



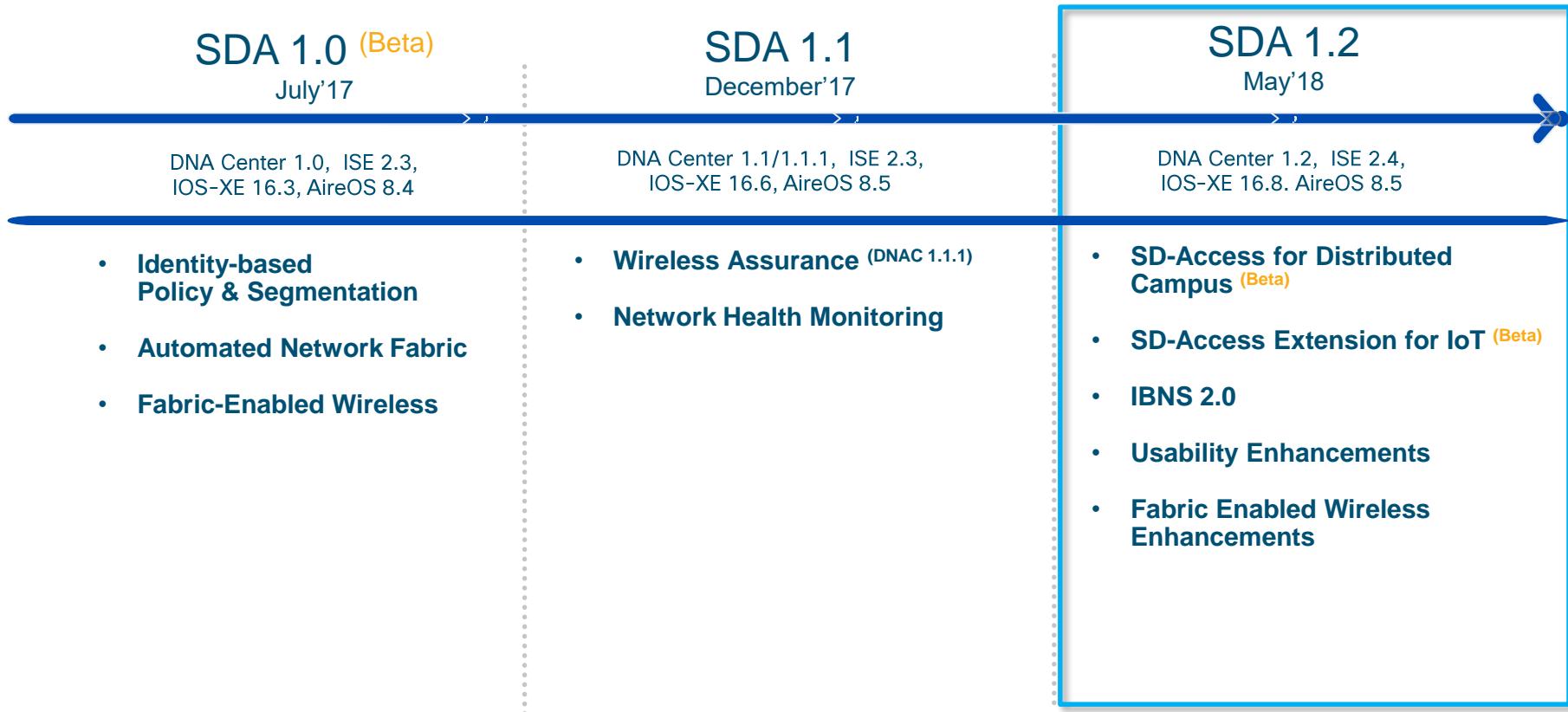
SD-Access 1.2 Update

Rene Andersen

Version 1.0

29/05/2018

SD-Access Roadmap



SD-Access Extension for IoT



for
Extended Enterprise



Warehouses



Manufacturing



Transportation



Outdoor Spaces



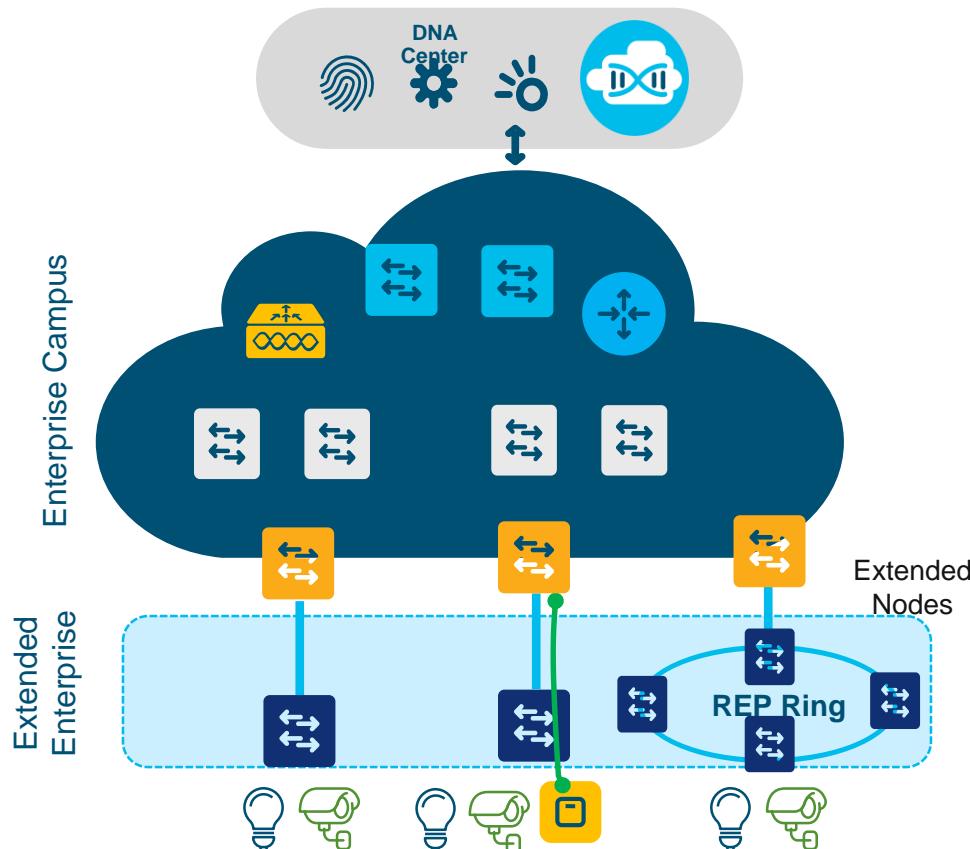
Workspace Switches



Connected Lighting

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



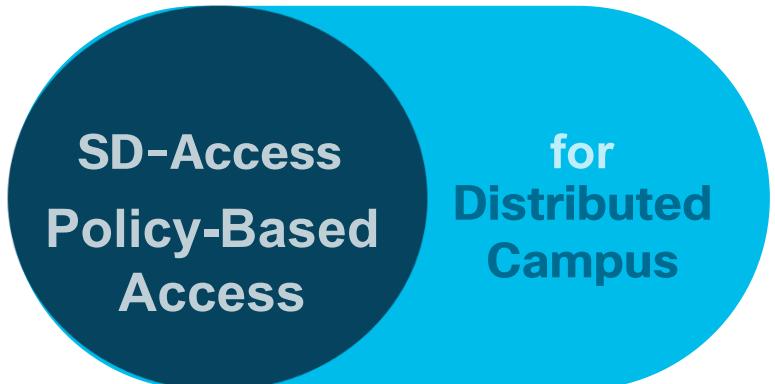
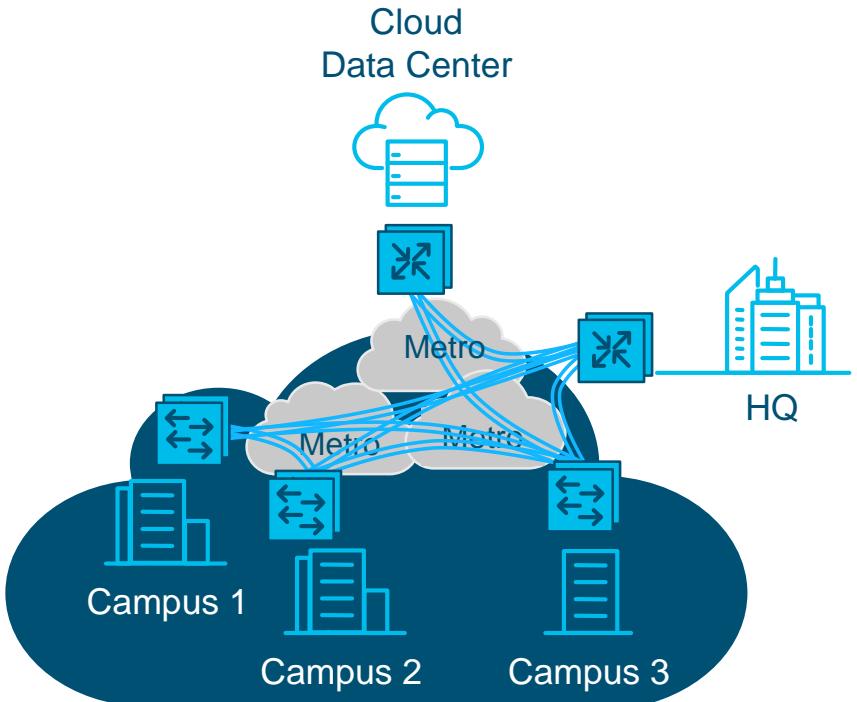
Catalyst Digital Building



