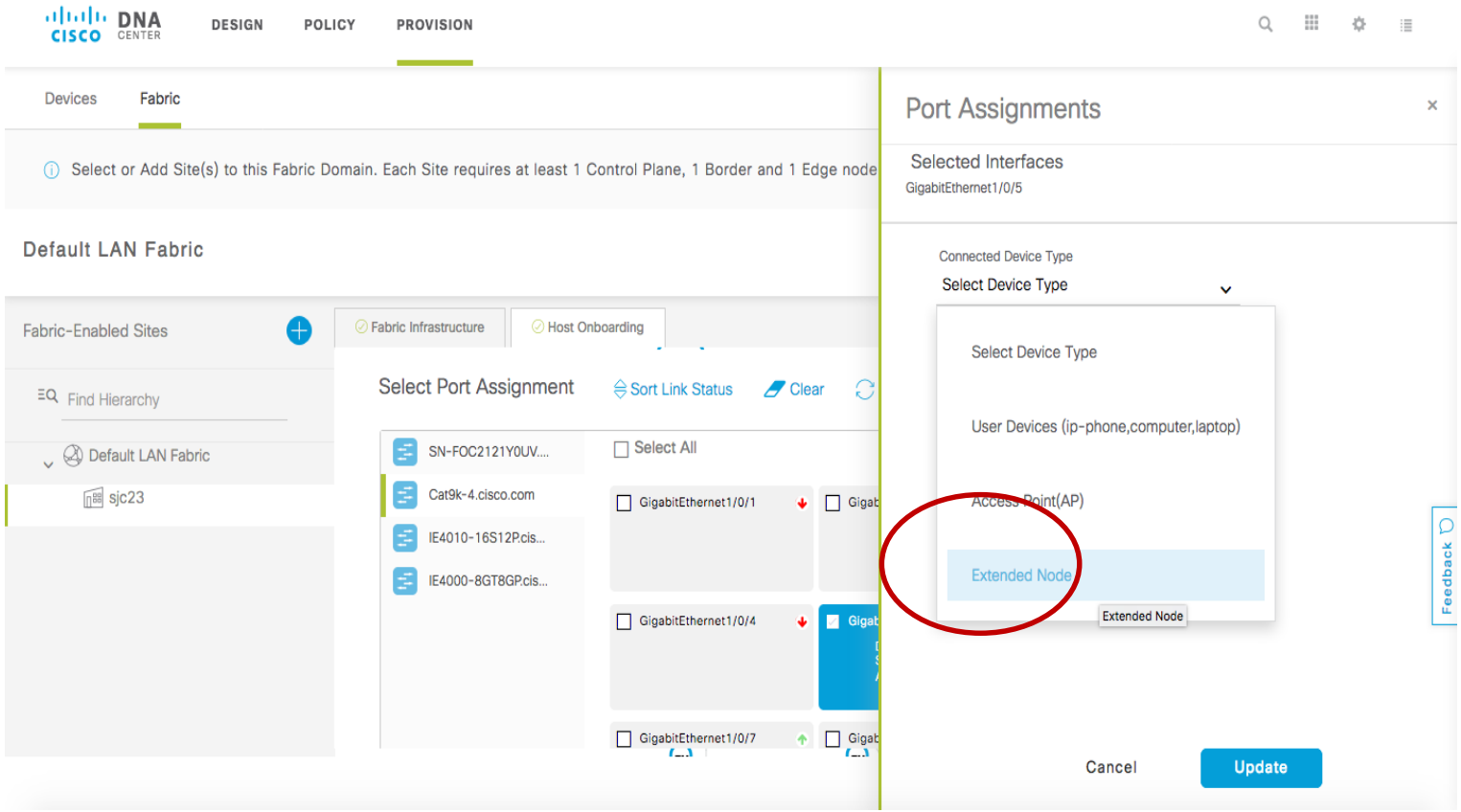
Select an IP Pool fro the INFRA_VN and enable it for Extended Nodes.

This will begin the automation process, to bring the new Extended Node into the Inventory.

SD-Access @ DNA Center

Enabling Fabric Extension (method 2)

* Static provision of Extended nodes



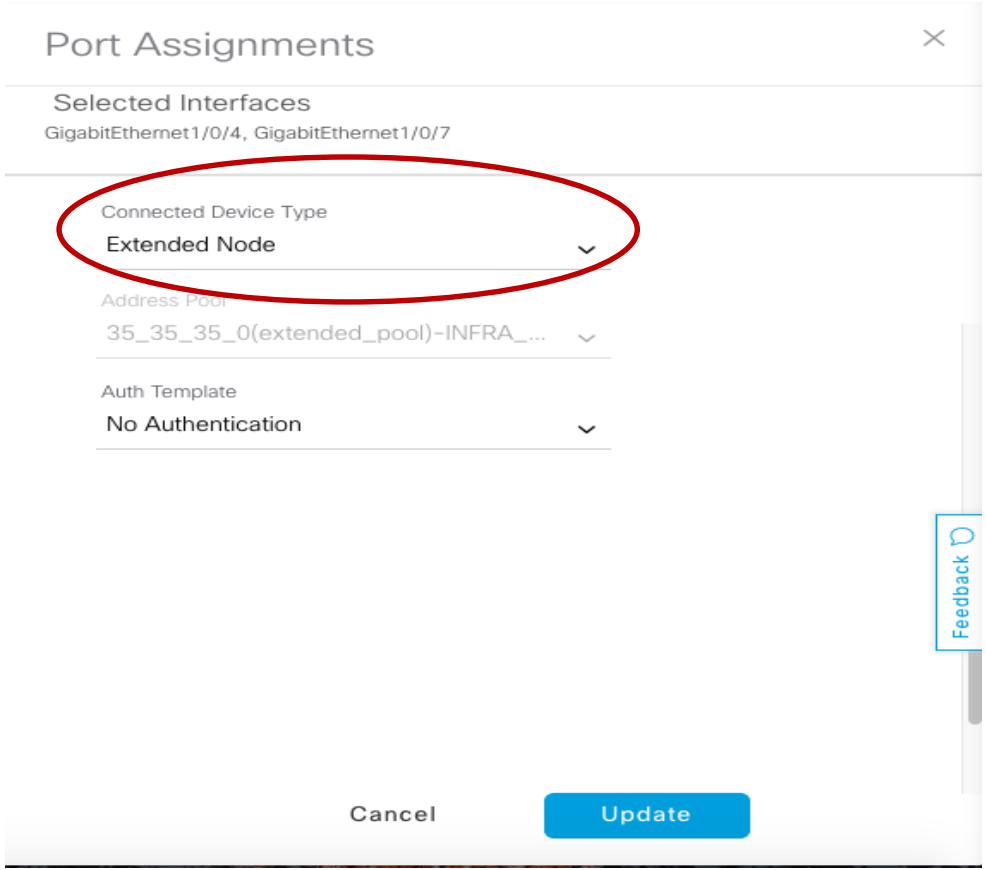
Select one or more interface(s) on the Edge node and enable it for Extended Node.

This will begin the discovery and automation process, to bring the new Extended Node into the Inventory.

SD-Access @ DNA Center

Enabling Fabric Extension (method 2)

* Static provision of Extended nodes



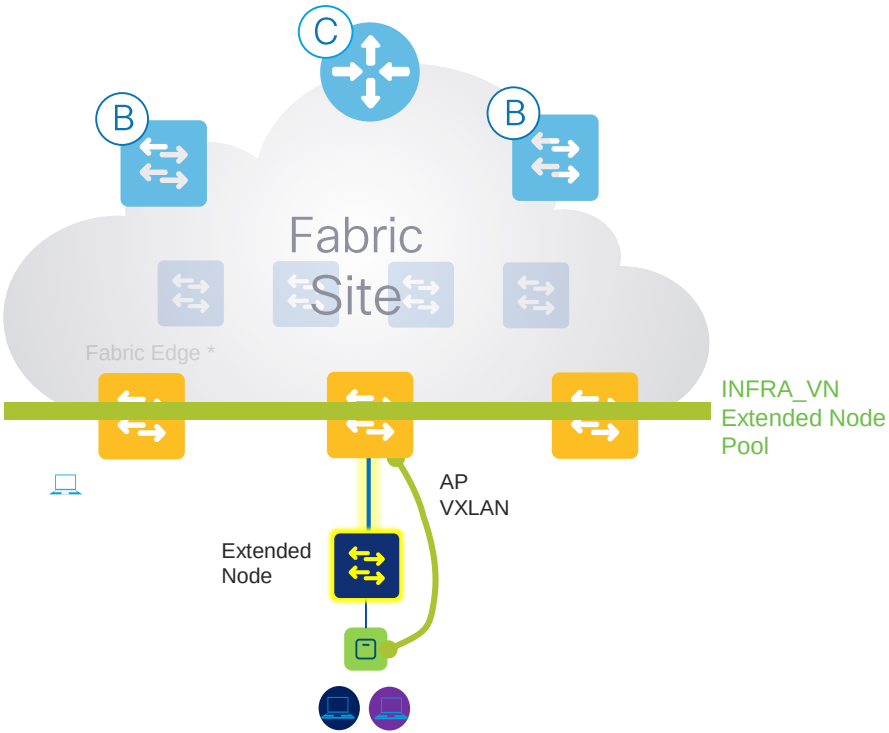
NOTE: Mockup only, subject to change.

Select one or more interface(s) on the Edge node and enable it for Extended Node.

This will begin the discovery and automation process, to bring the new Extended Node into the Inventory.

What Happens Underneath?

