
cisco Live!
TURN
IT
UP
#CiscoLive

The bridge to possible

Updated Cisco SD-Access Migration Strategies

Jerome Dolphin, Technical Marketing Engineer
CCIE#17805 (R&S, SEC), CCDE#2013::3

BRKENS-2008

Agenda

- Introduction
- Flexible Cisco SD-Access
- New Feature Summary
- Example Migration
- Layer 2 Access
- From Enterprise MPLS to Cisco SD-Access
- Conclusion

Introduction

Introduction

- The comprehensive history:
  - Locate DGTL-BRKENS-3822 on www.ciscolive.com
  - Enjoy (?) 3 hours of migration tools, strategies and demos

Introduction

- The comprehensive history:
  - Locate DGTL-BRKENS-3822 on www.ciscolive.com .
  - Enjoy (?) 3 hours of migration tools, strategies and demos.
- Added for your entertainment: background antics!

Introduction

- The plan for today:
  - Important updates to the comprehensive history in 45 minutes…

Introduction

- The plan for today:
  - Important updates to the comprehensive history in 45 minutes…

There will be Questions

- This presentation breaks the rules, for the right reasons, I hope.
- Ask the Cisco Sales or CX teams for help.
- Leverage the Cisco SD-Access communities: http://cs.co/sda-community .

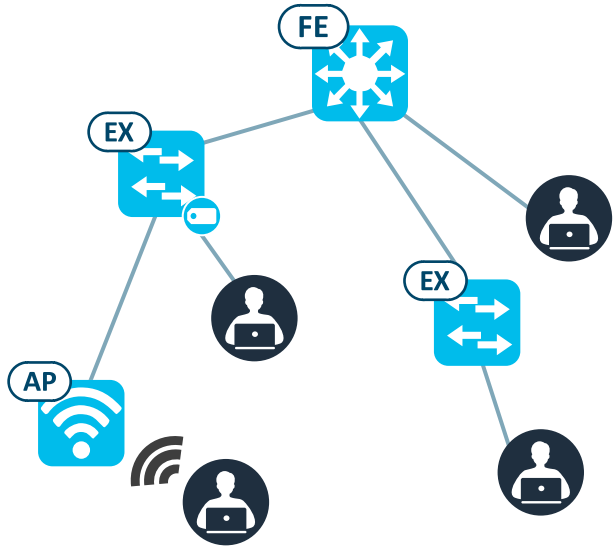
The “Best” Solution

- Cisco SD-Access to the Campus Edge of the network is the gold standard of Automation, Segmentation, Assurance and Analytics.

Automation
Segmentation
Assurance
Analytics

The “Best” Solution

- Cisco SD-Access to the Campus Edge of the network is the gold standard of Automation, Segmentation, Assurance and Analytics.
- This means every endpoint in the campus or branch is connected to one of the following:
  1. Fabric Edge Node
  2. Policy Extended Node
  3. Extended Node
  4. Fabric-Enabled Wireless SSID



Automation
Segmentation
Assurance
Analytics

The Reality of Some Networks

- Cisco SD-Access to the entire Campus Edge is not always possible on day 1, and sometimes, it may never possible.

Nomenclature

- Macro-segmentation. Separation of routing or switching domains. Traditionally a VRF or VLAN, but in the context of this presentation, L3VN and L2VN.
- Endpoint Analytics. Endpoint visibility solution. Gathers context from your network and peripherals to classify endpoints. Classifications can then be referenced in ISE to assign an SGT or a profile. Aka EA.
- Group Based Policy Analytics. An application in DNA Center which helps administrators understand group to group interactions and build Group Based Policies. Groups can be SGTs, ISE profiles or Stealthwatch Host Groups.
- Scalable Group Tag. A tag associated or attached to IP traffic from entities with equal security policy requirements. Aka SGT.
- Group Based Policy. Permit/Deny connectivity controls between different SGTs. Aka GBP or micro-segmentation.
- Fabric. In the context of this presentation, an overlay-based connectivity solution implemented by a Cisco SD-Access Border Nodes, Control Plane Nodes, Edge Nodes and optionally Fabric-Enabled Wireless.

Flexible Cisco SD-Access

cisco Live!

Flexible Cisco SD-Access

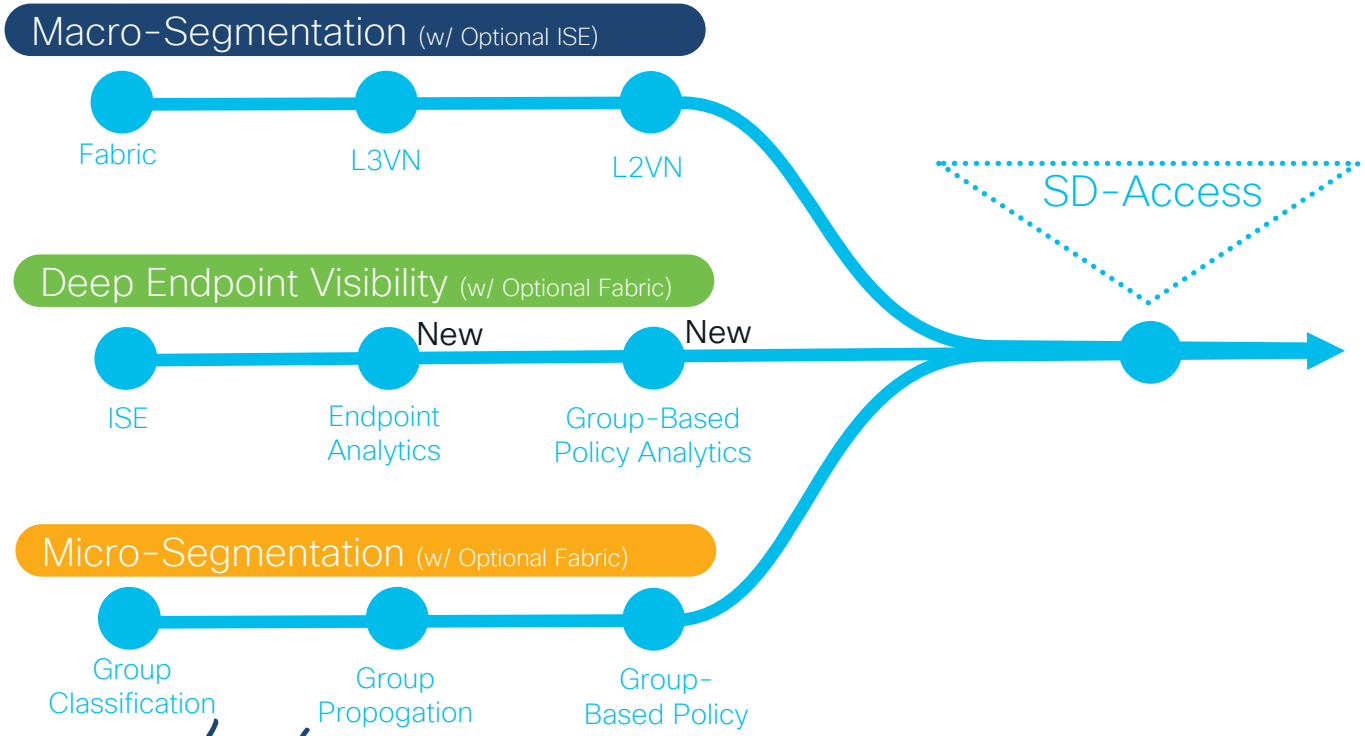
What and When?

Feature	DNA Center
Interop with traditional Cisco or 3rd party switching	2.1.2 – Available now
Fabric without ISE	2.1.2 – Available now
Add ISE to an operational fabric	2.1.2 – Available now
Customizable VLAN ID	2.2.2 – Q2CY2021
L2VN (Layer 2 Virtual Network)	Q3CY2021
Overlapping IP range in L3VN (Layer 3 Virtual Network)	Q3CY2021

Flexible Cisco SD-Access

Why?

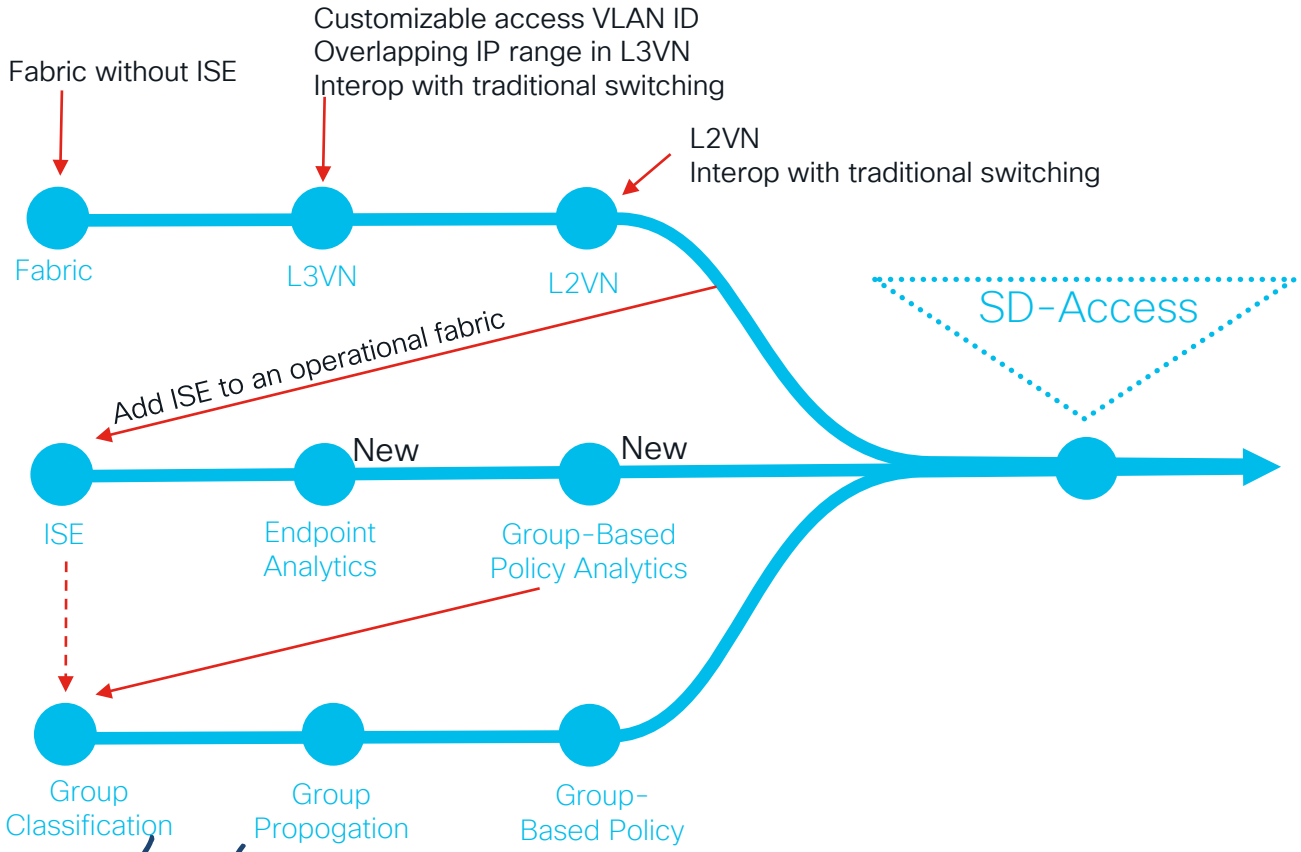
Customizable and phased implementation of an extensible network, capable of delivering a suite of Cisco value vectors best aligned to your needs.



- **Network Segmentation:** Leverage Fabric to provide L3, L2 Connectivity & network operations across Multi-Site LAN & WLAN with integrated identity-context
- **Endpoint Visibility:** Identify and group endpoints. Map their interactions and define access policies
- **Group Segmentation:** Enforce group-based access policies and secure network through segmentation

Flexible Cisco SD-Access

How?



- **Network Segmentation:** Leverage Fabric to provide L3, L2 Connectivity & network operations across Multi-Site LAN & WLAN with integrated identity-context
- **Endpoint Visibility:** Identify and group endpoints. Map their interactions and define access policies
- **Group Segmentation:** Enforce group-based access policies and secure network through segmentation

New Feature Summary

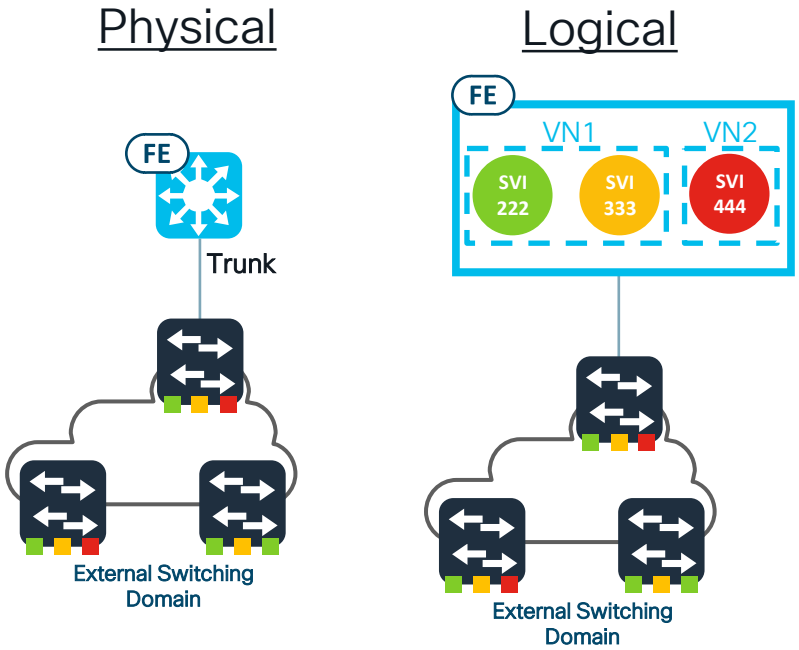
Custom VLAN ID

Summary

- Edge Node access VLAN ID is customizable to match external switching domain.
- Available in DNA Center 2.2.2 – ETA Q2CY2021.

More Details

- VLAN name will no longer be auto-generated by DNA Center. Efficient ISE policy design requires common VLAN names at different fabric sites.
- Custom VLAN ID also enhances L2 and L3 handoff flexibility on Border Node.
- See BRKENS-2006 or future Custom VLAN release collateral for more information.



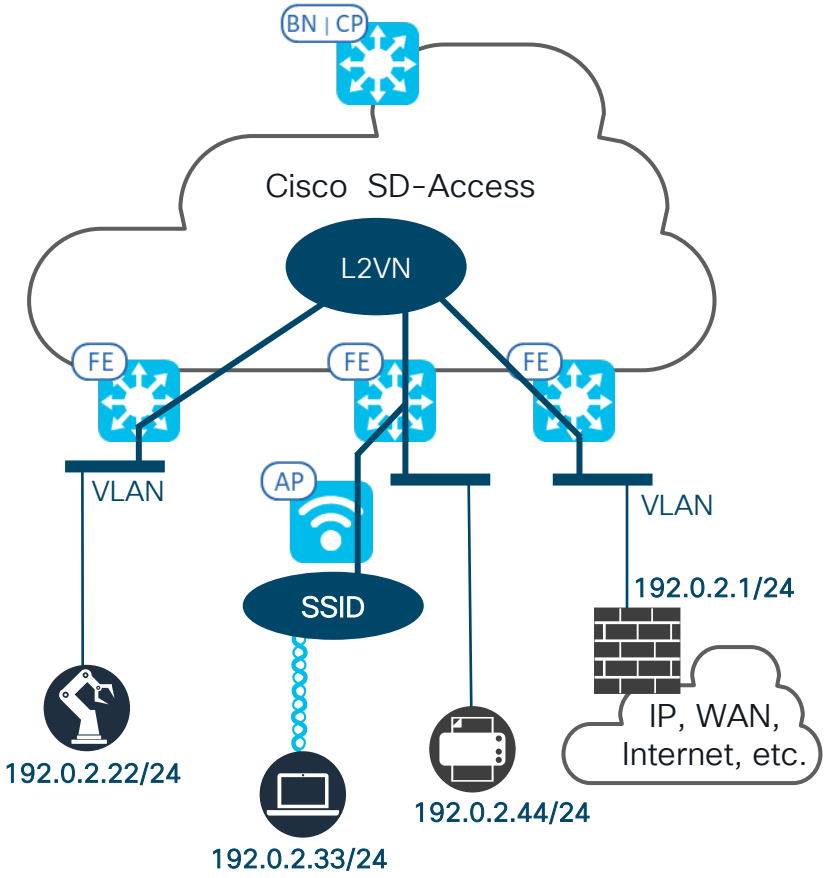
Layer 2 Virtual Network

Summary

- L2VN provides Layer 2 connectivity between wired and wireless endpoints, analogous to VLAN in traditional networking.
- L2VN is fabric site wide and topology agnostic.
- Used when IP gateway is not required within the SD-Access fabric.
- L2VN was always automatically created when IP gateway was inside the fabric (IP Pool anycast gateway).
- Availability ETA Q3CY2021.

More Details

- Specific functionality, design considerations and prerequisites will be shared in future L2VN release collateral.