3560-CX Compact



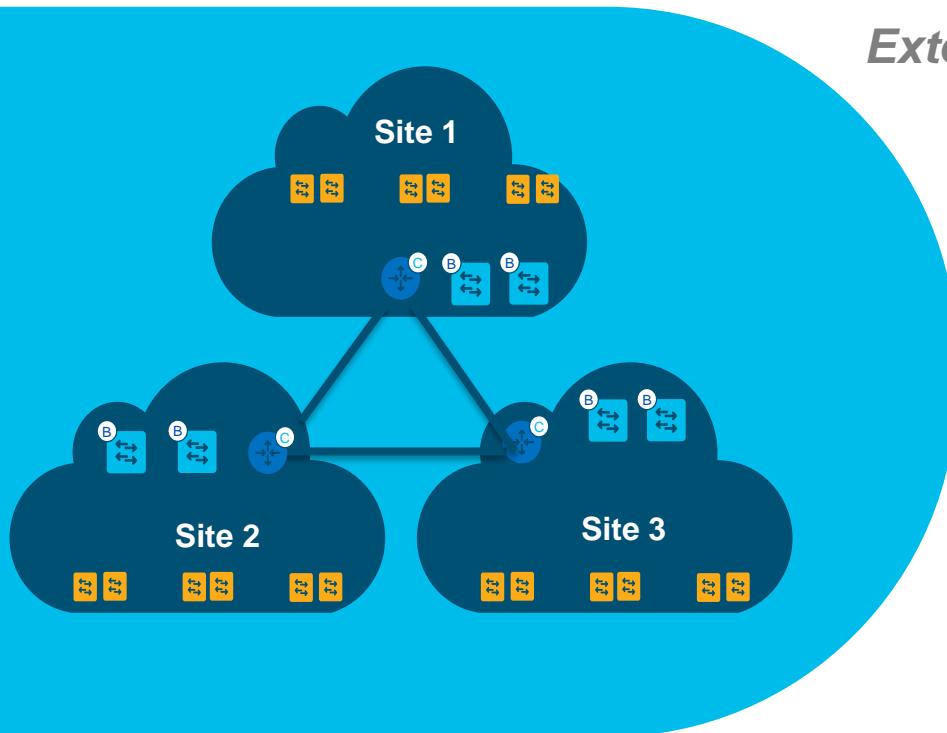
SD-Access for Distributed Campus



- ✓ 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



ISE



Catalyst 3K/9K



Catalyst 4500



Catalyst 6800



Nexus 7700



ASR1K/ISR4K/CSR



Wireless LAN



* 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

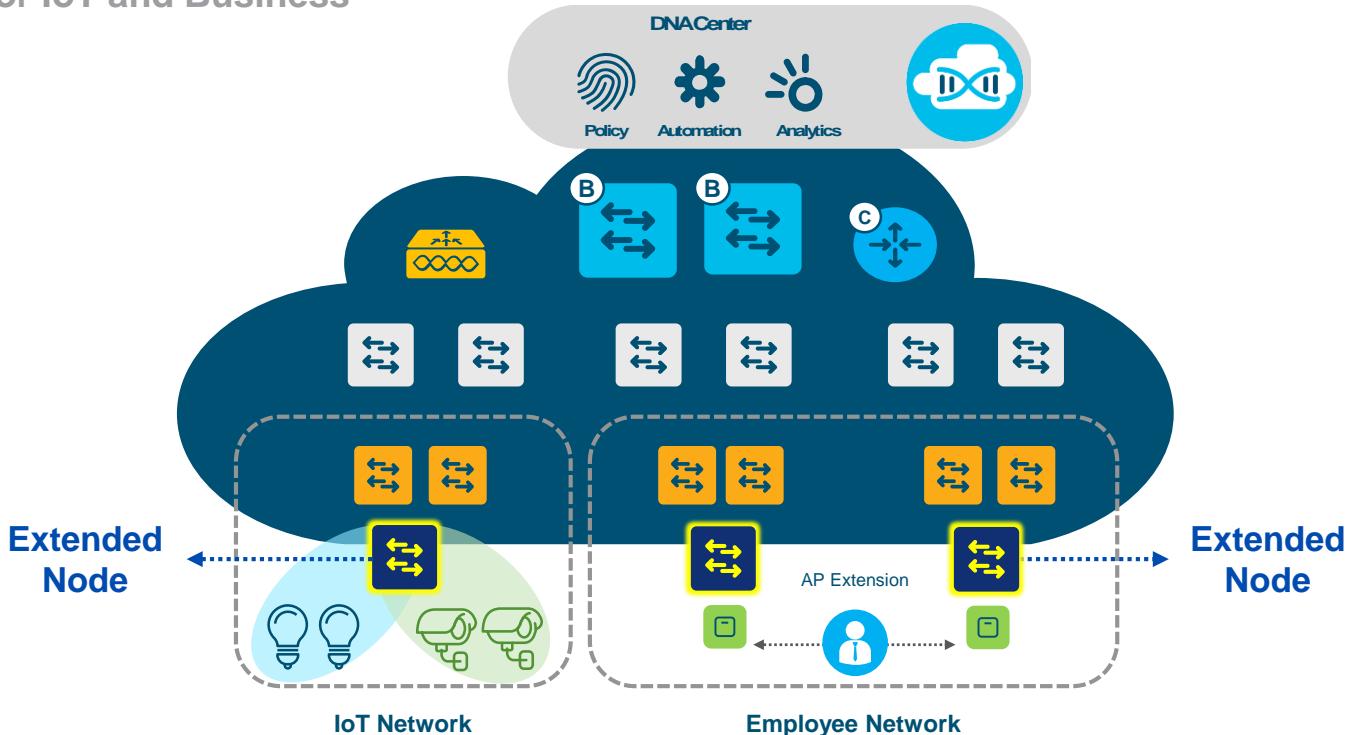
Below are the new features that are being introduced with DNAC/SD-Access 1.2

- 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



Purpose Built
Switches for IoT

Users, Device and IoT
Segmentation

Policy based
Automation

SD-Access Extension

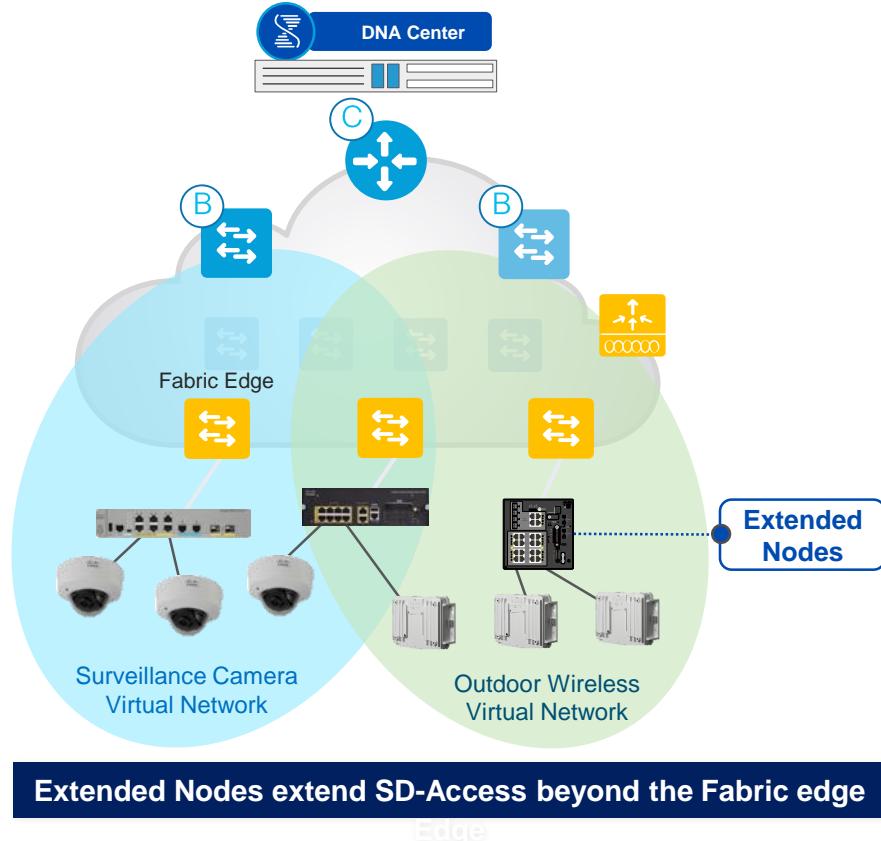
Key Benefits for IoT and Business

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

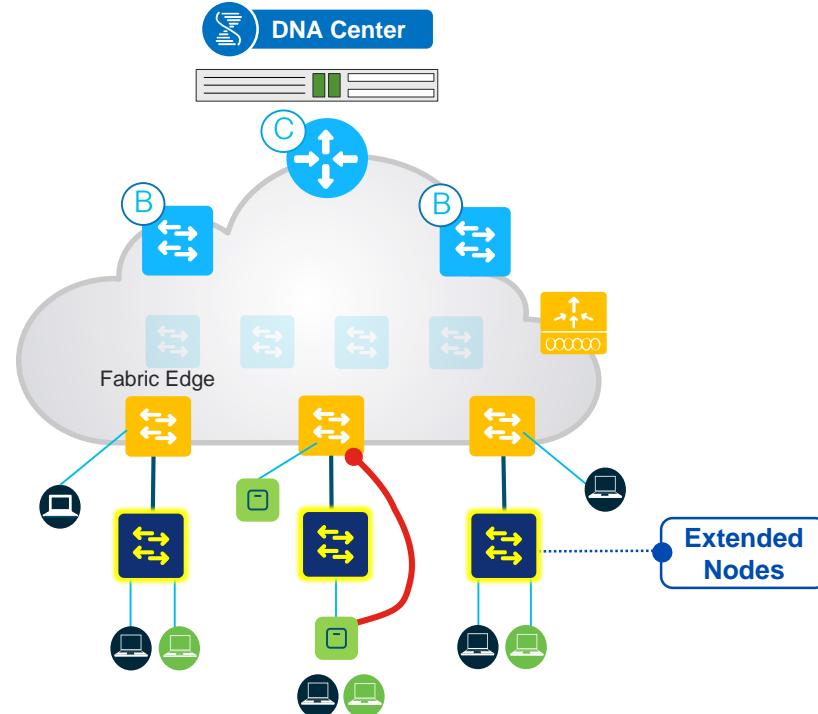


Traditional vs SD-Access Extension

| | Traditional | SD-Access Extended Node |
|--|---|---|
| Day 1 – Design and Installation | <ul style="list-style-type: none">• Manual “box by box” configuration• Networking expertise required to provision and deploy devices | <ul style="list-style-type: none">• Automated device deployment decreases time to operation• Zero touch configuration enables non-networking personnel to install |
| Day N – Operations and Updates | <ul style="list-style-type: none">• Network additions are complex• No automated workflows• Changes / Adds require manual configuration of multiple devices• Operation monitoring limited | <ul style="list-style-type: none">• 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 | <ul style="list-style-type: none">• Static L2 – L4 ACLs• Address based segmentation• Changes / Adds require manual configurations of multiple devices• Continuous auditing required to maintain security rule sets | <ul style="list-style-type: none">• 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**



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 |

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](#)

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

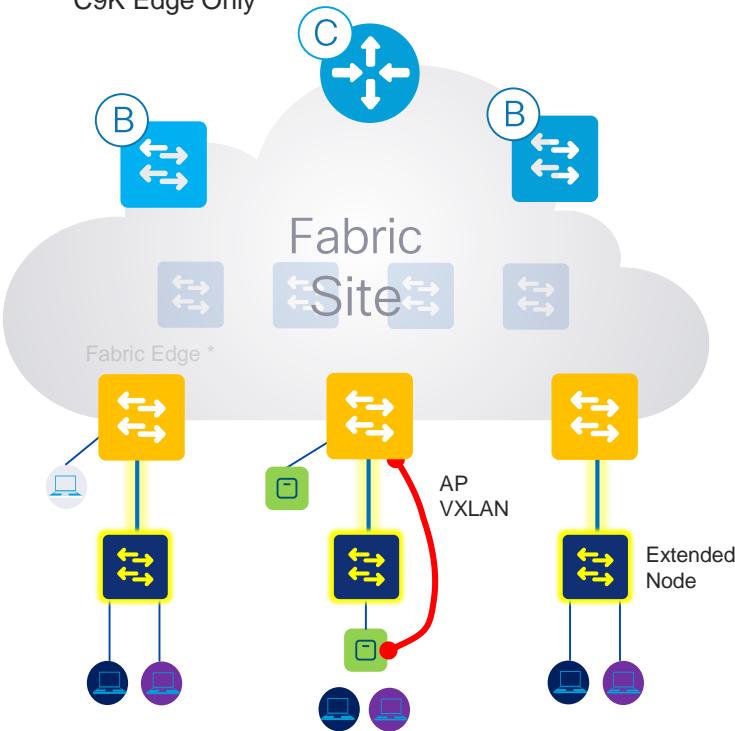
| License Type | IE2000 | IE3000 | IE4000 | IE4010 | IE5000 | C3560-CX | CDB |
|----------------|--------|--------|--------|--------|--------|----------|-----|
| DNA Essentials | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| DNA Advantage | No | No | Yes | Yes | Yes | Yes | Yes |