Extended node Deployment Details

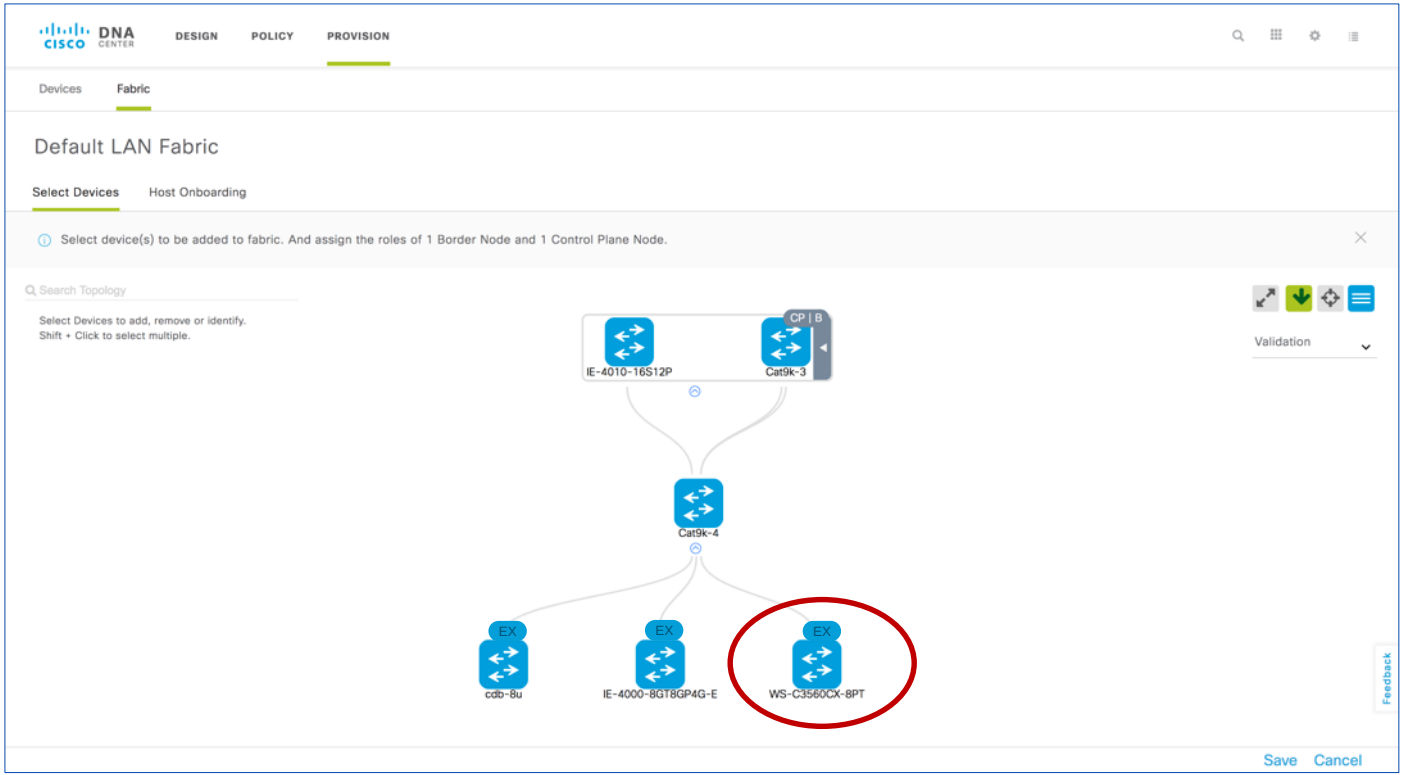


- The User and Management IP Subnets/VLAN's range for the Extended nodes are picked from the Selected IP Pools/(VLANs).
- Every Extended node will have one Management IP Pool, which is provisioned in the INFRA_VN and registered with the Control Plane.
- The Extended nodes connected to the Fabric Edge nodes are automatically detected by a MACRO running on the edge nodes.
- The MACRO detects the extended nodes and kick starts the PNP process and on boards the extended nodes into DNAC.
- The Border will advertise the IP Pool for Extended nodes to the external world as with other IP Pools.

SD-Access @ DNA Center

Fabric Extension Automation

NOTE: Mockup only, subject to change.

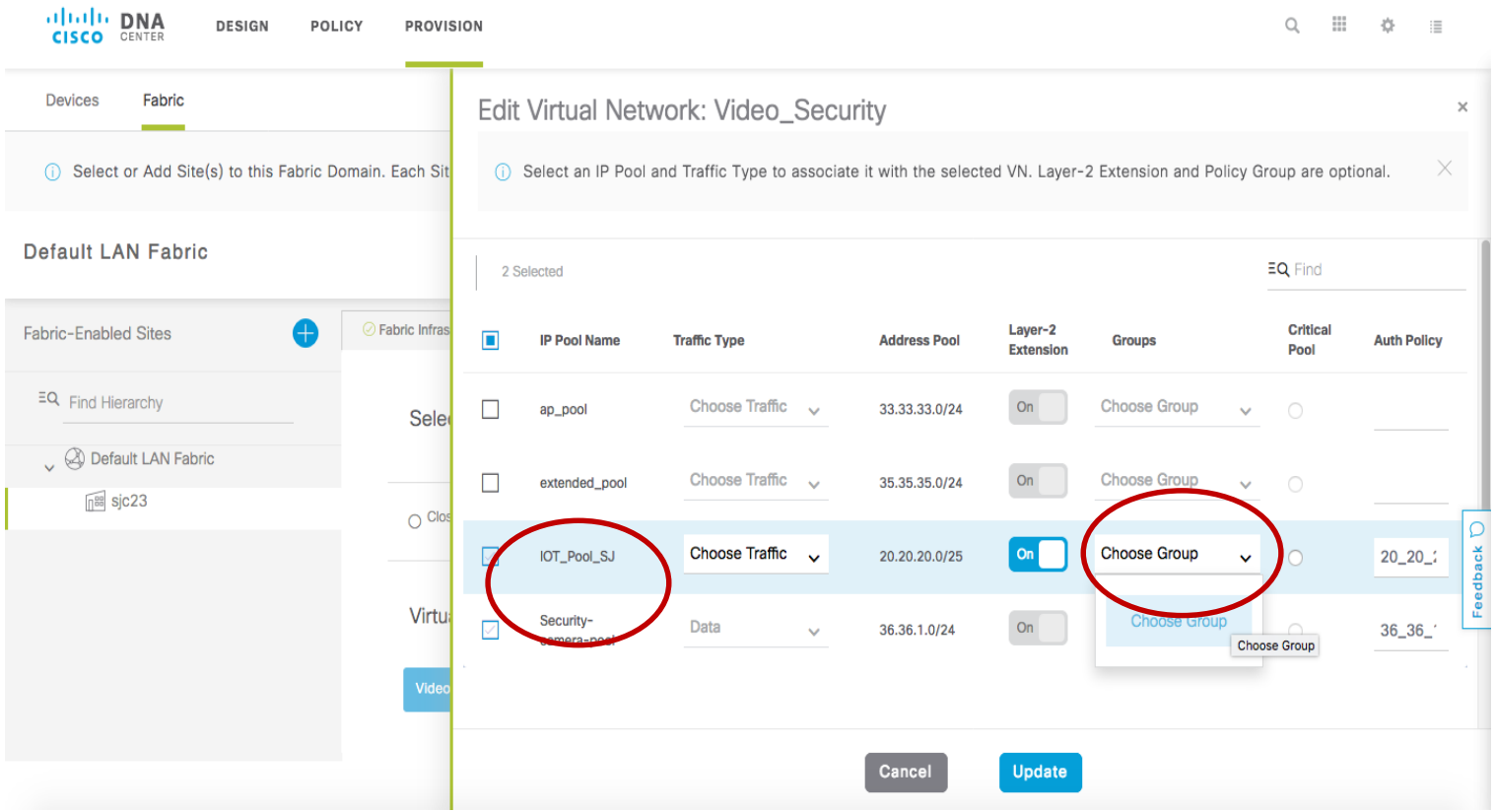


DNA Center will then automatically discover and automate the setup process

After the discovery and automation is complete, the new Extended node will appear in the Fabric topology with a tag indicating that it is an Extended Node

SD-Access @ DNA Center

Fabric Extension Automation

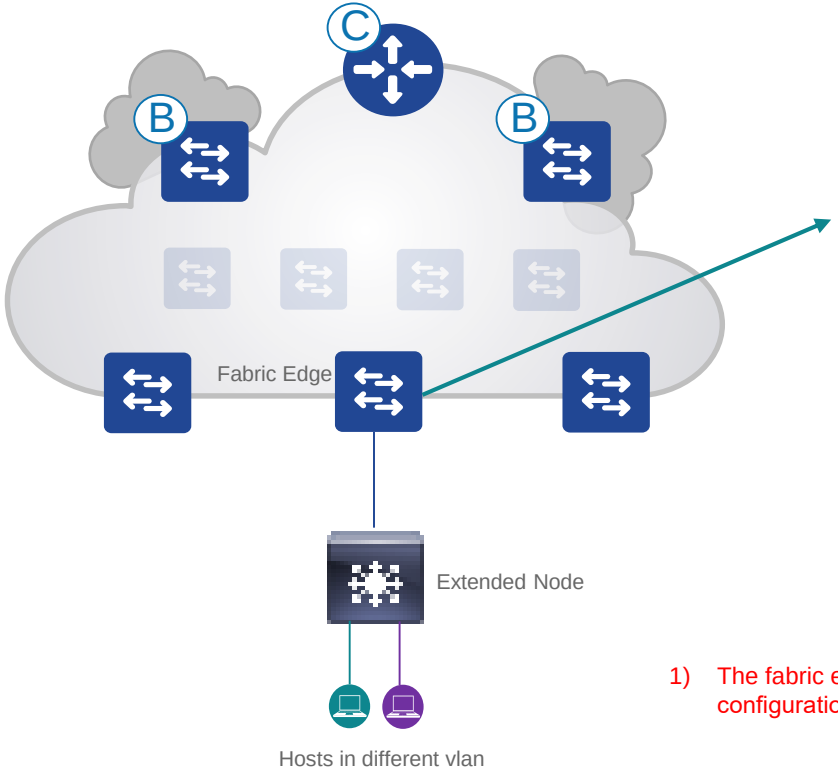


Select an IP_Pool for host end points that will connect to the extended nodes.

An Associated security group tag is also chosen for that IP subnet to enforce policy as needed

Single/Multi vlan Connecting to single fabric edge node

Static Configuration- Configuration

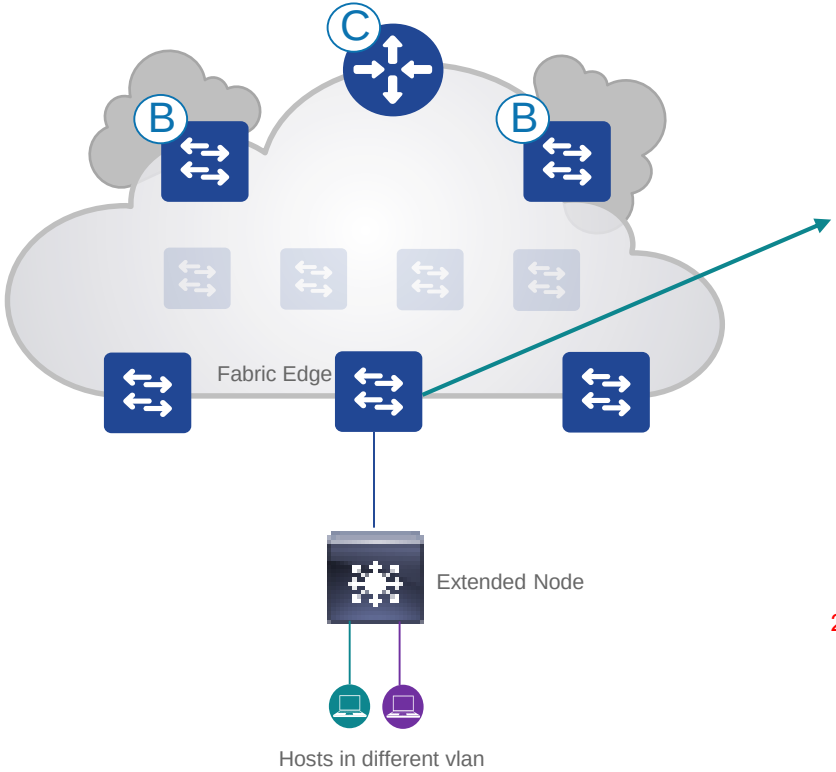



```
interface Vlan3001
 description ”User Subnet for Extended nodes"
 ip vrf forwarding Users_1
 ip address 20.20.20.254 255.255.255.0
 ip helper-address 1.1.1.1
 no ip redirects
 ip local-proxy-arp
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility eid_20_20_20_0
!
interface Vlan3002
 description ”User Subnet for Extended nodes"
 ip vrf forwarding Users_2
 ip address 20.20.21.254 255.255.255.0
 ip helper-address 1.1.1.1
 no ip redirects
 ip local-proxy-arp
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility eid_20_20_21_0
```

1) The fabric edge should be configured with the IP subnets and the associated SVI and fabric configuration that will be used for the hosts/users on the Extended nodes (cont’d from earlier slide)