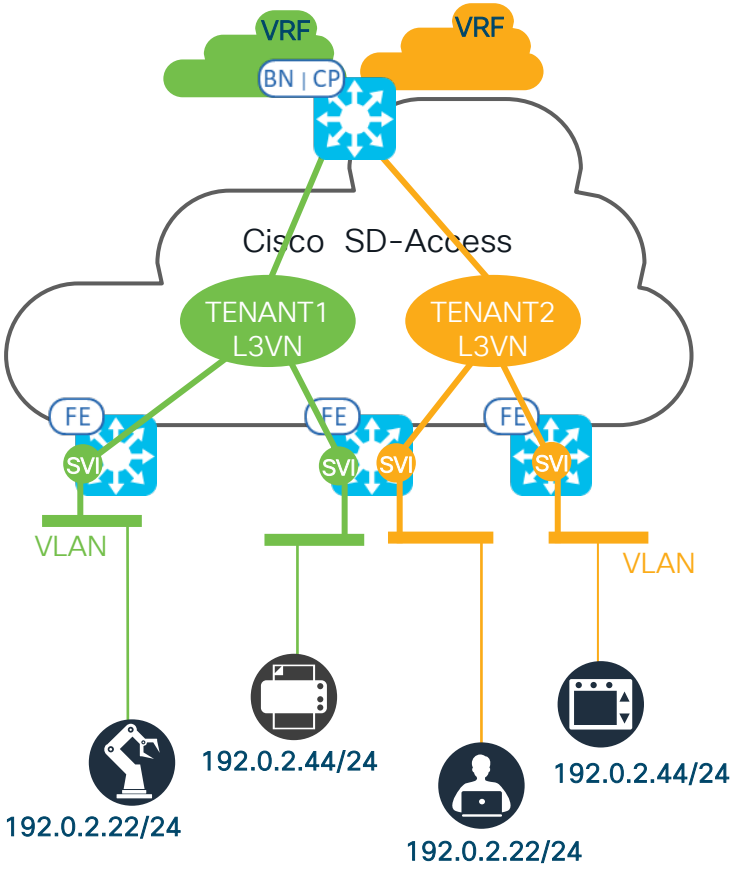
Layer 3 Virtual Networks with Overlapping IP Ranges

Summary

- Overlapping IP range can operate in different L3VNs in the same fabric site.
- Availability ETA Q3CY2021.

More Details

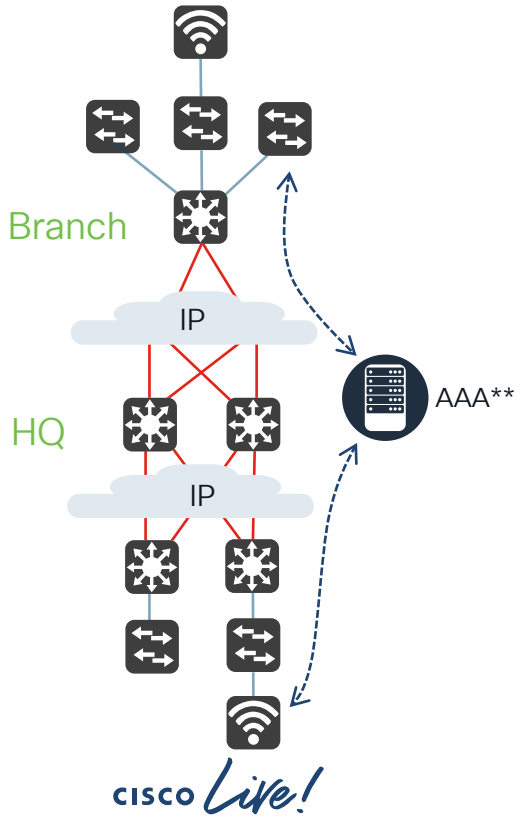
- Specific functionality, design considerations and prerequisites will be shared in future L3VN overlapping IP range release collateral.



Example Migration

Cisco SD-Access for Macro-Segmentation
Example

Step 0. Existing network.

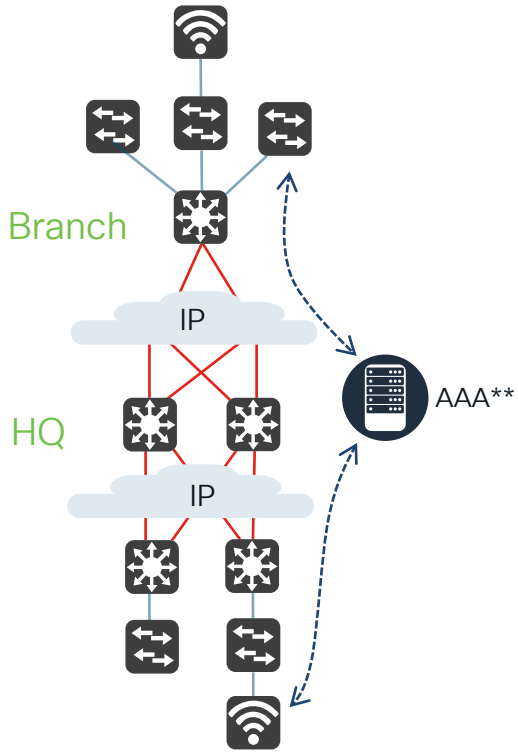


**ISE or 3rd party AAA

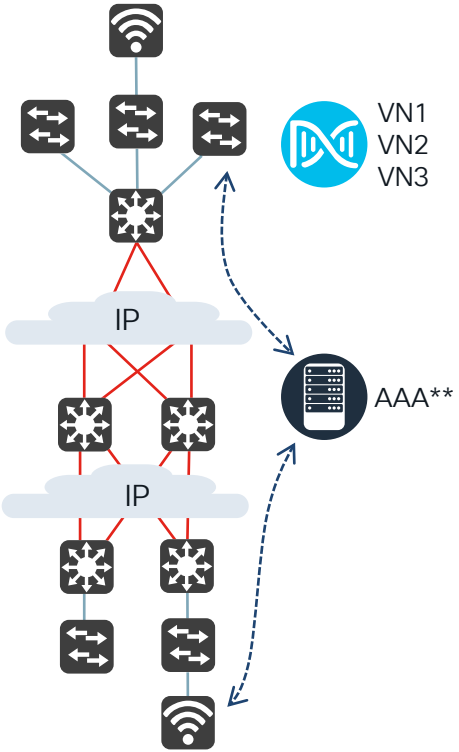
Cisco SD-Access for Macro-Segmentation

Example

Step 0. Existing network.



Step 1. Add Cisco DNA Center. Define VNs.



**ISE or 3rd party AAA

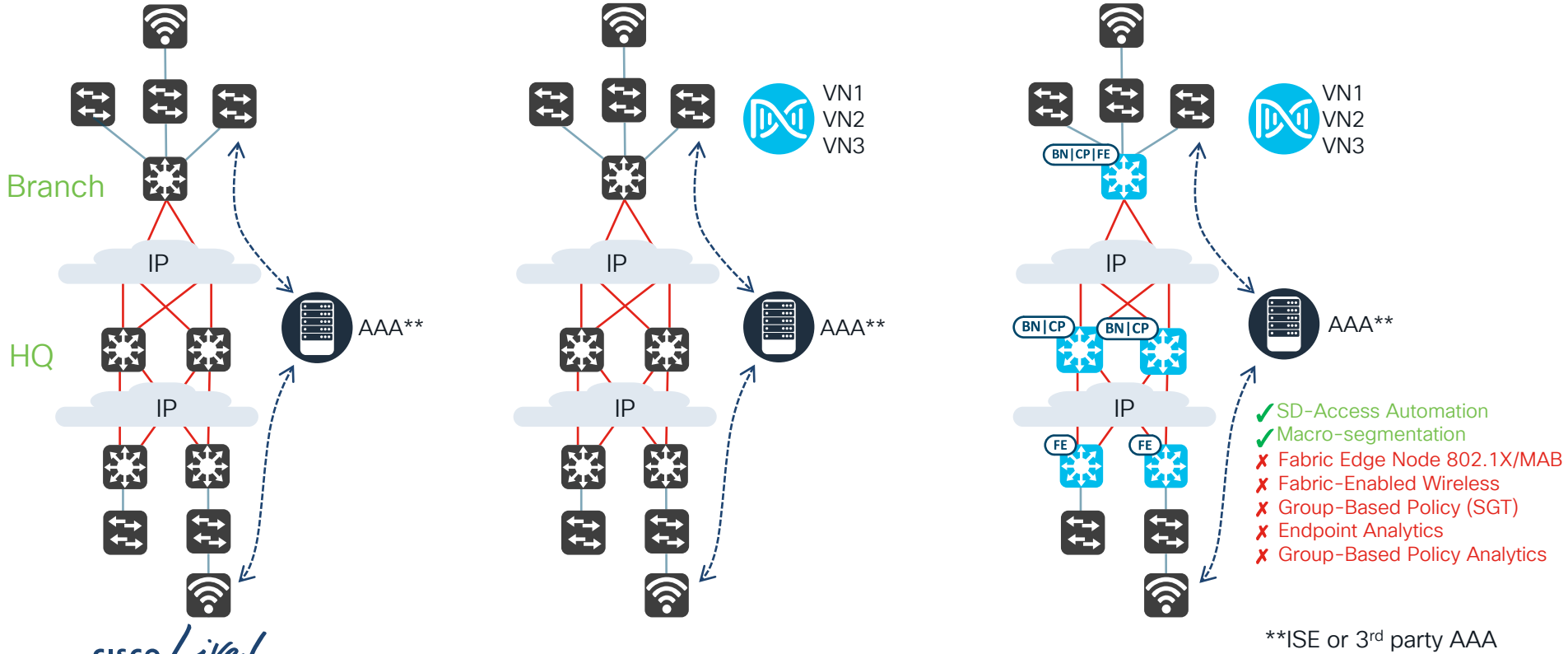
Cisco SD-Access for Macro-Segmentation

Example

Step 0. Existing network.

Step 1. Add Cisco DNA Center. Define VNs.

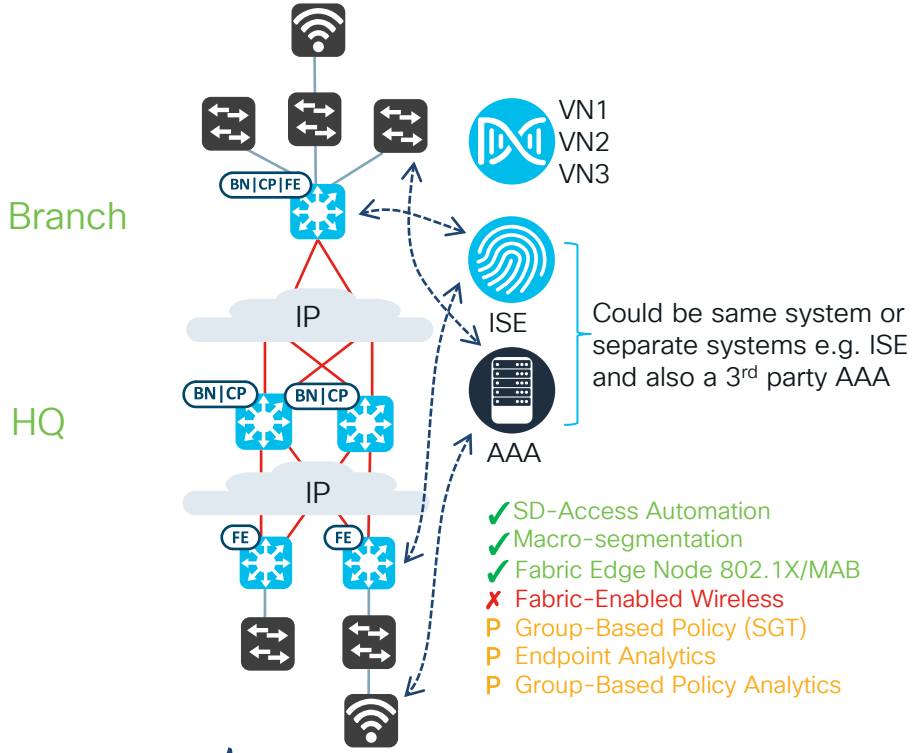
Step 2. Provision Fabric Nodes for VN-based macro-segmentation



**ISE or 3rd party AAA

Cisco SD-Access and Network Access Control
Example

Step 3. Integrate DNA Center and ISE. Provision ISE to existing SD-Access fabric as AAA server

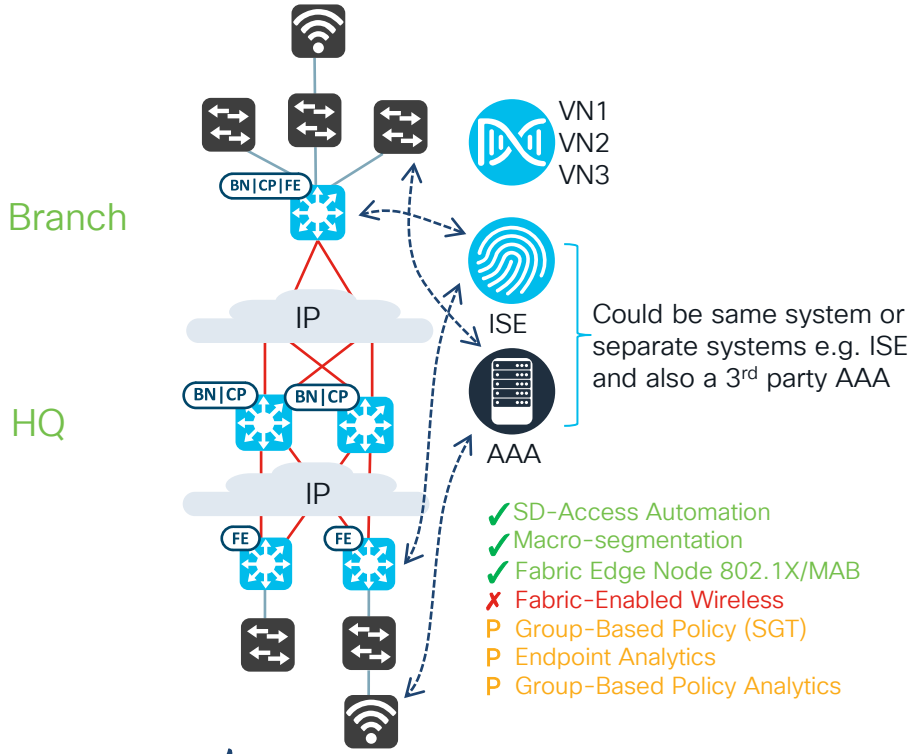


✓ SD-Access Automation
✓ Macro-segmentation
✓ Fabric Edge Node 802.1X/MAB
✗ Fabric-Enabled Wireless
P Group-Based Policy (SGT)
P Endpoint Analytics
P Group-Based Policy Analytics

P = Partial. Situationally dependent

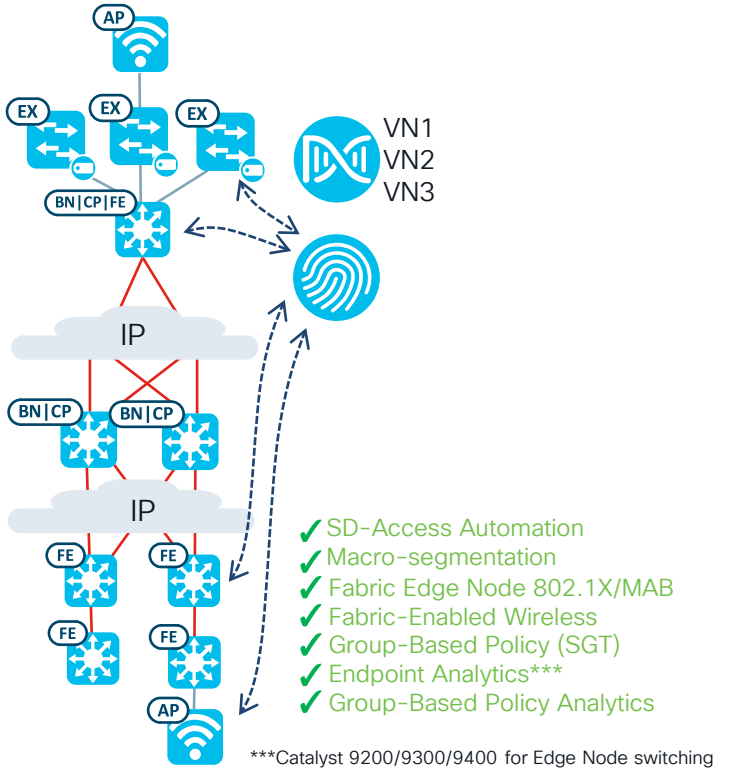
Cisco SD-Access Everywhere for Full Functionality
Example

Step 3. Integrate DNA Center and ISE. Provision ISE to existing SD-Access fabric as AAA server



P = Partial. Situationally dependent

Step 4. Upgrade switching and wireless to SD-Access

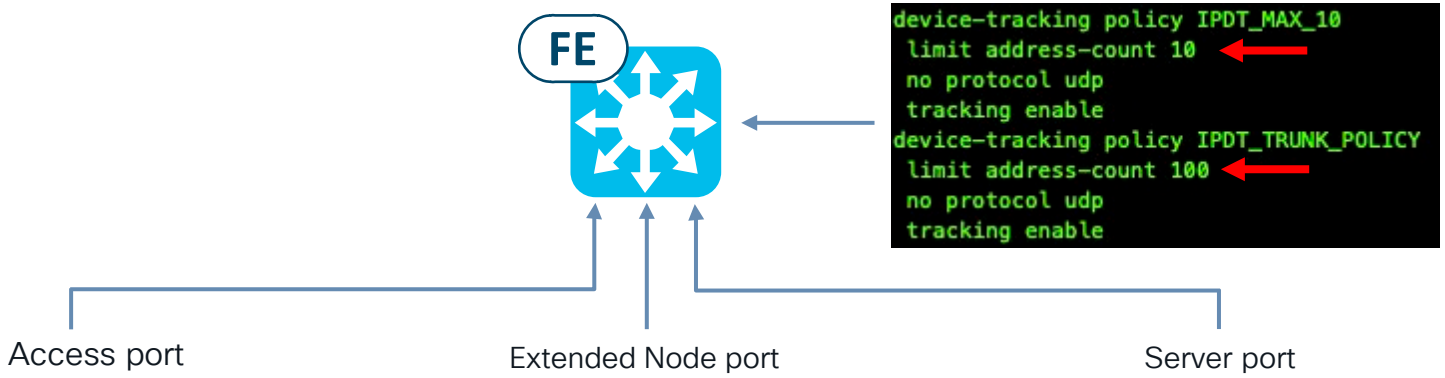


***Catalyst 9200/9300/9400 for Edge Node switching
***Telemetry Traffic Appliance for Fabric-Enabled Wireless

Layer 2 Access

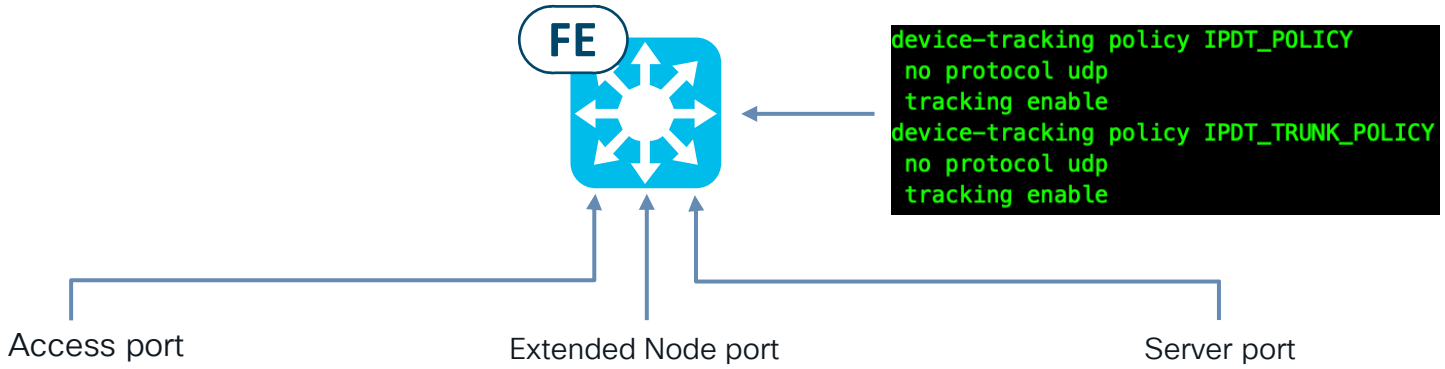
Fabric Edge Node IP Address Limits Removed

- Previously on an Edge Node:
  - Access ports were limited to ten (10) IP addresses
  - Server ports and Extended Node ports were limited to 100 IP addresses



Fabric Edge Node IP Address Limits Removed

- As of Cisco DNA Center 2.1.2, all Edge Node port IP address limits have been removed.



