cisco The bridge to possible

Real World Use Cases for Deploying and Operating Cisco SD-Access

Using Cisco DNA Center

Patrick Mosimann, Technical Solutions Architect
@PaeduMosi

Agenda

- Introduction
- Real World Use Cases
  - Onboard FiaBs attached to cEdges with Plug and Play
  - Connecting FlexConnect AP to Edge Nodes with dot1x
  - Day-N CLI template handling
- Conclusion

Introduction

Cisco Webex App

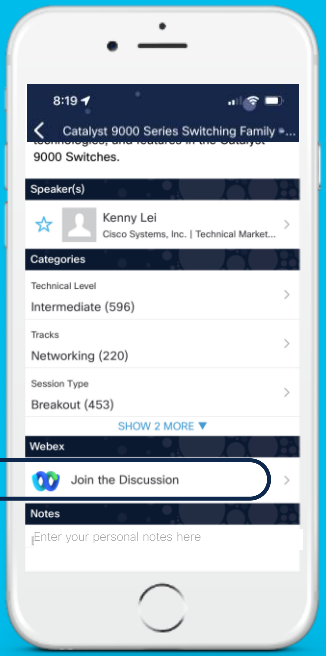
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated until February 24, 2023.



8:19

Catalyst 9000 Series Switching Family ...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

Webex

Notes

Enter your personal notes here

About Patrick...

3 Years as an End User
3 Years as a Partner
3 Years as a Competitor
7 Years at Cisco

Besides work:

- Dad
- Cook
- Traveler
- Runner
- Mountain biking
- Photographer

So... Why This Session?

Cisco SD-Access is real, it works and the time is NOW to start YOUR journey!

Cisco SD-Access journey is like climbing a mountain, small steps will bring you to the top!

The bridge to possible

SDA for everyone – now even ready for YOUR network!

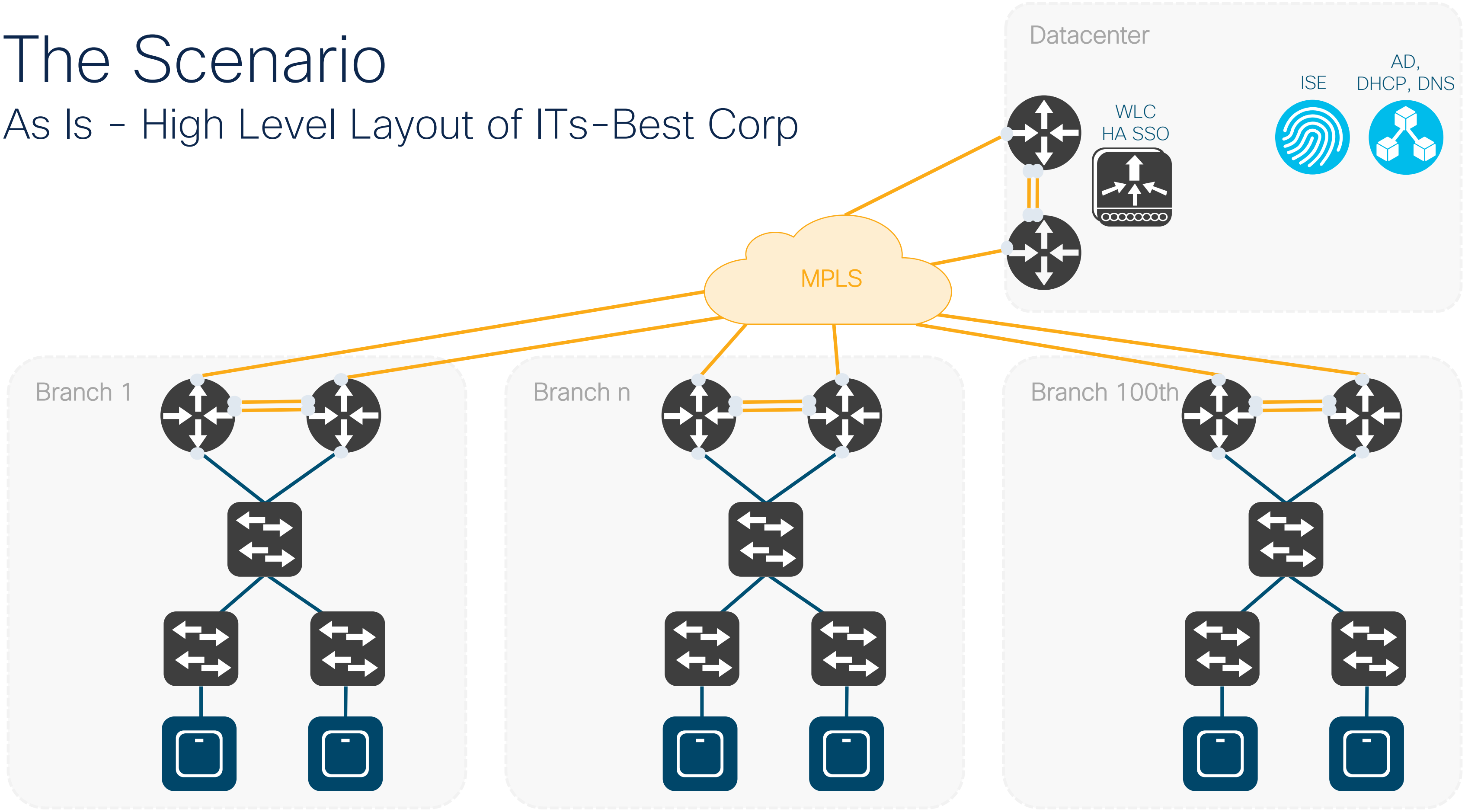
Patrick Mosimann, Technical Solutions Architect Cisco Switzerland
Peter Fuchs, Technical Solutions Architect Cisco Austria
Ivan Caduff, Technical Solutions Architect Cisco Switzerland
BRKEMT-2102

#CiscoLive

ALL IN with Cisco SD-Access at scale!

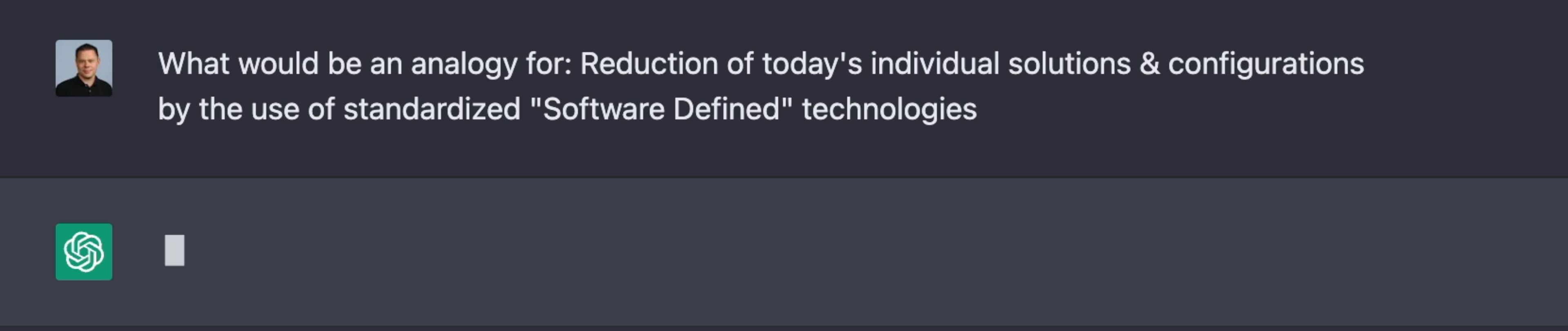
The Scenario

As Is - High Level Layout of ITs-Best Corp



Reduction of today's individual solutions & configurations using standardized "Software Defined" technologies