SD-Access Extended Nodes Deployment Models

SD-Access Extended Node

Point to Point Connection's

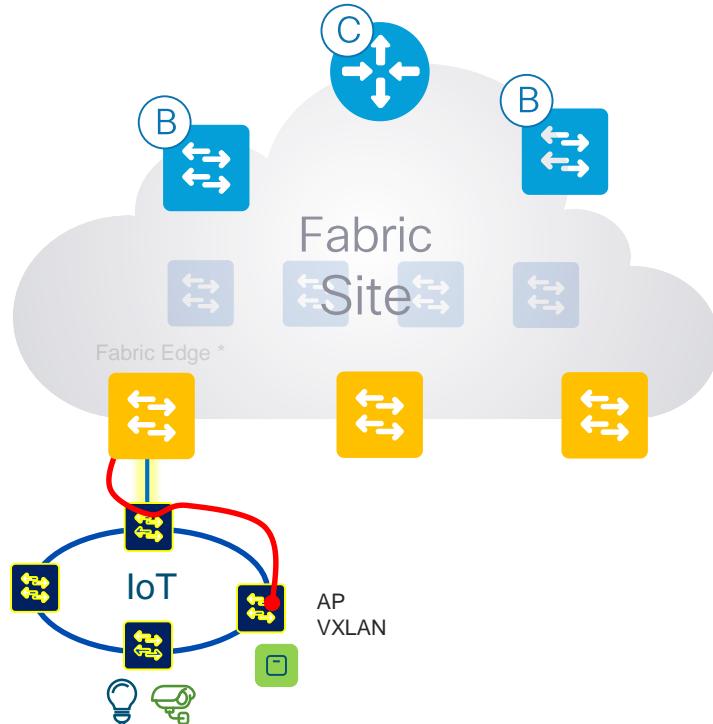
* C9K Edge Only



- 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

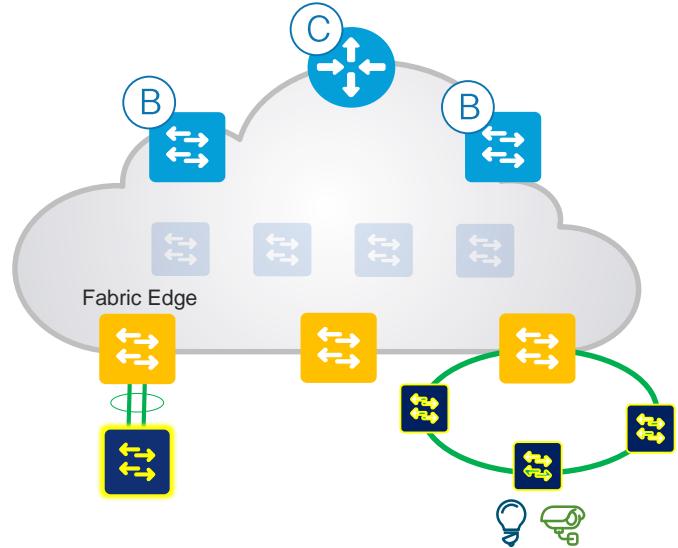
SD-Access Extended Node

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

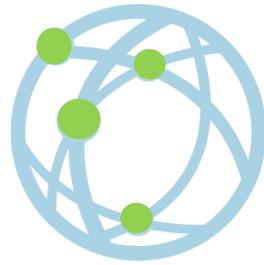
Zero Touch Provisioning Overview

Plan



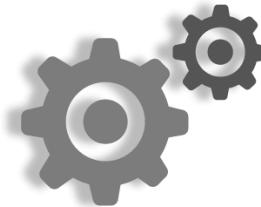
Verify Network Design
Verify System support
Prepare Extended Nodes

Design



Design IP Address Pools
Assign IP address Pools to
the right site

Provision



Dynamic discovery & automation
Static Discovery & automation
Host Onboarding settings

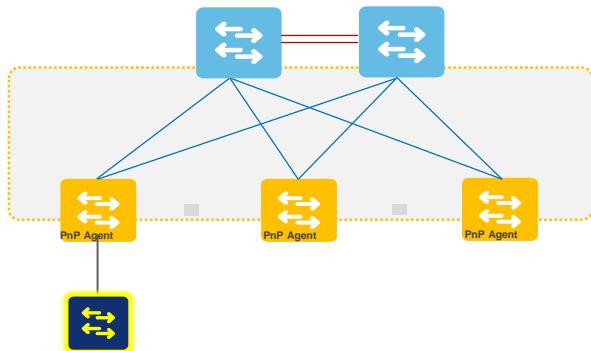
3 Step Process

IoT Ready Network

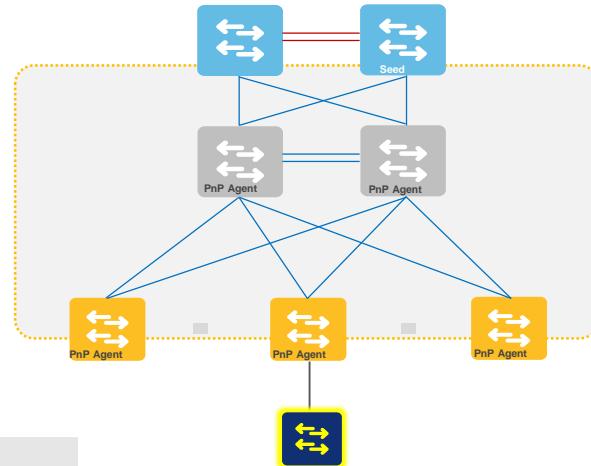
Plan – Network Design



2 Tier – Collapsed Core Design



3 Tier – Campus Design



Network Discovery

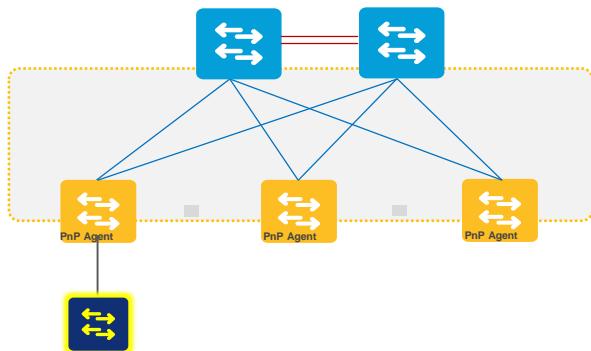
Dynamic and on-demand network discovery process

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

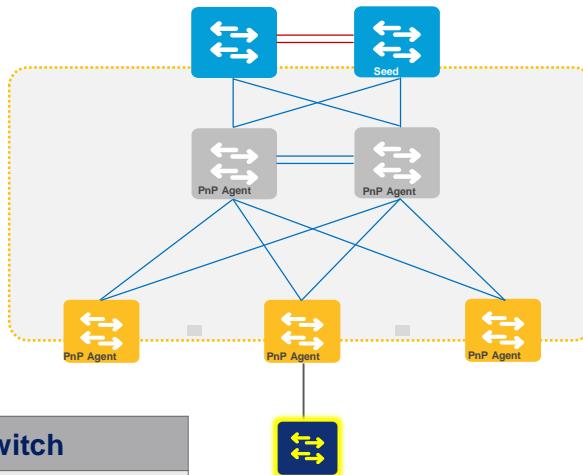
Plan – Catalyst Switch Role support



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

The screenshot shows the Cisco DNA Center interface for managing IP Address Pools. On the left, a tree view displays a global hierarchy with regions like AMER, APJC, EUR, UAE, UK, and US. The main pane shows a table of existing IP pools with columns for Name, IP Subnet Mask, Gateway, DHCP Server, and DN. A modal dialog titled "Add IP Pool" is open, prompting for a pool name ("extended_pool"), subnet ("35.35.35.0"), CIDR prefix ("/24 (255.255.255.0)"), gateway ("35.35.35.1"), and DHCP/DNS servers. The "Save" button is highlighted with a red box. A callout box labeled "1 Assign unique IP Pool" points to the pool name field. Another callout box labeled "2 Network Range for site Area" points to the subnet field. A third callout box labeled "3 Classful Network Mask" points to the CIDR prefix field. A fourth callout box labeled "4 Gateway IP Address" points to the gateway field. A large callout box at the bottom labeled "Global IP Pool" describes it as an IP address repository for multi-function distribution purpose to Area, Site etc., and mentions Reserve IP Pool from Area to automate extended nodes.

DESIGN POLICY PROVISION

Network Hierarchy Network Settings Image Management Network Profiles

Find Hierarchy

Global

- AMER - EAST
- AMER - WEST
- APJC - AUS EAST
- APJC - AUS WEST
- APJC - CHINA
- APJC - INDIA
- APJC - JAPAN
- EUR - NORTH
- EUR - SOUTH
- UAE - EAST
- UAE - WEST
- UK IRELAND
- US - EAST
- US - WEST

Network Device Credentials IP Address Pools Wireless

Add IP Pool

IP Pool Name * **extended_pool**

IP Subnet * **35.35.35.0**

CIDR Prefix **/24 (255.255.255.0)**

Gateway IP Address * **35.35.35.1**

DHCP Server(s) **31.31.31.0**

DNS Server(s) **8.8.8.8**

Cancel **Save**

1 Assign unique IP Pool

2 Network Range for site Area

3 Classful Network Mask

4 Gateway IP Address

Actions

Edit | Delete

Feedback

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

The screenshot shows the Cisco DNA Center interface under the DESIGN tab, specifically within the Network Settings section. The IP Address Pools tab is selected. A modal window titled "Reserve Extended node IP Pool" is open, providing instructions for creating a LAN pool.

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

The main configuration area includes:

- IP Pool Name: **extended_pool** (highlighted with a red box)
- Type: Generic
- Global IP Pool: ip_pool2 (35.35.35.0/24)
- CIDR Notation / No. of IP Addresses: 35.35.35.0/24 (255.255.255.0)
- Gateway IP Address: 35.35.35.1
- DHCP Server(s): 31.31.31.0
- DNS Server(s): (dropdown menu)

Buttons at the bottom of the modal:

- Cancel
- Save (highlighted with a red box)
- 5 Save to create new (partially visible)

On the right side of the interface, there is a vertical Actions panel with a "Reserve" button highlighted with a red box.

SD-Access @ DNA Center

Enabling Fabric Extension (method 1)

* Automated provision of Extended nodes

The screenshot shows the Cisco DNA Center interface. The top navigation bar includes the Cisco DNA Center logo, DESIGN, POLICY, and PROVISION tabs, with PROVISION selected. Below the navigation is a search bar and a settings icon.

The main area has two tabs: Devices and Fabric, with Fabric selected. A message indicates that sites must be added to the Fabric Domain. On the left, under 'Default LAN Fabric', there's a section for 'Fabric-Enabled Sites' with a '+' button, 'Find Hierarchy' search, and a 'Default LAN Fabric' entry for 'sjc23'. Below this are sections for 'Virtual Networks' (with 'Video_Security' and 'INFRA_VN' buttons, where 'INFRA_VN' is highlighted) and 'Wireless SSID's'.

A central modal window titled 'Edit Virtual Network: INFRA_VN' displays a table of IP pools:

| IP Pool Name | Address Pool | Pool Type | Layer-2 Extension |
|----------------------|---------------|---|-----------------------------|
| ap_pool | 33.33.33.0/24 | <input checked="" type="radio"/> AP <input type="radio"/> EXTENDED | <input type="checkbox"/> On |
| extended_pool | 35.35.35.0/24 | <input type="radio"/> AP <input checked="" type="radio"/> EXTENDED | <input type="checkbox"/> On |
| Security-camera-pool | 36.36.1.0/24 | <input type="radio"/> AP <input type="radio"/> EXTENDED | <input type="checkbox"/> On |

Two rows are circled in red: the second row ('extended_pool') and the third row ('Security-camera-pool').

At the bottom of the modal are 'Cancel' and 'Update' buttons.

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

The screenshot shows the Cisco DNA Center interface with the 'Fabric' tab selected. On the left, under 'Fabric-Enabled Sites', there is a list of sites including 'Default LAN Fabric' and 'sjc23'. In the center, a 'Select Port Assignment' table lists interfaces for various devices. On the right, a 'Port Assignments' modal window is open, showing 'Selected Interfaces' as 'GigabitEthernet1/0/5'. A dropdown menu 'Select Device Type' is open, with 'Extended Node' highlighted and circled in red. Other options like 'User Devices (ip-phone,computer,laptop)' and 'Access Point(AP)' are also visible.

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

Port Assignments X

Selected Interfaces
GigabitEthernet1/0/4, GigabitEthernet1/0/7

Connected Device Type Extended Node

Address Pool
35_35_35_0(extended_pool)-INFRA_...