Fabric Edge Node IP Address Limits Removed

- As of Cisco DNA Center 2.1.2, all Edge Node port IP address limits have been removed.


```
device-tracking policy IPDT_POLICY
 no protocol udp
 tracking enable
device-tracking policy IPDT_TRUNK_POLICY
 no protocol udp
 tracking enable
```

Access port

Extended Node port

Server port

```
interface GigabitEthernet1/0/13
 switchport mode access
 device-tracking attach-policy IPDT_POLICY
 access-session inherit disable interface-template-sticky
 access-session inherit disable autoconf
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 no macro auto processing
 source template DefaultWiredDot1xClosedAuth
 spanning-tree portfast
 spanning-tree bpduguard enable
```

Fabric Edge Node IP Address Limits Removed

- As of Cisco DNA Center 2.1.2, all Edge Node port IP address limits have been removed.


```
device-tracking policy IPDT_POLICY
 no protocol udp
 tracking enable
device-tracking policy IPDT_TRUNK_POLICY
 no protocol udp
 tracking enable
```

Access port

```
interface GigabitEthernet1/0/13
 switchport mode access
 device-tracking attach-policy IPDT_POLICY
 access-session inherit disable interface-template-sticky
 access-session inherit disable autoconf
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 no macro auto processing
 source template DefaultWiredDot1xClosedAuth
 spanning-tree portfast
 spanning-tree bpduguard enable
```

Extended Node port

```
interface Port-channel1
 switchport mode trunk
interface GigabitEthernet2/0/6
 switchport mode trunk
 channel-group 1 mode desirable
interface GigabitEthernet2/0/7
 switchport mode trunk
 channel-group 1 mode desirable
```

Server port

Fabric Edge Node IP Address Limits Removed

- As of Cisco DNA Center 2.1.2, all Edge Node port IP address limits have been removed.


```
device-tracking policy IPDT_POLICY
 no protocol udp
 tracking enable
device-tracking policy IPDT_TRUNK_POLICY
 no protocol udp
 tracking enable
```

Access port

```
interface GigabitEthernet1/0/13
 switchport mode access
 device-tracking attach-policy IPDT_POLICY
 access-session inherit disable interface-template-sticky
 access-session inherit disable autoconf
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 no macro auto processing
 source template DefaultWiredDot1xClosedAuth
 spanning-tree portfast
 spanning-tree bpduguard enable
```

Extended Node port

```
interface Port-channel1
 switchport mode trunk
interface GigabitEthernet2/0/6
 switchport mode trunk
 channel-group 1 mode desirable
interface GigabitEthernet2/0/7
 switchport mode trunk
 channel-group 1 mode desirable
```

Server port

```
interface GigabitEthernet1/0/14
 switchport mode trunk
 device-tracking attach-policy IPDT_TRUNK_POLICY
 access-session inherit disable interface-template-sticky
 access-session inherit disable autoconf
 no macro auto processing
```

Fabric Edge Node IP Address Limits Removed

- In Cisco DNA Center 2.2.2*, “Server” port has been renamed to “Trunk” port.

*ETA Q2 CY 2021


```
device-tracking policy IPDT_POLICY
 no protocol udp
 tracking enable
device-tracking policy IPDT_TRUNK_POLICY
 no protocol udp
 tracking enable
```

Access port

```
interface GigabitEthernet1/0/13
 switchport mode access
 device-tracking attach-policy IPDT_POLICY
 access-session inherit disable interface-template-sticky
 access-session inherit disable autoconf
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 no macro auto processing
 source template DefaultWiredDot1xClosedAuth
 spanning-tree portfast
 spanning-tree bpduguard enable
```

Extended Node port

```
interface Port-channel1
 switchport mode trunk
interface GigabitEthernet2/0/6
 switchport mode trunk
 channel-group 1 mode desirable
interface GigabitEthernet2/0/7
 switchport mode trunk
 channel-group 1 mode desirable
```

~~Server~~ Trunk port

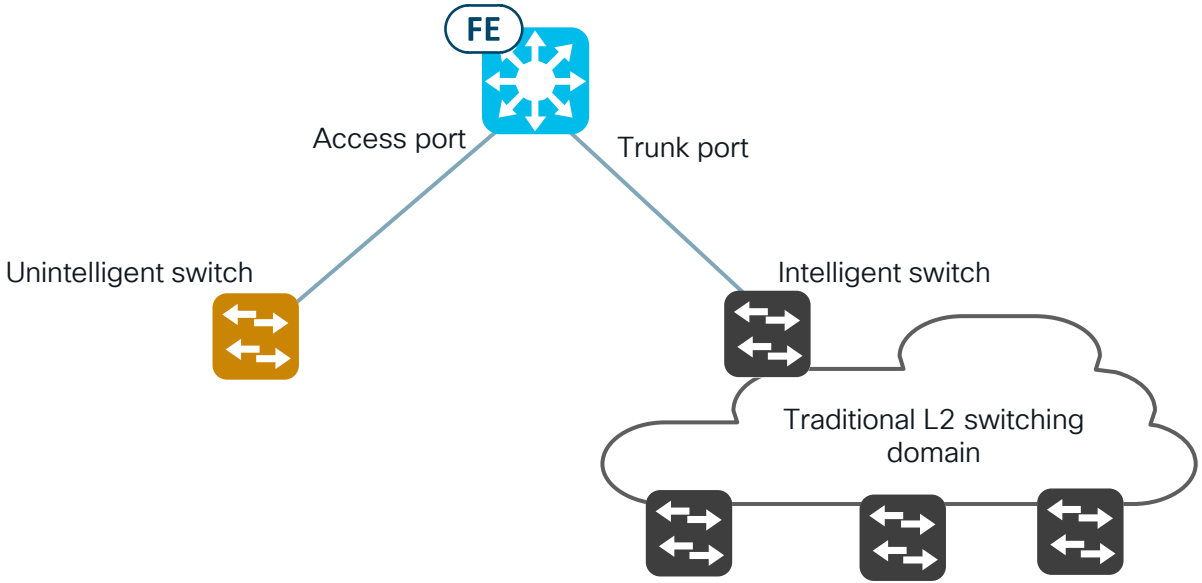
```
interface GigabitEthernet1/0/14
 switchport mode trunk
 device-tracking attach-policy IPDT_TRUNK_POLICY
 access-session inherit disable interface-template-sticky
 access-session inherit disable autoconf
 no macro auto processing
```

Fabric Edge Node Address Limits Removed

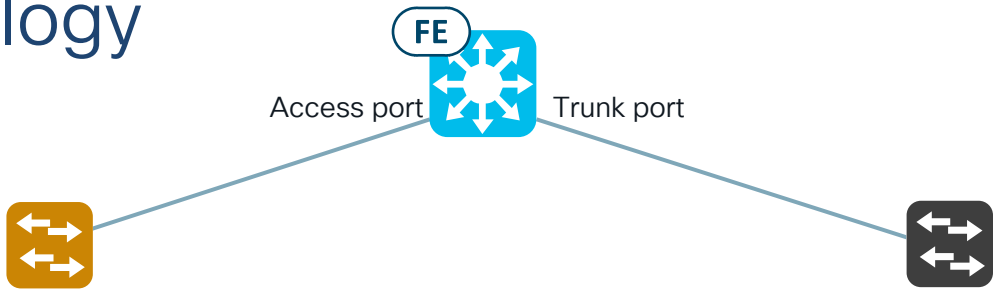
Why remove the Fabric Edge Node port IP address limits?

a. An *Unintelligent* switch connected to Edge Node access port

b. Traditional Layer 2 switching domains connected to Edge Node trunk port



Terminology



Unintelligent switch

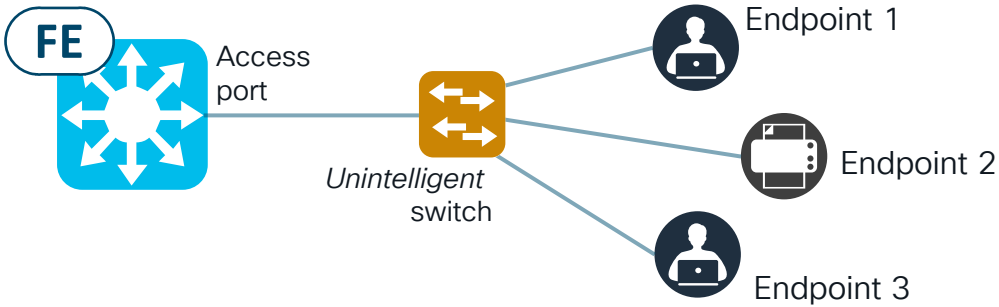
- Not configurable
- Does not support VLANs
- Does not generate STP BPDUs
- Does not consume EAPoL
- Not part of the Cisco SD-Access fabric
- Connects to Edge Node “Access” port

Intelligent switch

- Configurable
- Supports VLANs
- Generates STP BPDUs
- Consumes EAPoL
- Not part of the Cisco SD-Access fabric
- Connects to Edge Node “Trunk” port

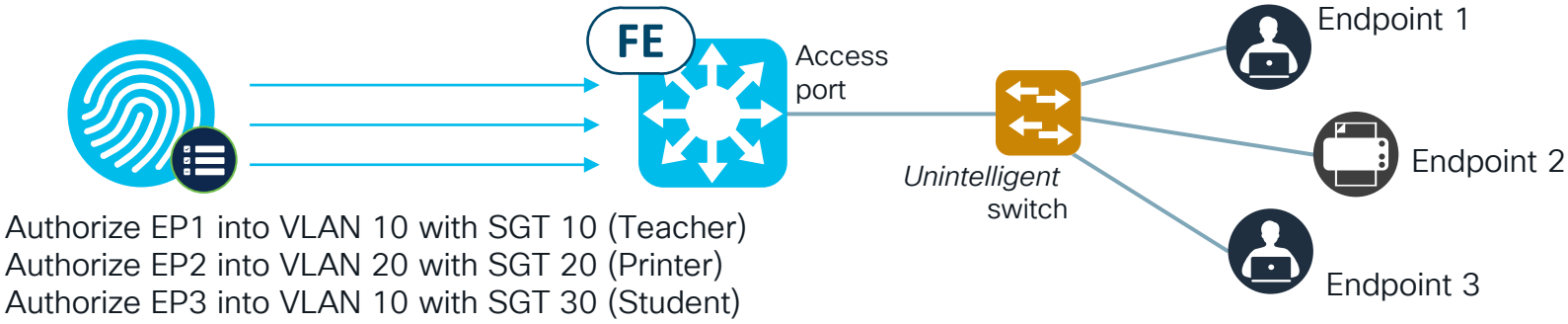
Unintelligent Switch Connected to Fabric Edge

- If the switch between the Edge Node and endpoints consumes EAPoL, then it breaks 802.1X.
- Finding an *Unintelligent* switch is responsibility of partner / customer.
- Unintelligent switch tradeoffs:
  - Micro-segmentation between endpoints physically connected to the switch is not possible.
  - Cisco DNA Center Assurance and Automation are not possible for the unintelligent switch.
  - Cisco TAC does not support the unintelligent switch.



Unintelligent Switch Connected to Fabric Edge

- If authentication is enabled on the Edge Node access port, then each endpoint can be dynamically authorized into a different VLAN and SGT, if required.
  - This does **NOT** solve for micro-segmentation within the unintelligent switch.
  - Multi-Auth Per User VLAN and SGT assignment is an ISE and Switch platform capability and documented in the appropriate Switch Configuration Guide.



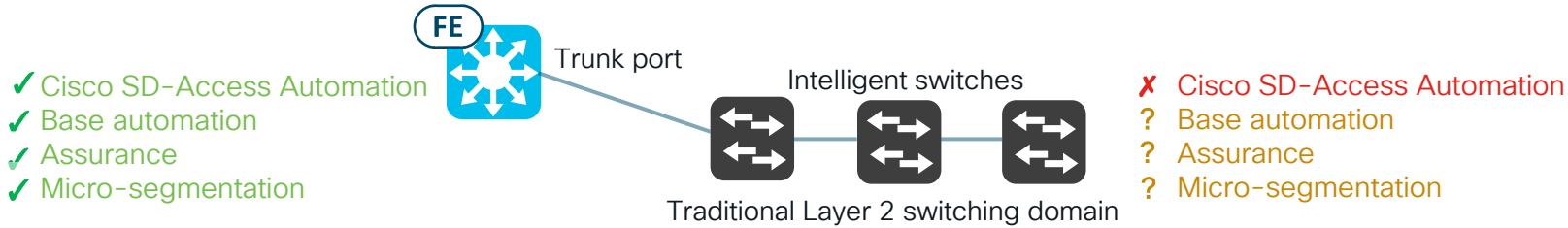
Traditional Switching Domain Connected to Edge Node

Significant use cases:

- Cisco DNA Center automated segmentation (VN and SGT) over an IP core
- Phased migration to Cisco SD-Access
- Connection of third-party networking solutions
- Anycast IP gateway – any IP address anywhere

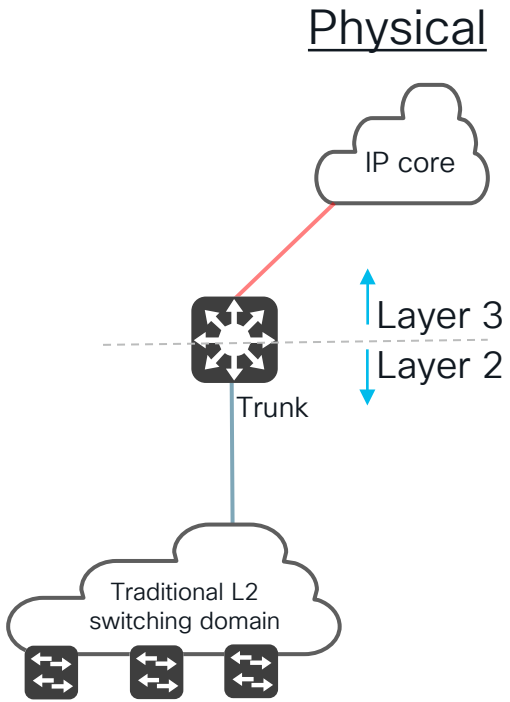
Tradeoffs for the traditional Layer 2 switching domain:

- Not automated by the Cisco SD-Access workflows
- Unlikely to support Group-Based Policy.
  - GBP could start at the Edge Node.
- May not receive the benefits of Cisco DNA Center base Automation and Assurance



