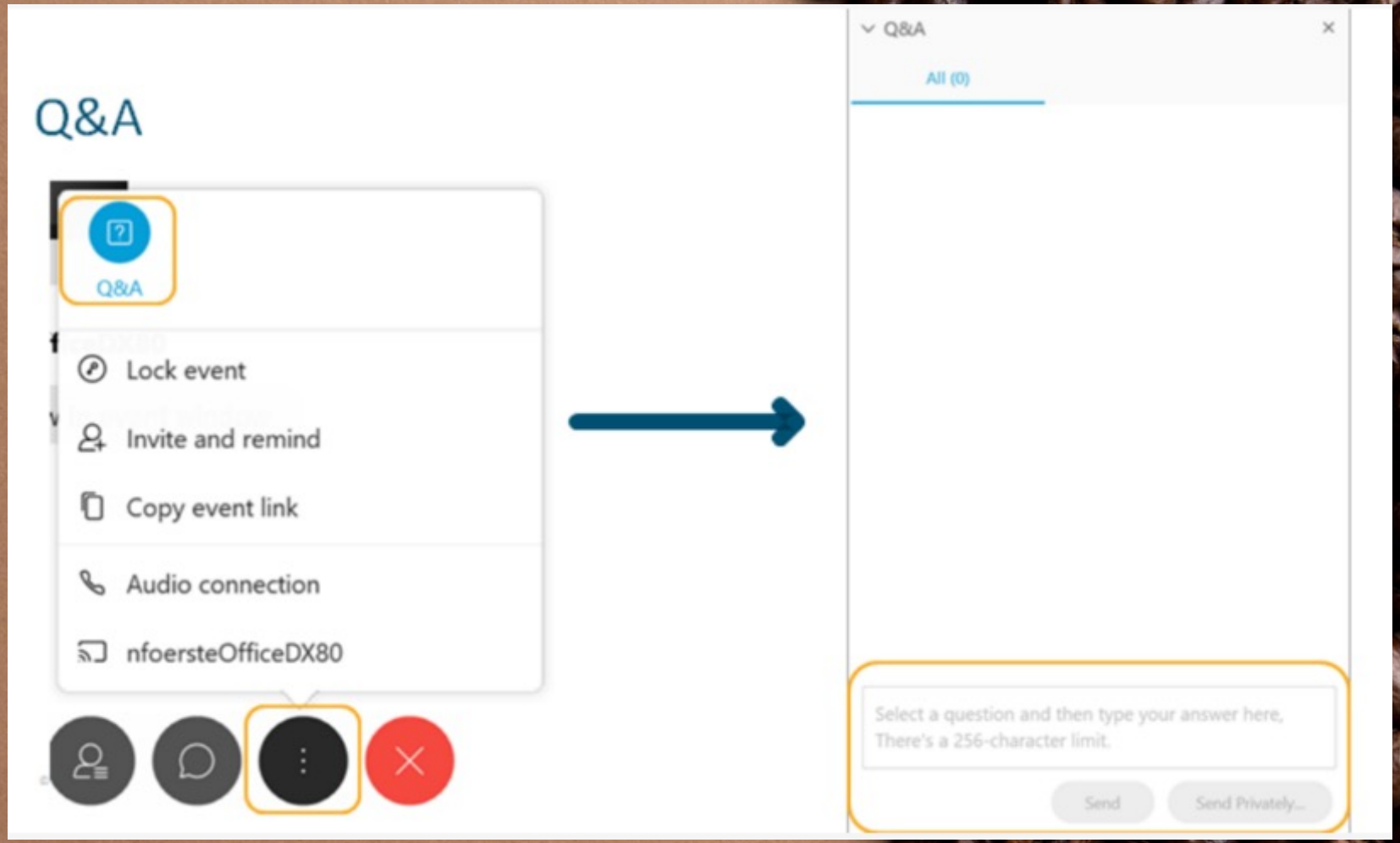
Cisco SD-Access Migrationsszenarien

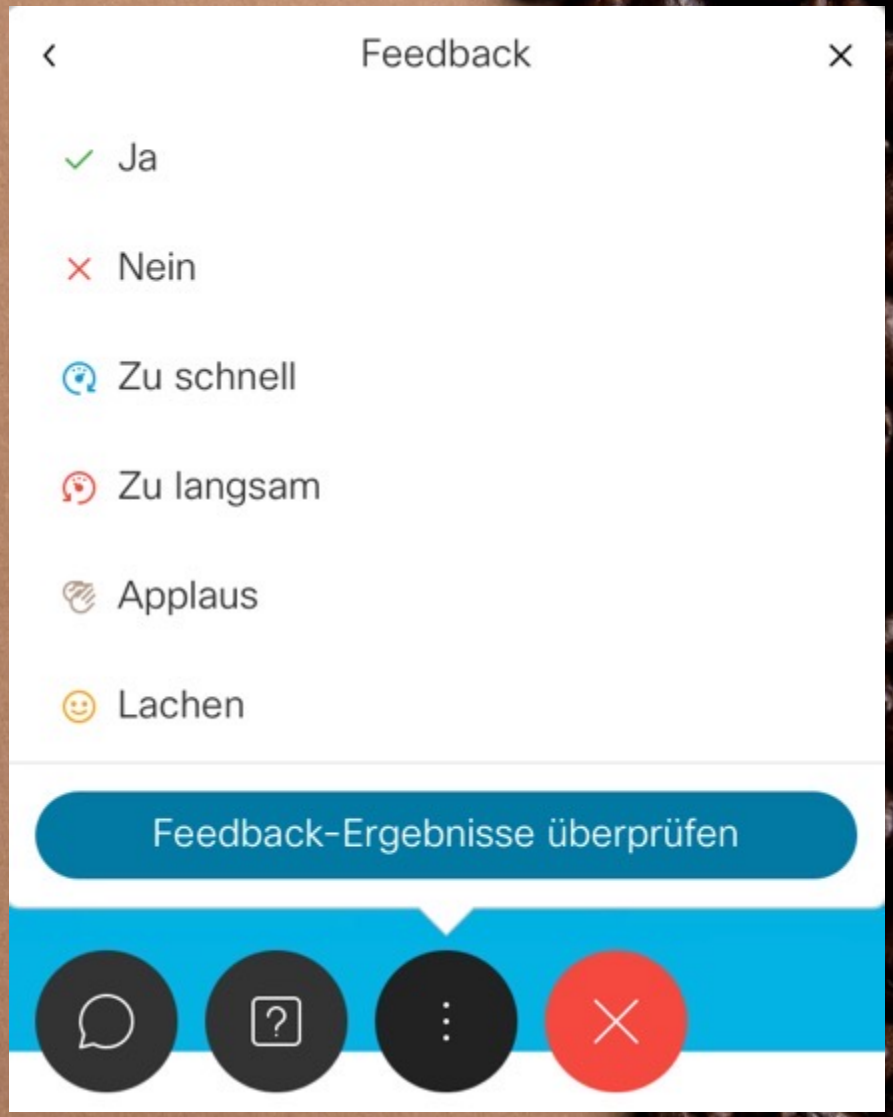
Virtual Espresso Webinar

Mittwoch, 22. Dezember 2021, 15:00 Uhr

👉 please utilise the Q&A function to get your question answered



👉 and use feedback button for answering polling questions



👉 and stay focused during the session...

There will be a Quiz at the end with a Chance to win nice Prices!