Auth Template
No Authentication

Feedback

Cancel Update

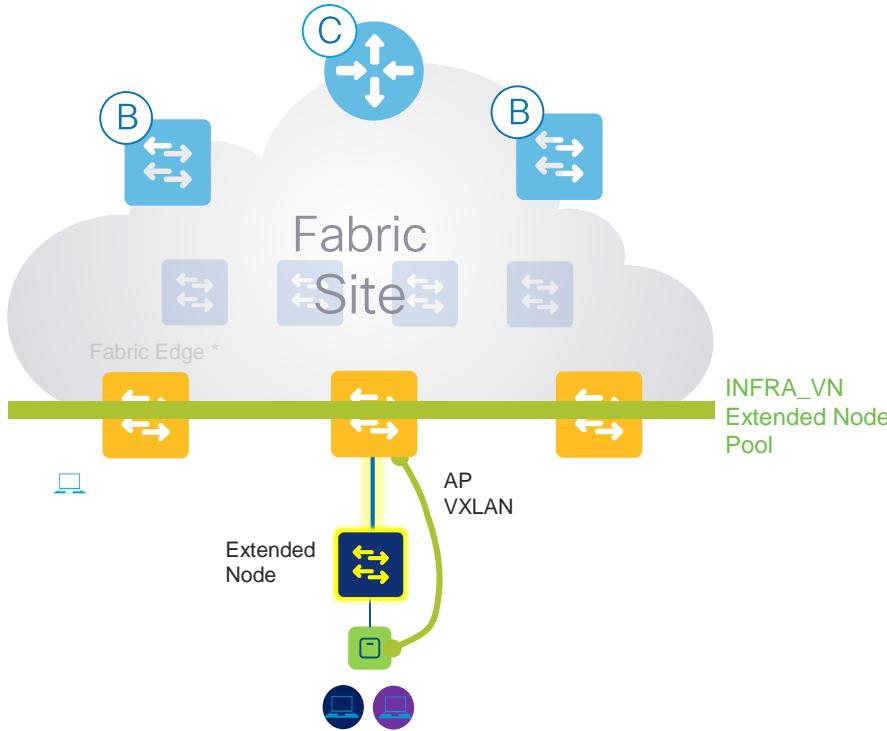
NOTE: Mockup only, subject to change.

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.

Screenshot of the Cisco DNA Center interface showing the Fabric Extension Automation process:

- Header:** Cisco DNA CENTER, DESIGN, POLICY, PROVISION (highlighted), SEARCH, FILTERS, SETTINGS.
- Left Sidebar:** Devices (selected), Fabric (highlighted).
- Section:** Default LAN Fabric.
- Sub-section:** Select Devices, Host Onboarding.
- Text:** Select device(s) to be added to fabric. And assign the roles of 1 Border Node and 1 Control Plane Node.
- Search Bar:** Search Topology.
- Text:** Select Devices to add, remove or identify. Shift + Click to select multiple.
- Topology View:** A network diagram showing four nodes:
 - Top Left: IE-4010-16S12P (with two blue double-headed arrows)
 - Top Right: Cat9k-3 (with two blue double-headed arrows)
 - Middle: Cat9k-4 (with three blue double-headed arrows)
 - Bottom Right: WS-C3560CX-8PT (with three blue double-headed arrows, circled in red)The nodes are interconnected by light gray lines representing fabric links.
- Validation:** Validation status and validation icon.
- Feedback:** Feedback button.
- Buttons:** Save, Cancel.

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

The screenshot shows the Cisco DNA Center interface with the 'Fabric' tab selected. On the left, there's a sidebar for 'Default LAN Fabric' with sections for 'Fabric-Enabled Sites' and 'Virtual Networks'. A red circle highlights the 'Video' tab in the sidebar.

The main area displays the 'Edit Virtual Network: Video_Security' dialog box. It contains a table with columns: IP Pool Name, Traffic Type, Address Pool, Layer-2 Extension, Groups, Critical Pool, and Auth Policy. Two rows are listed:

| IP Pool Name | Traffic Type | Address Pool | Layer-2 Extension | Groups | Critical Pool | Auth Policy |
|----------------------|----------------|---------------|-------------------|--------------|---------------|-------------|
| ap_pool | Choose Traffic | 33.33.33.0/24 | On | Choose Group | | |
| extended_pool | Choose Traffic | 35.35.35.0/24 | On | Choose Group | | |
| IOT_Pool_SJ | Choose Traffic | 20.20.20.0/25 | On | Choose Group | 20_20_ | |
| Security-camera-pool | Data | 36.36.1.0/24 | On | Choose Group | 36_36_ | |

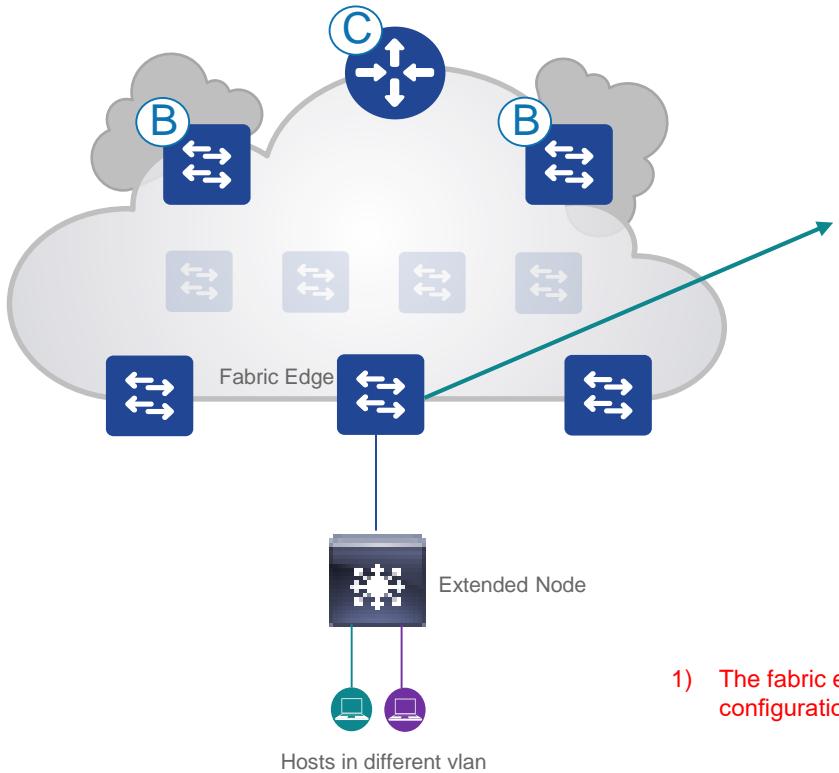
At the bottom of the dialog box are 'Cancel' and 'Update' buttons.

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

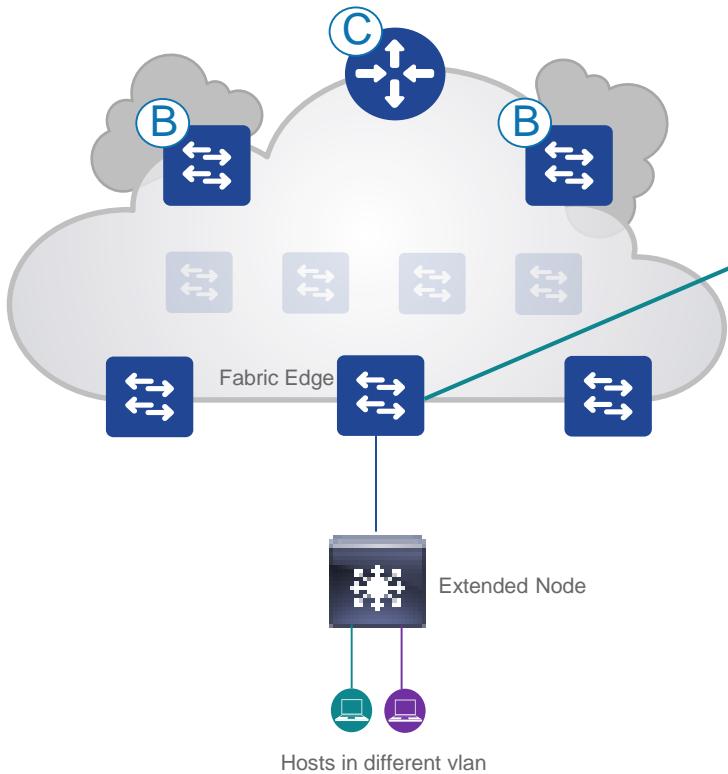


```
interface Vlan3001
description "User Subnet for Extended nodes"
ip vrf forwarding Users_1
ip address 20.20.20.254 255.255.255.0
ip helper-address 1.1.1.1
no ip redirects
ip local-proxy-arp
ip route-cache same-interface
no lisp mobility liveness test
lisp mobility eid_20_20_20_0
!
interface Vlan3002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

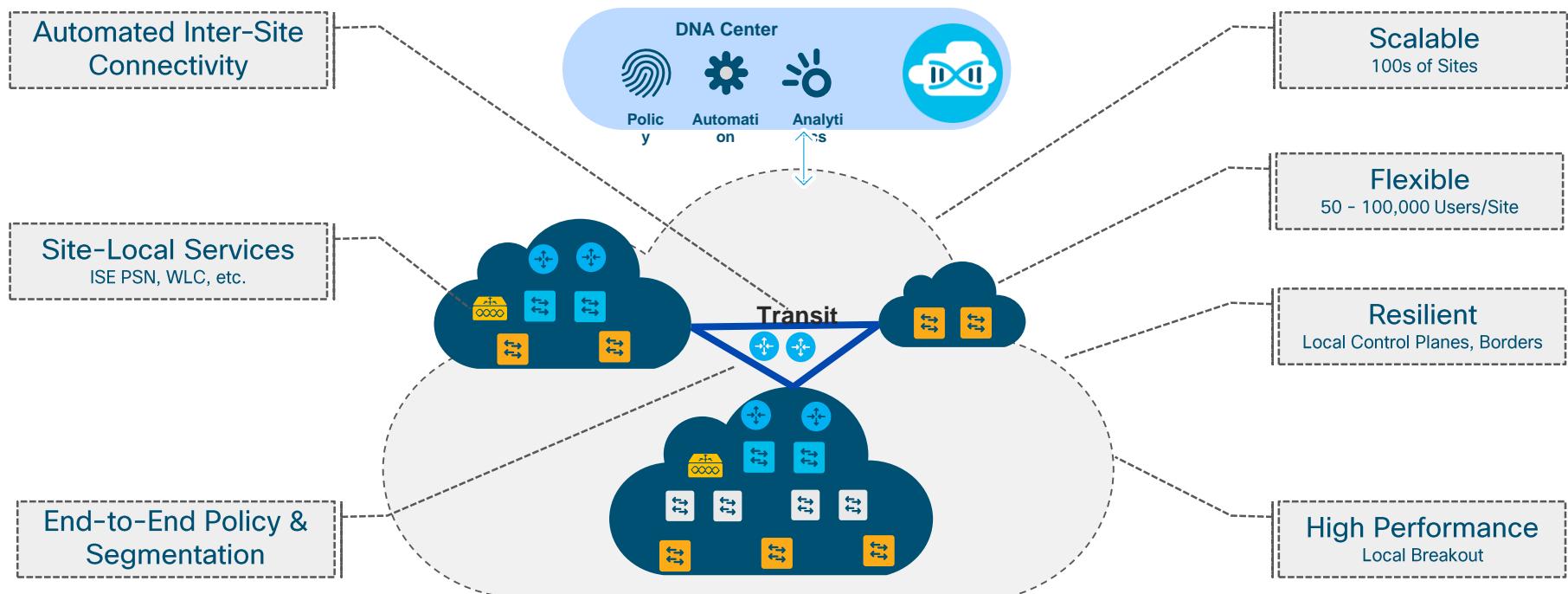