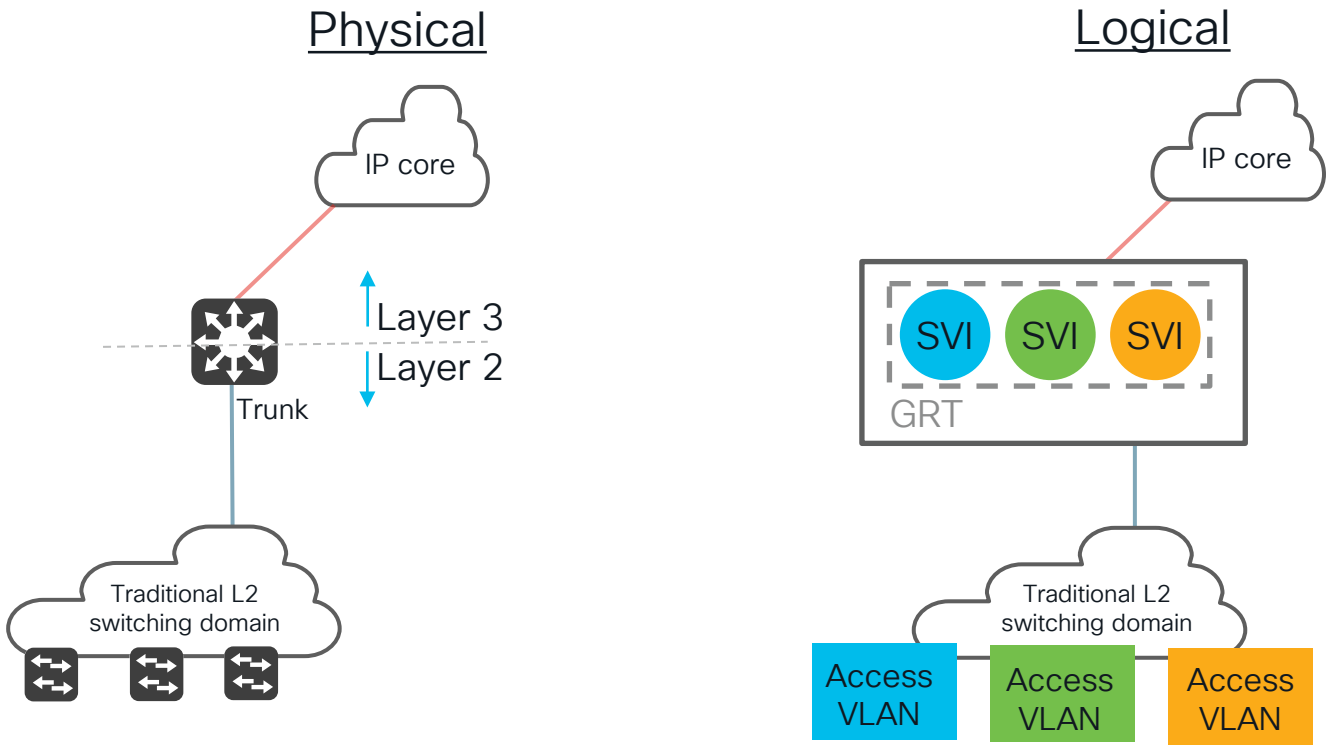
Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 1. Automated VN-based macro-segmentation over an IP core



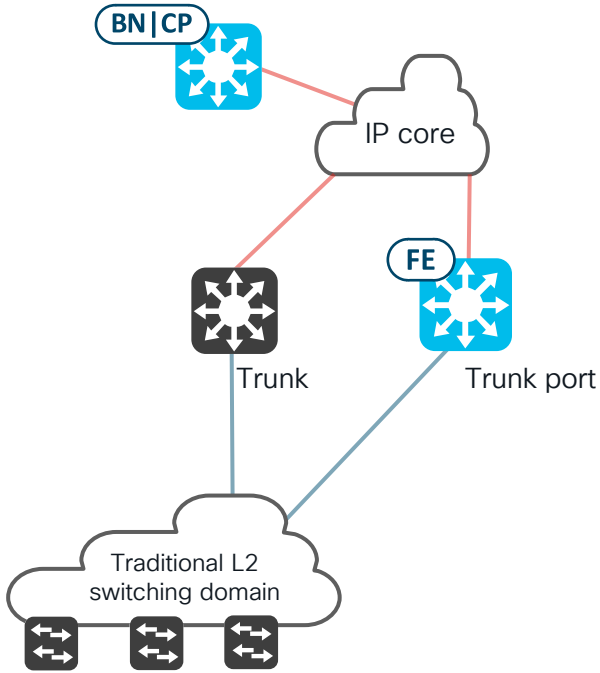
Traditional Layer 2 Switching Domain Connected to Fabric Edge

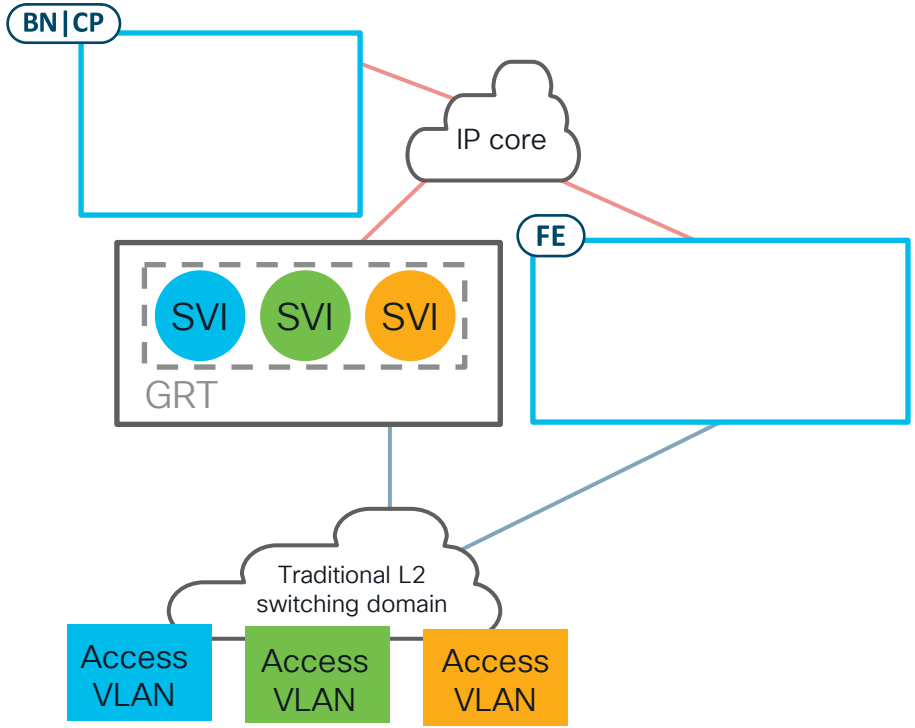
Use Case 1. Automated VN-based macro-segmentation over an IP core



Traditional Layer 2 Switching Domain Connected to Fabric Edge

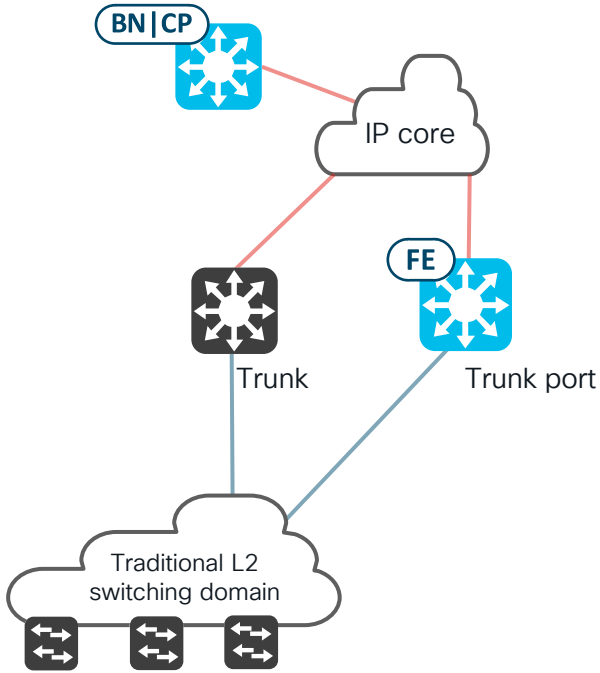
Use Case 1. Automated VN-based macro-segmentation over an IP core

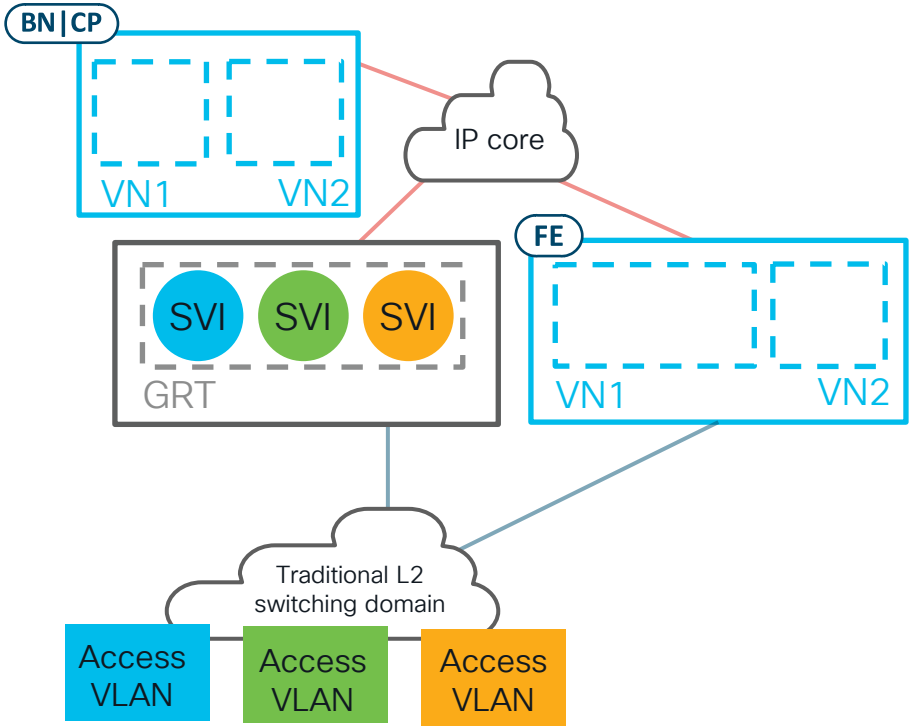




Traditional Layer 2 Switching Domain Connected to Fabric Edge

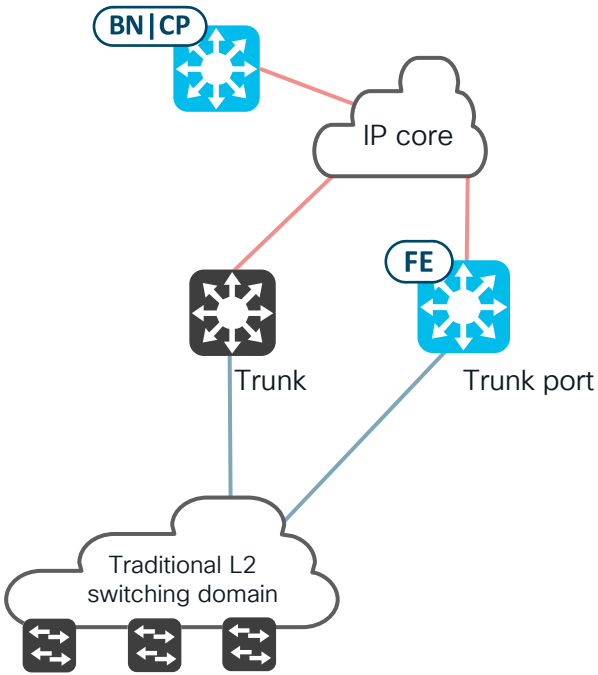
Use Case 1. Automated VN-based macro-segmentation over an IP core

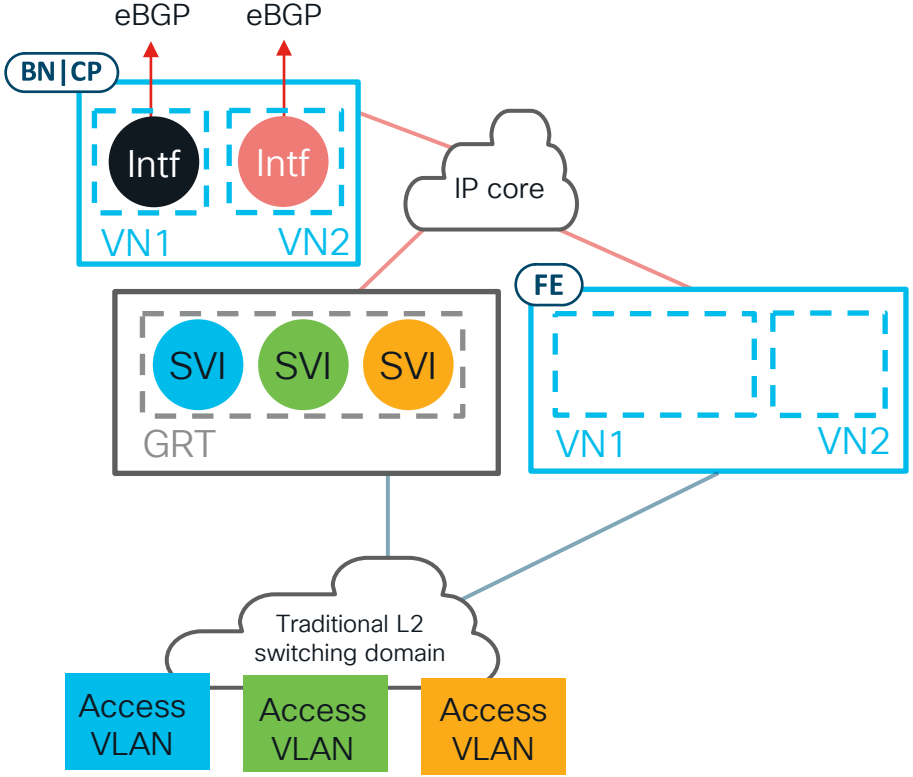




Traditional Layer 2 Switching Domain Connected to Fabric Edge

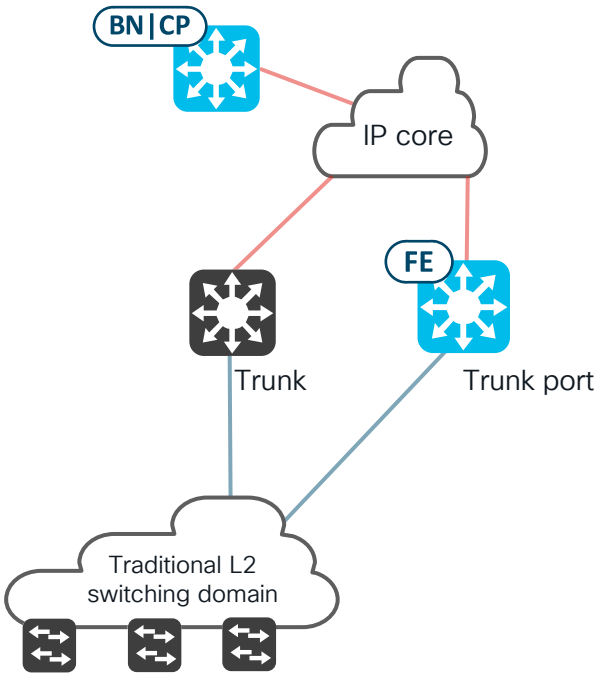
Use Case 1. Automated VN-based macro-segmentation over an IP core

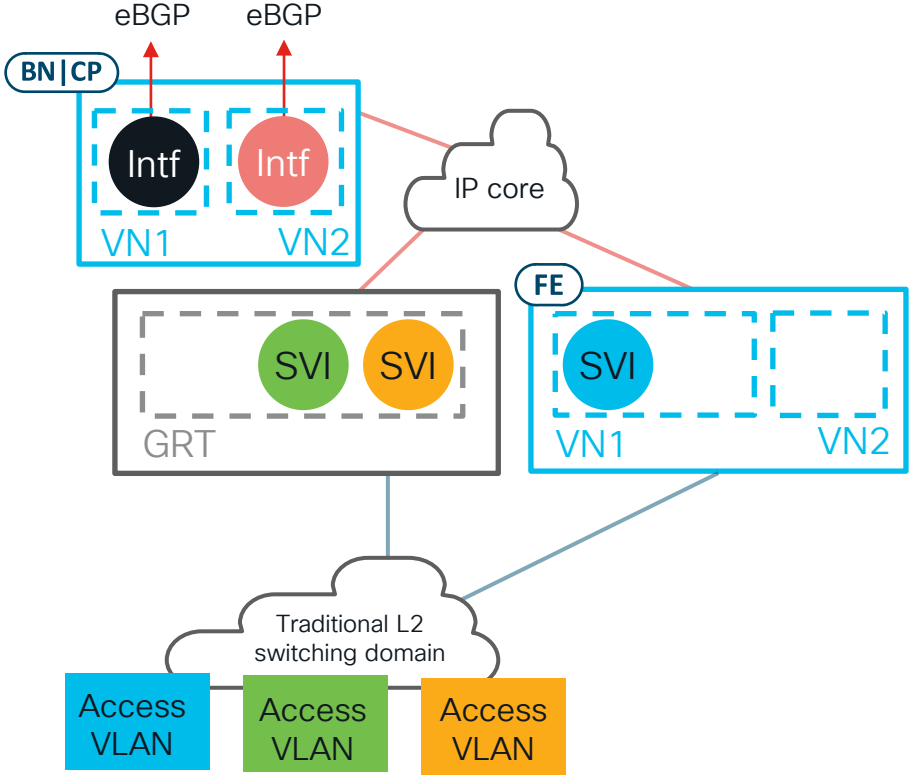




Traditional Layer 2 Switching Domain Connected to Fabric Edge

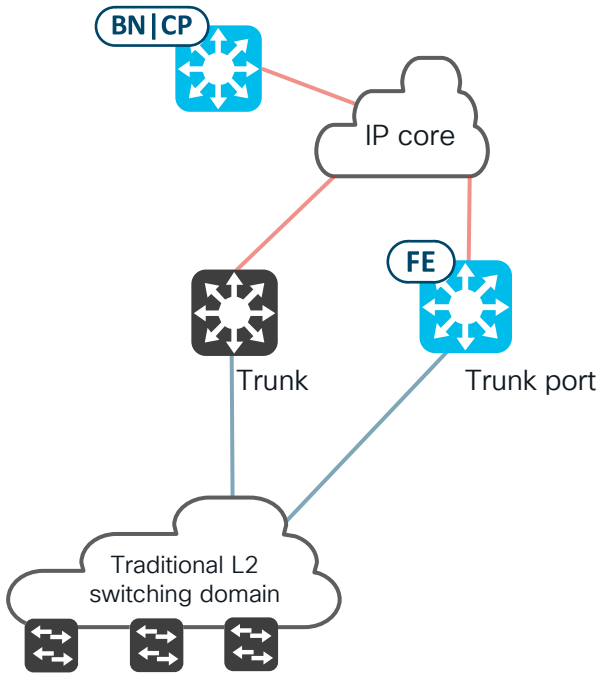
Use Case 1. Automated VN-based macro-segmentation over an IP core