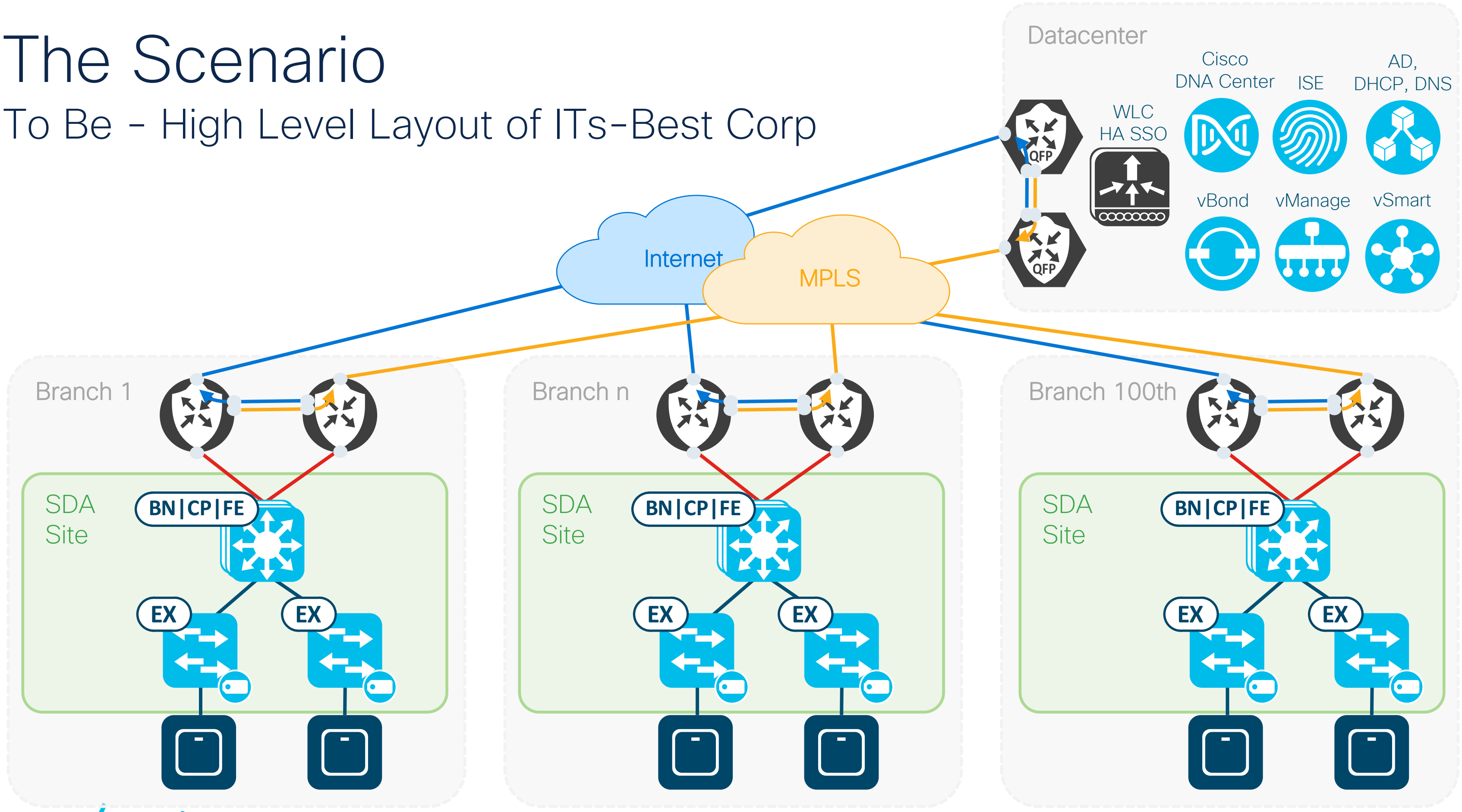
Project Goal of ITs-Best Corp



What would be an analogy for: Reduction of today's individual solutions & configurations by the use of standardized "Software Defined" technologies

The Scenario

To Be - High Level Layout of ITs-Best Corp



The Scenario

Challenges of ITs-Best Corp

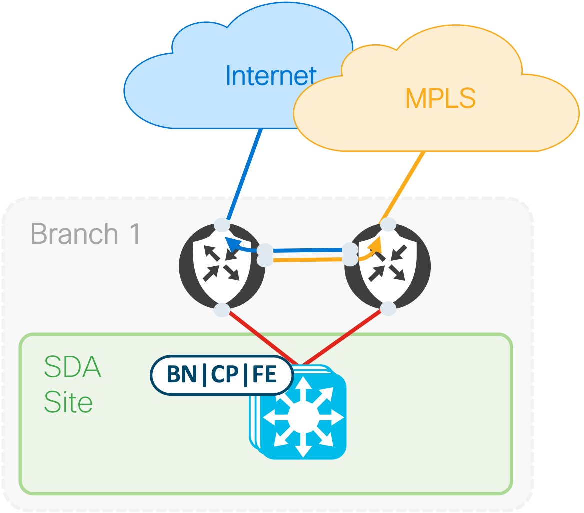
- Day-0
  - Onboard Fabric in Box (FiaB) for many small sites
- Day-1
  - Connect FlexConnect AP to the Fabric with dot1x
- Day-N
  - Handling multiple CLI Templates in Cisco DNA Center