Single/Multi vlan Connecting to single fabric edge node

Static Configuration- Configuration

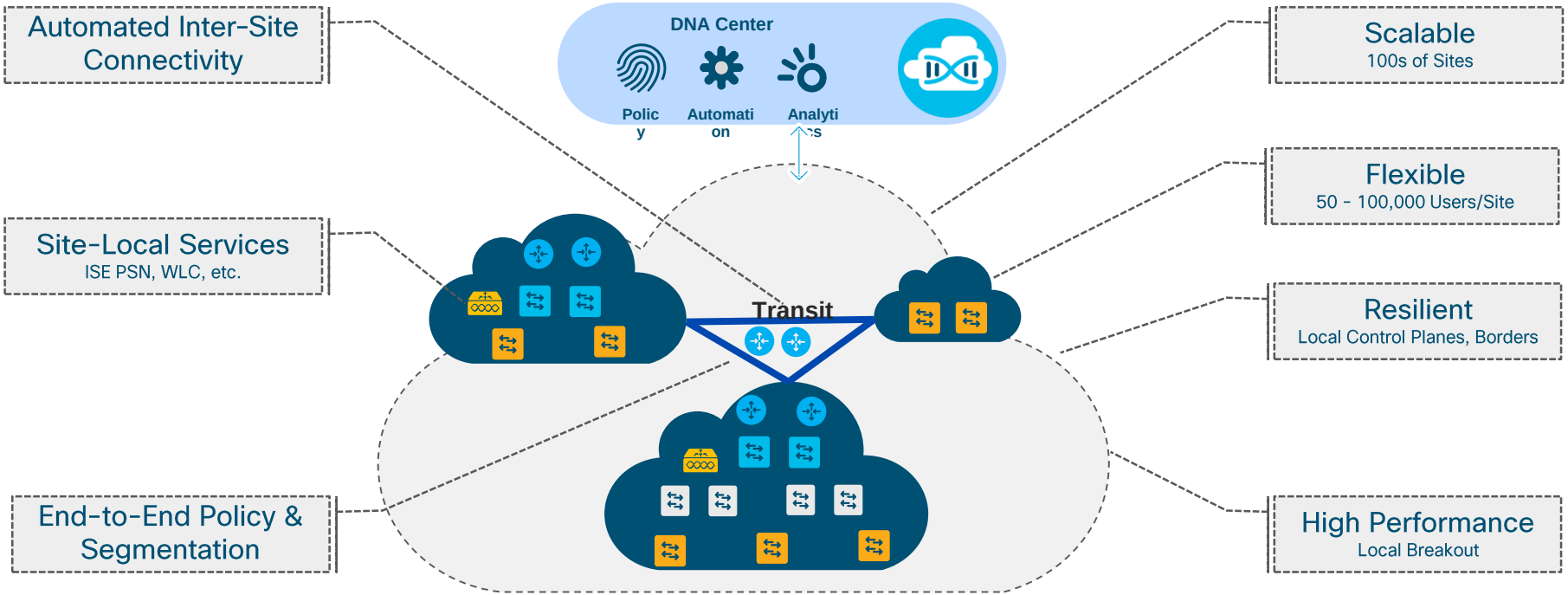



```
interface GigabitEthernet1/0/6
 description "Connecting to Extended Switch 3560-CX"
 switchport mode trunk
 macro description CISCO_SWITCH_EVENT
 !
cts role-based sgt-map vlan-list 3001 sgt 8   < map an vlan to an SGT value>
cts role-based sgt-map vlan-list 3002 sgt 9   < map an vlan to an SGT value>
!
```

2) Configure the fabric edge downstream port as trunk port and map the vlan's to an SGT value

SD-Access for Distributed Campus

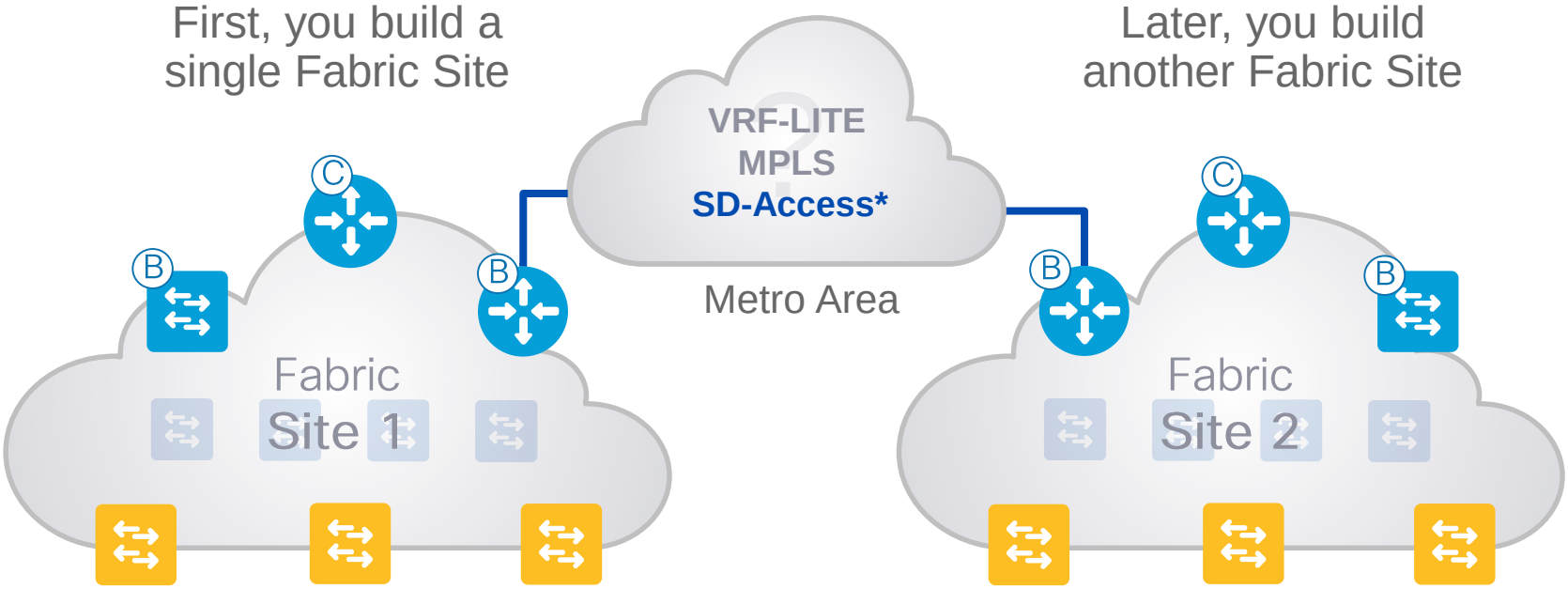
SD-Access for Distributed Campus



Fabric Sites & Domains

Connecting Multiple Fabrics

* Beta in SDA 1.2



How do you connect them together?

Beta in SDA 1.2.1

SD-Access Distributed campus

Fabric Border Support Matrix

SDA Border Node	SD-Access Distributed campus (SD-Access Transit)	SD-Access Distributed Campus (IP Transit)
C9K	YES	YES
ASR1K/ISR4K	YES	YES
C6K	No	YES
N7K	NO	YES

Beta in SDA 1.2.1

SD-Access for Distributed Campus

Fabric Sites and Domains

A **Fabric Site** is an independent fabric area of a with a unique set of network devices: Control Plane, Border, Edge, WLC, ISE PSN

Different levels of redundancy and scale can be designed per Site by including local resources: DHCP, AAA, DNS, Internet, etc.

A Fabric Site may cover a single **physical location**, **multiple locations**, or just a **subset of a location**

- Single Location ➔ Branch, Campus or Metro Campus
- Multiple Locations ➔ Metro Campus + Multiple Branches
- Subset of a Location ➔ Building or Area within a Campus

Beta in SDA 1.2.1

SD-Access for Distributed Campus

Fabric Sites and Domains

A **Fabric Domain** may consist of one or more Fabric Sites + Transit

Multiple Fabric Sites are connected to each other using a **Transit Site**

There are two types of Transit:

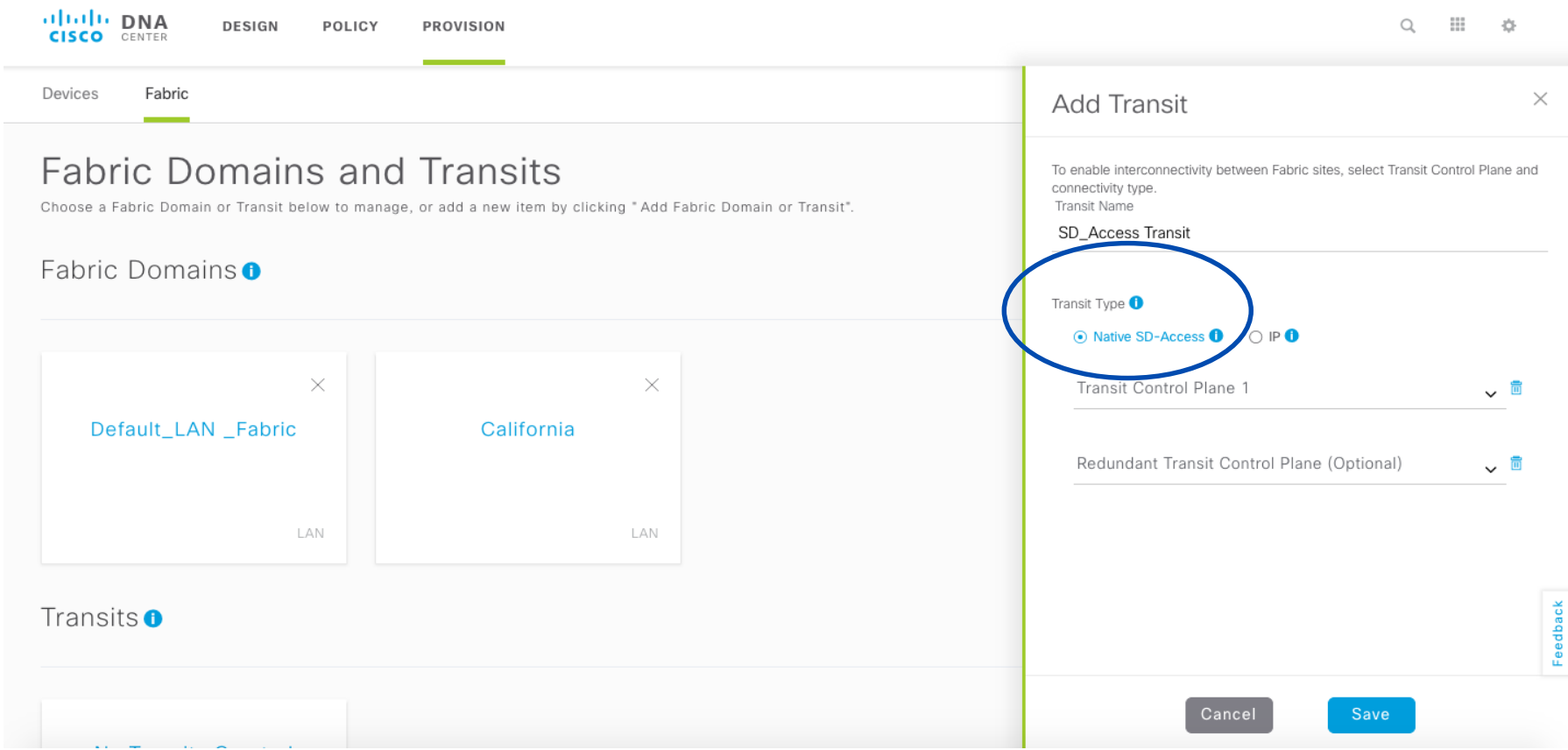
- **SD-Access Transit** - Enables a native SD-Access (LISP,VXLAN,CTS) fabric, with a domain-wide Control Plane node for inter-site communication