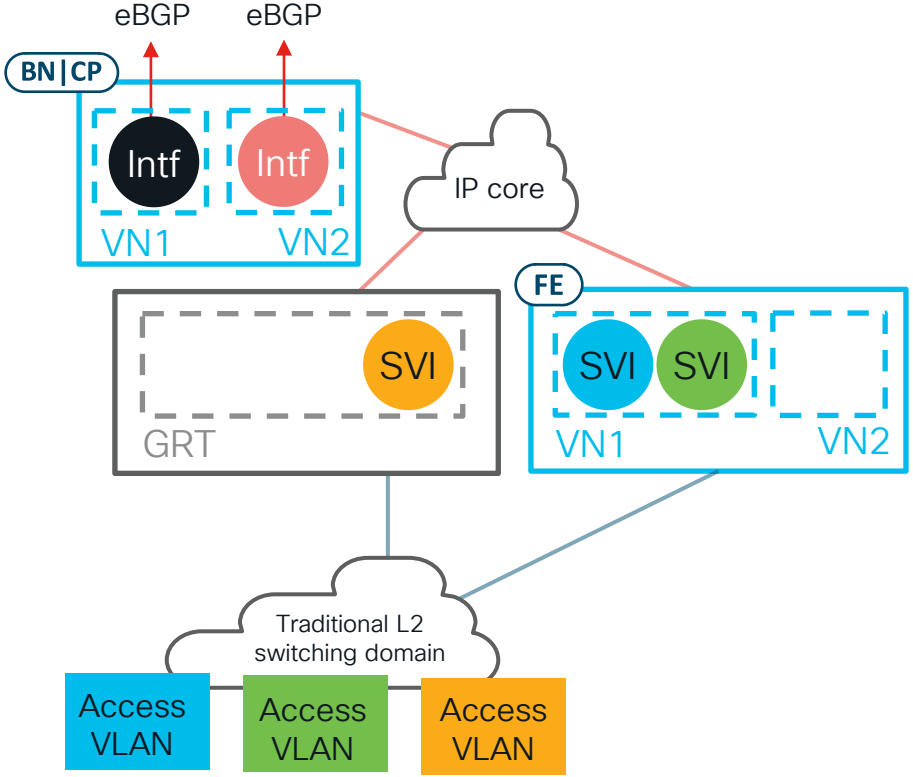




Traditional Layer 2 Switching Domain Connected to Fabric Edge

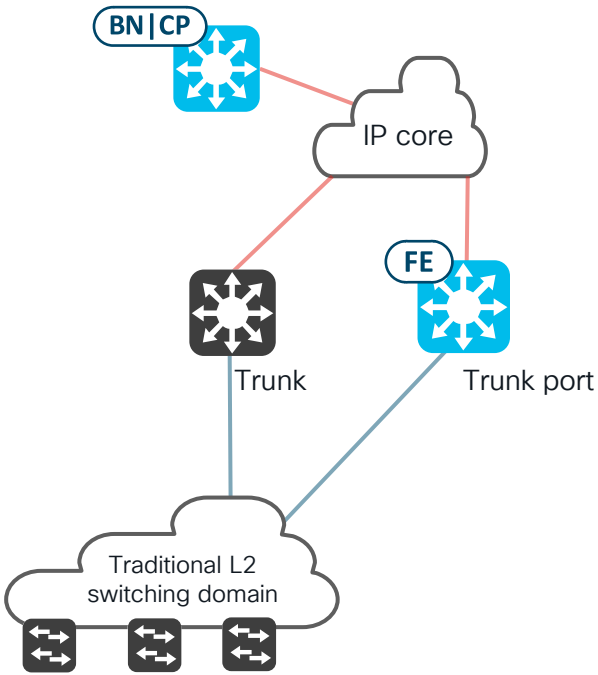
Use Case 1. Automated VN-based macro-segmentation over an IP core

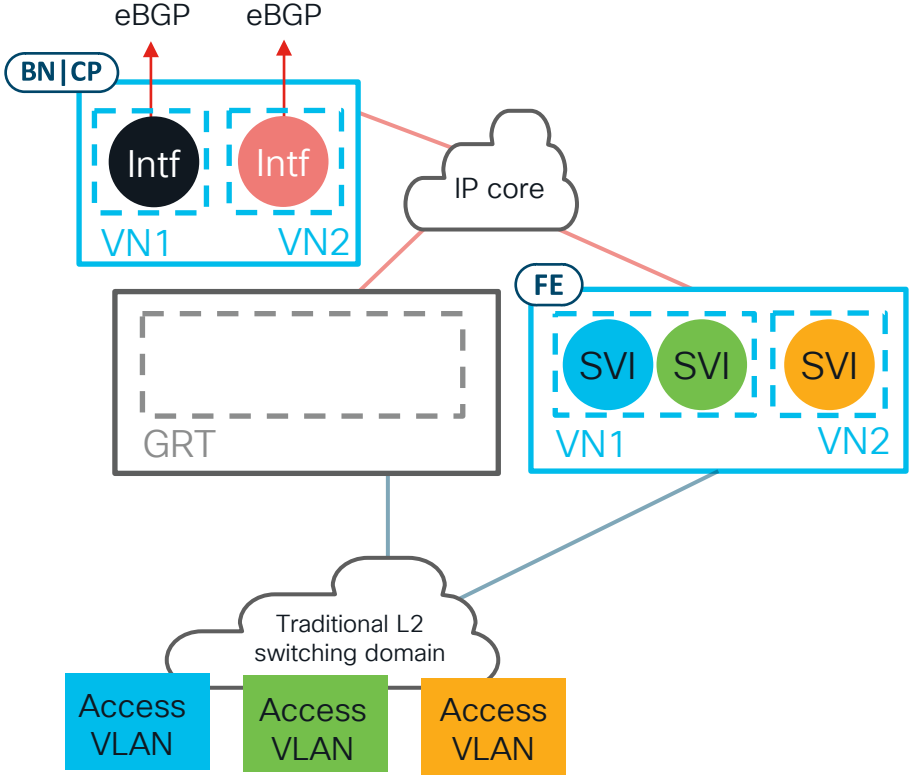




Traditional Layer 2 Switching Domain Connected to Fabric Edge

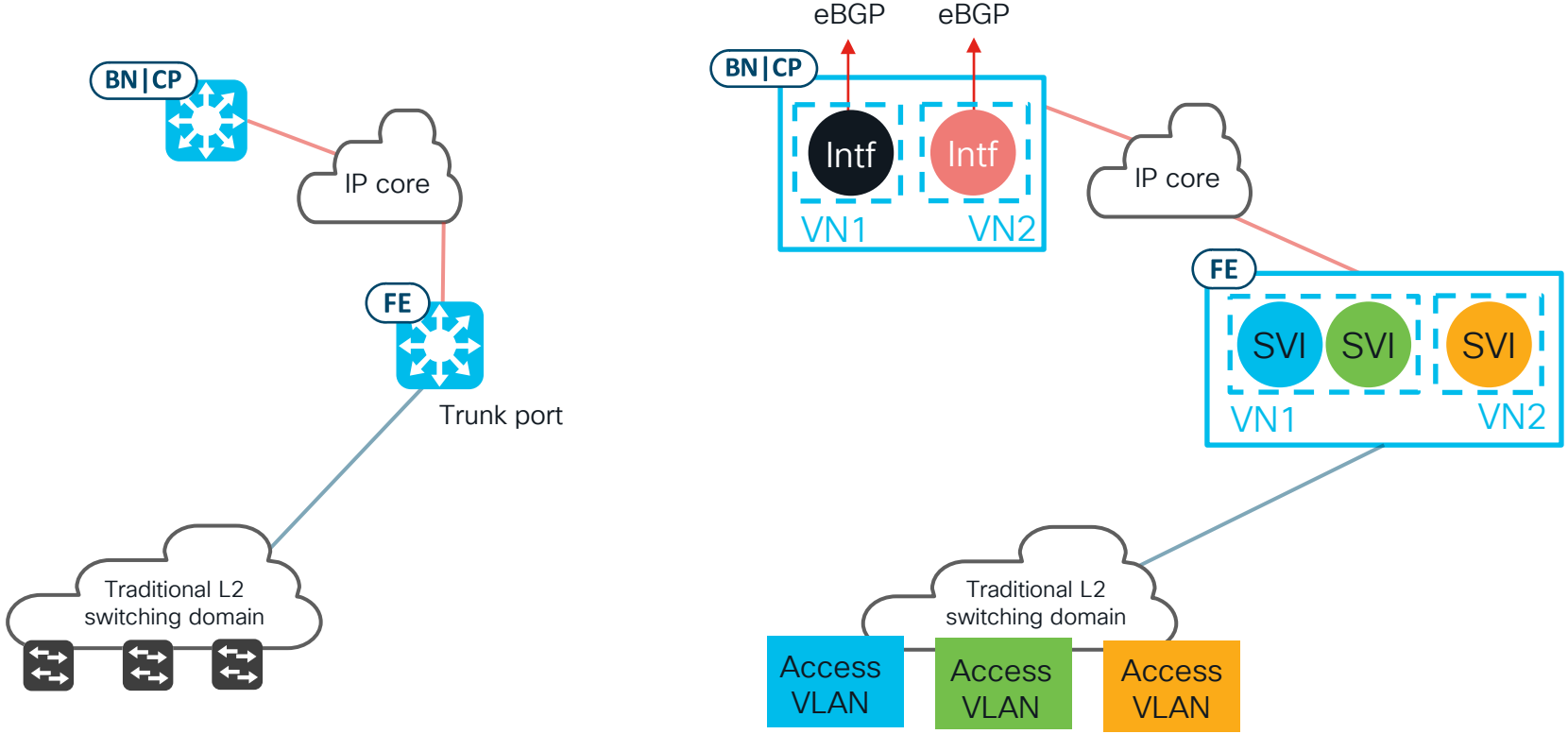
Use Case 1. Automated VN-based macro-segmentation over an IP core





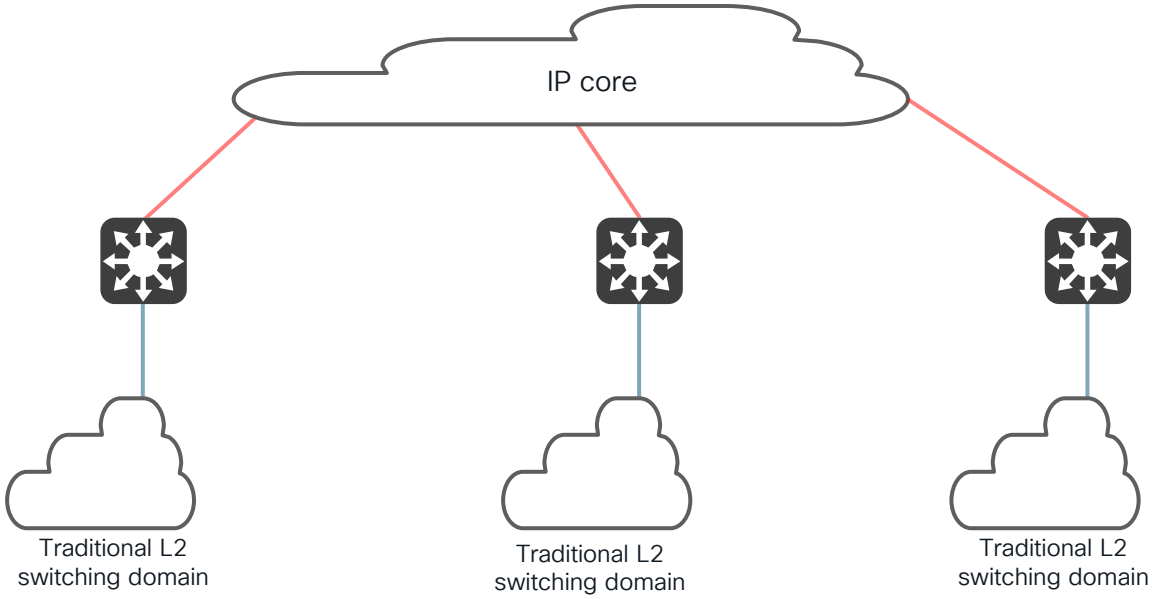
Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 1. Automated VN-based macro-segmentation over an IP core



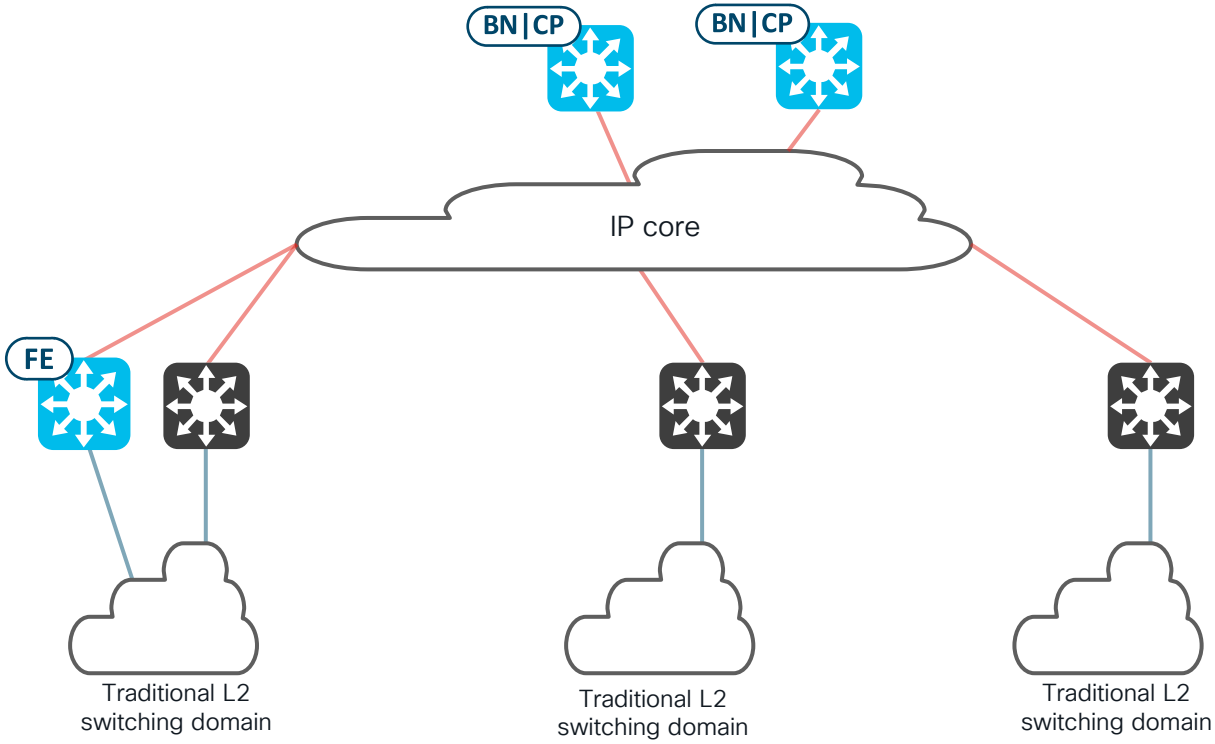
Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 1. Automated VN-based macro-segmentation over an IP core



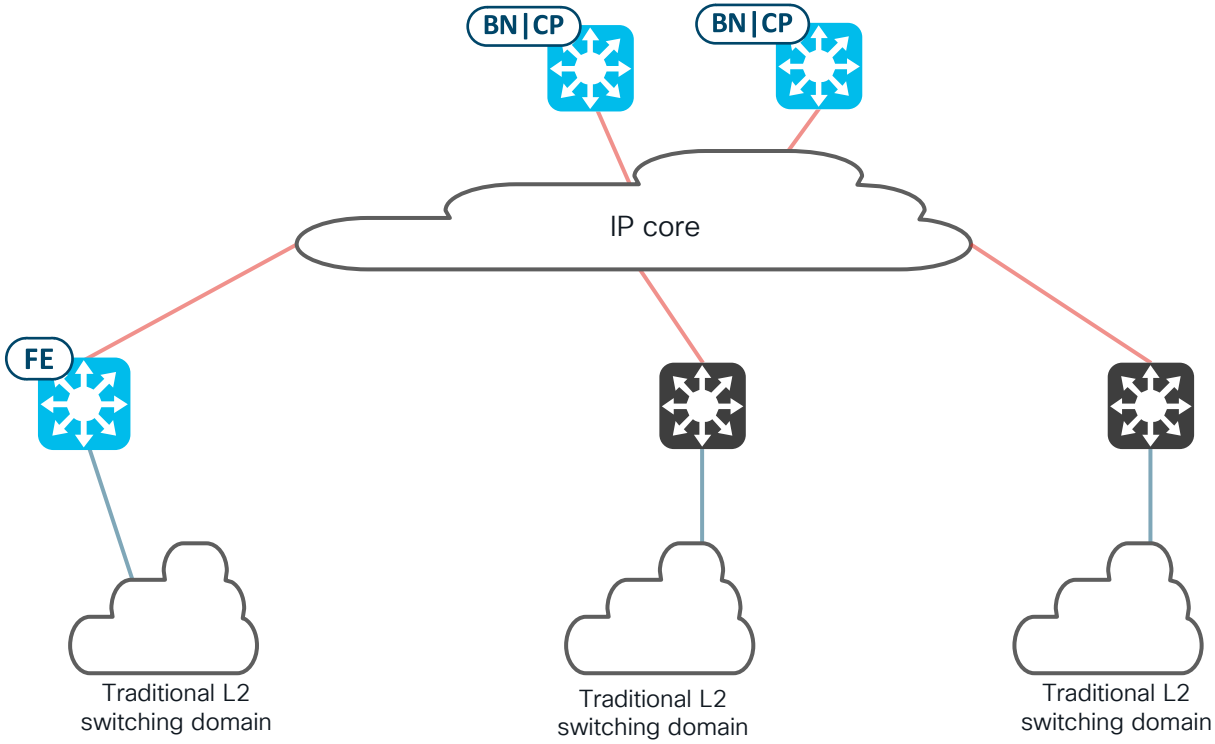
Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 1. Automated VN-based macro-segmentation over an IP core