Onboard FiaBs attached to cEdges with Plug and Play

Use Case Starting Situation

0

Onboard FiaBs attached to cEdges with Plug and Play

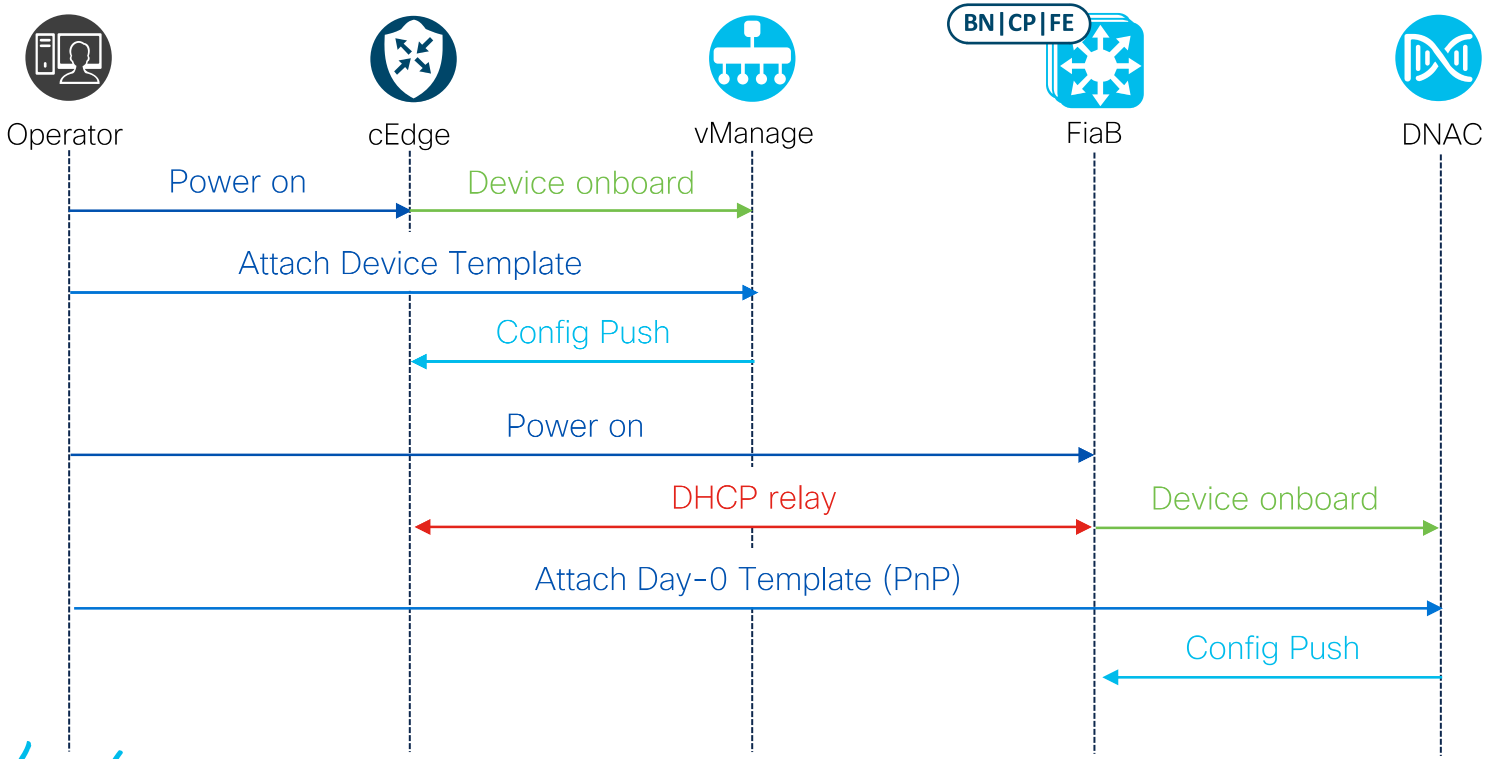


- Cisco SD-WAN Overlay with multiple VPNs and using one for underlay of SD-Access
- Onboard FiaBs for many small sites attached to a Cisco SD-WAN router
- Define a standardized workflow which can be automated

Reference

Use Case Workflow (1/2)

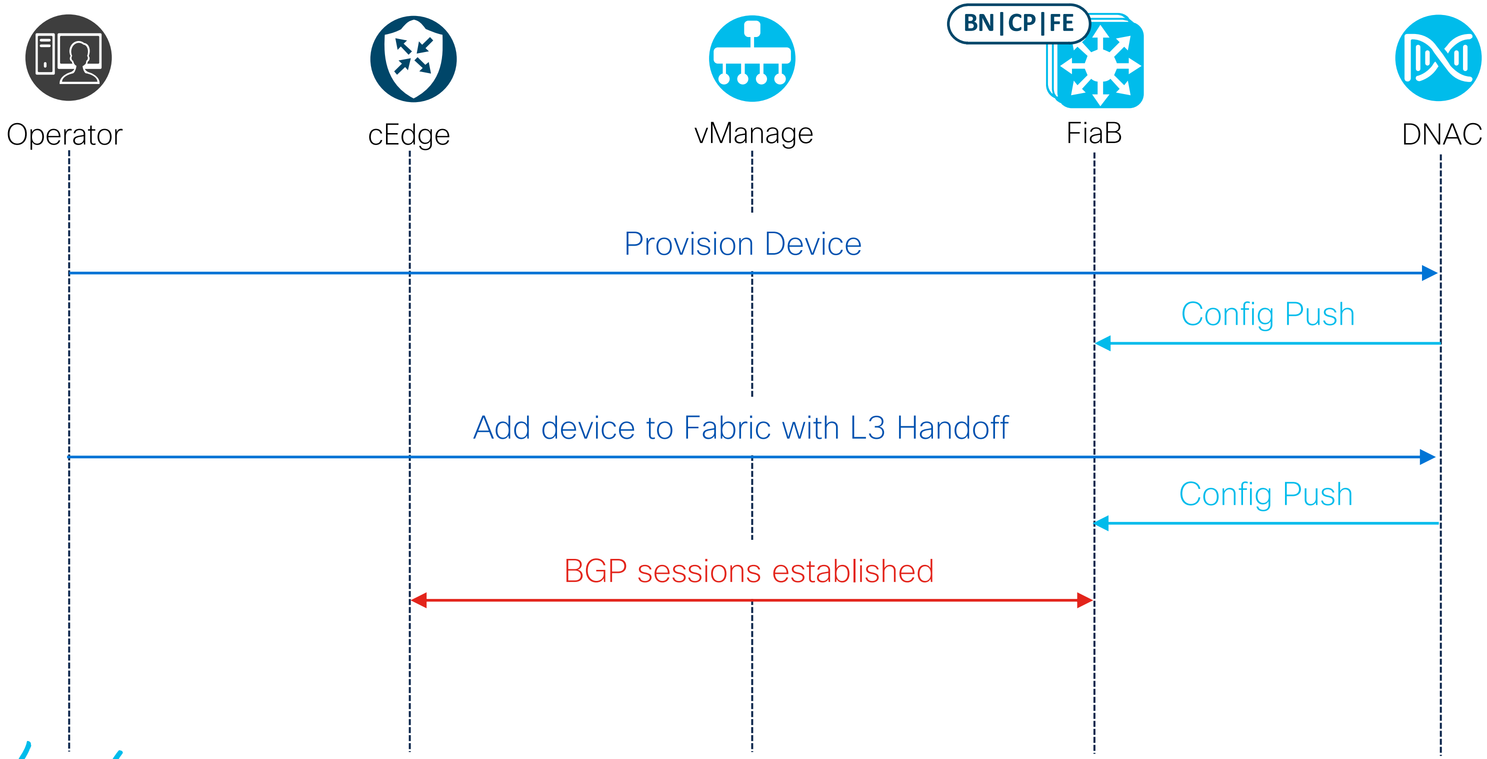
Onboard FiaBs attached to cEdges with Plug and Play



Reference

Use Case Workflow (2/2)

Onboard FiaBs attached to cEdges with Plug and Play



Reference

Cisco DNA Center Plug and Play

PnP Access VLAN 1

```
interface gi1/0/1
 switchport mode access
```

```
interface gi1/0/1
!
interface Vlan 1
 ip address dhcp
```

PnP Trunk Uplink

```
pnp start-up vlan 20
!
interface gi1/0/1
 switchport mode trunk
```

```
interface gi1/0/1
 switchport mode trunk
!
interface Vlan 20
 ip address dhcp
```