3rd Price
Coffee Cup

1st Price
Cisco Headset HS730

2nd Price
Thermo Bottle

Cisco SD-Access Migrationsszenarien

Virtual Espresso Webinar

Patrick Mosimann, Technical Solutions Architect
Vitus Andreoli, Technical Solutions Architect
22. Dezember 2021


Rome
Rome


SD-Access
SD-Access

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

Agenda

1. Connecting L2 domains on Fabric Edge
2. Connecting L2 domains on L2 Border
3. Phased migration
4. L2 Border migration
5. Cisco SJC migration

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

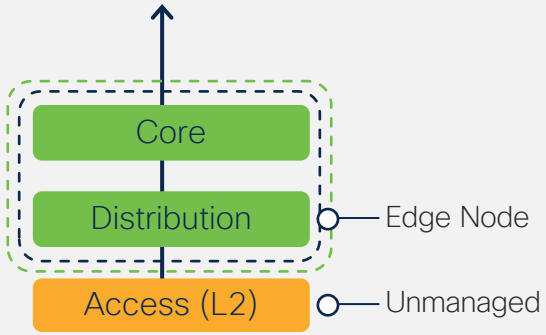
Cisco SD-Access Migrationsszenarien

1. Connecting L2 domains on Fabric Edge
2. Connecting L2 domains on L2 Border
3. Phased migration
4. L2 Border migration
5. Cisco SJC migration

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Different options for **connecting L2 domains**

Fabric with unmanaged Layer 2 switched access

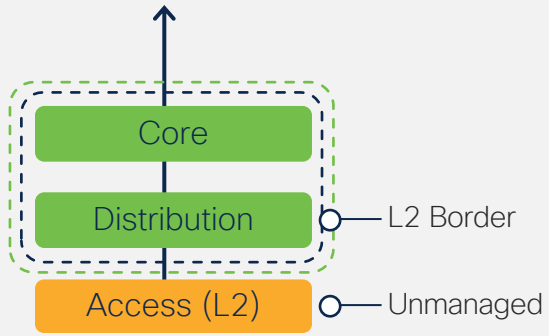


Use case: Keep your existing unmanaged switches

- Segmentation starts at distribution layer
- Integrated wired and wireless

Benefit: Allow tenants to bring their own network.

Fabric with unmanaged Connected Layer 2 domain

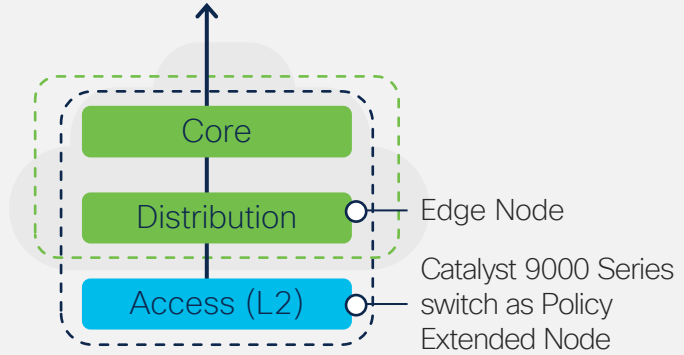


Use case: Connect a legacy/unmanaged network to the fabric

- Segmentation starts at L2 border
- Integrated wired and wireless

Benefit: Allow migrate towards a fabric.

Fabric with managed Layer 2 switched access



Use case: Retain Layer 2 access

- Extend segmentation down to Layer 2
- Integrated wired and wireless

Benefit: Security and automation at every layer

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

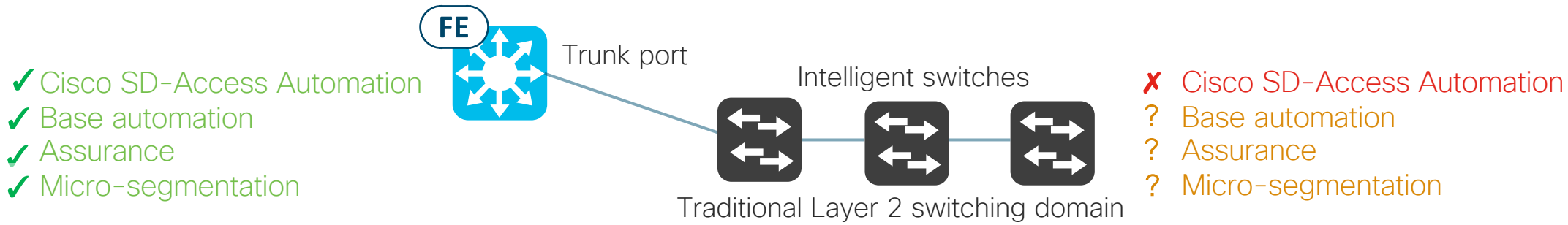
Connecting L2 domains on Fabric Edge

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

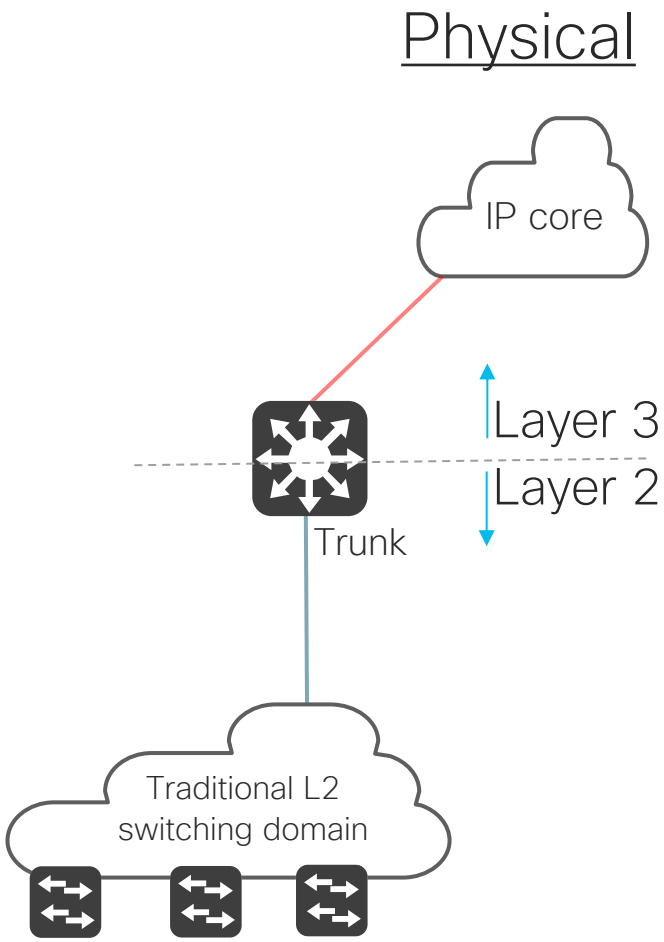
Tradeoffs for the traditional Layer 2 switching domain:

- 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



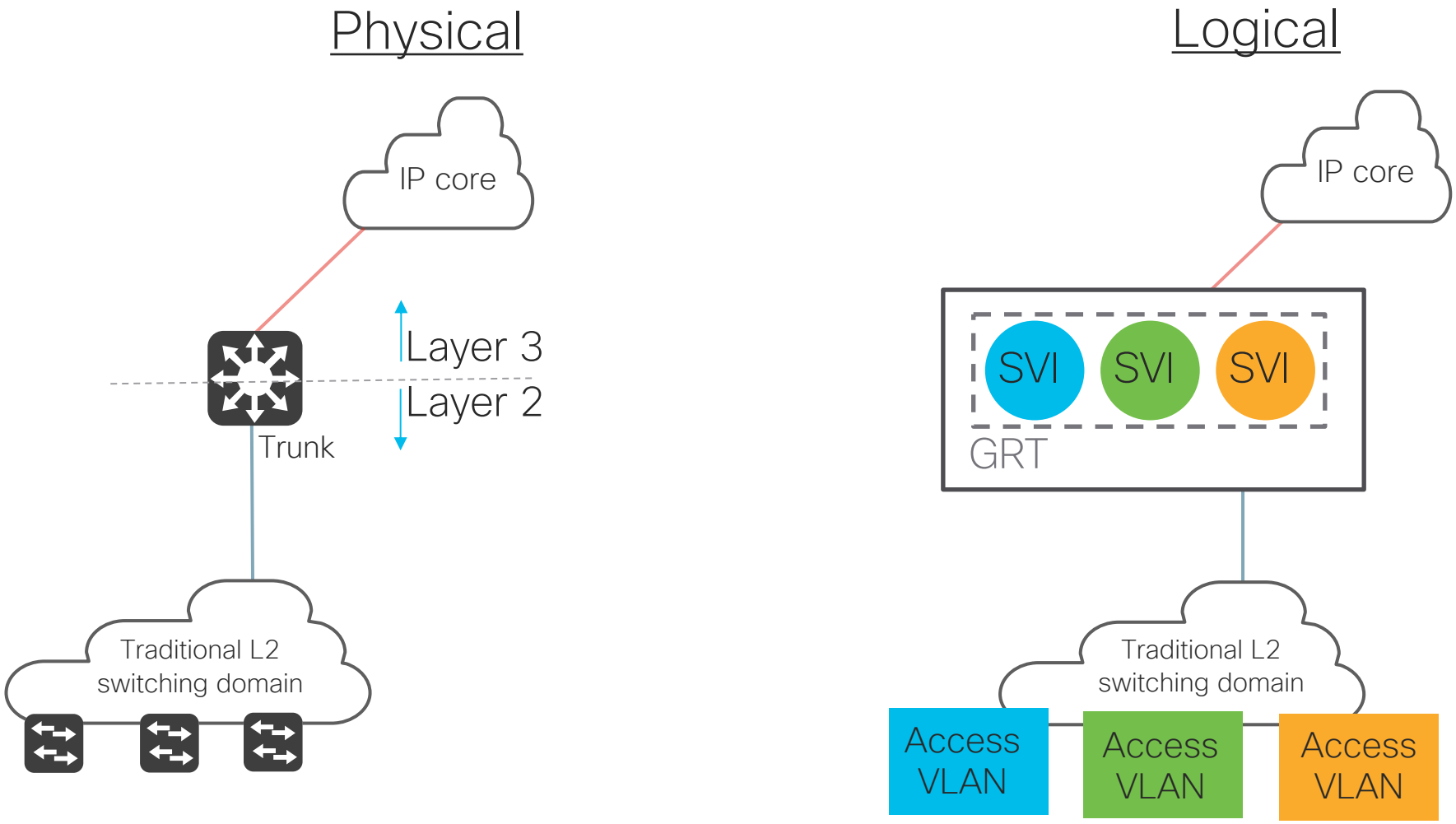
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Connecting L2 domains on Fabric Edge
Automated VN-based macro-segmentation over an IP core (1/9)