- **IP-Based Transit** - Leverages a traditional IP-based (VRF-LITE, MPLS) network, which requires remapping of VRFs and SGTs between sites

SD-Access for Distributed Campus

SD-Access Transit

Beta in SDA 1.2.1

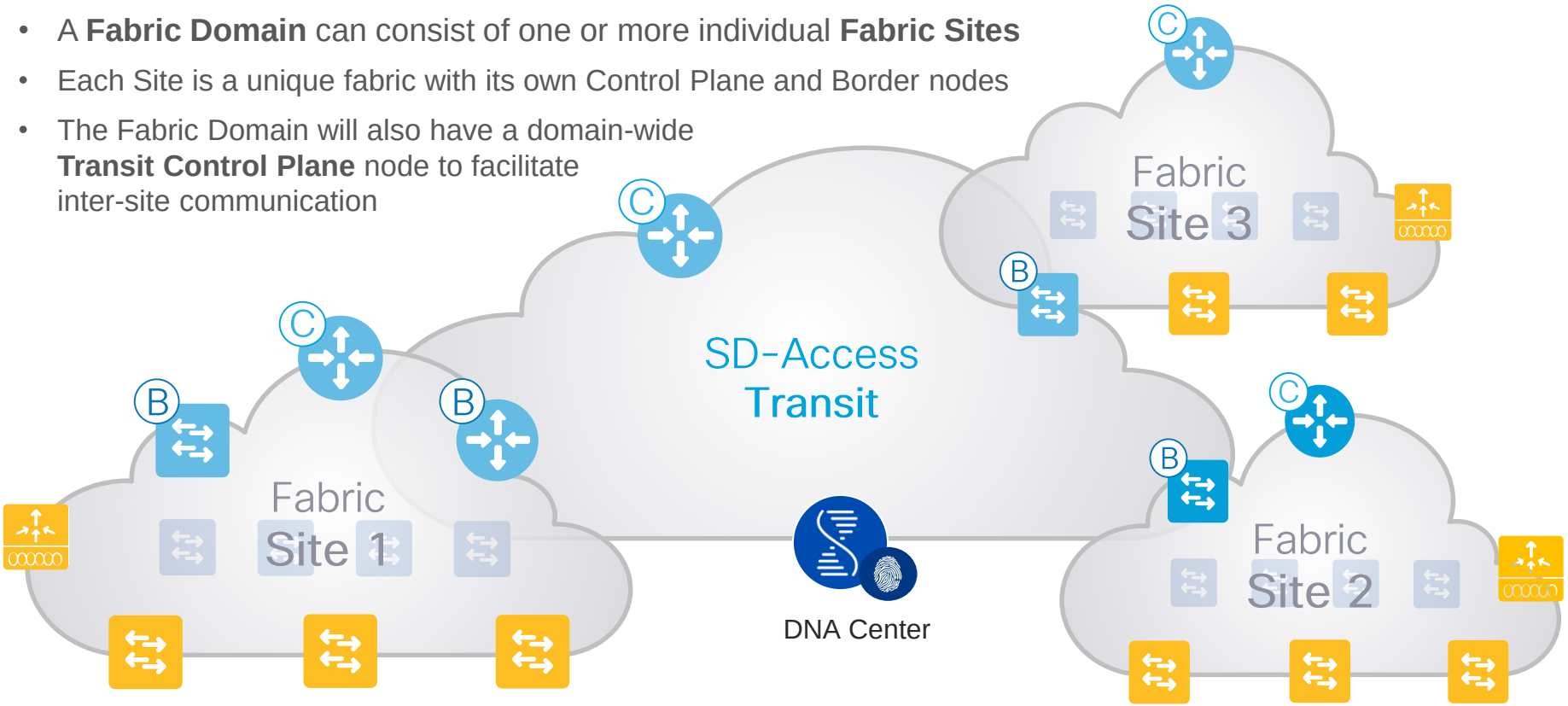


SD-Access for Distributed Campus

SD-Access Transit

Beta in SDA 1.2.1

- A **Fabric Domain** can consist of one or more individual **Fabric Sites**
- Each Site is a unique fabric with its own Control Plane and Border nodes
- The Fabric Domain will also have a domain-wide **Transit Control Plane** node to facilitate inter-site communication

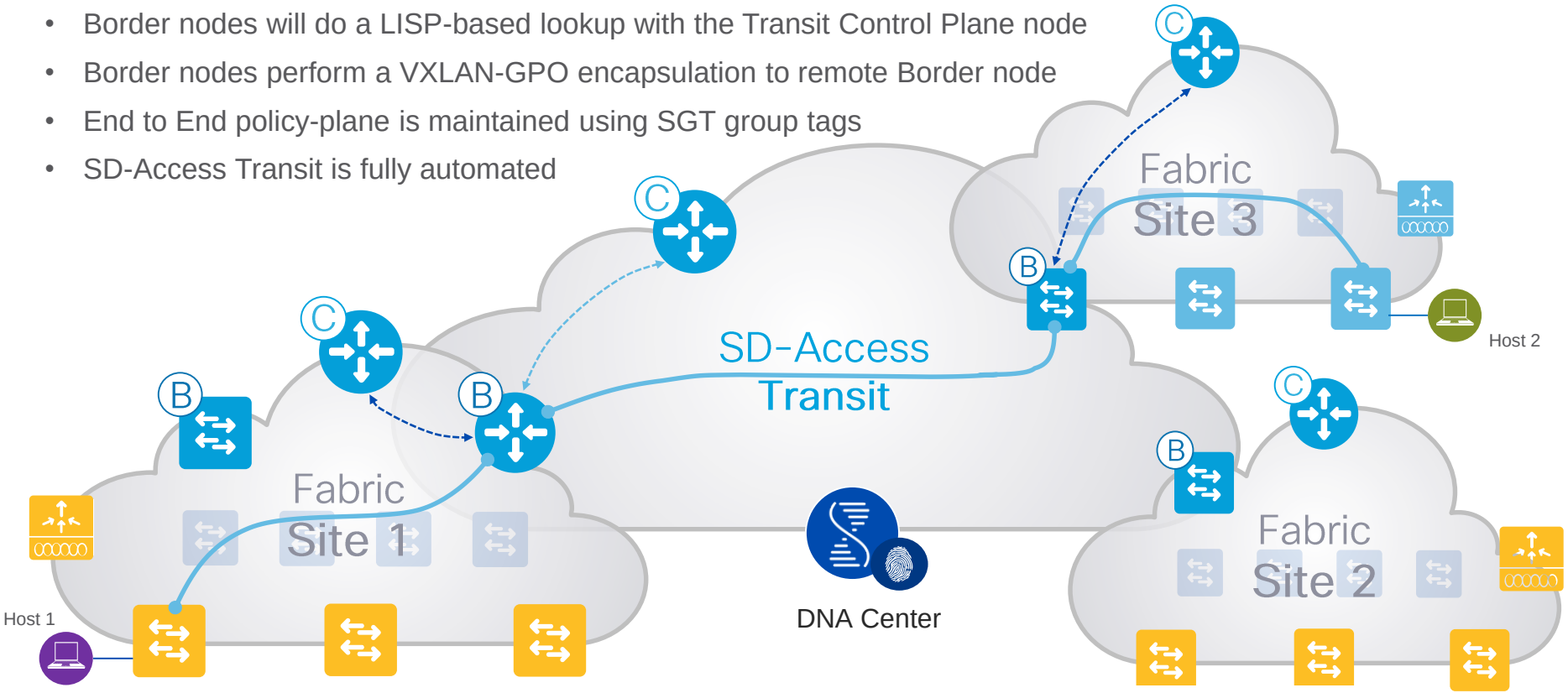


SD-Access for Distributed Campus

SD-Access Transit

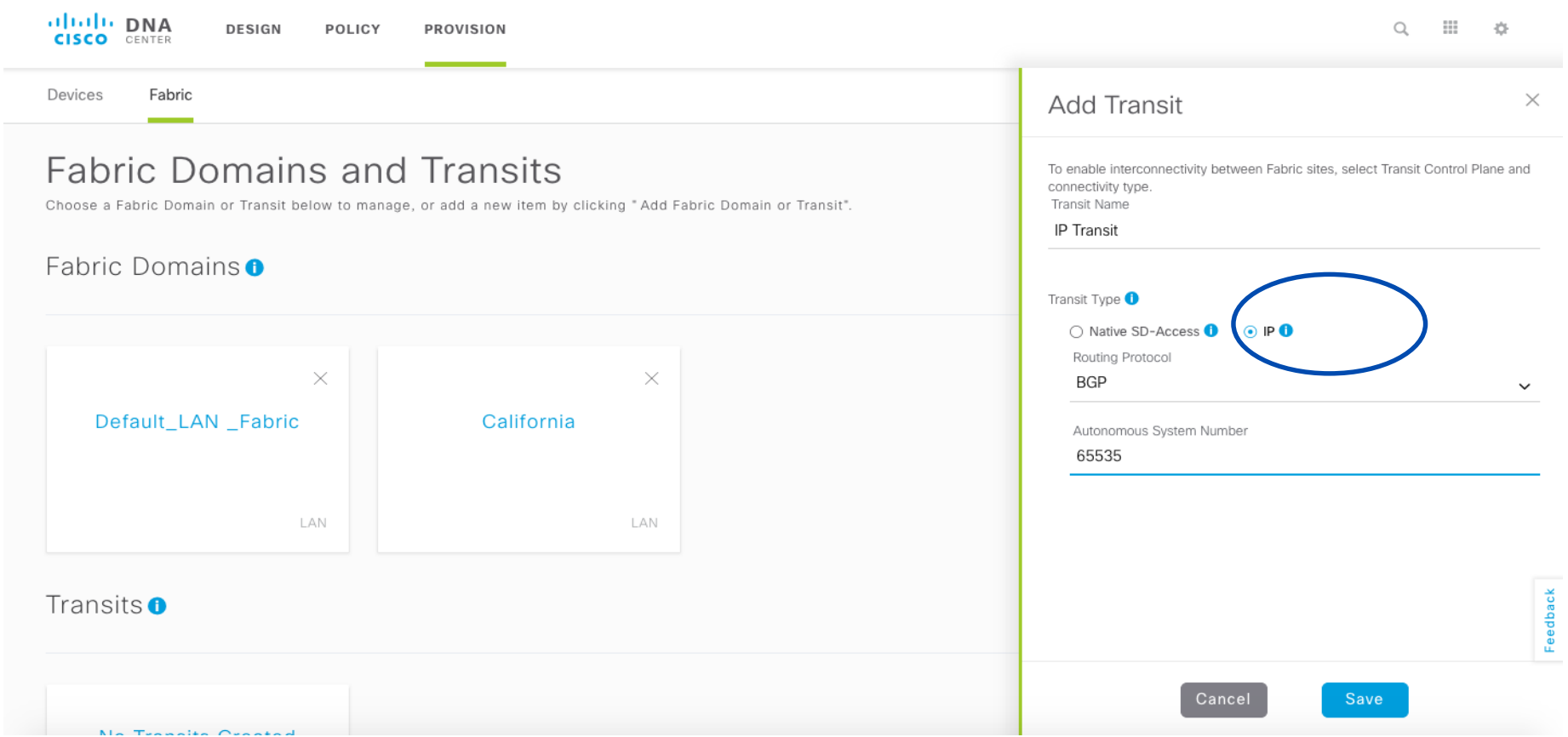
Beta in SDA 1.2.1

- Border nodes will do a LISP-based lookup with the Transit Control Plane node
- Border nodes perform a VXLAN-GPO encapsulation to remote Border node
- End to End policy-plane is maintained using SGT group tags
- SD-Access Transit is fully automated