PnP Management Port

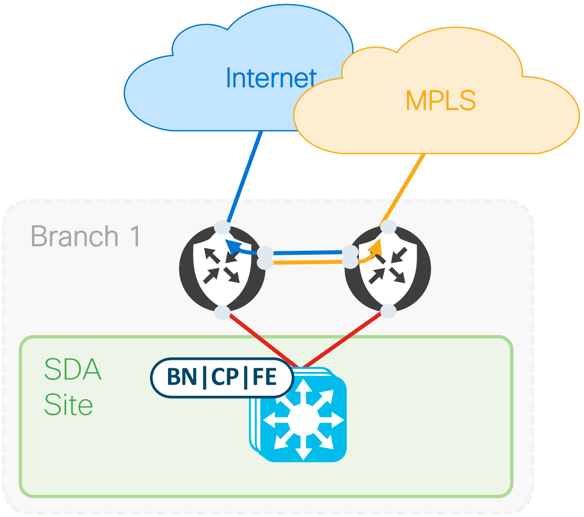
```
interface gi1/0/1
 switchport mode access
```

```
interface gi0/0
 vrf forwarding Mgmt-vrf
 ip address dhcp
```

https://blogs.cisco.com/developer/dna-center-pnp-day-0

Use Case Challenges

Onboard FiaBs attached to cEdges with Plug and Play



- In Cisco vManage the CLI command `pnp startup-vlan xx` is not qualified for a CLI add-on feature template and it’s not possible to push the config with a feature template

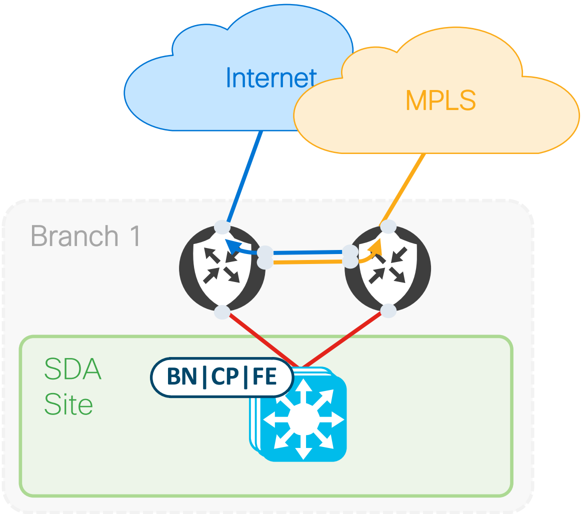
- When you onboard the FiaB via the management interface (Gig0/0) you need to change over to in-band management for SDA.

- Trunk Port is needed for Border Handoff

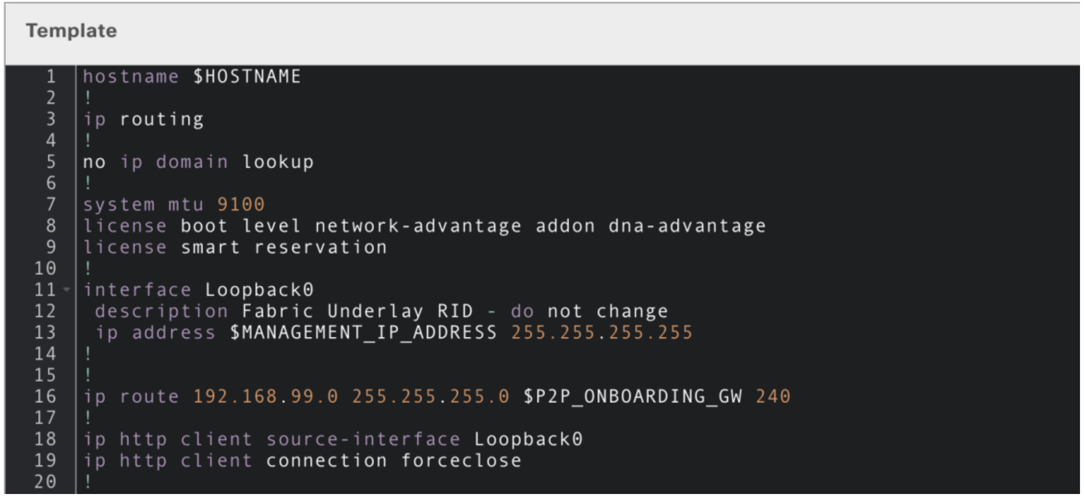
Demo Day-0

Use Case Conclusion (1/2)

Onboard FiaBs attached to cEdges with Plug and Play



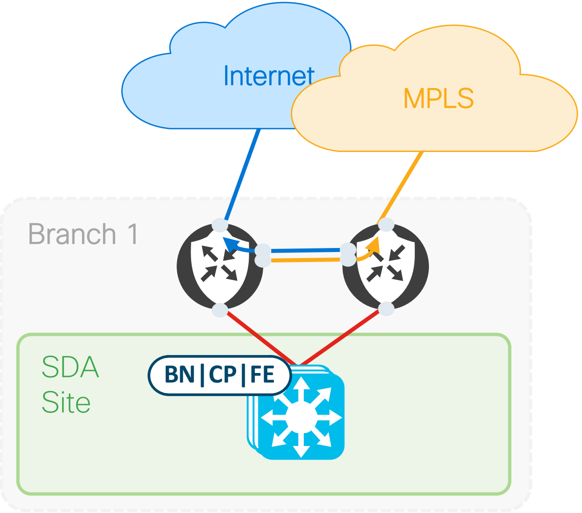
- Onboard FiaB using PnP with Access VLAN 1
- Static Route from cEdge toward Loopback0
- Change Uplink Port to a Trunk Port using EEM script in Onboard Template:

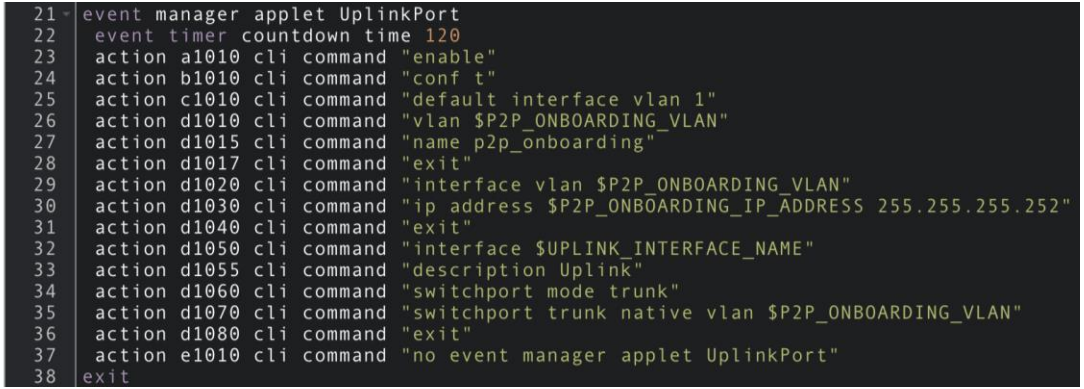

Template

```
hostname $HOSTNAME
!
ip routing
!
no ip domain lookup
!
system mtu 9100
license boot level network-advantage addon dna-advantage
license smart reservation
!
interface Loopback0
 description Fabric Underlay RID - do not change
 ip address $MANAGEMENT_IP_ADDRESS 255.255.255.255
!
!
ip route 192.168.99.0 255.255.255.0 $P2P_ONBOARDING_GW 240
!
ip http client source-interface Loopback0
ip http client connection forceclose
!
```

Use Case Conclusion (2/2)