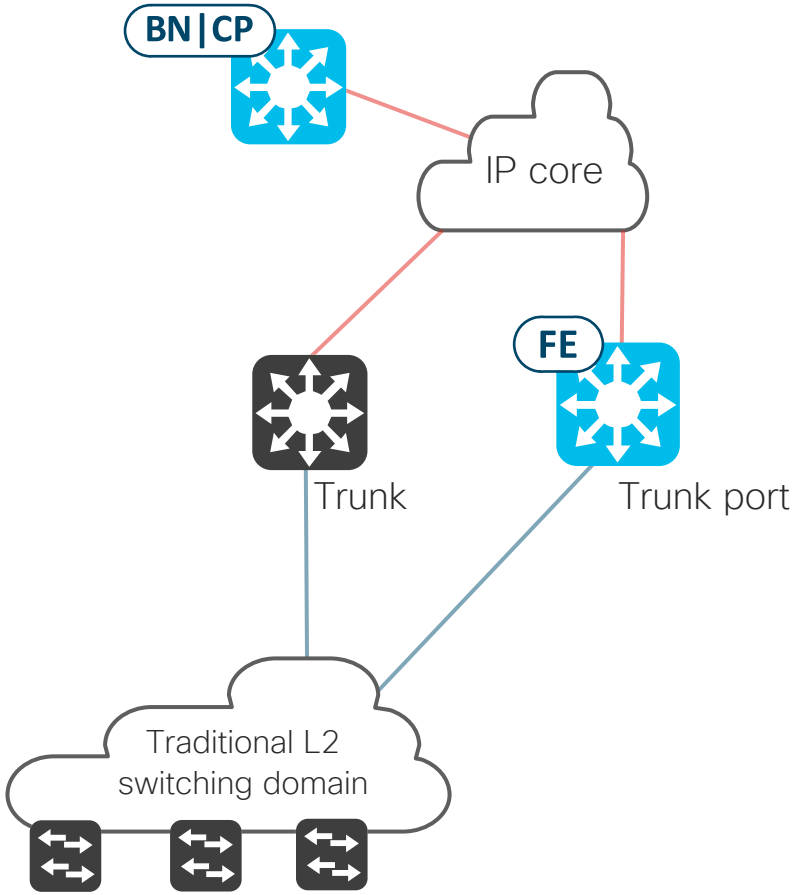
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

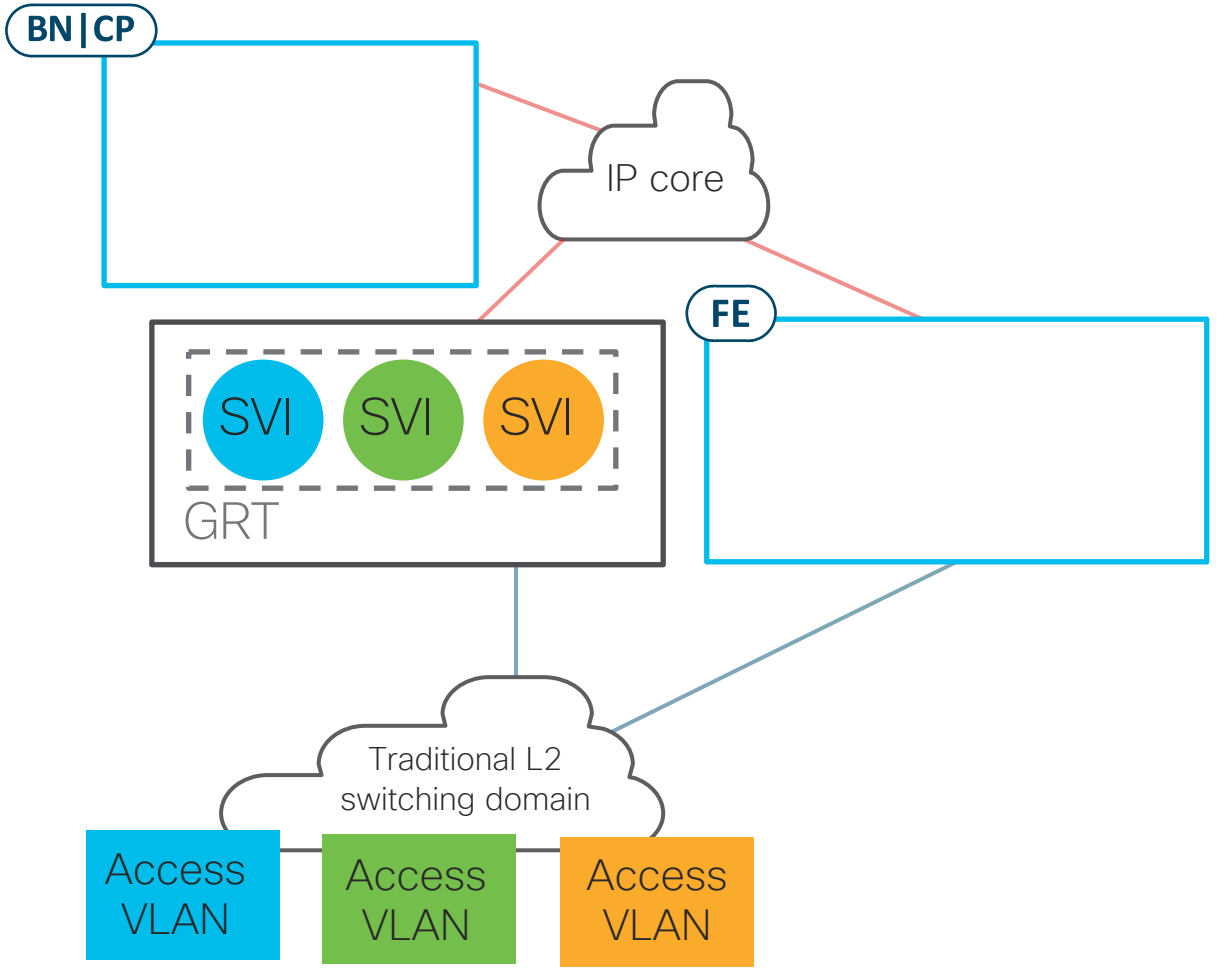
Connecting L2 domains on Fabric Edge
Automated VN-based macro-segmentation over an IP core (2/9)