SD-Access for Distributed Campus

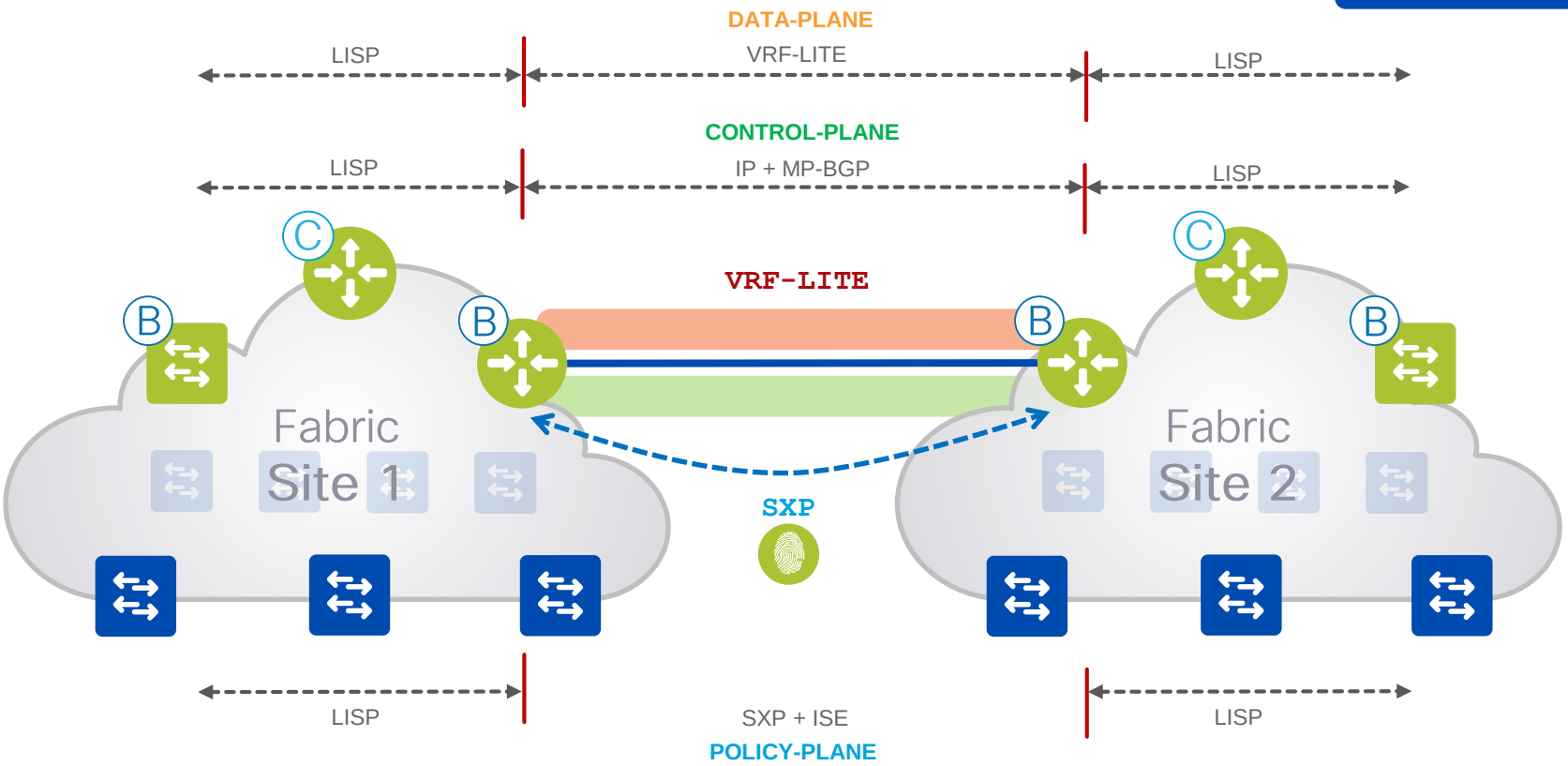
IP based Transit



Inter-Connecting Fabric Sites

Multiple Fabric Domains with VRF-LITE Transit

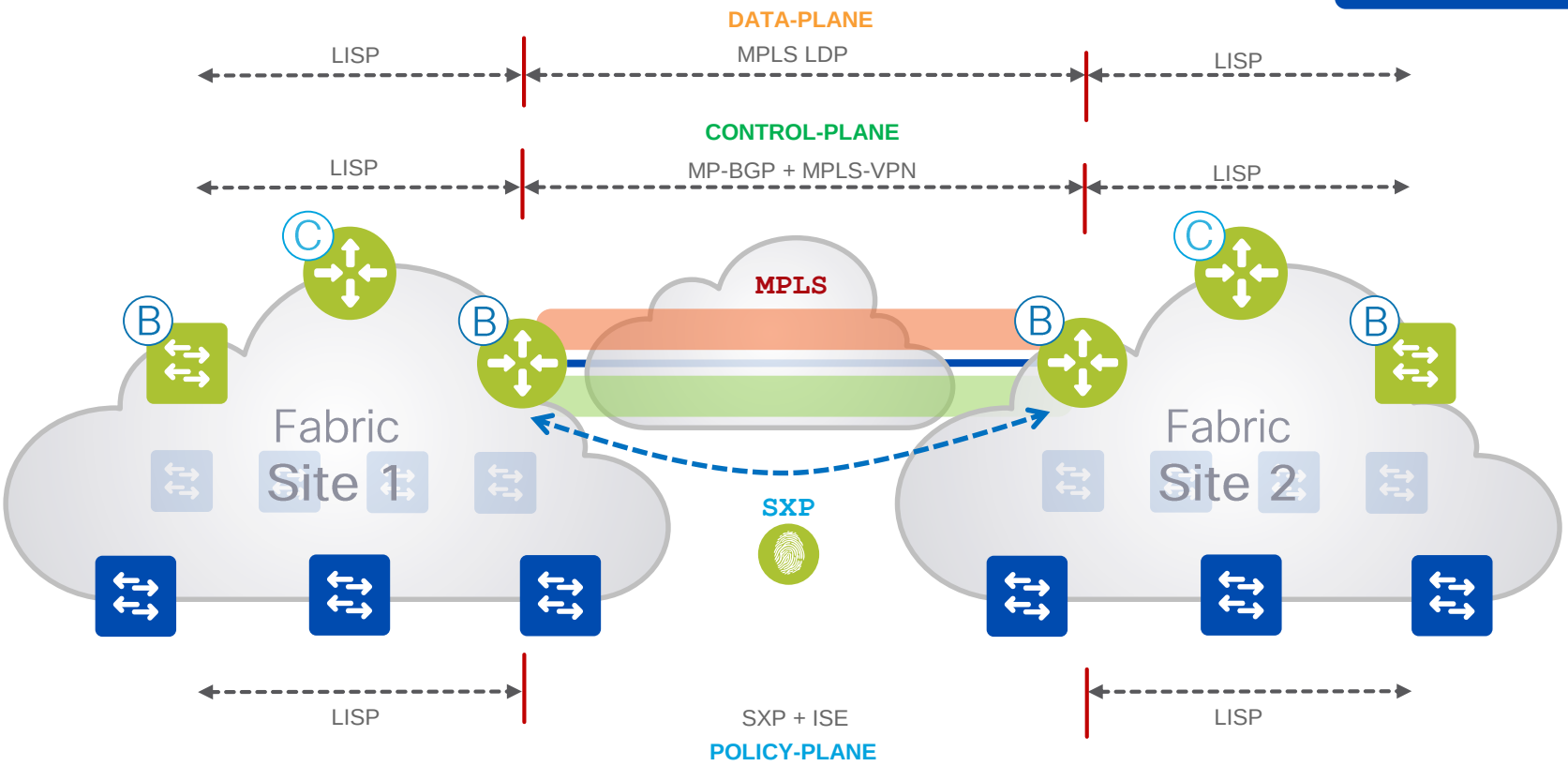
SDA 1.0 - 1.1



Inter-Connecting Fabric Sites

Multiple Fabric Domains with MPLS Transit

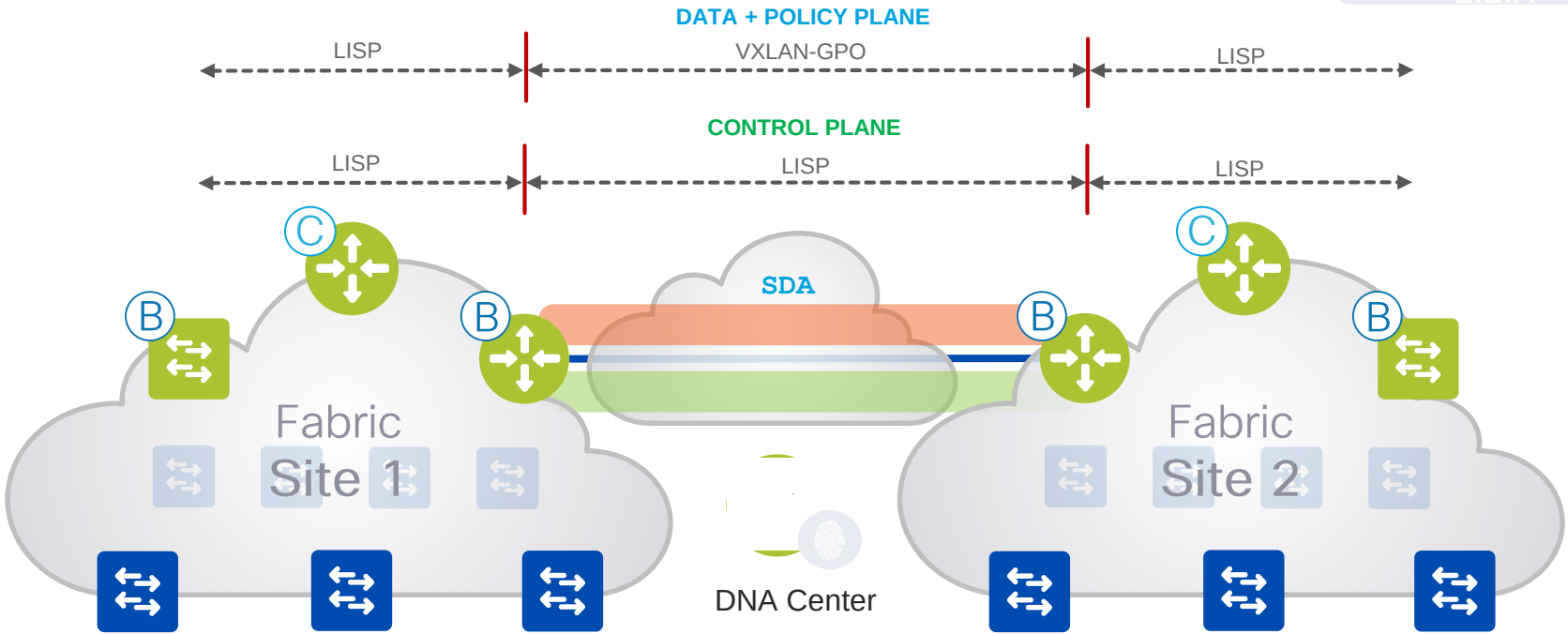
SDA 1.0 - 1.1



Inter-Connecting Fabric Sites

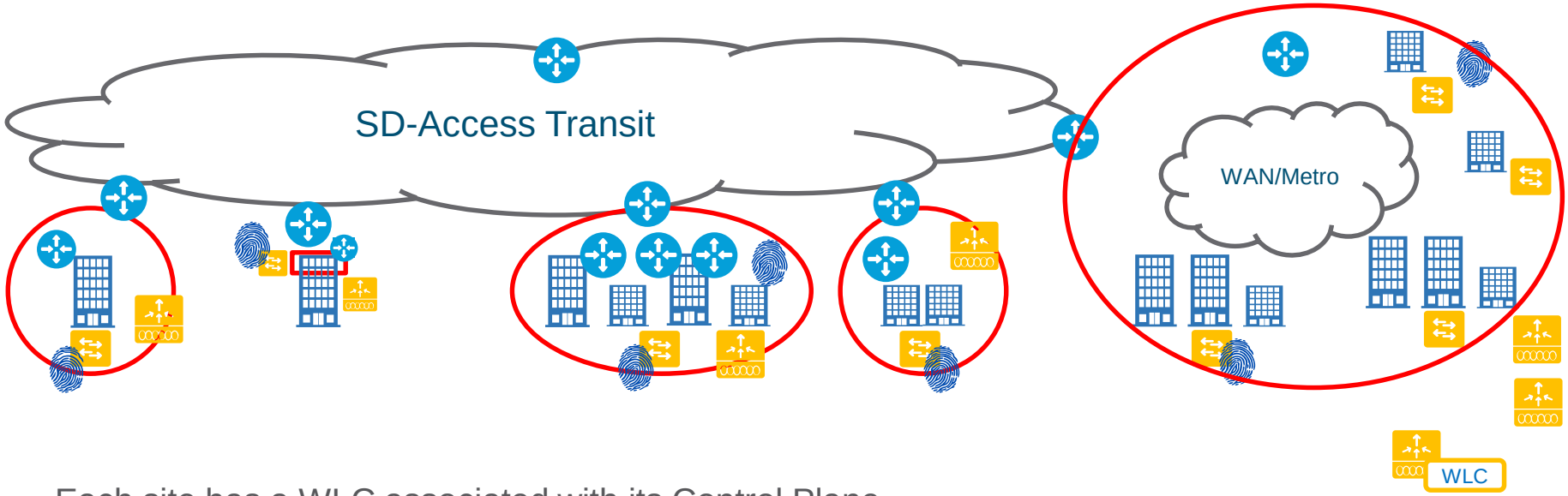