Onboard FiaBs attached to cEdges with Plug and Play





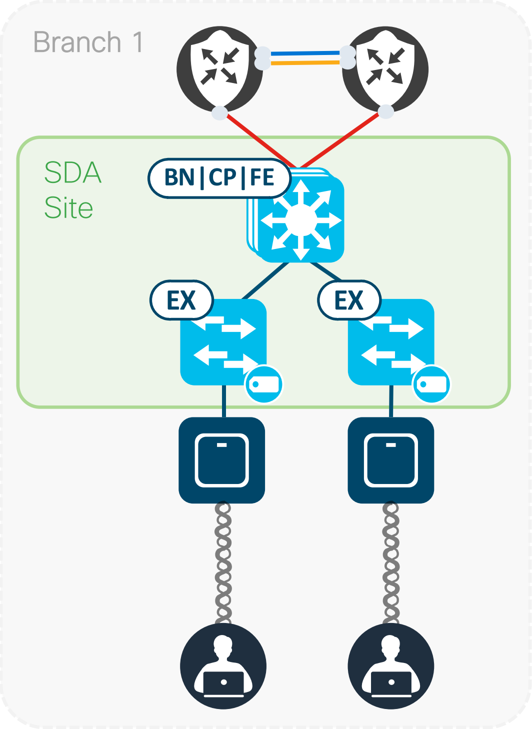
```
event manager applet UplinkPort
 event timer countdown time 120
 action a1010 cli command "enable"
 action b1010 cli command "conf t"
 action c1010 cli command "default interface vlan 1"
 action d1010 cli command "vlan $P2P_ONBOARDING_VLAN"
 action d1015 cli command "name p2p_onboarding"
 action d1017 cli command "exit"
 action d1020 cli command "interface vlan $P2P_ONBOARDING_VLAN"
 action d1030 cli command "ip address $P2P_ONBOARDING_IP_ADDRESS 255.255.255.252"
 action d1040 cli command "exit"
 action d1050 cli command "interface $UPLINK_INTERFACE_NAME"
 action d1055 cli command "description Uplink"
 action d1060 cli command "switchport mode trunk"
 action d1070 cli command "switchport trunk native vlan $P2P_ONBOARDING_VLAN"
 action d1080 cli command "exit"
 action e1010 cli command "no event manager applet UplinkPort"
exit
```

Connecting FlexConnect AP to Edge Nodes with dot1x

Use Case Starting Situation

Connecting FlexConnect AP to Edge Nodes with dot1x

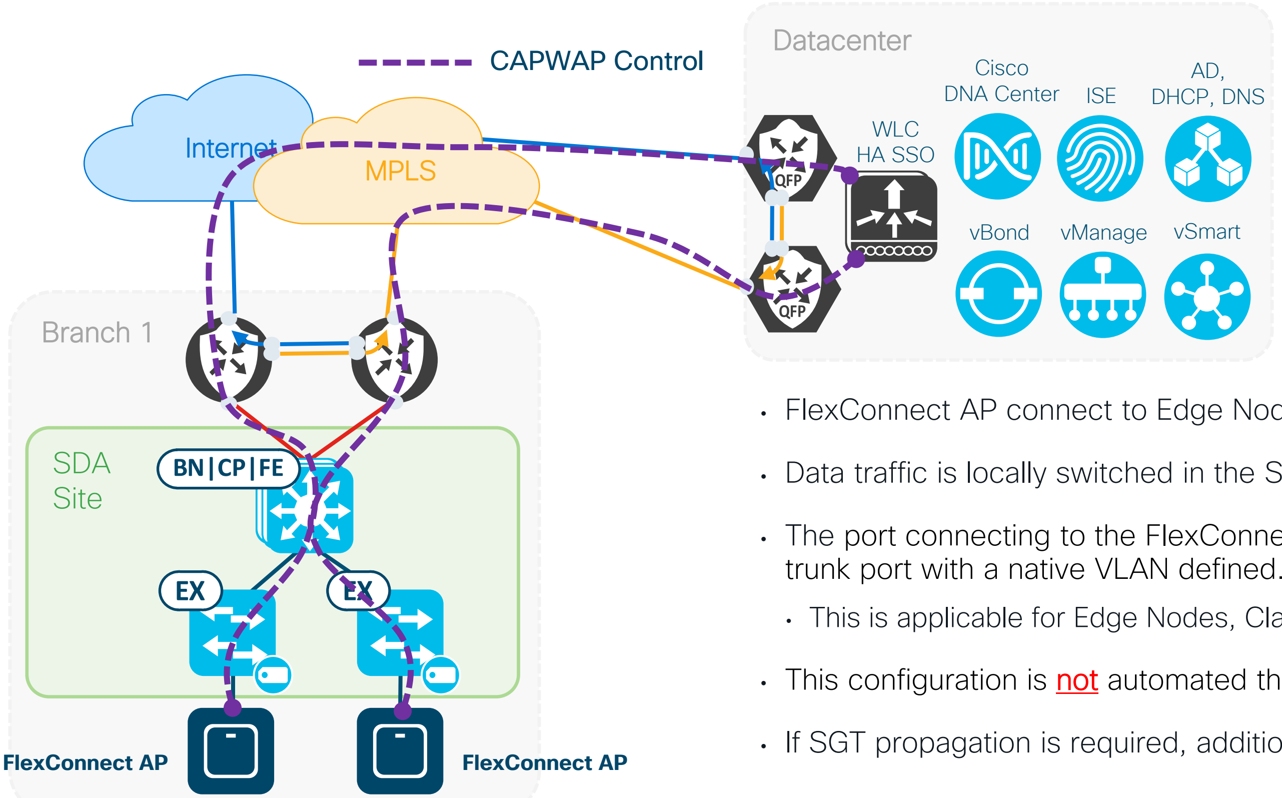
1



- FlexConnect Over-the-Top Wireless and Controllers in the DC
  - Trunk Port for FlexConnect AP
- Introduction of Identity Based Networking Services (IBNS 2.0)
  - Access Points Authentication

Reference

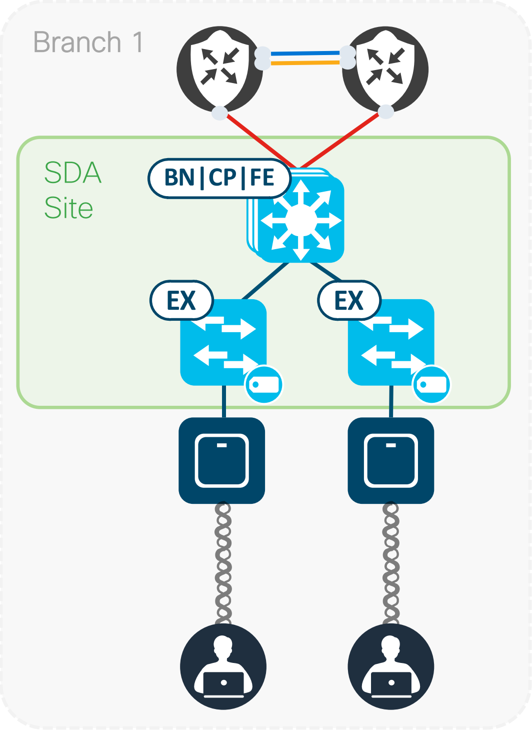
FlexConnect Over-the-Top



- FlexConnect AP connect to Edge Nodes.
- Data traffic is locally switched in the SD-Access fabric.
- The port connecting to the FlexConnect AP must be configurated as a trunk port with a native VLAN defined.
  - This is applicable for Edge Nodes, Classic, and Policy Extended Nodes.
- This configuration is not automated through SD-Access workflows.
- If SGT propagation is required, additional configuration is needed.