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

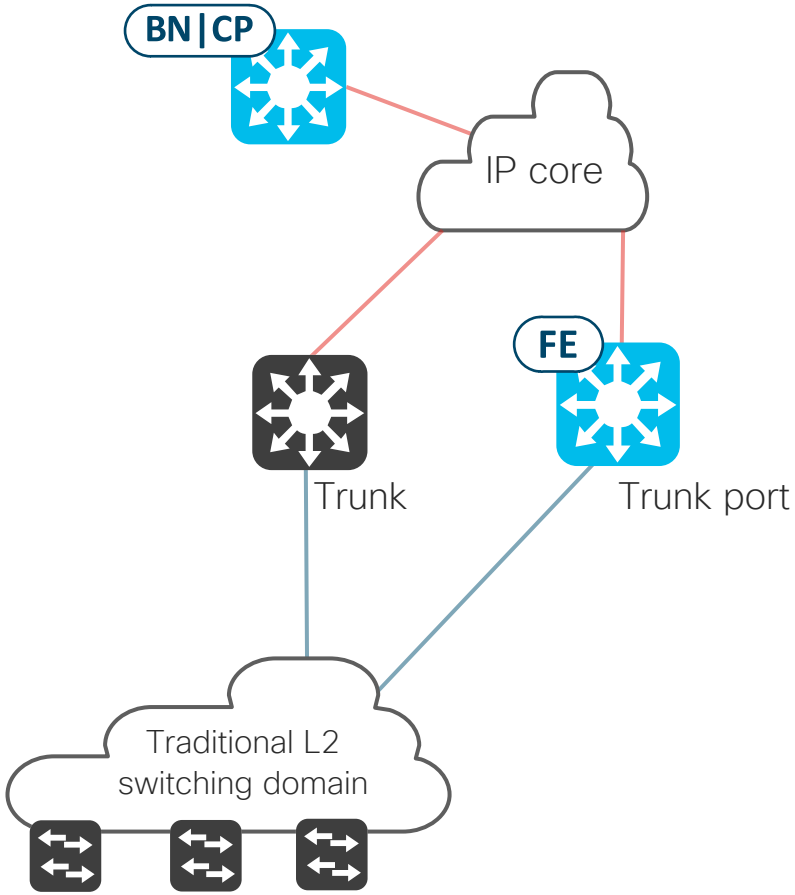
Connecting L2 domains on Fabric Edge
Automated VN-based macro-segmentation over an IP core (3/9)

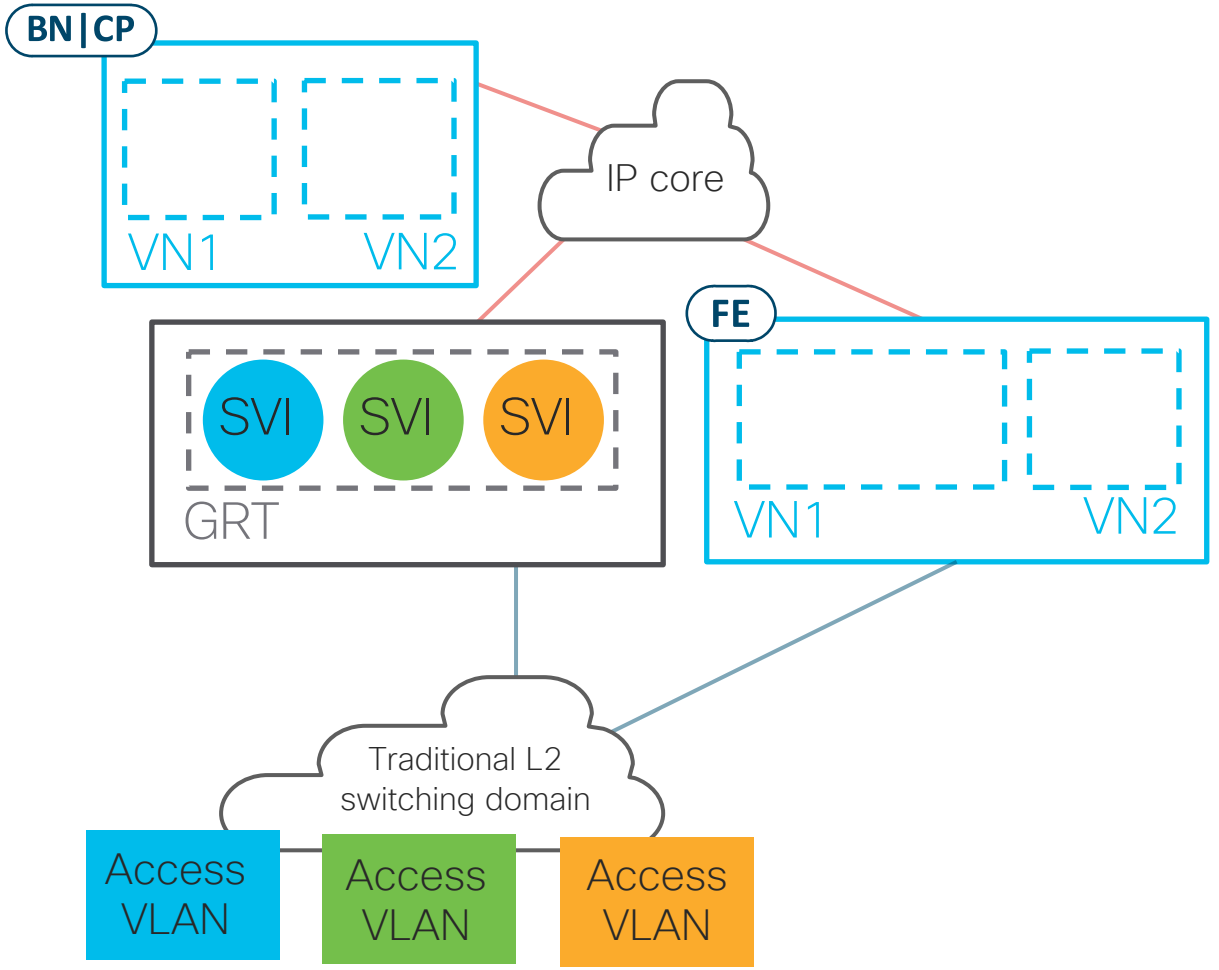




© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Connecting L2 domains on Fabric Edge
Automated VN-based macro-segmentation over an IP core (4/9)