```
interface GigabitEthernet1/0/6
description "Connecting to Extended Switch 3560-CX"
switchport mode trunk
macro description CISCO_SWITCH_EVENT
!
cts role-based sgt-map vlan-list 3001 sgt 8 < map an vlan to an SGT value>
cts role-based sgt-map vlan-list 3002 sgt 9 < map an vlan to an SGT value>
!
```

- 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

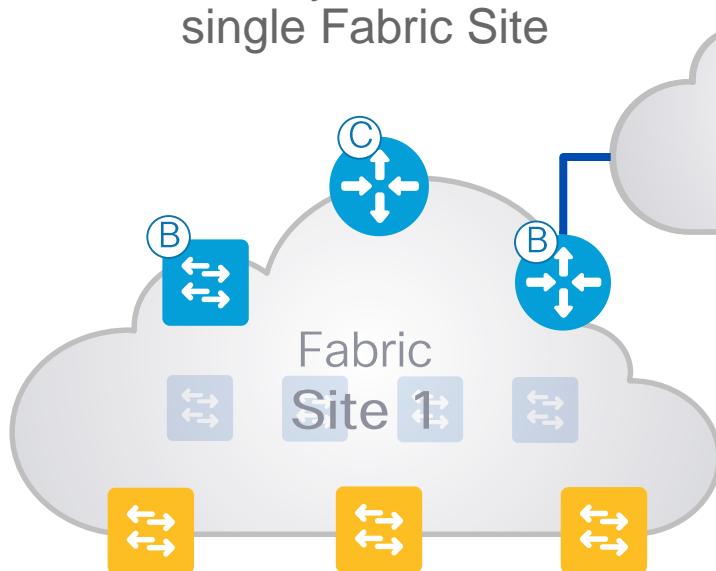


* Beta in SDA 1.2

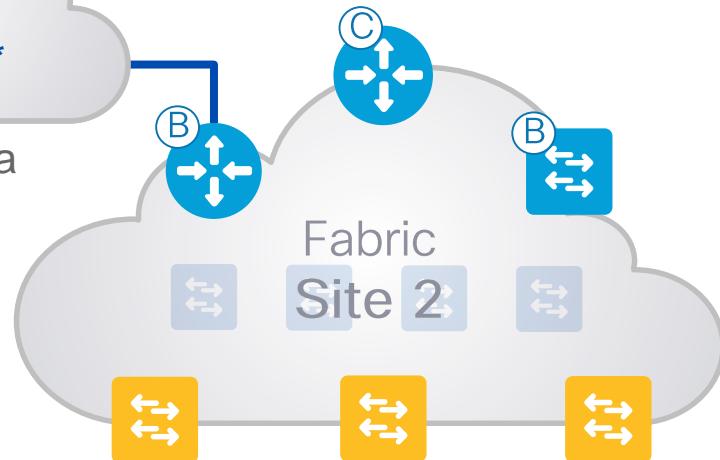
Fabric Sites & Domains

Connecting Multiple Fabrics

First, you build a single Fabric Site



Later, you build another Fabric Site



How do you connect them together?

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 |

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

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

The screenshot shows the Cisco DNA Center interface for managing SD-Access transit. The top navigation bar includes the Cisco DNA CENTER logo, DESIGN, POLICY, PROVISION (which is highlighted in green), and search/filter icons.

The main left panel displays 'Fabric Domains and Transits'. Under 'Fabric Domains', two domains are listed: 'Default_LAN_Fabric' and 'California', both categorized as LAN. Under 'Transits', no items are currently listed.

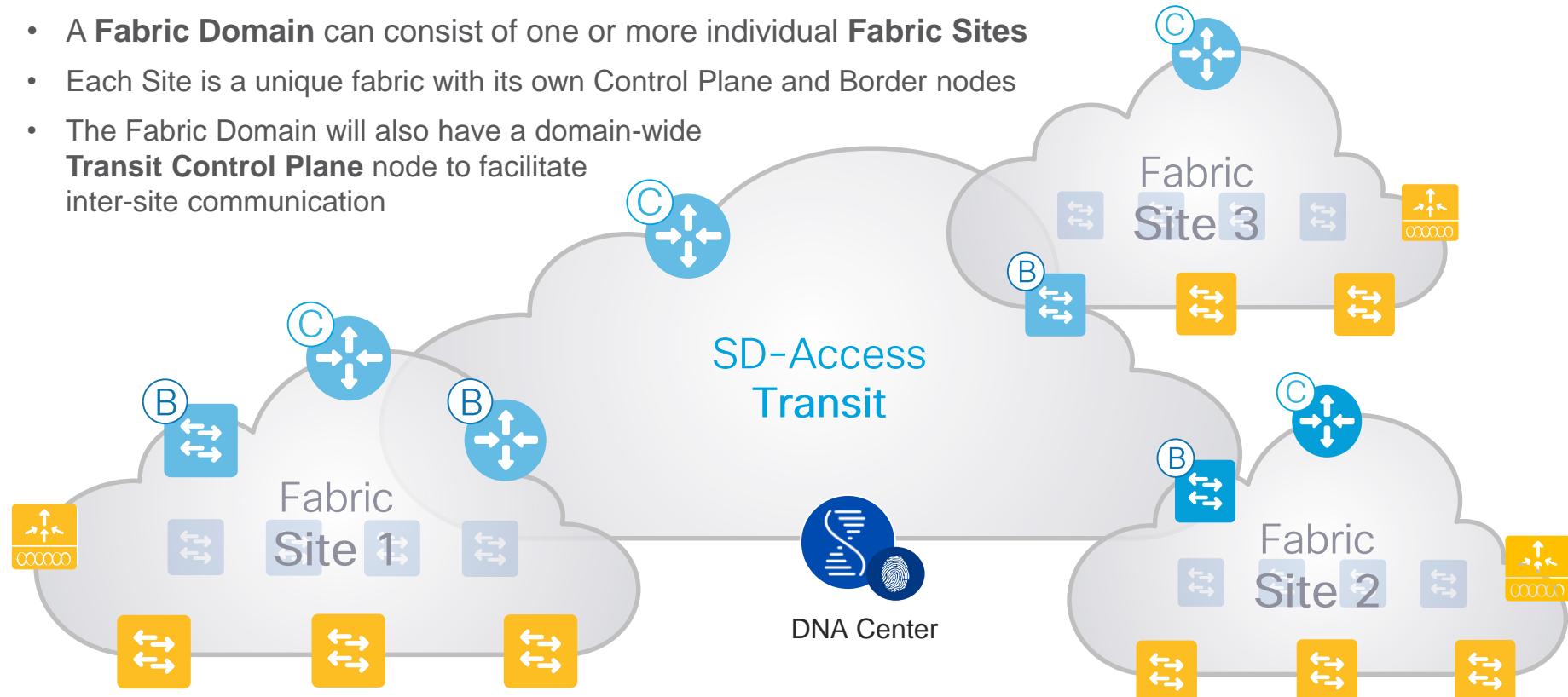
A modal window titled 'Add Transit' is open on the right, titled 'Add Transit'. It contains instructions: 'To enable interconnectivity between Fabric sites, select Transit Control Plane and connectivity type.' It asks for a 'Transit Name' (set to 'SD_Access Transit') and a 'Transit Type' (with 'Native SD-Access' selected, indicated by a blue circle). A note states: 'Transit Type: Native SD-Access provides the best performance and reliability for campus interconnectivity. IP transit type is recommended for connecting to external networks or for specific use cases like roaming or guest access.' Below these fields are dropdown menus for 'Transit Control Plane 1' (set to 'Transit Control Plane 1') and 'Redundant Transit Control Plane (Optional)'. At the bottom of the modal are 'Cancel' and 'Save' buttons, with 'Save' being highlighted in blue.

SD-Access for Distributed Campus

Beta in SDA 1.2.1

SD-Access Transit

- 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

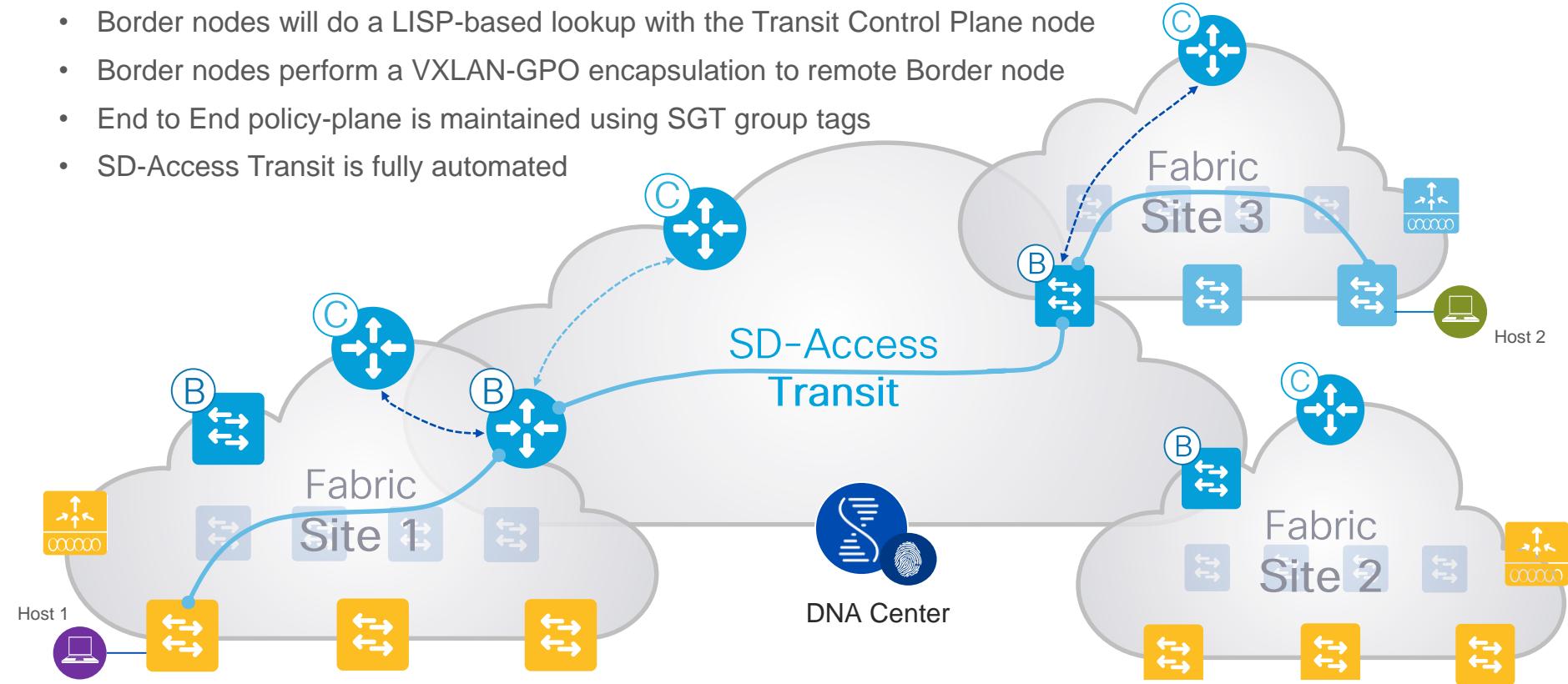


SD-Access for Distributed Campus

Beta in SDA 1.2.1

SD-Access Transit

- 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

CISCO DNA CENTER DESIGN POLICY PROVISION

Devices Fabric

Fabric Domains and Transits

Choose a Fabric Domain or Transit below to manage, or add a new item by clicking "Add Fabric Domain or Transit".

Fabric Domains

- Default_LAN_Fabric
- California

Transits

No Transits Created

Add Transit

To enable interconnectivity between Fabric sites, select Transit Control Plane and connectivity type.

Transit Name: IP Transit

Transit Type: IP Native SD-Access

Routing Protocol: BGP

Autonomous System Number: 65535

Feedback

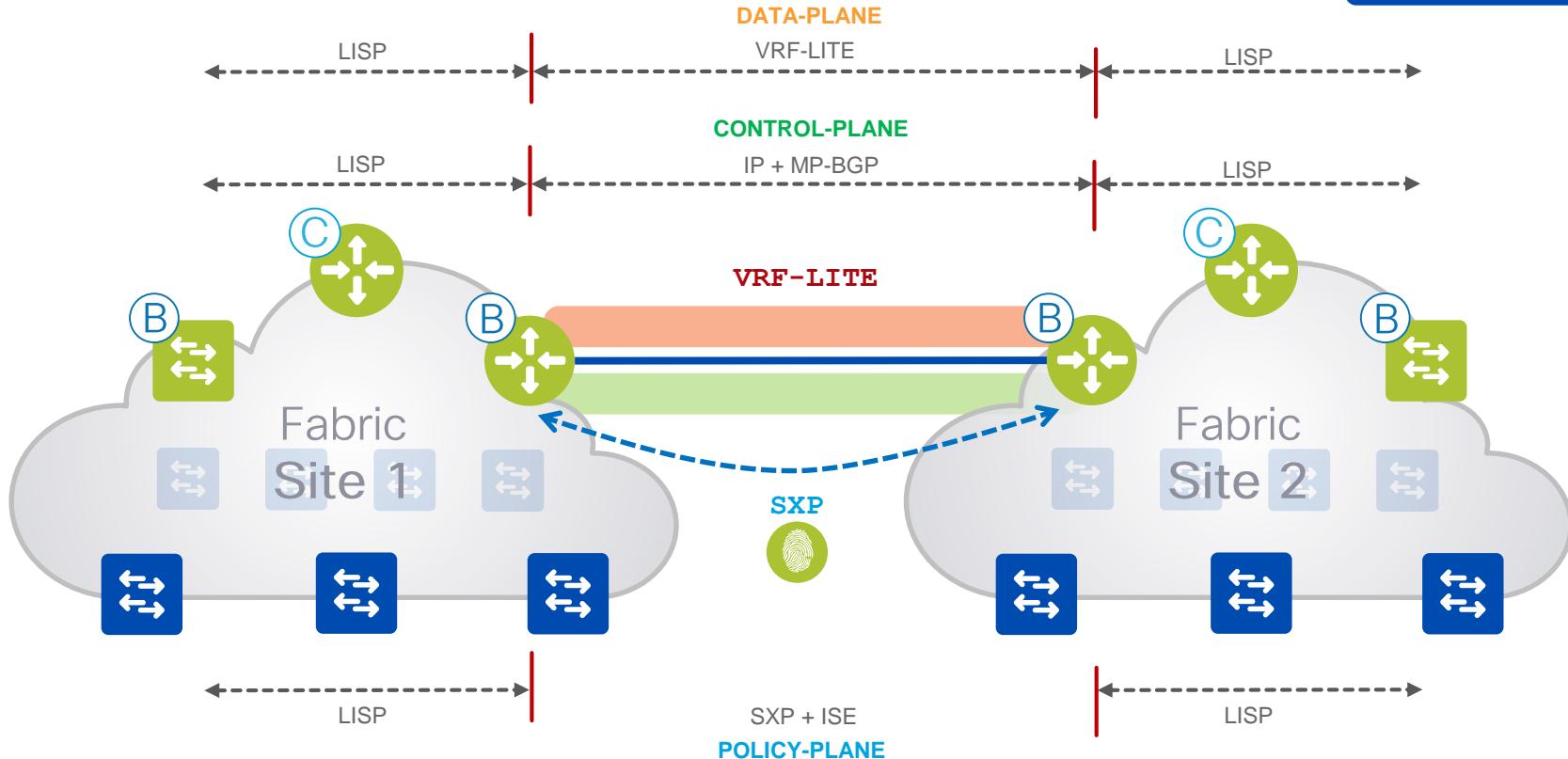
Cancel Save

Inter-Connecting Fabric Sites

Multiple Fabric Domains with VRF-LITE Transit



SDA 1.0 - 1.1

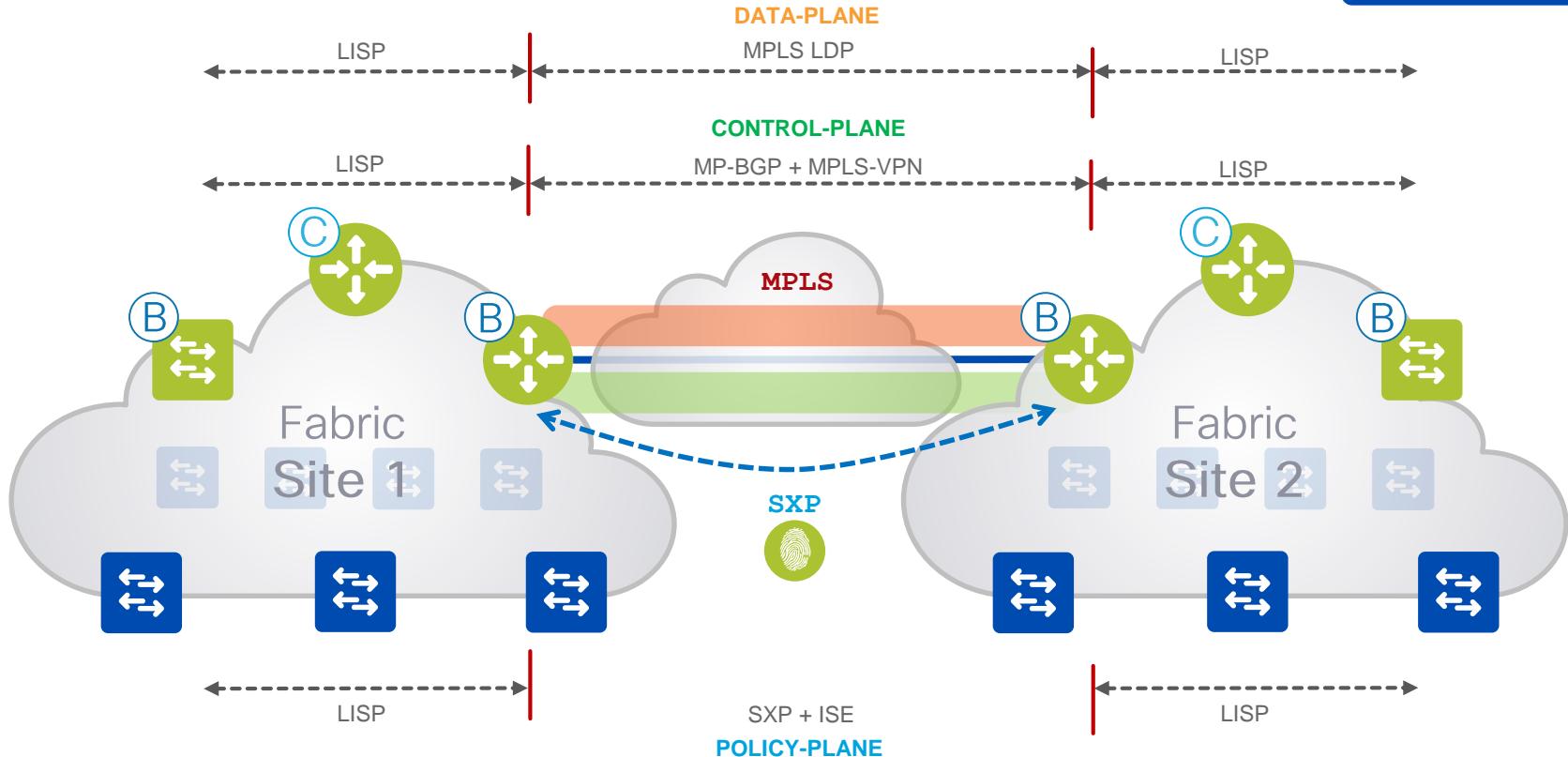


Inter-Connecting Fabric Sites

Multiple Fabric Domains with MPLS Transit



SDA 1.0 - 1.1

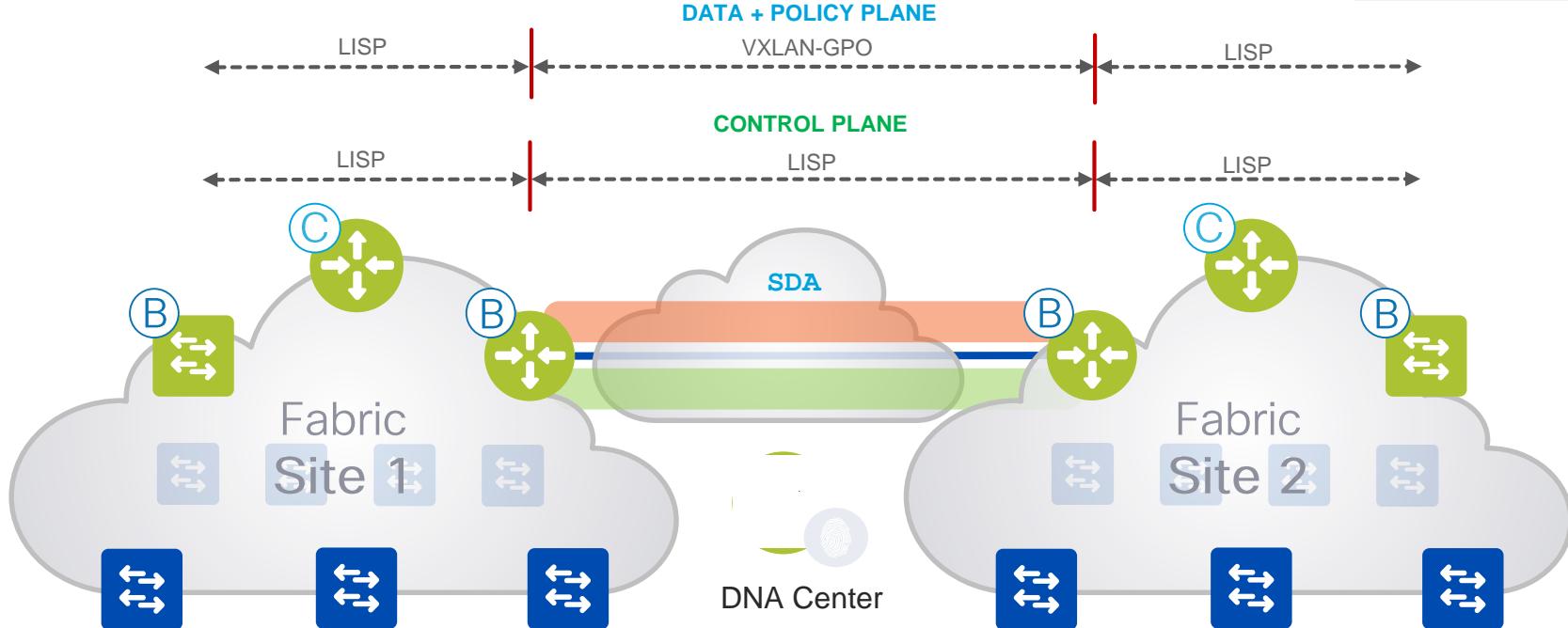


Inter-Connecting Fabric Sites

Multiple Fabric Domains with Native SDA Transit

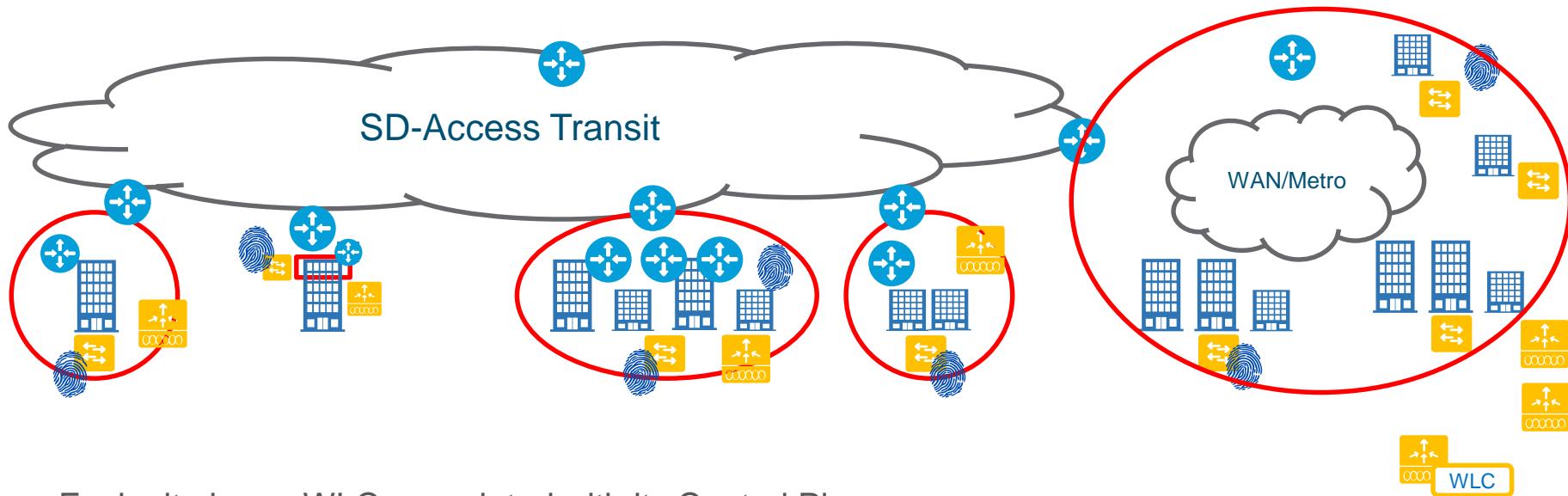


New in SDA
1.2.X



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)

CISCO DNA CENTER DESIGN POLICY PROVISION

Device Inventory

Inventory (30) Unclaimed Devices

Select device(s) to assign to a Site and Provision network settings from the Network Hierarchy.

| | | LAN Automation | LAN Auto Status | Network Telemetry | Upgrade Status | Refresh | | | | | |
|---|---------|----------------|------------------|-------------------|---------------------|---------------------|------------|-------------|----------------------|------------------|-----------------|