Use Case Challenges

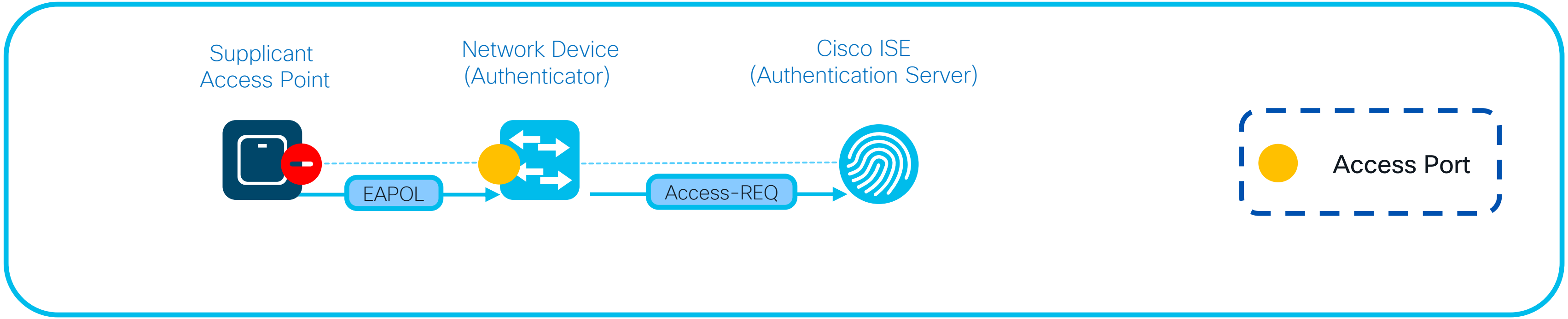
Connecting FlexConnect AP to Edge Nodes with dot1x



- The port connecting to the FlexConnect AP must be configured as a trunk port with a native VLAN and port needs to be configured with dot1x for Access Points Authentication
- This configuration is not automated through SD-Access workflows.

Interface Template (1/3)

Network Edge Authentication Topology (NEAT)


Supplicant Access Point
Network Device (Authenticator)
Cisco ISE (Authentication Server)
EAPOL
Access-REQ
● Access Port

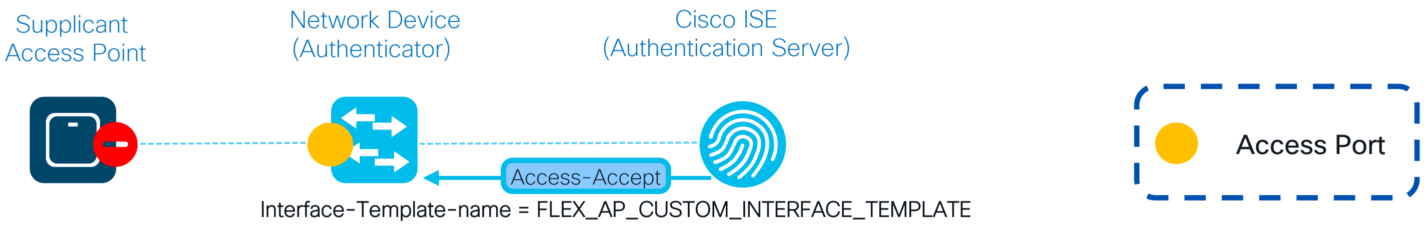
Before Supplicant Access Point Authentication

```
interface GigabitEthernet1/0/1
 switchport mode access
 device-tracking attach-policy IPDT_POLICY
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 source template DefaultWiredDot1xClosedAuth
 ...
end
```

Reference

Interface Template (2/3)

Network Edge Authentication Topology (NEAT)



Interface-Template-name = FLEX_AP_CUSTOM_INTERFACE_TEMPLATE

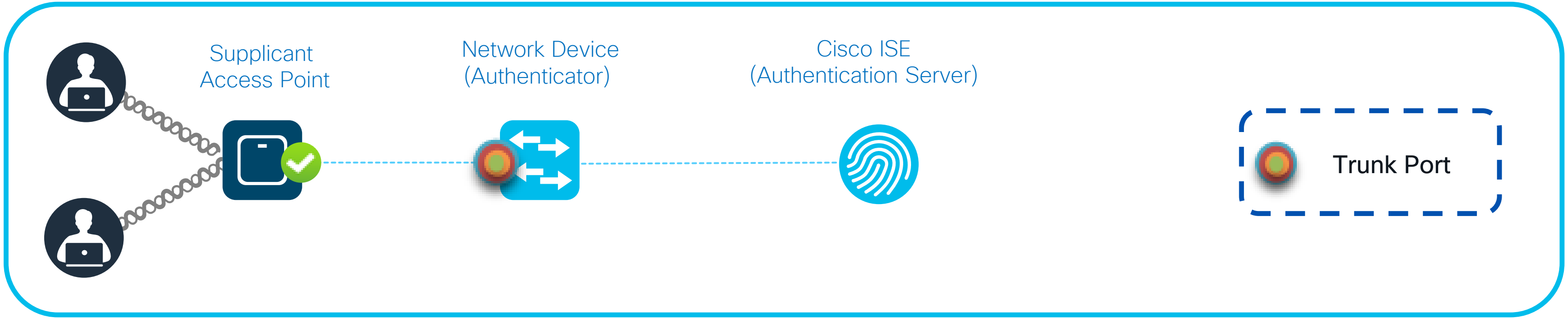
Before Supplicant Access Point Authentication

```
interface GigabitEthernet1/0/1
 switchport mode access
 device-tracking attach-policy IPDT_POLICY
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 source template DefaultWiredDot1xClosedAuth
 ...
end
```

Reference

Interface Template (3/3)

Network Edge Authentication Topology (NEAT)



Before Supplicant Access Point Authentication	After Supplicant Switch Authentication

Before Supplicant Access Point Authentication

```
interface GigabitEthernet1/0/1
 switchport mode access
 device-tracking attach-policy IPDT_POLICY
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 source template DefaultWiredDot1xClosedAuth
 ...
end
```

After Supplicant Switch Authentication

```
interface GigabitEthernet1/0/1
 description FLEX-AP
 switchport trunk native vlan 1021
 switchport trunk allowed vlan 1021-1023
 switchport mode trunk
 access-session host-mode multi-host
 ...
end
```

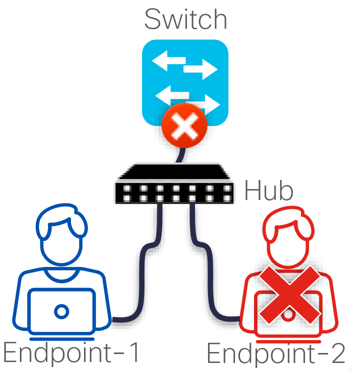
Reference

Switchport Host Modes

Single Host Mode

Only 'one' MAC Address is allowed. Second MAC Address causes Security Violation

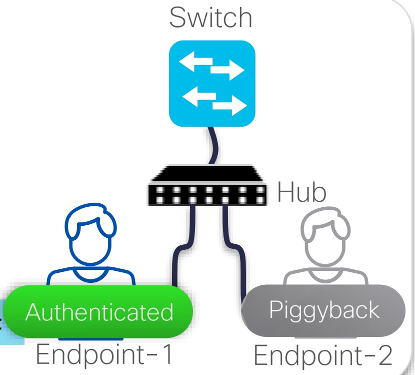
```
access-session host-mode single-host
```



Multi-Host Mode

1st MAC Address is authenticated. 2nd endpoint piggybacks on 1st MAC Address authentication and bypasses authentication