Multiple Fabric Domains with Native SDA Transit

New in SDA 1.2.X



SD-Access Distributed Campus Deployment Models

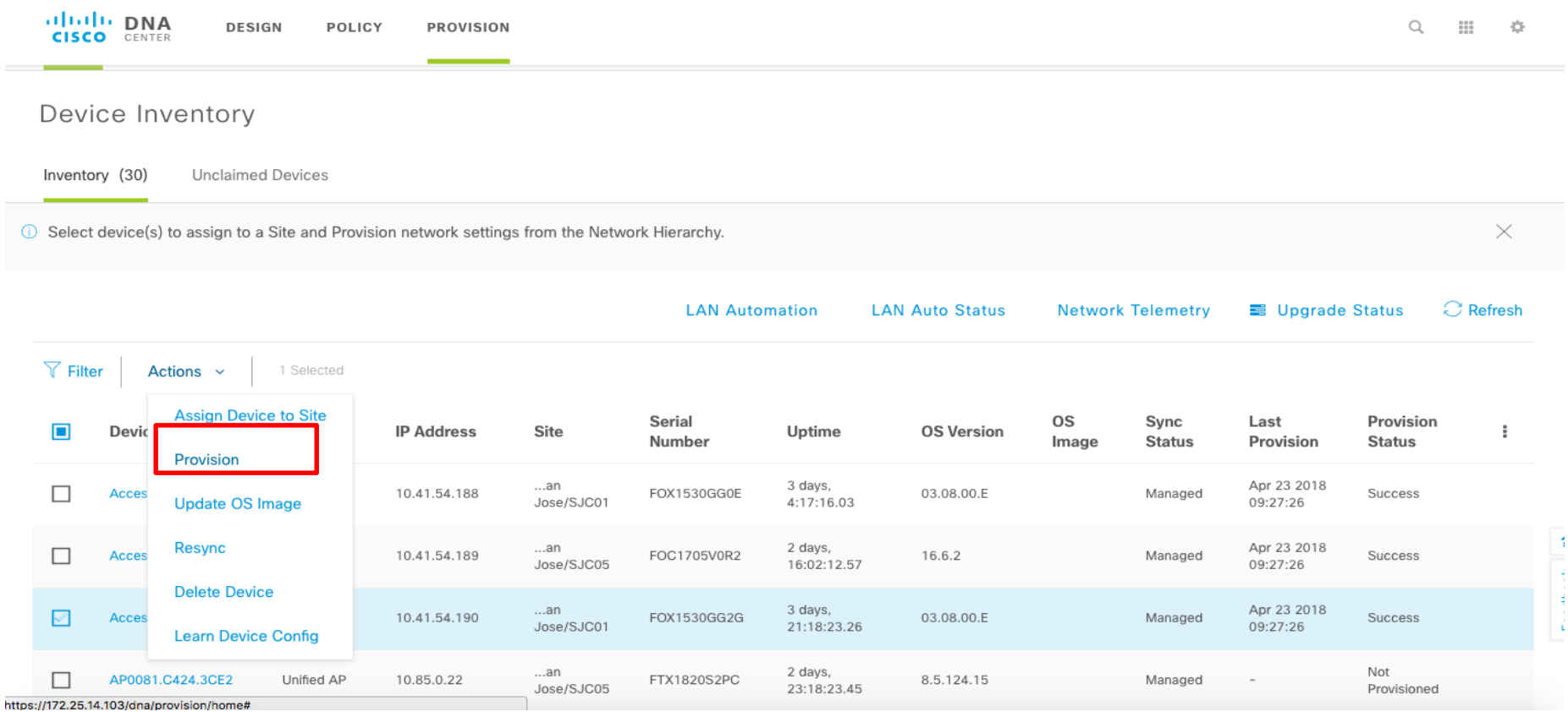
SD-Access for Distributed Campus- Wireless



- Each site has a WLC associated with its Control Plane
- Smaller locations in the same metro site may share a WLC

Host On-Boarding Enhancements

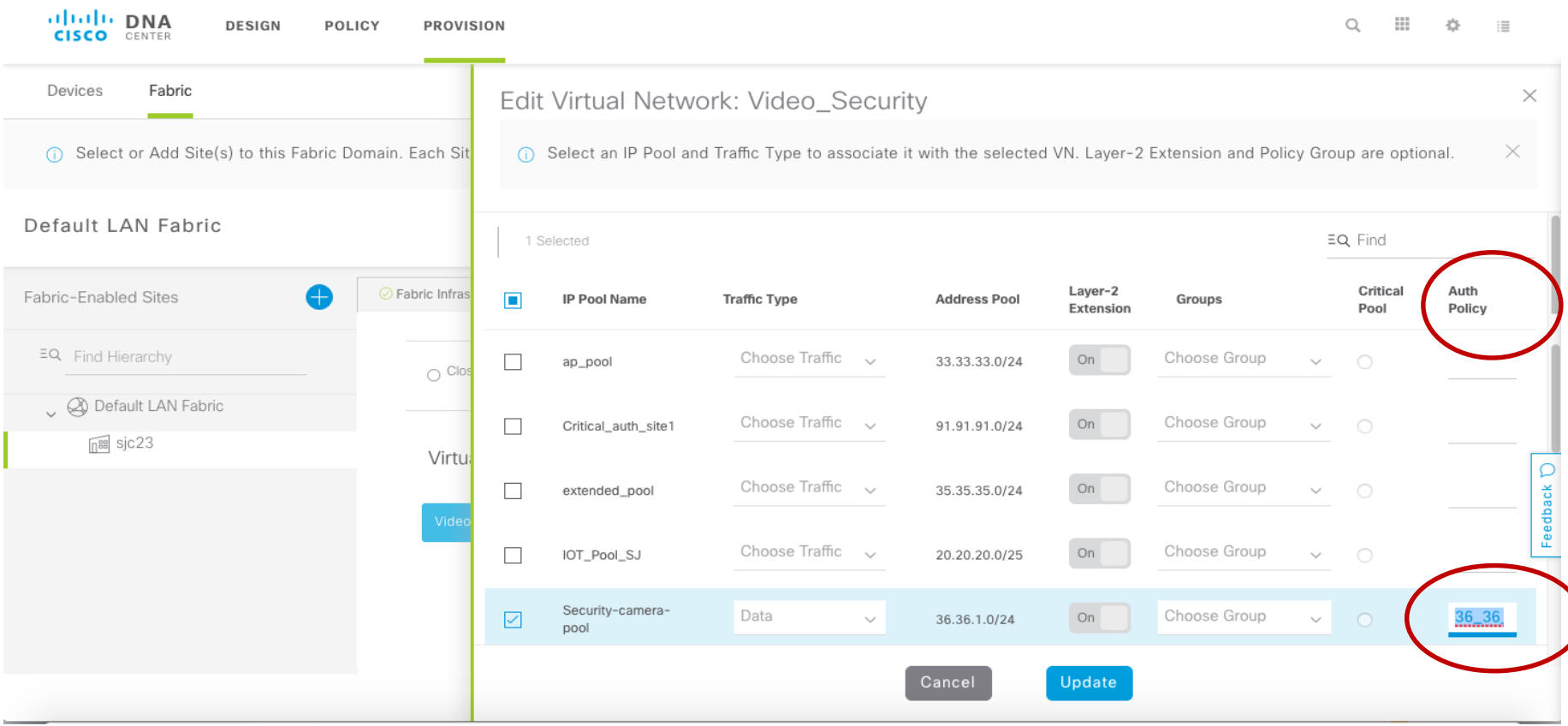
IBNS 1.0 to IBS 2.0 Migration (Manually Triggered)