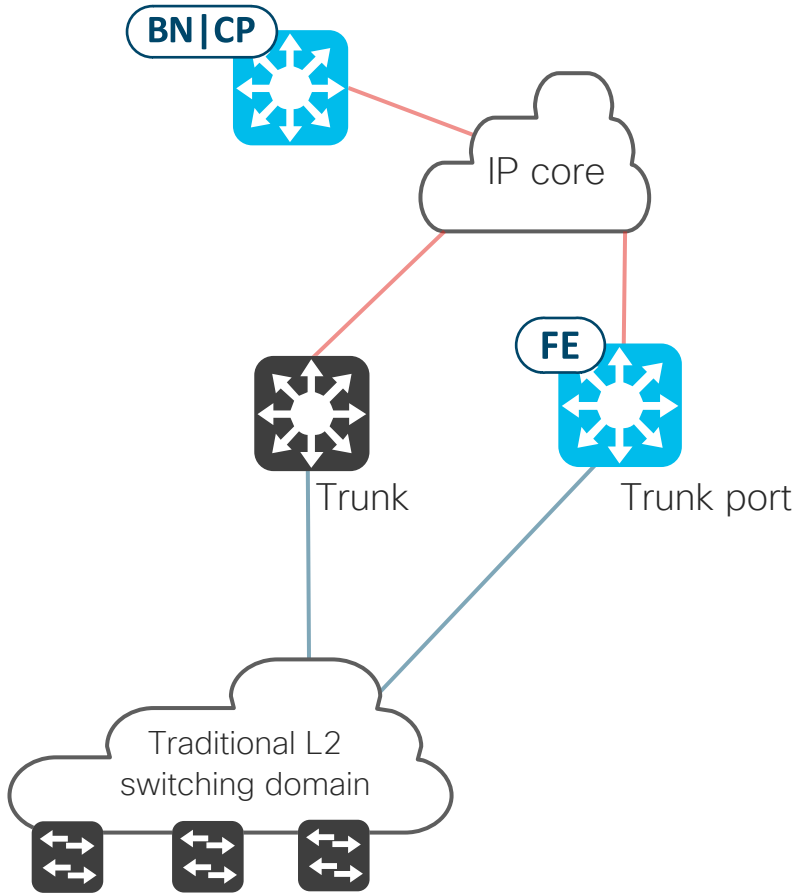


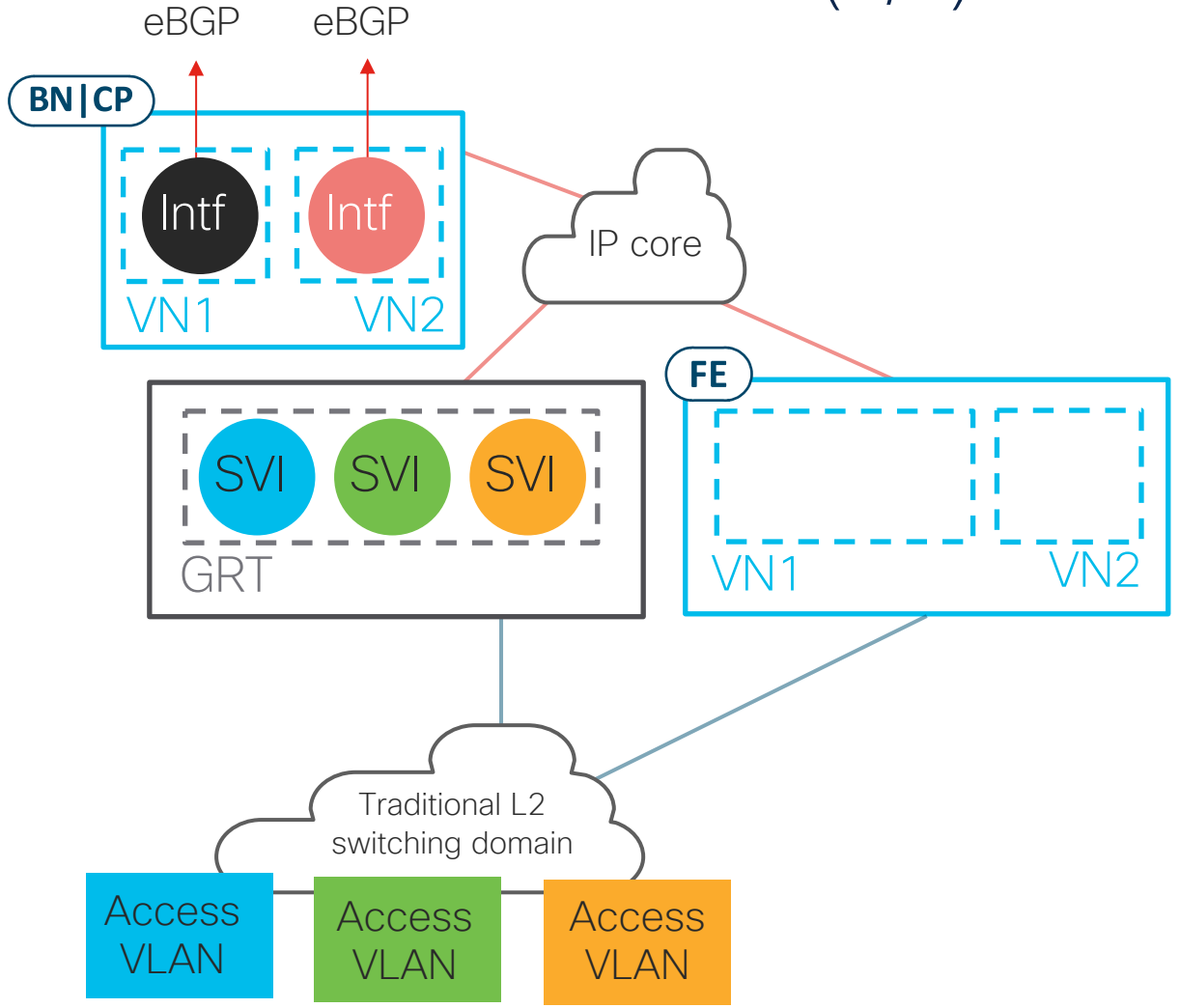


© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Connecting L2 domains on Fabric Edge

Automated VN-based macro-segmentation over an IP core (5/9)

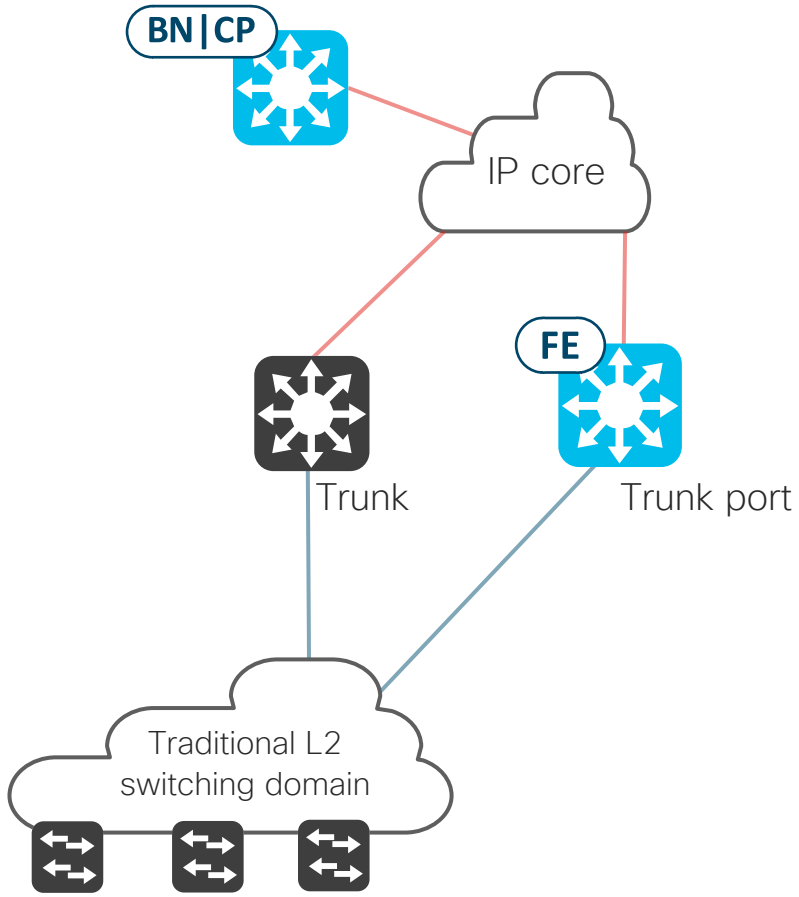


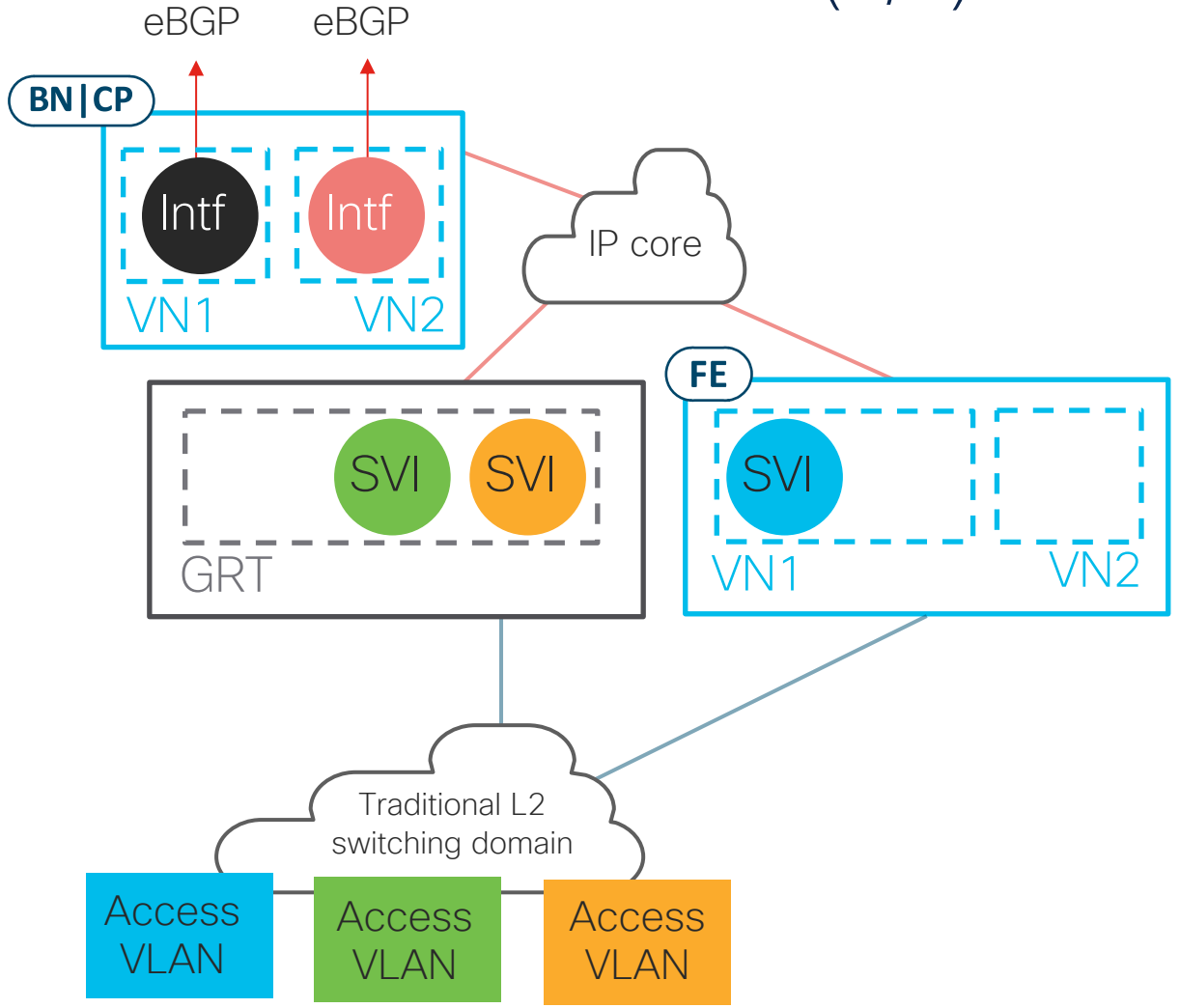


© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Connecting L2 domains on Fabric Edge