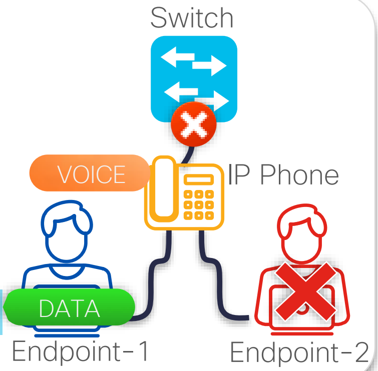
```
access-session host-mode multi-host
```



Multi-Domain Mode

Each domain (Voice or Data) authenticates one MAC address. 2nd MAC address on each domain causes security violation

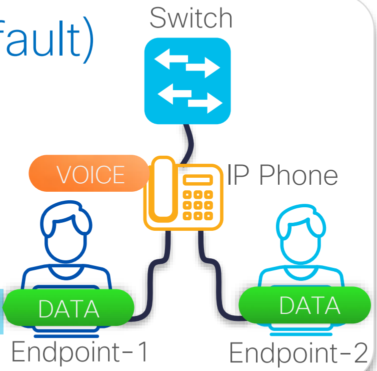
```
access-session host-mode multi-domain
```



Multi-Auth Mode(Default)

Voice domain authenticates one MAC address. Data domain authenticates multiple MAC addresses. dACL or single VLAN Assignment for all devices are supported

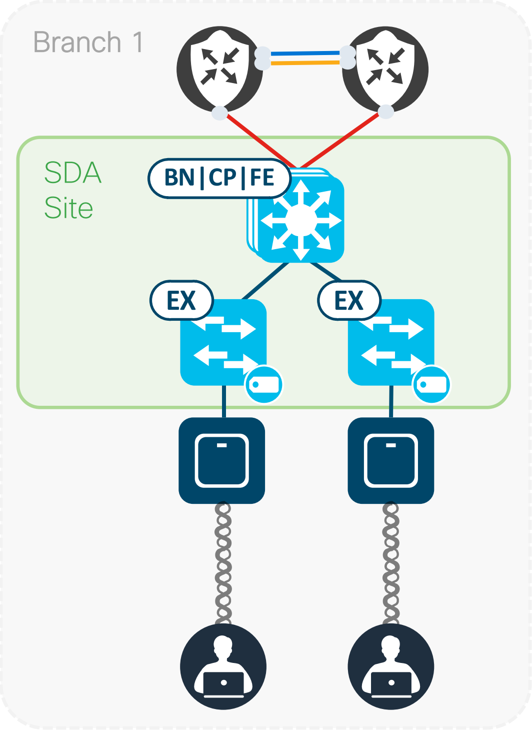
```
access-session host-mode multi-auth
```



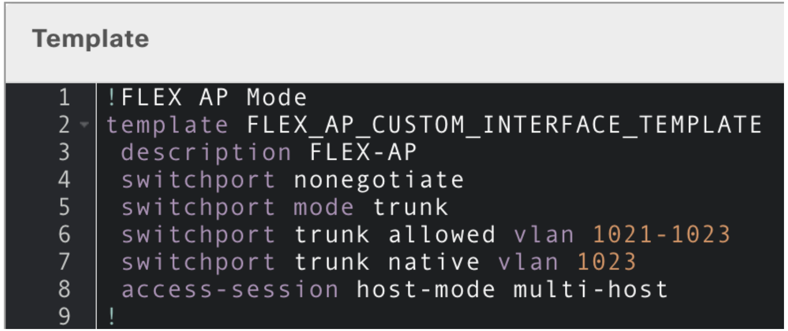
Demo Day-1

Use Case Conclusion

Connecting FlexConnect AP to Edge Nodes with dot1x



- Authenticate Access Point via dot1x or MAB
- Return interface template as an Authentication Result
  - cisco-av-pair= interface-template-name= FLEX_AP_CUSTOM_INTERFACE_TEMPLATE
- Deploy below interface template via Day-N template in DNAC before onboard first Access Point:

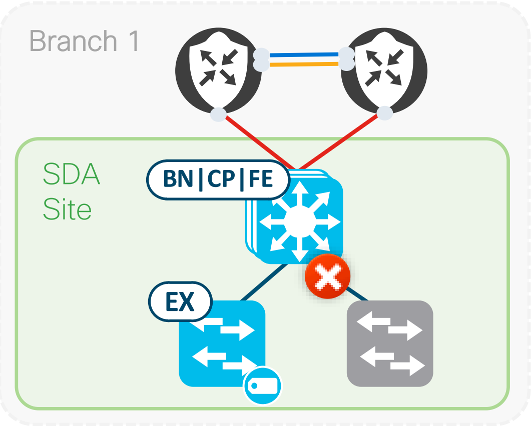


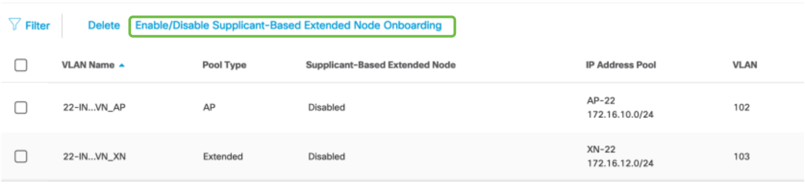
```
!FLEX AP Mode
template FLEX_AP_CUSTOM_INTERFACE_TEMPLATE
 description FLEX-AP
 switchport nonegotiate
 switchport mode trunk
 switchport trunk allowed vlan 1021-1023
 switchport trunk native vlan 1023
 access-session host-mode multi-host
!
```

SUPER BONUS
BLECARNIVAL
MARBLECARNIVAL

Bonus Use Case

Connecting Supplicant-Based Extended Node (SBEN) with dot1x





□	VLAN Name ▲	Pool Type	Supplicant-Based Extended Node	IP Address Pool	VLAN
□	22-IN...VN_AP	AP	Disabled	AP-22 172.16.10.0/24	102
□	22-IN...VN_XN	Extended	Disabled	XN-22 172.16.12.0/24	103

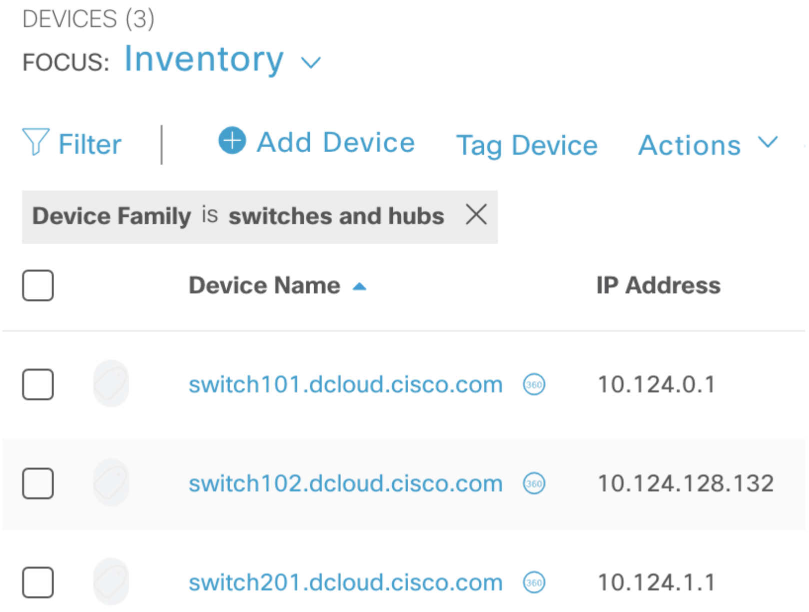
- Supplicant-Based Extended Nodes (SBEN) onboarding is designed to onboard EN using PNP in a zero-trust environment.
- Cisco ISE authorizes the **MAB** request with limited access. Cisco DNA Center provisions the ACL and **interface template** on fabric devices.
- Cisco DNA Center as part of the PnP workflow provisions dot1x credentials and enables **dot1x supplicant** on the extended node.