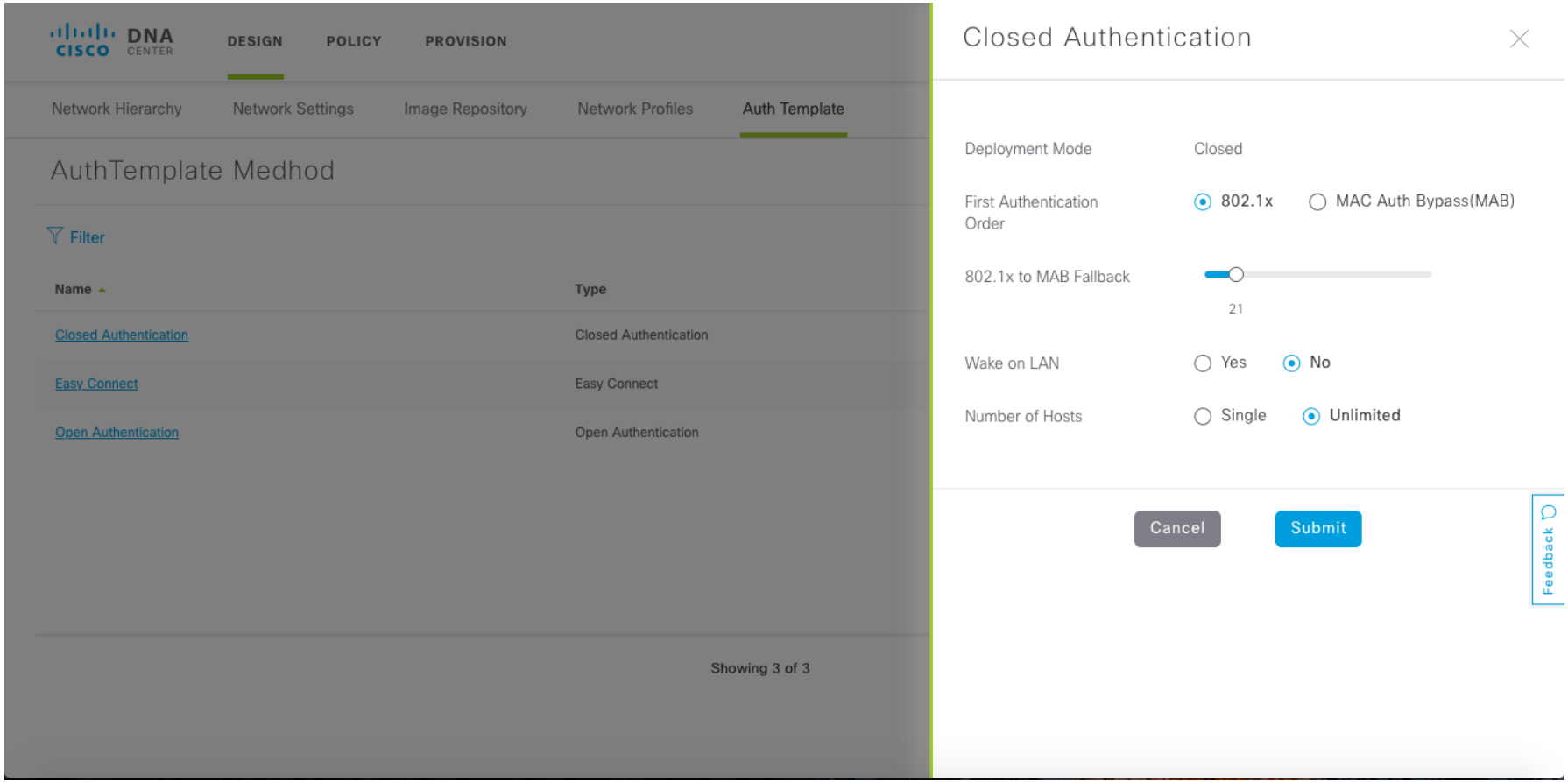
DNAC 1.2 Host On-boarding Enhancements

- Authentication template customization
- AAA server failure handling (Critical Auth Vlan)
- Low Impact Mode for Easy Connect
- Device Sensor for ISE Profiling (June Patch)
- Authorization vlan(IP subnet) name customization

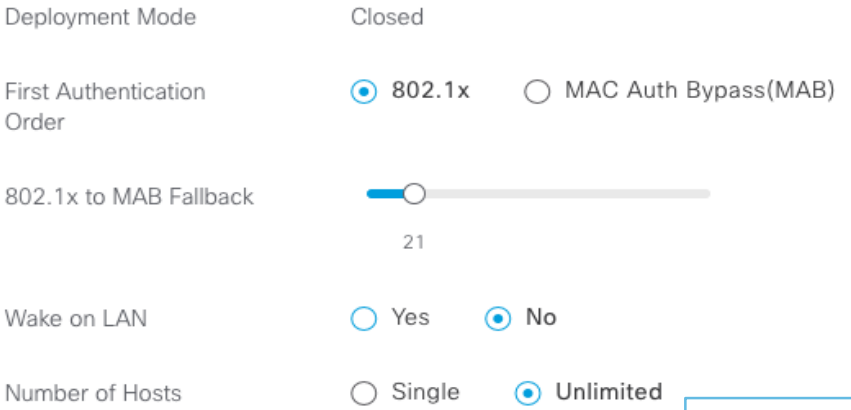
Authorization vlan(IP subnet) name customization



Authentication Template ‘Edit’ options



Customization: Authentication order



This is why we need ‘2’ policies per auth template.

Authentication priority must always be 802.1X

For authentication order 802.1X, MAB:

```
template DefaultWiredDot1xClosedAuth
service-policy type control subscriber DefaultWiredDot1xClosedAuth_1X_MAB
```

For authentication order MAB, 802.1X:

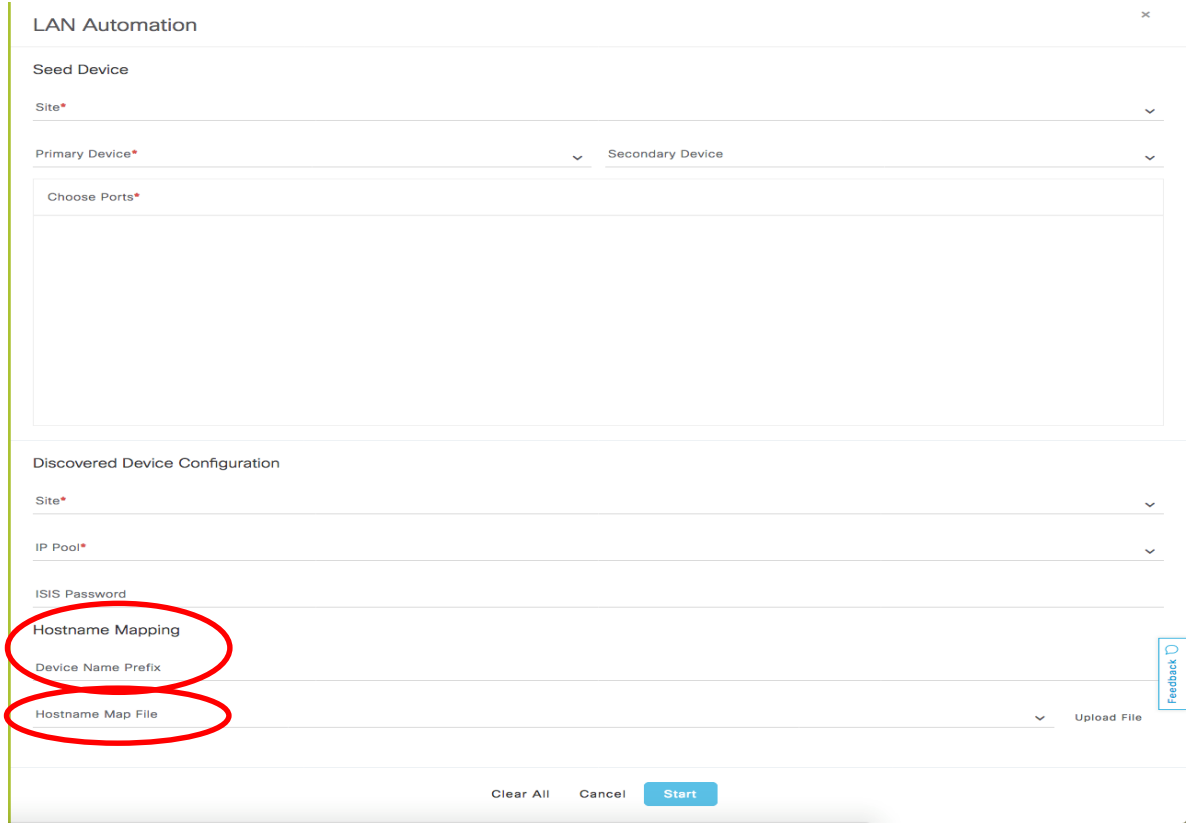
```
template DefaultWiredDot1xClosedAuth
service-policy type control subscriber DefaultWiredDot1xClosedAuth_MAB_1X
```

Lan Automation Enhancements

DNAC 1.2 Lan Automation Enhancements

- Configurable IS-IS domain password
- Configurable device host name
- Re-use the same seed device to run underlay on multiple sites
- LAN Automation page re-design (UI changes only on functionality changes)
- LAN Automation Status page re-design (UI changes only on functionality changes)

Configurable Device host name



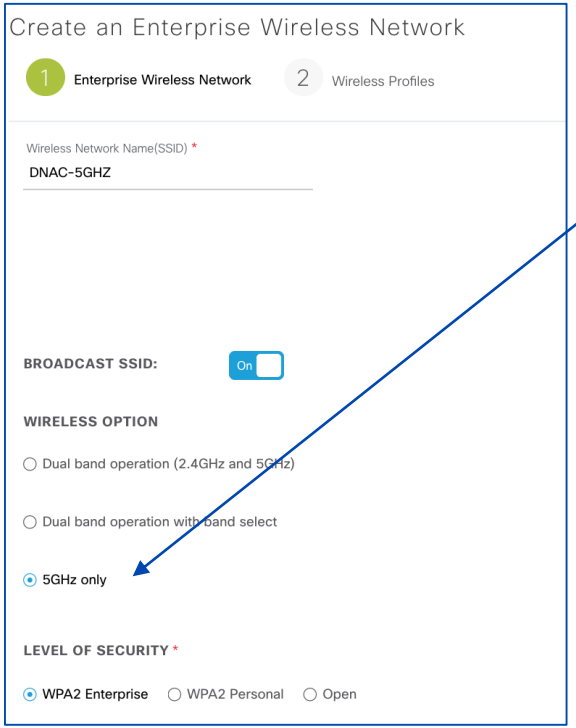
* Configurable device host name

Wireless Enhancements

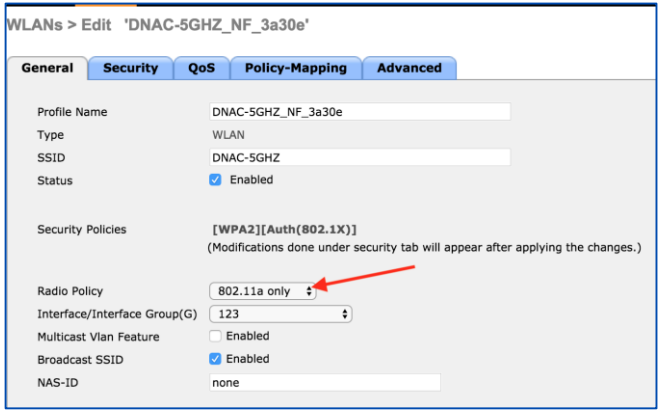
New wireless features available in SDA 1.2

- Advanced RF support
  - Default RF
  - Band Select
  - Broadcast SSID
  - Override PSK
- Zero Touch Provisioning (ZTP) of AP
- Guest SSID with Anchor WLC (for migration, OTT)
- Brownfield Support (for migration)
- Same WLC for fabric and non fabric SSID’s

DNAC 1.2 Advanced RF (5GHz only)



- Radio Policy configuration
- 5GHz only will apply Radio policy 802.11a only to the WLAN.