| Filter | Actions | 1 Selected | | | | | | | | | |
| <input type="checkbox"/> | Device | IP Address | Site | Serial Number | Uptime | OS Version | OS Image | Sync Status | Last Provision | Provision Status | ⋮ |
| Assign Device to Site | | | | | | | | | | | |
| Provision | | | | | | | | | | | |
| Update OS Image | | 10.41.54.188 | ...an Jose/SJC01 | FOX1530GG0E | 3 days, 4:17:16.03 | 03.08.00.E | | Managed | Apr 23 2018 09:27:26 | Success | |
| Resync | | 10.41.54.189 | ...an Jose/SJC05 | FOC1705V0R2 | 2 days, 16:02:12.57 | 16.6.2 | | Managed | Apr 23 2018 09:27:26 | Success | |
| Delete Device | | 10.41.54.190 | ...an Jose/SJC01 | FOX1530GG2G | 3 days, 21:18:23.26 | 03.08.00.E | | Managed | Apr 23 2018 09:27:26 | Success | |
| Learn Device Config | | | | | | | | | | | |
| <input type="checkbox"/> AP0081.C424.3CE2 | | Unified AP | 10.85.0.22 | ...an Jose/SJC05 | FTX1820S2PC | 2 days, 23:18:23.45 | 8.5.124.15 | | Managed | - | Not Provisioned |

<https://172.25.14.103/dna/provision/home#>

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

CISCO DNA CENTER DESIGN POLICY PROVISION

Devices Fabric

Select or Add Site(s) to this Fabric Domain. Each Site

Default LAN Fabric

Fabric-Enabled Sites +

Fabric Infras

Find Hierarchy

Default LAN Fabric

sjc23

Virtua

Video

Edit Virtual Network: Video_Security

Select an IP Pool and Traffic Type to associate it with the selected VN. Layer-2 Extension and Policy Group are optional.

| IP Pool Name | Traffic Type | Address Pool | Layer-2 Extension | Groups | Critical Pool | Auth Policy |
|----------------------|----------------|---------------|-------------------|--------------|---------------|-------------|
| ap_pool | Choose Traffic | 33.33.33.0/24 | On | Choose Group | | |
| Critical_auth_site1 | Choose Traffic | 91.91.91.0/24 | On | Choose Group | | |
| extended_pool | Choose Traffic | 35.35.35.0/24 | On | Choose Group | | |
| IOT_Pool_SJ | Choose Traffic | 20.20.20.0/25 | On | Choose Group | | |
| Security-camera-pool | Data | 36.36.1.0/24 | On | Choose Group | | 36_36 |

Feedback D

Cancel Update

The screenshot shows the Cisco DNA Center interface for managing Virtual Networks (VNs). The top navigation bar includes DESIGN, POLICY, and PROVISION tabs, with PROVISION selected. Below the tabs, there are sections for Devices and Fabric. A message indicates that sites need to be selected or added to the Fabric Domain. The main area displays the 'Edit Virtual Network: Video_Security' configuration. It lists five IP pools: ap_pool, Critical_auth_site1, extended_pool, IOT_Pool_SJ, and Security-camera-pool. The Security-camera-pool is currently selected, as indicated by a checked checkbox and highlighted rows. The configuration table includes columns for IP Pool Name, Traffic Type, Address Pool, Layer-2 Extension (set to On), Groups, Critical Pool, and Auth Policy. The 'Auth Policy' column for the selected pool shows the value '36_36'. A red circle highlights the 'Auth Policy' column header, and another red circle highlights the '36_36' value in the row for the selected pool. A feedback button is visible on the right side of the table.

Authentication Template ‘Edit’ options

CISCO DNA CENTER

DESIGN POLICY PROVISION

Network Hierarchy Network Settings Image Repository Network Profiles Auth Template

AuthTemplate Medhod

Filter

| Name | Type |
|---------------------------------------|-----------------------|
| Closed Authentication | Closed Authentication |
| Easy Connect | Easy Connect |
| Open Authentication | Open Authentication |

Showing 3 of 3

Closed Authentication

X

Deployment Mode: Closed

First Authentication Order: 802.1x MAC Auth Bypass(MAB)

802.1x to MAB Fallback: 21

Wake on LAN: Yes No

Number of Hosts: Single Unlimited

Cancel Submit

Feedback ⓘ

Customization: Authentication order

| | |
|----------------------------|--|
| Deployment Mode | Closed |