Cisco DNA Center User Guide, Configure Supplicant-Based Extended Nodes

Day-N CLI template handling

Use Case Starting Situation

Day-N CLI template handling



DEVICES (3)

FOCUS: Inventory ⌄

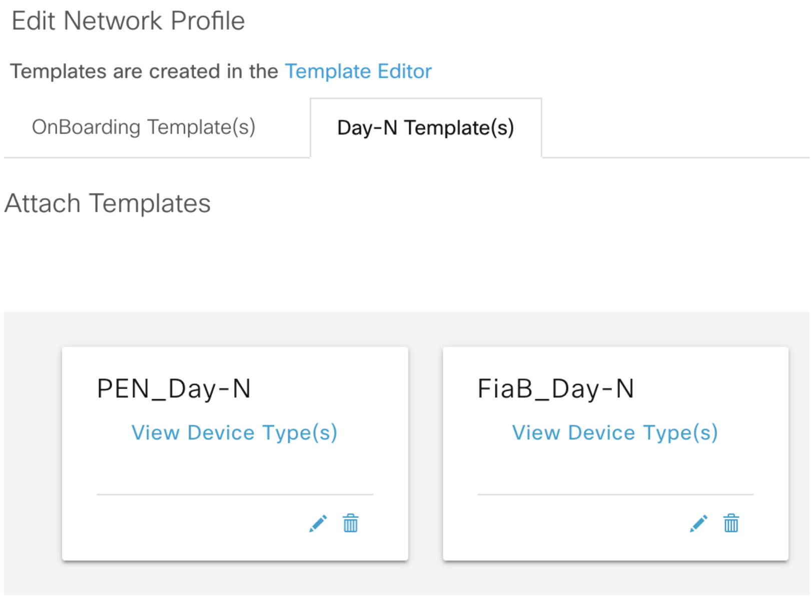
Device Family is switches and hubs ✕

□	Device Name ▲	IP Address
□	switch101.dcloud.cisco.com	10.124.0.1
□	switch102.dcloud.cisco.com	10.124.128.132
□	switch201.dcloud.cisco.com	10.124.1.1

- Get a fast overview of Fabric Device Role in the Inventory List
- Attach CLI templates based on this Device Role

Use Case Challenges

Day-N CLI template handling



Edit Network Profile

Templates are created in the Template Editor

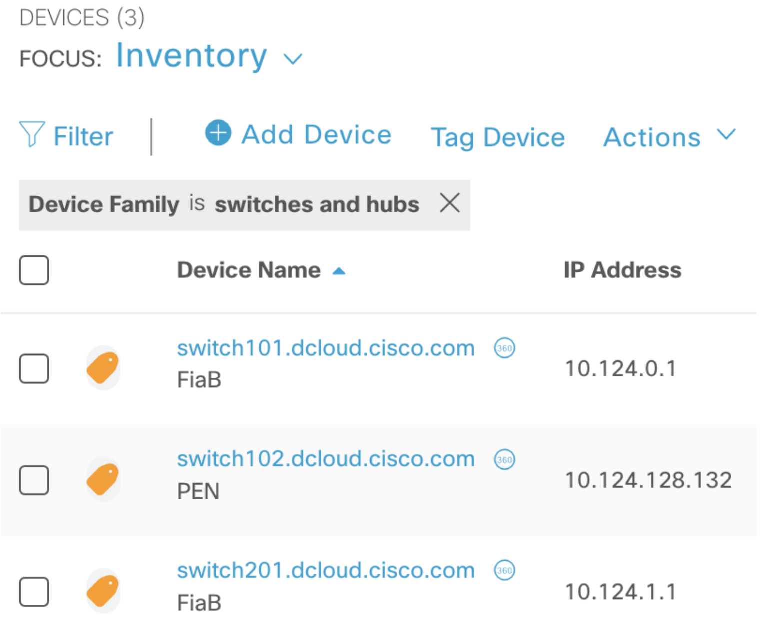
Attach Templates

- Need different Day-N Templates based on Fabric Device Role
- Switch Model is the same

Demo Day-N

Use Case Conclusion (1/2)

Day-N CLI template handling



DEVICES (3)

FOCUS: Inventory

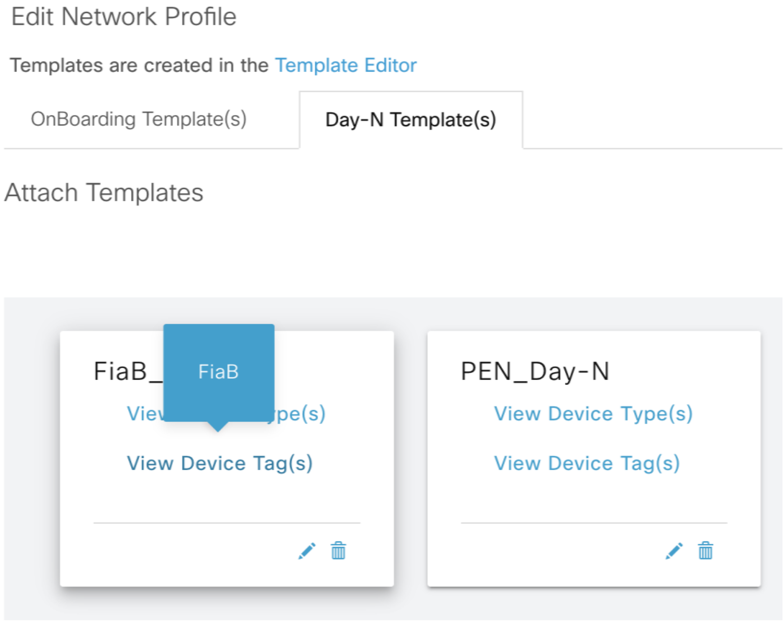
Device Family is switches and hubs

□		Device Name	IP Address
□		switch101.dcloud.cisco.com FiaB	10.124.0.1
□		switch102.dcloud.cisco.com PEN	10.124.128.132
□		switch201.dcloud.cisco.com FiaB	10.124.1.1

- Create a Device Tag for Fiab and Policy Extend Nodes (PEN)
- Tag Device based on Fabric Device Role

Use Case Conclusion (2/2)

Day-N CLI template handling



Edit Network Profile

Templates are created in the Template Editor

Attach Templates

- Select the corresponding Device Tag when attaching the Template in the Network Profile

Conclusion

Conclusion

- Day-0
  - Onboard Fabric in Box (FiaB) for many small sites
- Day-1
  - Connect FlexConnect AP to the Fabric with dot1x
- Day-N
  - Handling multiple CLI Templates in Cisco DNA Center

ALL IN with Cisco SD-Access at scale!

Complete your 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 (open from 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 Session Catalog and clicking the "Attendee Dashboard” at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

- Book your one-on-one Meet the Engineer meeting.
- Attend Introduction to Infrastructure as Code for Cisco DNA Center with Terraform - BRKOPS-1183 tomorrow at 13:30

The bridge to possible

Thank you

cisco Live!