Automated VN-based macro-segmentation over an IP core (6/9)

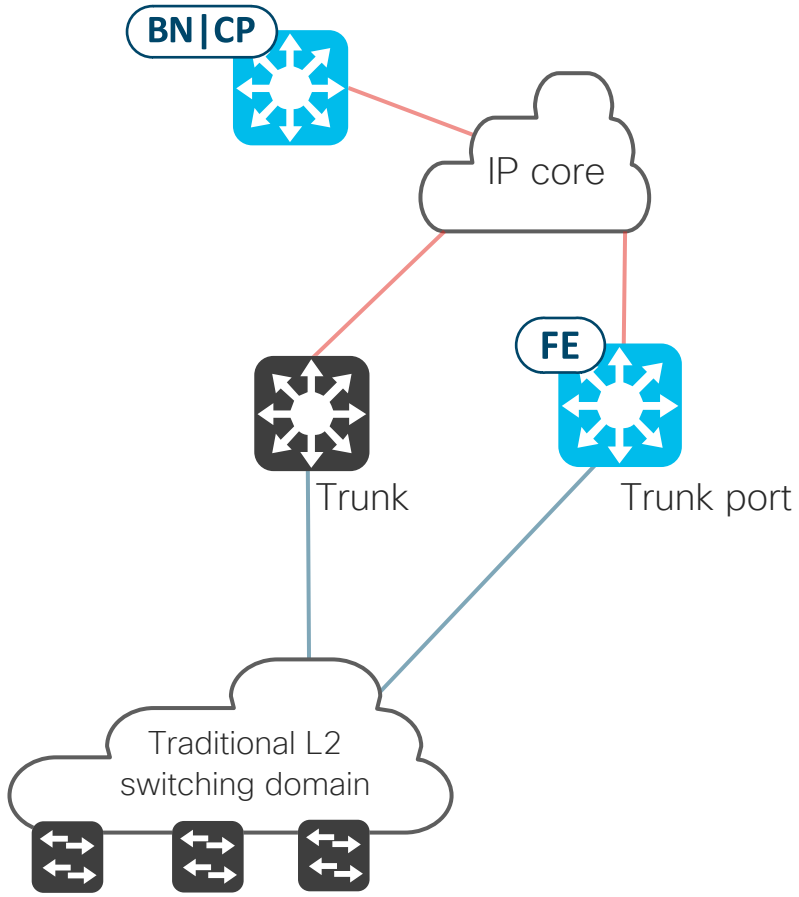


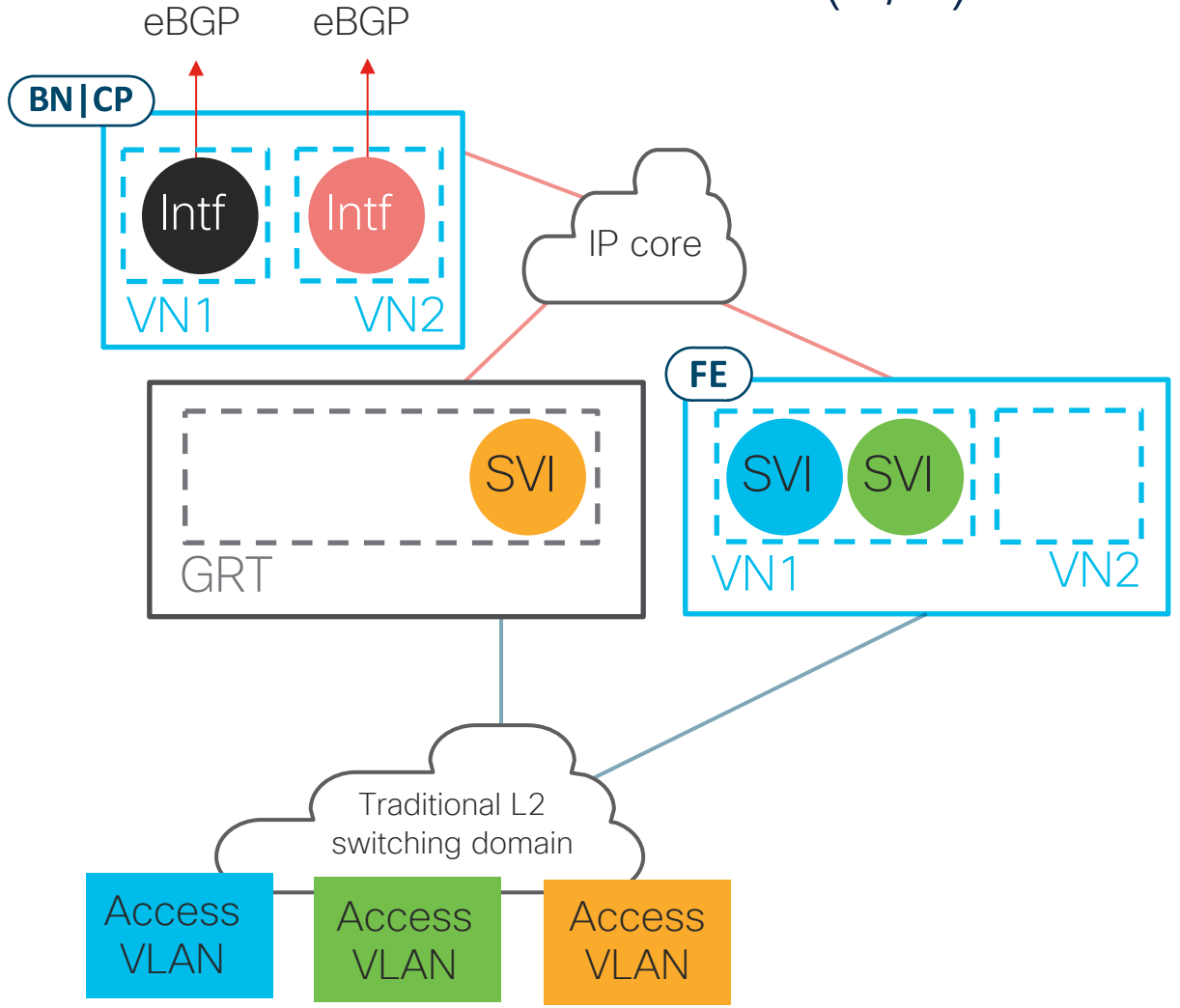


© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Connecting L2 domains on Fabric Edge

Automated VN-based macro-segmentation over an IP core (7/9)