| First Authentication Order | <input checked="" type="radio"/> 802.1x <input type="radio"/> MAC Auth Bypass(MAB) |
| 802.1x to MAB Fallback |  |
| Wake on LAN | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Number of Hosts | <input type="radio"/> Single <input checked="" type="radio"/> Unlimited |

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

LAN Automation

Seed Device

Site*

Primary Device*

Secondary Device

Choose Ports*

Discovered Device Configuration

Site*

IP Pool*

ISIS Password

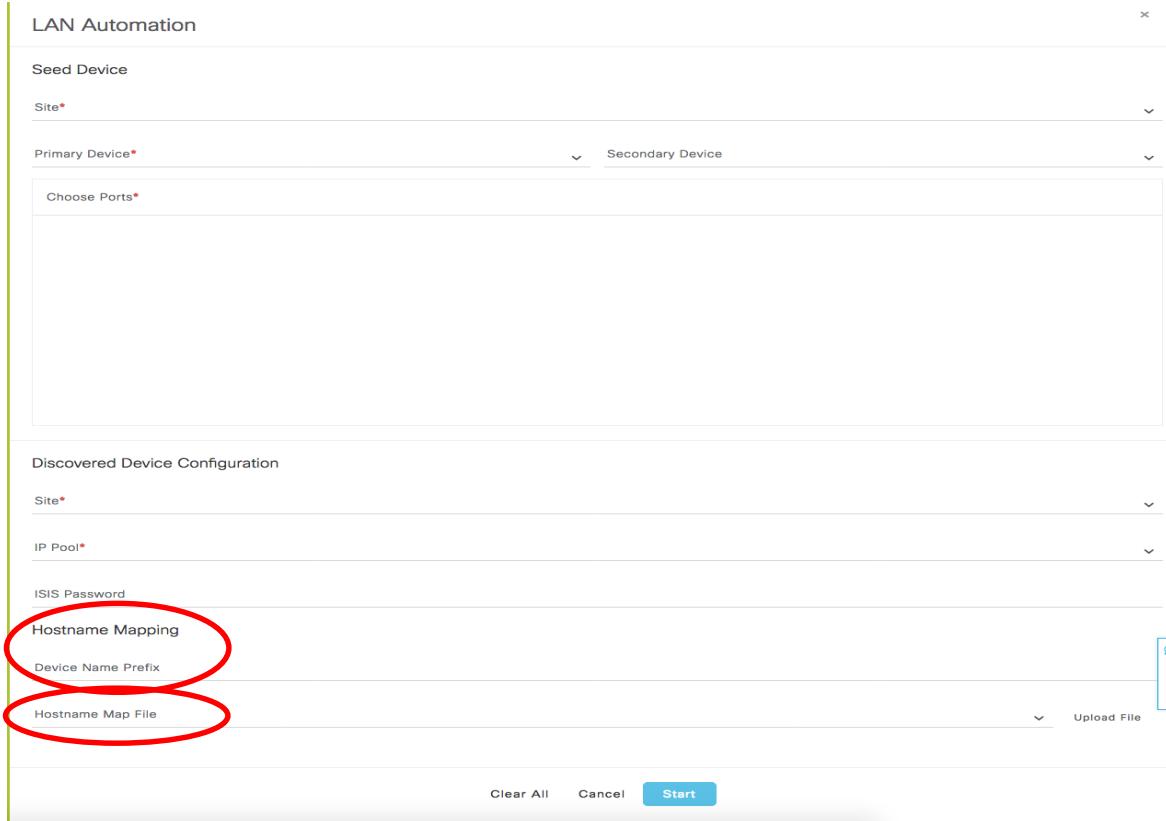
Hostname Mapping

Device Name Prefix

Hostname Map File

Feedback

Clear All Cancel Start Upload File



* 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)

Create an Enterprise Wireless Network

1 Enterprise Wireless Network 2 Wireless Profiles

Wireless Network Name(SSID) *
DNAC-5GHZ

BROADCAST SSID: On

WIRELESS OPTION

Dual band operation (2.4GHz and 5GHz)
 Dual band operation with band select
 5GHz only

LEVEL OF SECURITY *
 WPA2 Enterprise WPA2 Personal Open

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

WLANS > Edit "DNAC-5GHZ_NF_3a30e"

General Security QoS Policy-Mapping Advanced

Profile Name: DNAC-5GHZ_NF_3a30e
Type: WLAN
SSID: DNAC-5GHZ
Status: Enabled

Security Policies: [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: 802.11a only (highlighted with a red arrow)

Interface/Interface Group(G): 123
Multicast Vlan Feature: Enabled
Broadcast SSID: Enabled
NAS-ID: none

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.

2

| Network Name (SSID) | Security | Wireless Profiles |
|---------------------|---------------|-------------------|
| ABC-PSK | wpa2_personal | abc |
| DNAc-PSK | wpa2_personal | abc |
| DNAc_SSID_1 | open | |
| DNAc_SSID_2 | open | |

1

Create an Enterprise Wireless Network

1 Enterprise Wireless Network 2 Wireless Profiles

Wireless Network Name(SSID) * DNAc-PSK

BROADCAST SSID:

WIRELESS OPTION

Dual band operation (2.4GHz and 5GHz)

Dual band operation with band select

5GHz only

LEVEL OF SECURITY *

WPA2 Enterprise WPA2 Personal Open

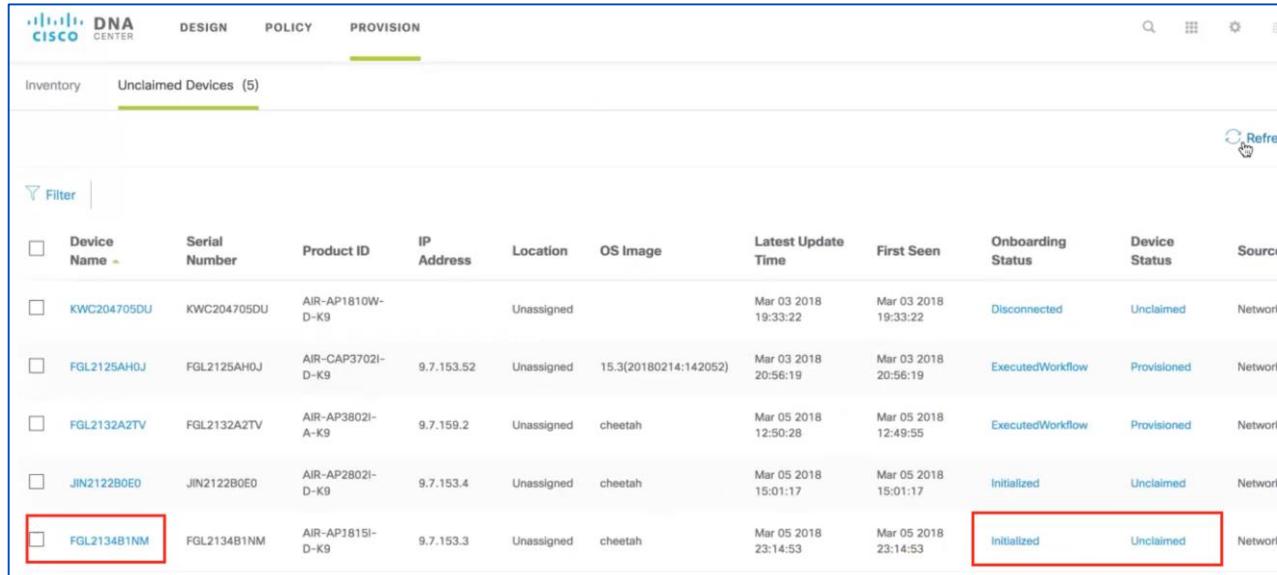
More secure
A password (Pre-Shared Key PSK with WPA2 encryption) is needed to access the wireless network

Pass Phrase*

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

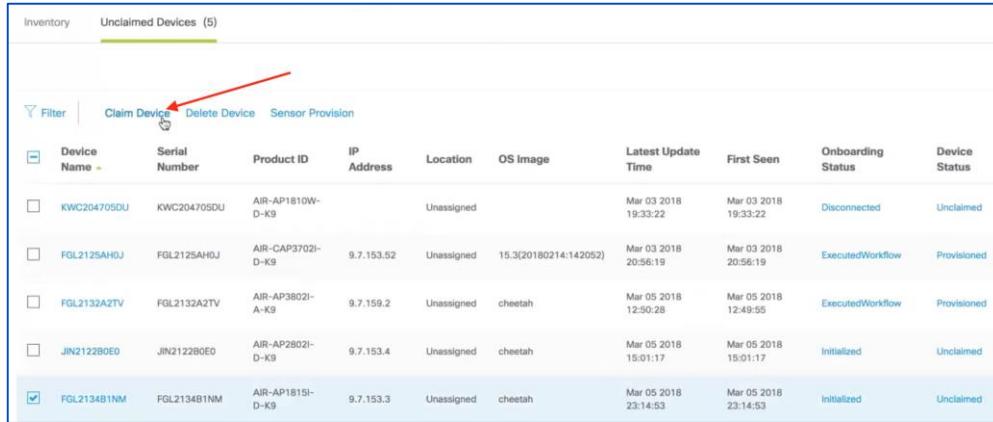


The screenshot shows the Cisco DNA Center interface with the 'Provision' tab selected. Under the 'Unclaimed Devices' section, there are five entries listed. The last entry, 'FGL2134B1NM', has its Device Name and Status columns highlighted with red boxes. The status 'Initialized' is in the Device Status column and 'Unclaimed' is in the Onboarding Status column.

| <input type="checkbox"/> | Device Name | Serial Number | Product ID | IP Address | Location | OS Image | Latest Update Time | First Seen | Onboarding Status | Device Status | Source |
|--------------------------|-------------|---------------|-------------------|------------|------------|-----------------------|----------------------|----------------------|-------------------|---------------|---------|
| <input type="checkbox"/> | KWC204705DU | KWC204705DU | AIR-AP1810W-D-K9 | | Unassigned | | Mar 03 2018 19:33:22 | Mar 03 2018 19:33:22 | Disconnected | Unclaimed | Network |
| <input type="checkbox"/> | FGL2125AH0J | FGL2125AH0J | AIR-CAP3702I-D-K9 | 9.7.153.52 | Unassigned | 15.3(20180214:142052) | Mar 03 2018 20:56:19 | Mar 03 2018 20:56:19 | ExecutedWorkflow | Provisioned | Network |
| <input type="checkbox"/> | FGL2132A2TV | FGL2132A2TV | AIR-AP3802I-A-K9 | 9.7.159.2 | Unassigned | cheetah | Mar 05 2018 12:50:28 | Mar 05 2018 12:49:55 | ExecutedWorkflow | Provisioned | Network |
| <input type="checkbox"/> | JIN2122B0E0 | JIN2122B0E0 | AIR-AP2802I-D-K9 | 9.7.153.4 | Unassigned | cheetah | Mar 05 2018 15:01:17 | Mar 05 2018 15:01:17 | Initialized | Unclaimed | Network |