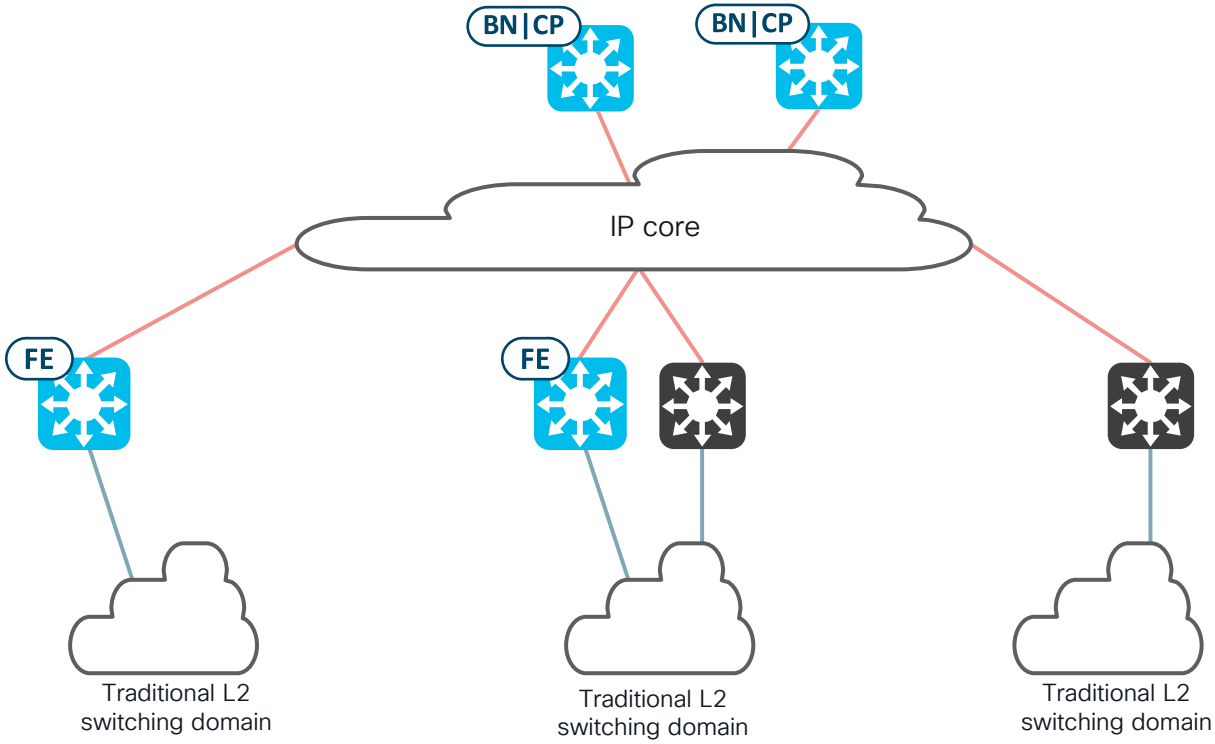
Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 1. Automated VN-based macro-segmentation over an IP core



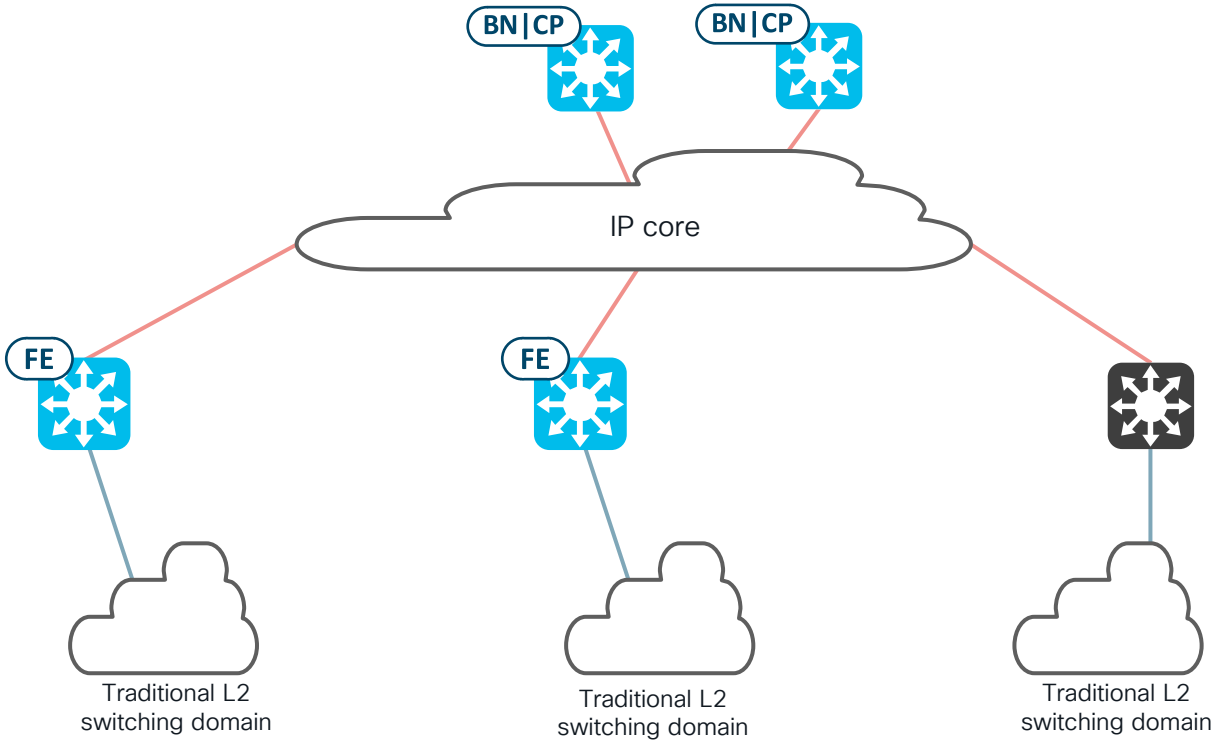
Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 1. Automated VN-based macro-segmentation over an IP core



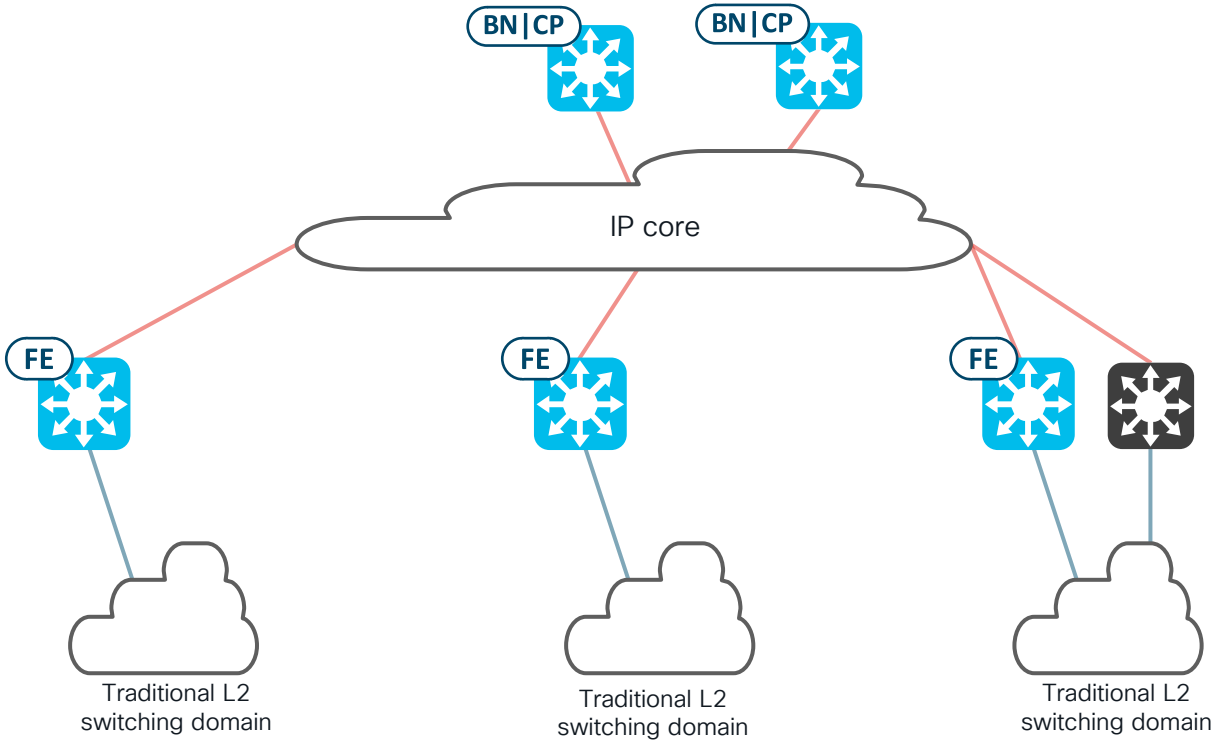
Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 1. Automated VN-based macro-segmentation over an IP core



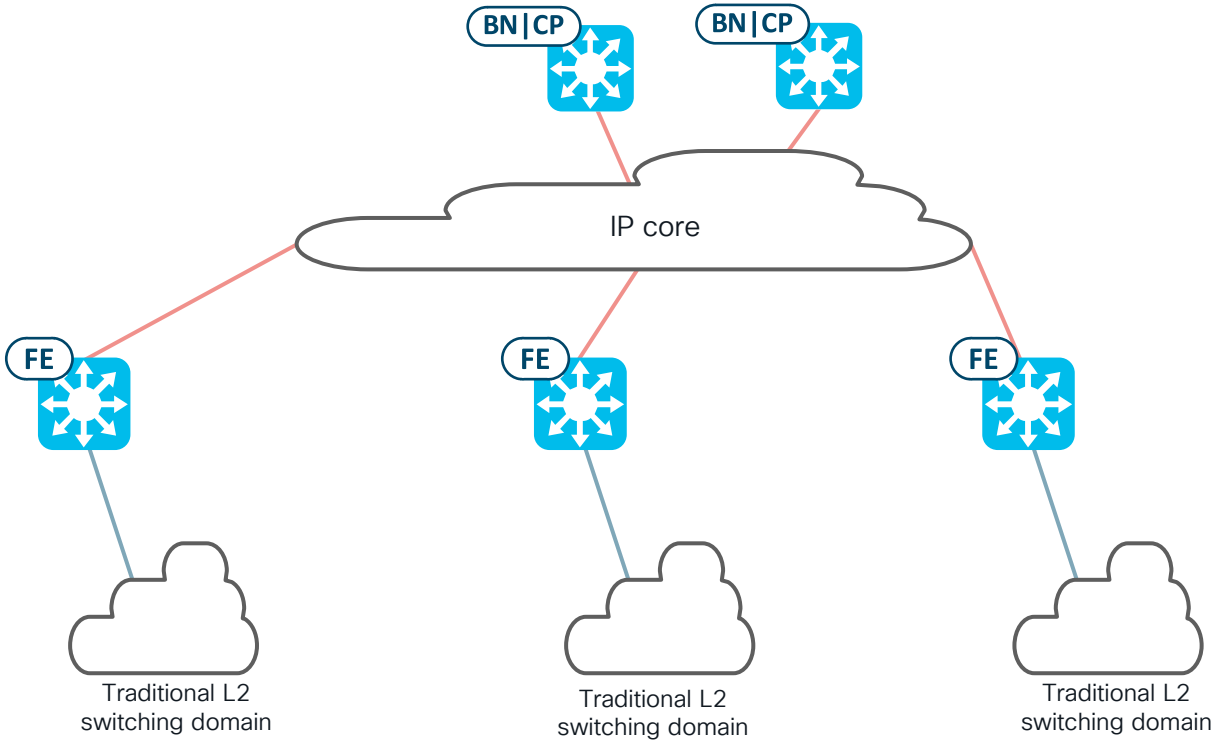
Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 1. Automated VN-based macro-segmentation over an IP core



Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 1. Automated VN-based macro-segmentation over an IP core



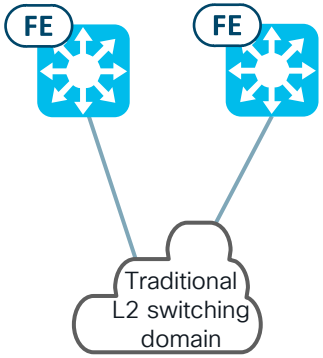
Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 1. Important Considerations

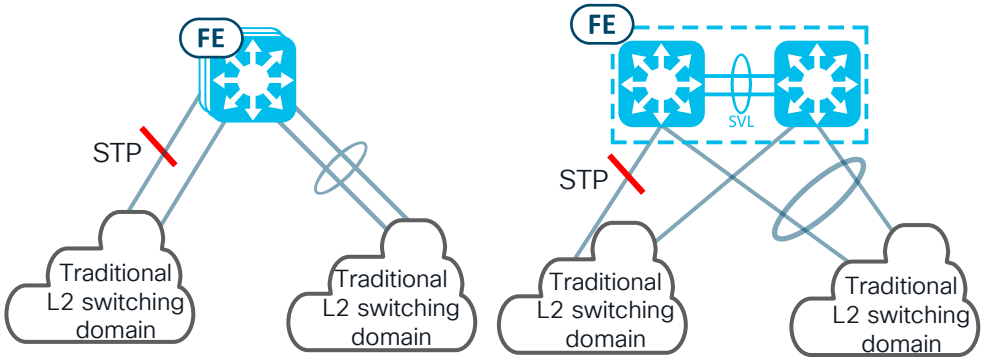
Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 1. Important Considerations

- Switching loops, StackWise (hardware stacking), and StackWise Virtual



✗ Same VLAN connected to two different Edge Nodes = switching loop



✓ Same VLAN connected to different ports on a StackWise or StackWise Virtual switch is fine.

Use STP or port-channel(s) to prevent loops between Edge Nodes and traditional Layer 2 switching domain.

Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 1. Important Considerations

- No roaming latency concerns for Fabric-Enabled Wireless and Over The Top (concentrator-based) wireless.
- For endpoints roaming between SD-Access Edge Nodes, the endpoint roaming latency will be inappropriate for real-time roaming applications, such as Voice over flex or flex-like wireless.
  - Feature for fast roaming between Edge Node switch ports is in planning now.

Typical Wireless Roaming Times with Cisco SD-Access 2.1.2

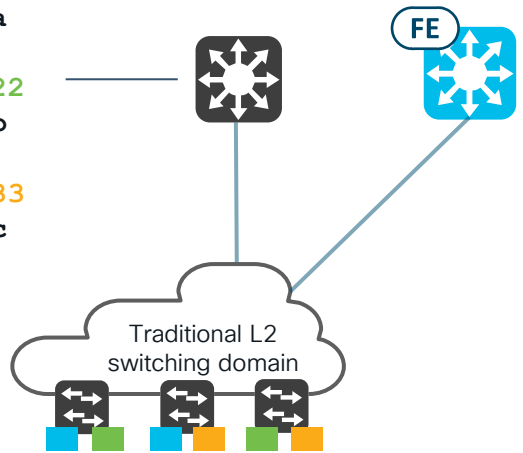
Wireless Deployment Type	Roam Pattern	Average Observed Roam Latency
SD-Access Wireless	APs connected to the **same** edge node	70 ms
SD-Access Wireless	APs connected to **different** edge nodes	85 ms

Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 1. Important Considerations

- Cisco SD-Access Custom VLAN ID* feature is required to match already-configured traditional L2 switching domain VLAN ID.

```
interface VLAN111
  ip address aaa
  shutdown
interface VLAN222
  ip address bbb
  shutdown
interface VLAN333
  ip address ccc
  no shutdown
```



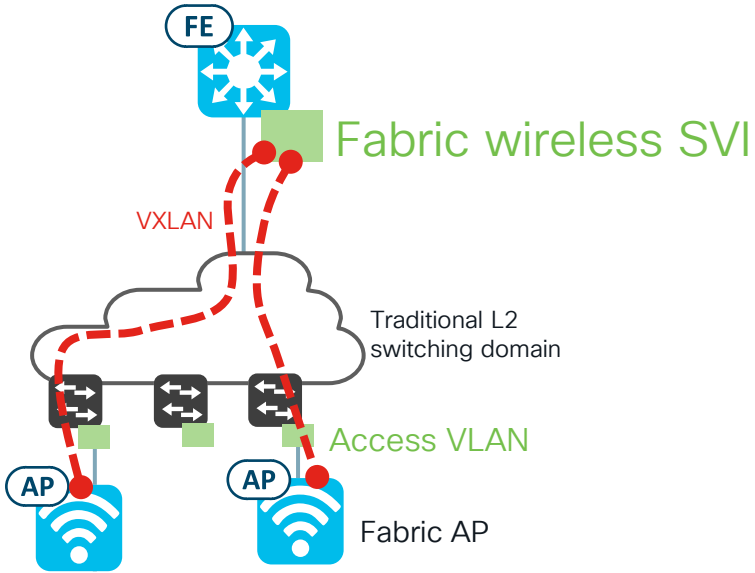

```
interface VLAN111
  vrf forwarding CORP
  ip address aaa
  no shutdown
interface VLAN222
  vrf forwarding CCTV
  ip address bbb
  no shutdown
```

*ETA Q2CY2021

Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 1. Important Considerations

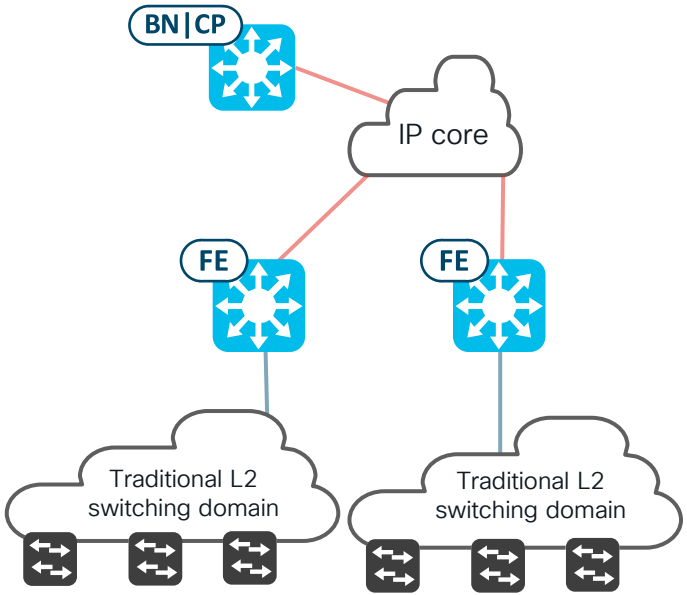
- Fabric APs connected to traditional L2 switching domain are already supported.
  - This enables a rapid realization of the benefits of Fabric-Enabled Wireless (SGT, Automation, Assurance, wireless data plane switched locally on Edge Node, etc.)



Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 1. Important Considerations

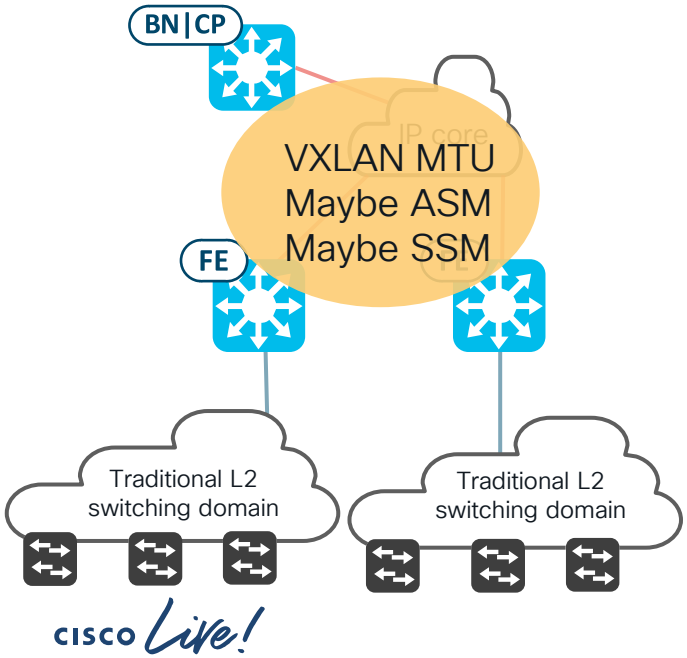
- The IP core may need to support multicast and jumbo MTU (depends on size of overlay packets).
  - Covered heavily in DGTL-BRKENS-3822. But in short:



Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 1. Important Considerations

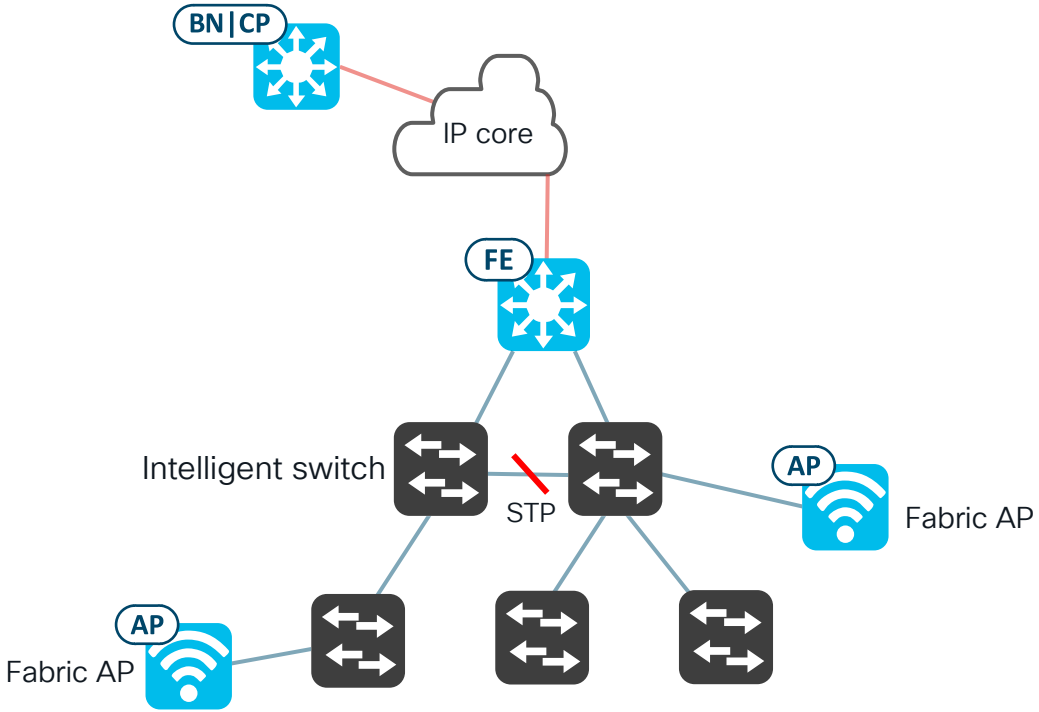
- The IP core may need to support multicast and jumbo MTU (depends on size of overlay packets).
  - Covered heavily in DGTL-BRKENS-3822. But in short:



- Fabric Edge Node SVIs cannot fragment overlay payloads.
- The IP core will need to accommodate the Cisco SD-Access VXLAN MTU.
  - VXLAN cannot be fragmented.
  - The Overlay can use *TCP adjust-MSS* for large TCP flows.
  - Large UDP in Overlay needs to be addressed outside of fabric e.g. external Layer 3 device or on the endpoint.
- IP core may need to support ASM and SSM
  - SD-Access Layer 2 Flooding feature uses underlay ASM.
  - SD-Access Native Multicast feature uses underlay SSM.

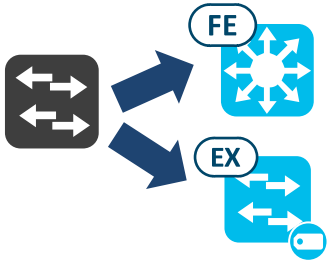
Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 2. Phased migration to Cisco SD-Access



Recap: Convert a Traditional Switch to Cisco SD-Access Mode

RECAP

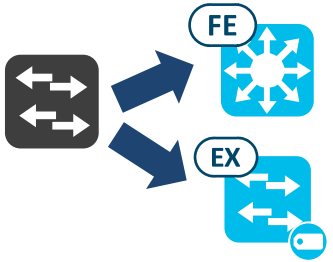


Recap: Convert a Traditional Switch to Cisco SD-Access Mode

Rebuild the switch:

1. IOS XE version complies with the SD-Access Compatibility Matrix.
2. License level / subscription level sufficient.

RECAP



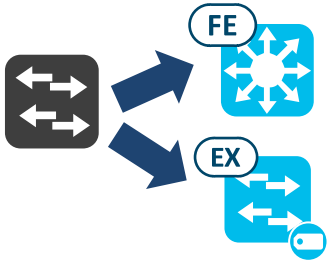
Recap: Convert a Traditional Switch to Cisco SD-Access Mode

RECAP

Rebuild the switch:

1. IOS XE version complies with the SD-Access Compatibility Matrix.
2. License level / subscription level sufficient.

LAN Automation or
Extended Node Onboarding



3. Factory reset the switch as per LAN Automation Deployment Guide.
4. Execute LAN automation or Extended Node onboarding.
5. Add to Fabric Site as Edge Node or Extended Node.
6. Provision Edge Node ports in Host Onboarding.

Recap: Convert a Traditional Switch to Cisco SD-Access Mode

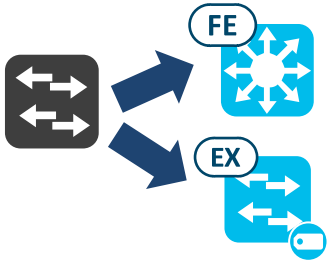
RECAP

Rebuild the switch:

1. IOS XE version complies with the SD-Access Compatibility Matrix.
2. License level / subscription level sufficient.

LAN Automation or Extended Node Onboarding

Manual conversion to Fabric Edge Node



3. Factory reset the switch as per LAN Automation Deployment Guide.
4. Execute LAN automation or Extended Node onboarding.
5. Add to Fabric Site as Edge Node or Extended Node.
6. Provision Edge Node ports in Host Onboarding.

3. Replace startup configuration with tailored startup configuration and reload the switch:
   - Routed p2p uplinks, Loopback0
   - MTU that accommodates VXLAN overhead
   - Multicast routing and PIM, if required
   - SSH and SNMP credentials
4. Modify distribution layer to have routed downlinks or repatch switch to new distribution.
5. Discover just-reloaded switch in Cisco DNA Center, Provision, and add to fabric site as Edge Node.
6. Provision Edge Node ports in Host Onboarding, if required.

Recap: Convert a Traditional Switch to Cisco SD-Access Mode

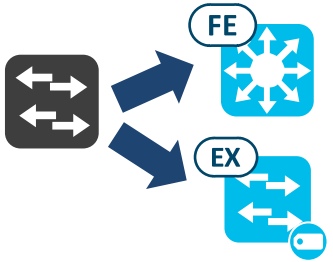
RECAP

Rebuild the switch:

1. IOS XE version complies with the SD-Access Compatibility Matrix.
2. License level / subscription level sufficient.

LAN Automation or Extended Node Onboarding

Manual conversion to Fabric Edge Node



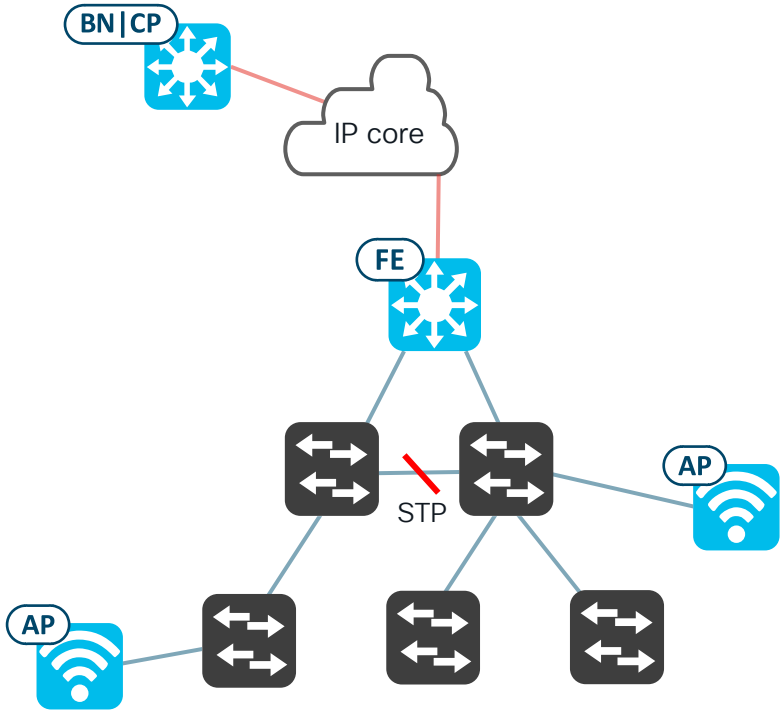
3. Factory reset the switch as per LAN Automation Deployment Guide.
4. Execute LAN automation or Extended Node onboarding.
5. Add to Fabric Site as Edge Node or Extended Node.
6. Provision Edge Node ports in Host Onboarding.

~40K ports migrated

3. Replace startup configuration with tailored startup configuration and reload the switch:
   - Routed p2p uplinks, Loopback0
   - MTU that accommodates VXLAN overhead
   - Multicast routing and PIM, if required
   - SSH and SNMP credentials
4. Modify distribution layer to have routed downlinks or repatch switch to new distribution.
5. Discover just-reloaded switch in Cisco DNA Center, Provision, and add to fabric site as Edge Node.
6. Provision Edge Node ports in Host Onboarding, if required.

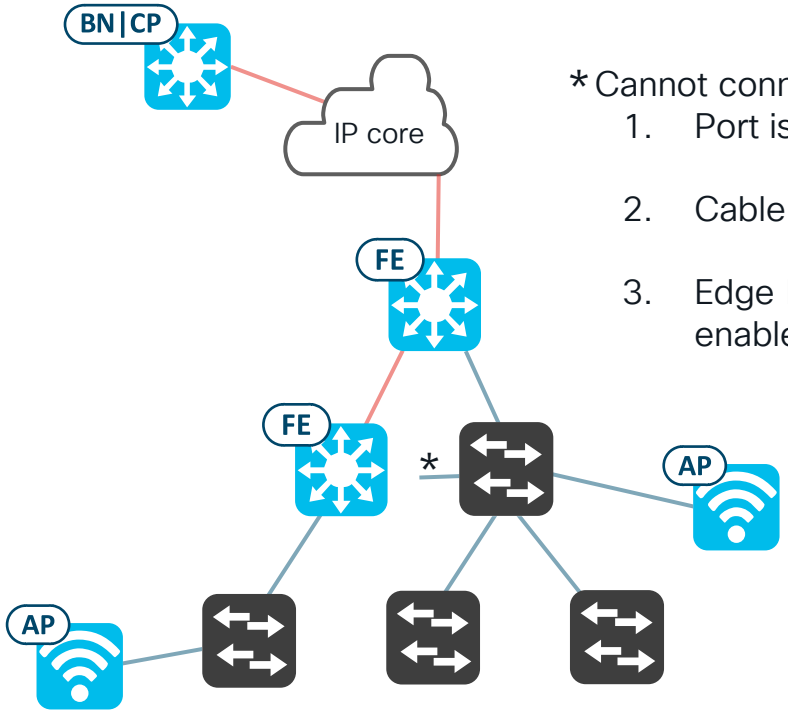
Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 2. Phased migration to Cisco SD-Access



Traditional Layer 2 Switching Domain Connected to Fabric Edge

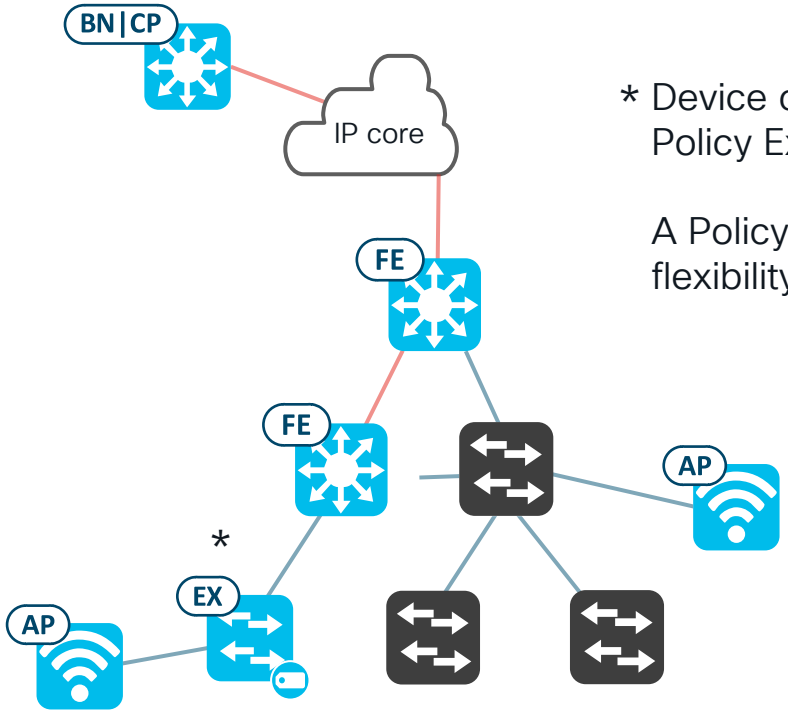
Use Case 2. Phased migration to Cisco SD-Access



* Cannot connect same Layer 2 domain to two Edge Nodes. Thus:
  1. Port is shutdown on the Edge Node
     -or-
  2. Cable is temporarily disconnected
     -or-
  3. Edge Node port is Closed Authentication so that trunk is not enabled

Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 2. Phased migration to Cisco SD-Access

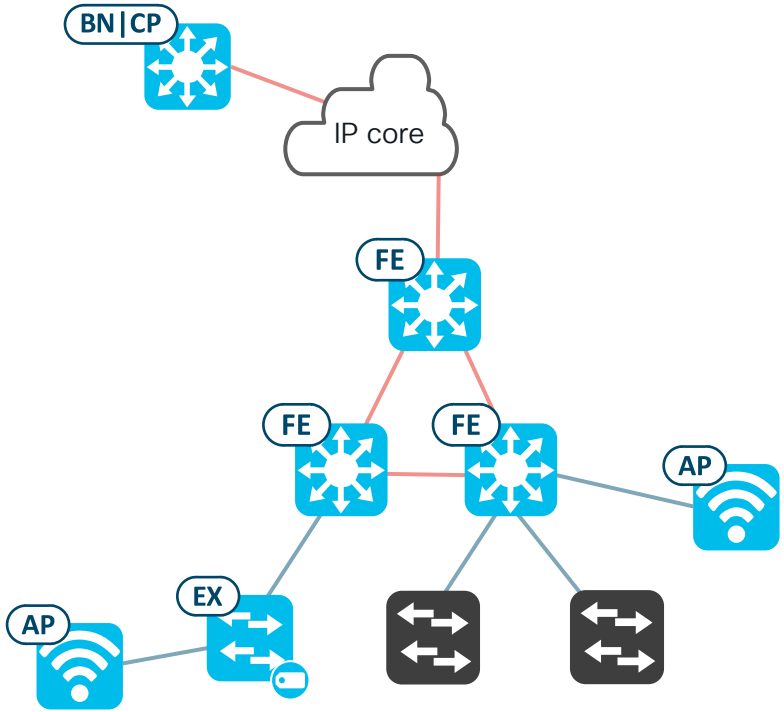


* Device could be provisioned as an Edge Node or Policy Extended Node.

A Policy Extended Node is depicted to showcase flexibility of options.