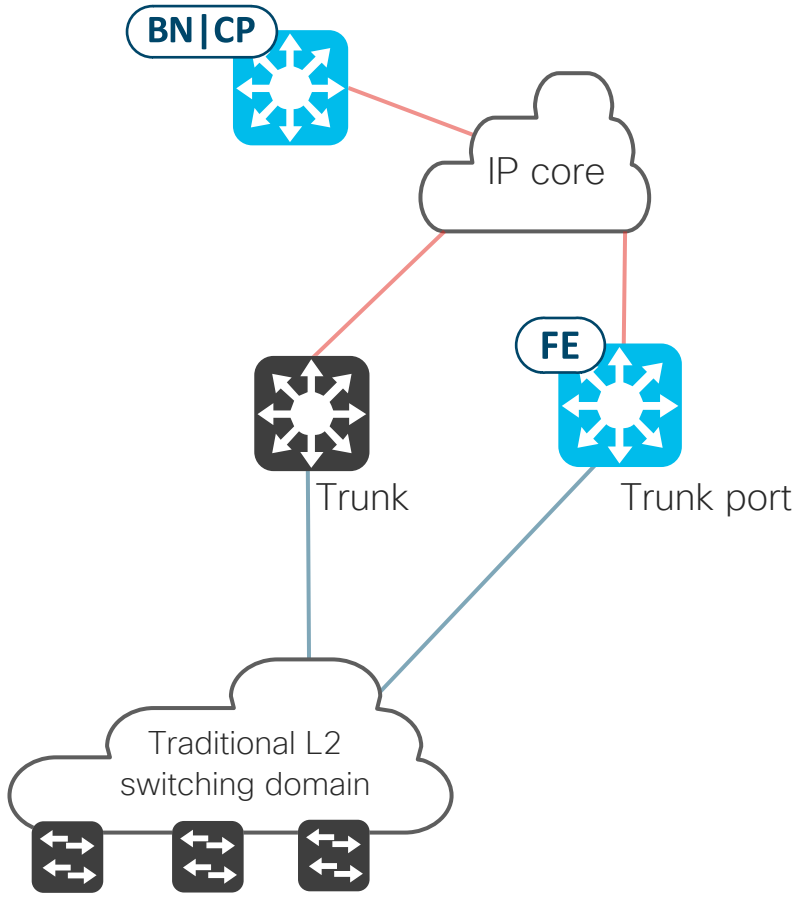


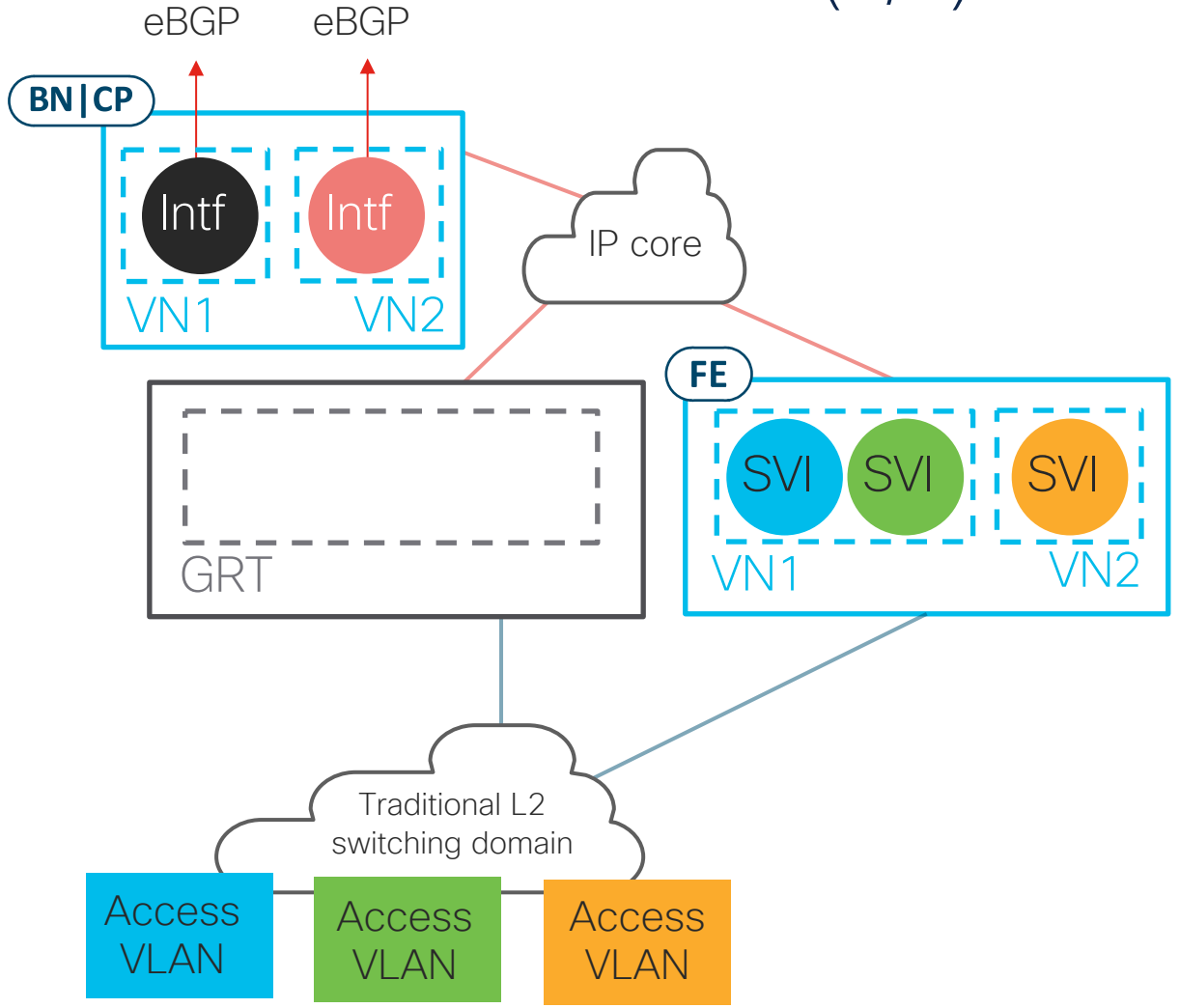


© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Connecting L2 domains on Fabric Edge

Automated VN-based macro-segmentation over an IP core (8/9)