| <input type="checkbox"/> | FGL2134B1NM | FGL2134B1NM | AIR-AP1815I-D-K9 | 9.7.153.3 | Unassigned | cheetah | Mar 05 2018 23:14:53 | Mar 05 2018 23:14:53 | Initialized | Unclaimed | Network |

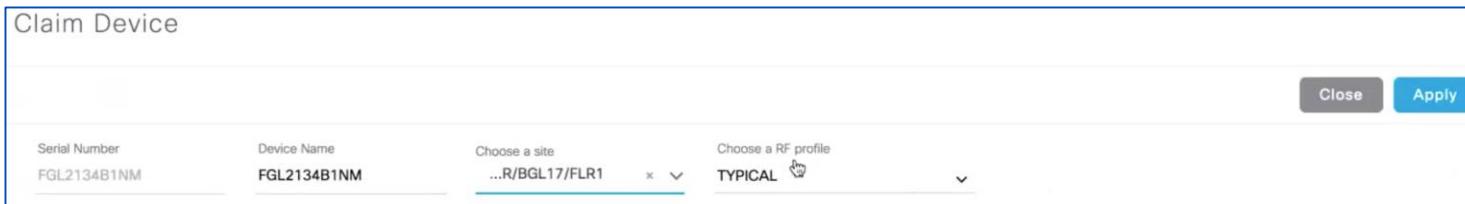
DNAC 1.2 : PnP for AP Provisioning (Cont..)

2 Select the AP and claim device



| Unclaimed Devices (5) | | | | | | | | | |
|---|---------------|-------------------|------------|------------|-----------------------|----------------------|----------------------|-------------------|---------------|
| Device Name - | Serial Number | Product ID | IP Address | Location | OS Image | Latest Update Time | First Seen | Onboarding Status | Device Status |
| <input type="checkbox"/> KWC204705DU | KWC204705DU | AIR-AP1810W-D-K9 | | Unassigned | | Mar 03 2018 19:33:22 | Mar 03 2018 19:33:22 | Disconnected | Unclaimed |
| <input type="checkbox"/> FGL2125AH0J | FGL2125AH0J | AIR-CAP3702I-D-K9 | 9.7.153.52 | Unassigned | 15.3(20180214:142052) | Mar 03 2018 20:56:19 | Mar 03 2018 20:56:19 | ExecutedWorkflow | Provisioned |
| <input type="checkbox"/> FGL2132A2TV | FGL2132A2TV | AIR-AP3802I-A-K9 | 9.7.159.2 | Unassigned | cheetah | Mar 05 2018 12:50:28 | Mar 05 2018 12:49:55 | ExecutedWorkflow | Provisioned |
| <input type="checkbox"/> JIN2122B0E0 | JIN2122B0E0 | AIR-AP2802I-D-K9 | 9.7.153.4 | Unassigned | cheetah | Mar 05 2018 15:01:17 | Mar 05 2018 15:01:17 | Initialized | Unclaimed |
| <input checked="" type="checkbox"/> FGL2134B1NM | FGL2134B1NM | AIR-AP1815I-D-K9 | 9.7.153.3 | Unassigned | cheetah | Mar 05 2018 23:14:53 | Mar 05 2018 23:14:53 | Initialized | Unclaimed |

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



Claim Device

Serial Number: FGL2134B1NM Device Name: FGL2134B1NM Choose a site: ...R/BGL17/FLR1 Choose a RF profile: TYPICAL

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

| <input type="checkbox"/> | Device Name | Serial Number | CISCO DNA CENTER | DESIGN | POLICY | PROVISION | <input type="checkbox"/> | Network Telemetry | <input type="checkbox"/> | Upgrade Status | <input type="checkbox"/> |
|--------------------------|------------------|---------------------|---------------------------------|----------------------------------|---------------|---------------------|--------------------------|-----------------------------|--------------------------|----------------------|---|
| <input type="checkbox"/> | KWC204705DU | KWC204705DU | | | | | | | | | |
| <input type="checkbox"/> | FGL2125AH0J | FGL2125AH0J | | | | | | | | | |
| <input type="checkbox"/> | FGL2132A2TV | FGL2132A2TV | | | | | | | | | |
| <input type="checkbox"/> | JIN2122B0E0 | JIN2122B0E0 | | | | | | | | | |
| <input type="checkbox"/> | FGL2134B1NM | FGL2134B1NM | | | | | | | | | |
| | | | <input type="checkbox"/> Filter | <input type="checkbox"/> Actions | | | | | | | |
| <input type="checkbox"/> | Device Name | Device Type | IP Address | Site | Serial Number | Uptime | OS Version | OS Image | Sync Status | Last Provision | Provision Status |
| <input type="checkbox"/> | AP4001.7a56.5ea4 | Unified AP | 9.7.153.53 | ...LR/BGL17/FLR1 | FGL2125AH0J | 2days 02:10:59.770 | 8.5.124.17 | Not Available | Managed | - | Not Provisioned |
| <input type="checkbox"/> | Badri-AP-2012 | Unified AP | 0.0.0.0 | | FGL1747W460 | 00:00:00.710 | 8.5.124.13 | Not Available | Unassociated | - | Not Provisioned |
| <input type="checkbox"/> | Badri-WLC203 | Wireless Controller | 10.104.178.203 | ...ISCOBLR/BGL17 | FCH1839V2E8 | 5 days, 01:00:00.00 | 8.5.124.17 | Cisco Control... Tag Golden | Managed | Mar 05 2018 12:51:11 | Success Out of Date |
| <input type="checkbox"/> | FGL2132A2TV | Unified AP | 9.7.159.2 | ...LR/BGL17/FLR1 | FGL2132A2TV | 10:26:30.770 | 8.5.124.17 | Not Available | Managed | - | Not Provisioned |
| <input type="checkbox"/> | FGL2134B1NM | Unified AP | 9.7.153.3 | ...LR/BGL17/FLR1 | FGL2134B1NM | 00:06:39.780 | 8.5.124.17 | Not Available | Managed | Mar 05 2018 11:26:01 | Success Out of Date |

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