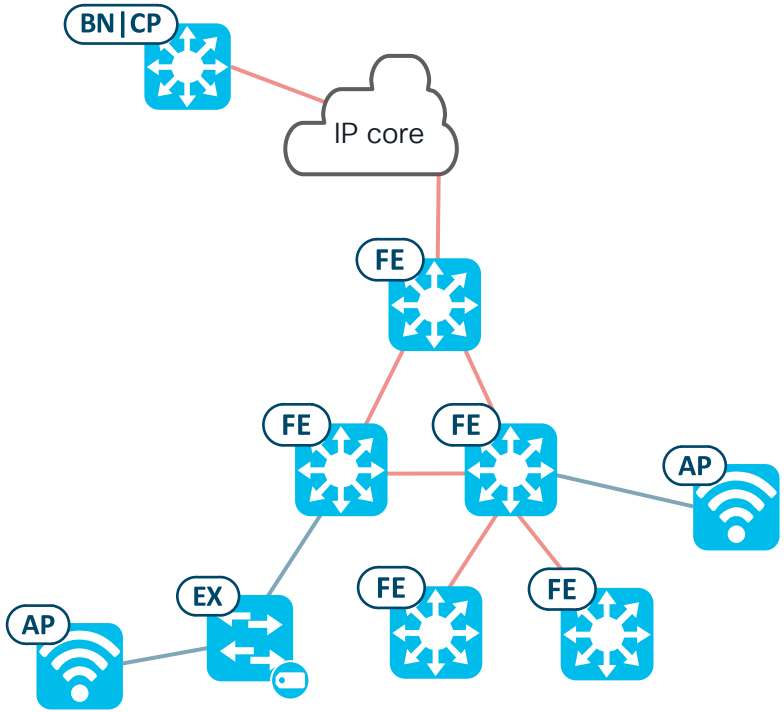
Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 2. Phased migration to Cisco SD-Access



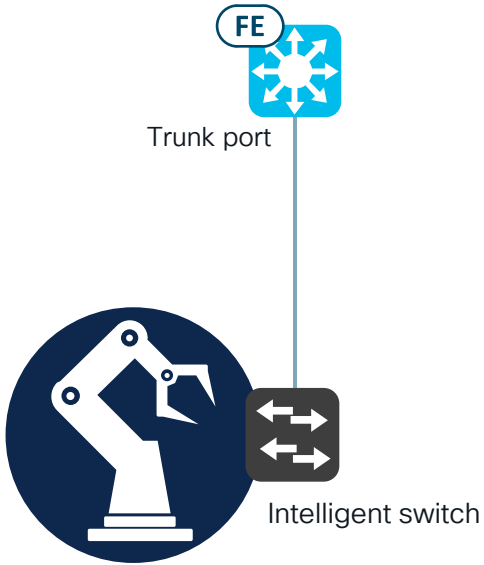
Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 2. Phased migration to Cisco SD-Access



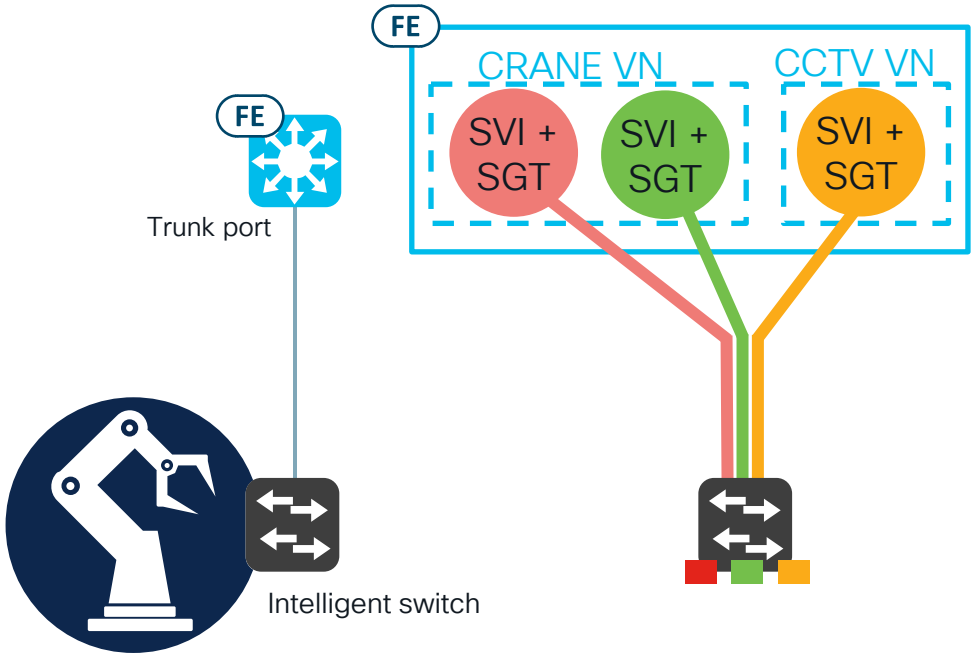
Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 3. Third-party networking connected to Cisco SD-Access



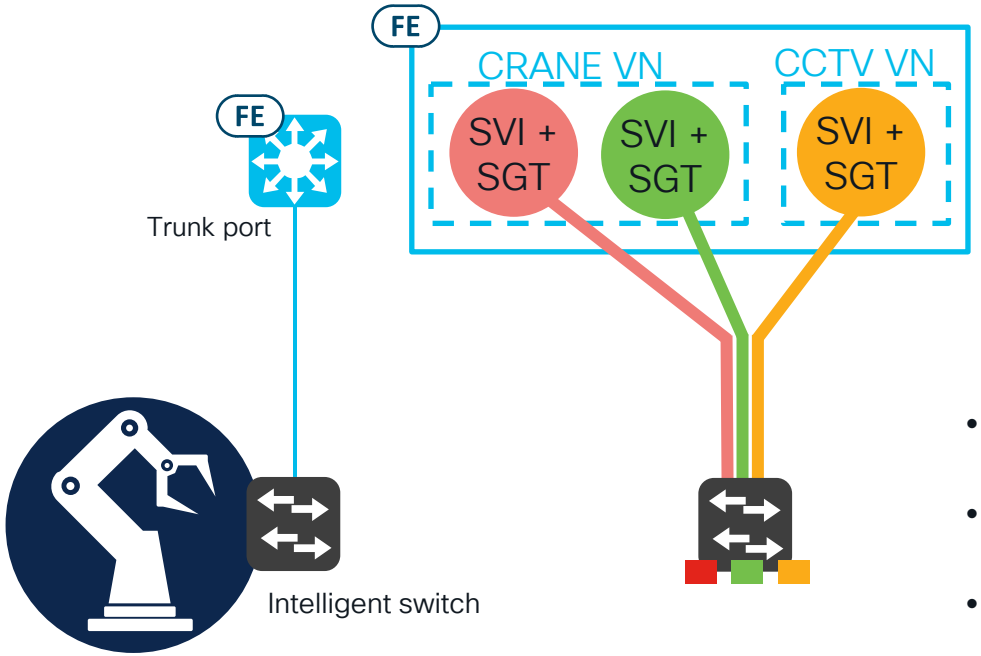
Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 3. Third-party networking connected to Cisco SD-Access



Traditional Layer 2 Switching Domain Connected to Fabric Edge

Use Case 3. Third-party networking connected to Cisco SD-Access



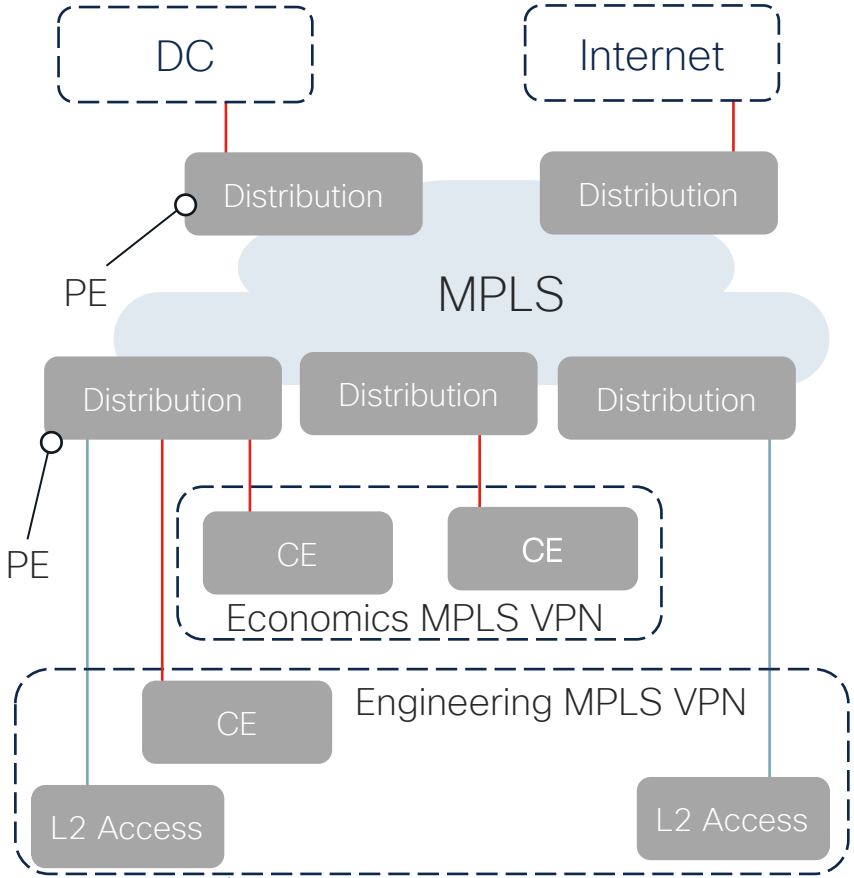

```
FABRIC_EDGE_NODE#show vrf | sec CRANE|CCTV
  CCTV                            <not set>            ipv4       Vl1026
                                                                  LI0.4100
  CRANE                           <not set>            ipv4       Vl1025
                                                                  Vl1024
                                                                  LI0.4101


FABRIC_EDGE_NODE#show ip inter brief | i 102[4-6]
Vlan1024               10.4.4.1        YES manual up                    up
Vlan1025               10.4.0.1        YES manual up                    up
Vlan1026               10.3.0.1        YES manual up                    up
FABRIC_EDGE_NODE#show run | i cts role-
cts role-based sgt-map vlan-list 1025 sgt 8
cts role-based sgt-map vlan-list 1024 sgt 18
cts role-based sgt-map vlan-list 1026 sgt 19
cts role-based enforcement
cts role-based enforcement vlan-list 1021,1023-1026
FABRIC_EDGE_NODE#
```

- No endpoint authentication/authorization on Edge Node trunk port
- Access VLAN is statically mapped to an SGT from Cisco DNA Center Host Onboarding screen
- All endpoints in the VLAN without dynamic ISE-assigned SGT receive the Group-Based Policy for static SGT.

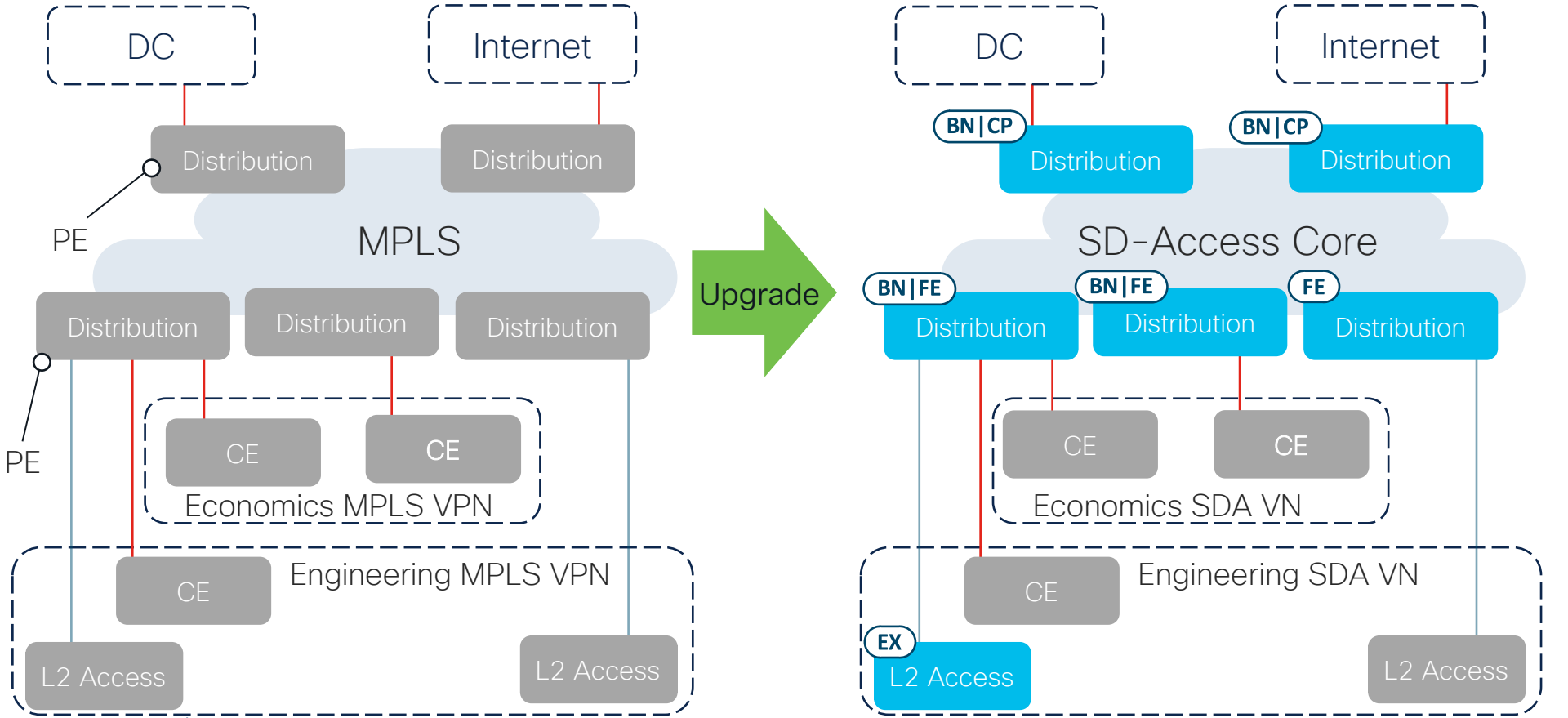
From Enterprise MPLS to Cisco SD-Access

cisco Live!

Cisco SD-Access as an Enterprise Core



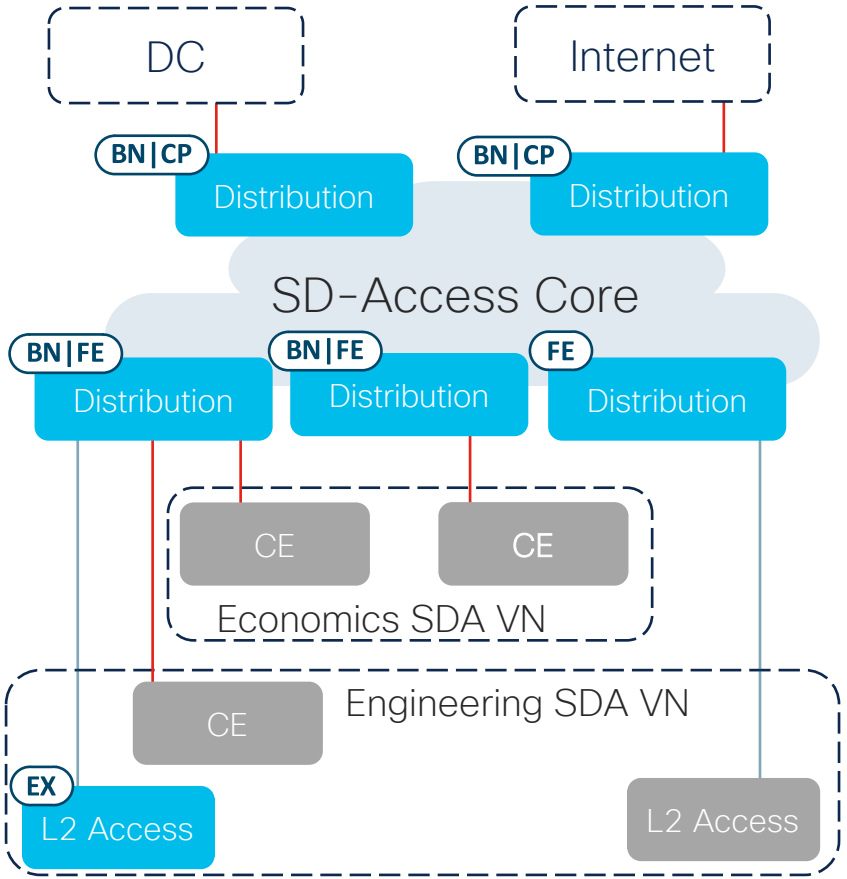
Cisco SD-Access as an Enterprise Core



Cisco SD-Access as an Enterprise Core

Why?

- Cisco SD-Access automation supplants manual box-by-box MPLS configuration / management.
- SD-Access overlay (VXLAN) provides native support for Group-Based Policy (SGT / micro-segmentation) in the wired and wireless domains.
- Prepare the network to receive the present and future benefits of Cisco SD-Access and DNA Center e.g. Automation, Assurance, Fabric-Enabled Wireless, Endpoint Analytics, Group Based Policy Analytics, Group-Based Policy (micro-segmentation), etc.



Conclusion

Summary

- Thank you. We can't do this without you! ☺
- Keep sharing the feedback. We are listening.
- Go deep. Familiarize yourself with DGTL-BRKENS-3822.
- Ask the Cisco Sales or CX teams for help.
- Ask questions on the Cisco SD-Access communities: http://cs.co/sda-community .
- Go Cisco SD-Access!

Cisco Live 2021 – SD-Access Resources

Would you like to know more?

- BRKENS-2006 – What's New in Cisco SD-Access
- BRKENS-2007 – Top Design Questions for Cisco SD-Access
- BRKENS-2008 – Updated Cisco SD-Access Migration Strategies
- BRKENS-2000 – Applying Zero Trust Security Policies to Your Workplace
- BRKENS-2022 – The Value and Details of Multidomain Pairwise Integration Between Cisco SD-Access and Cisco SD-WAN

The bridge to possible

Thank you


cisco Live!
TURN
IT
UP
#CiscoLive