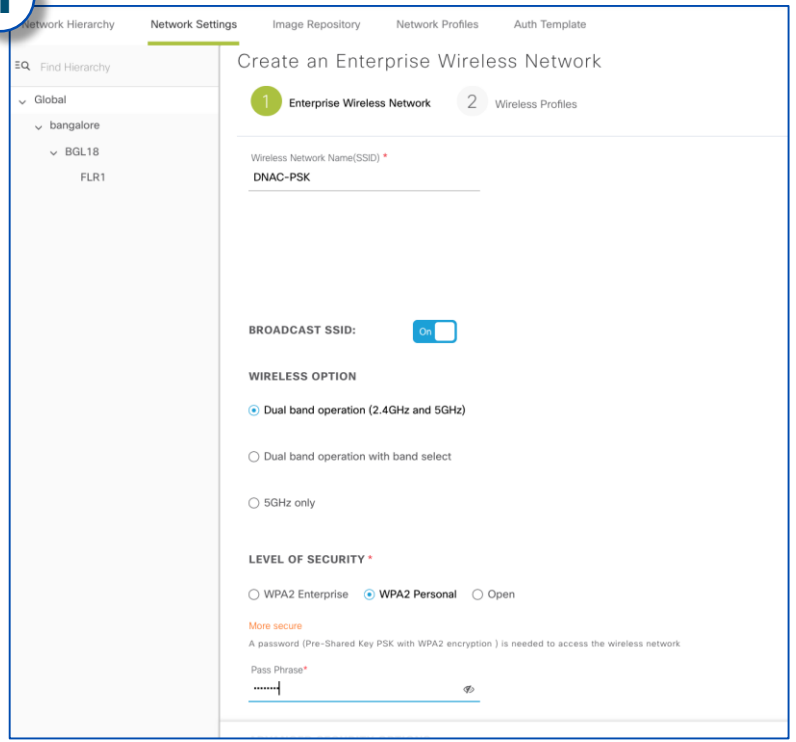
DNAC 1.2 Advanced RF (Override PSK)

In DNAC 1.2, PSK for SSID can be site specific. Each site can have different PSK SSID.

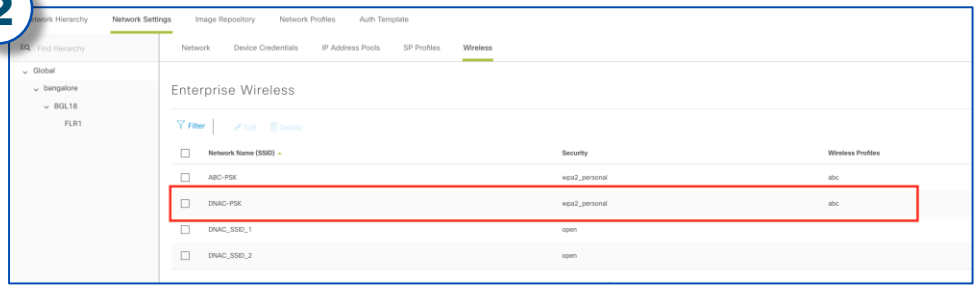
Step 1 : Create a PSK SSID under Global

Step 2 : PSK SSID is created successfully, as shown in below screenshot.

1



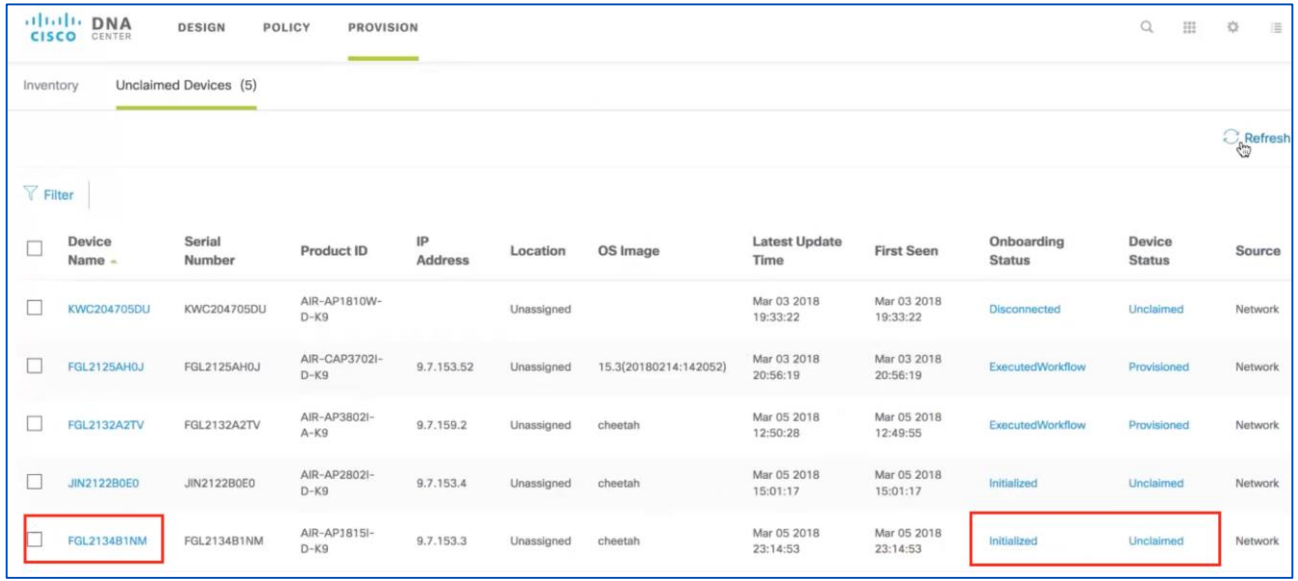
2



DNAC 1.2 : PnP for AP Provisioning

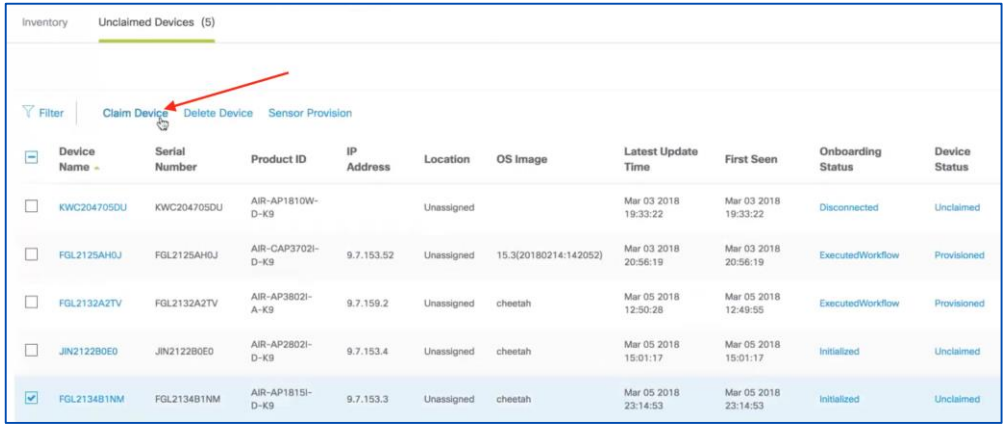
DNAC 1.2 supports PnP for APs (AP sensor is there already in 1.1.x)

1. AP shows in DNAC -> Provision Page -> Unclaimed Devices. AP will be in Initialized Unclaimed status

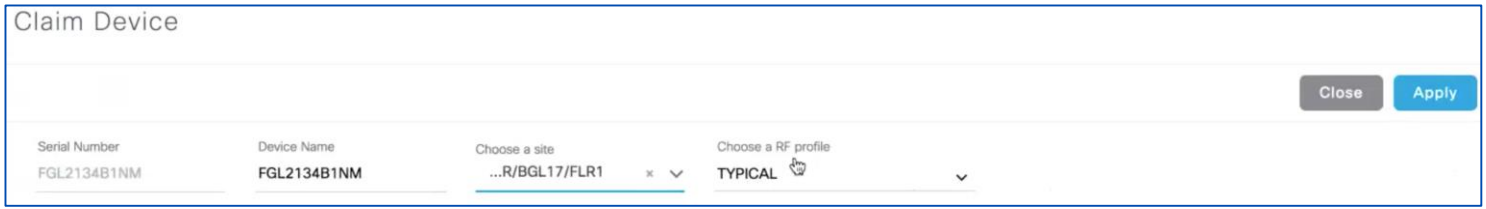


DNAC 1.2 : PnP for AP Provisioning (Cont..)

2 Select the AP and claim device

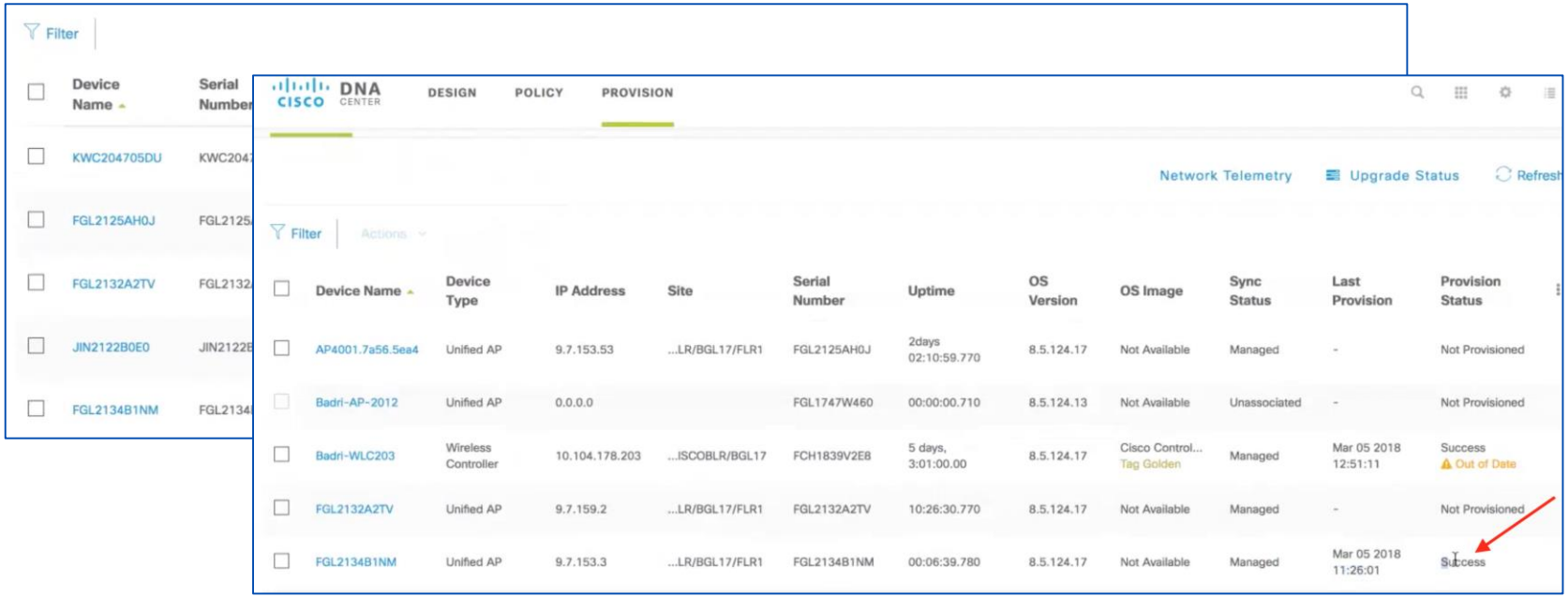


3 Claim the device which prompts to assign site and RF profile.



DNAC 1.2 : PnP for AP Provisioning (Cont..)

4 AP gets the PnP config with WLC details from DNAC and will be in Onboarding state for a bit and the Success



Brownfield WLC support

Ability for DNA-C to import configuration from a brownfield (existing deployed) Cisco WLC and import parameters into DNA Center Design and Provision module.

Imported configuration: SSID, RF profile, AAA Global settings, AP Groups etc.

Limitations:

- Only configurations recognized by DNA-C will be populated
- DNAC will not be able to learn device credentials
- PSK pwd or shared secret for AAA are not learnt. User will have to insert as part of the brownfield flow
- DNS, webauth redirect url and syslog setting are not currently learnt by DNAC
- As usual, when during provisioning phase, APs will reboot to get assigned to a site

Common WLC for Fabric/Non-Fabric per Site

- With this feature, Cisco customers can use fabric and non-fabric SSID across multiple sites on a single WLC


CISCO