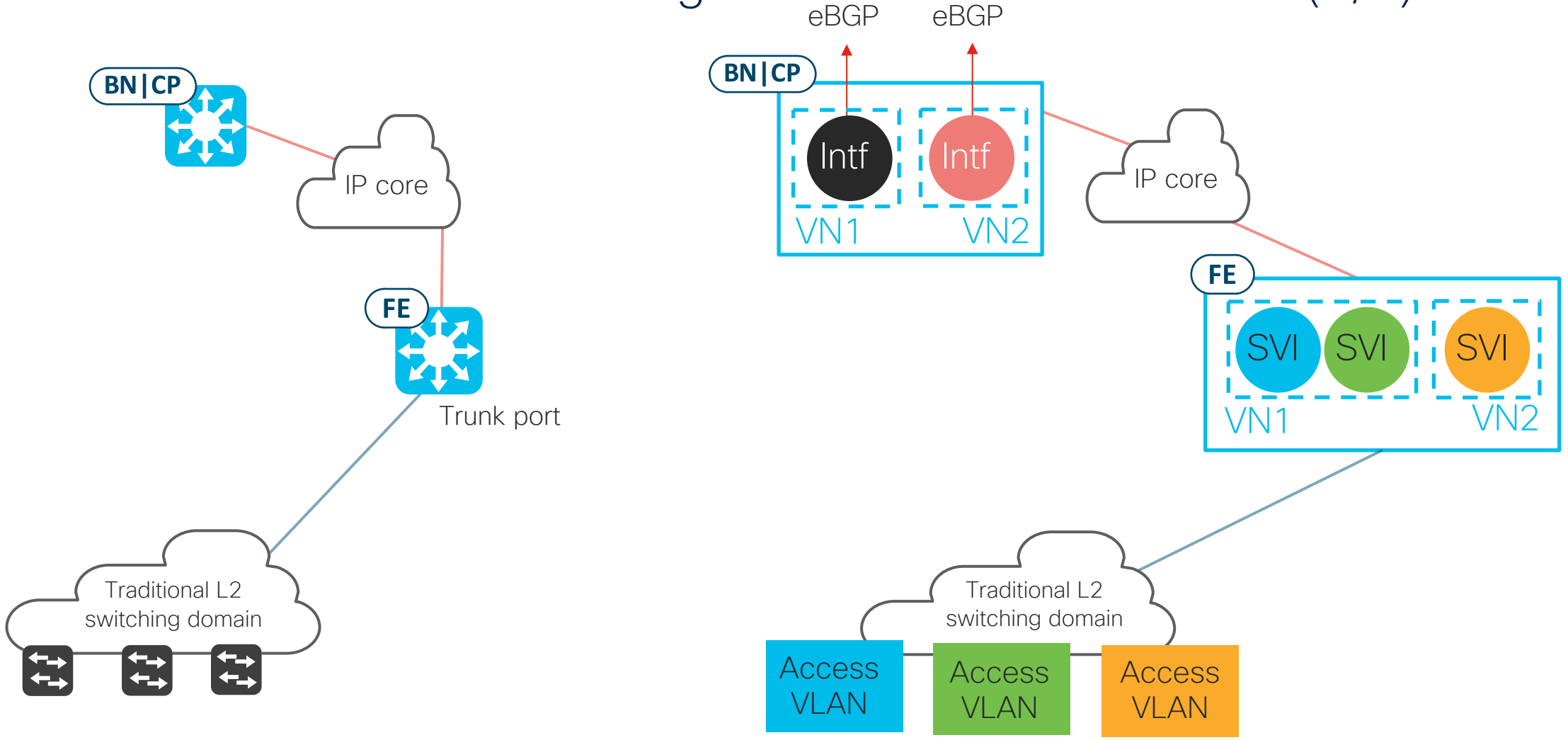




© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

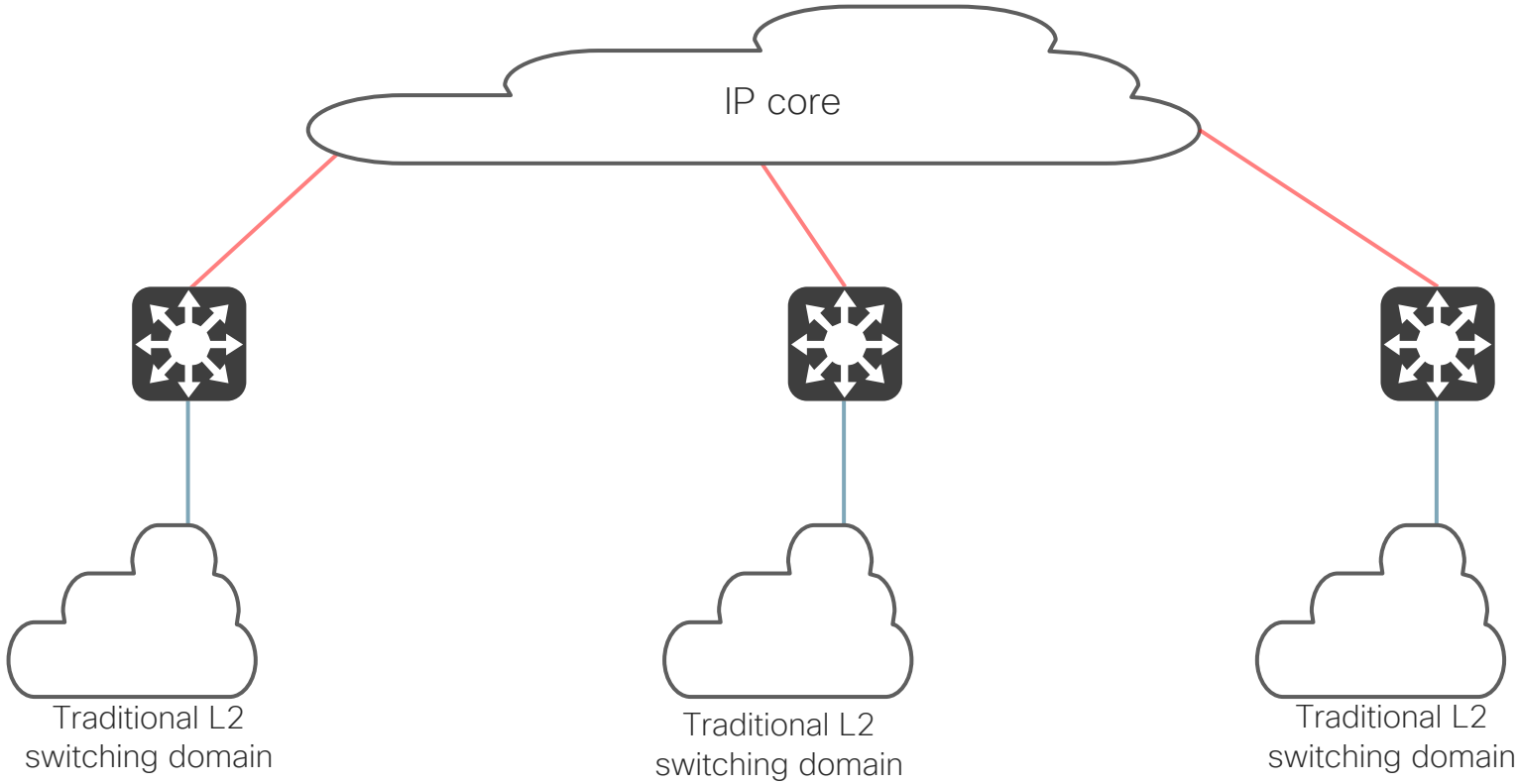
Connecting L2 domains on Fabric Edge

Automated VN-based macro-segmentation over an IP core (9/9)



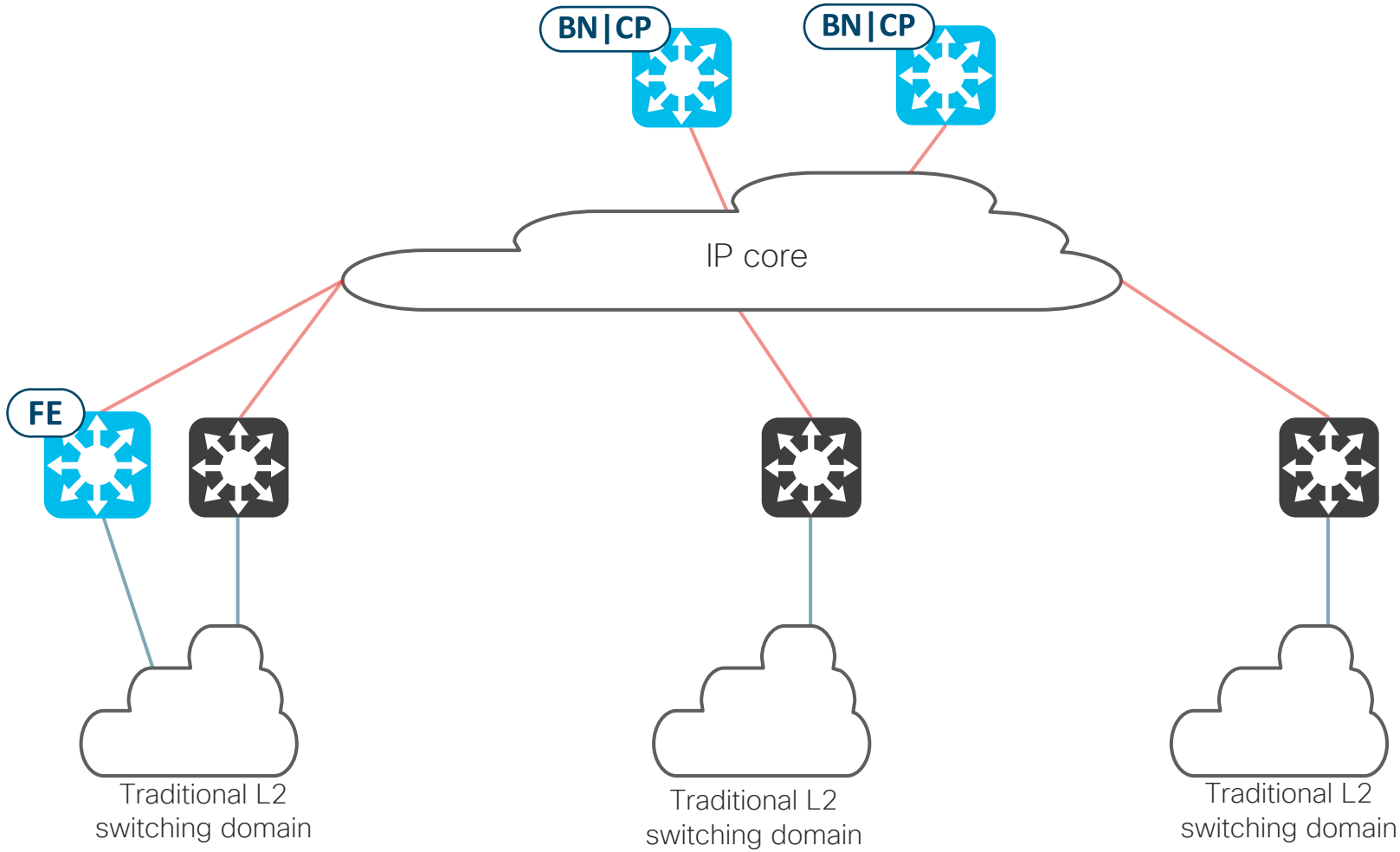
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Connecting L2 domains on Fabric Edge
Adding multiple L2 switching domains (1/7)



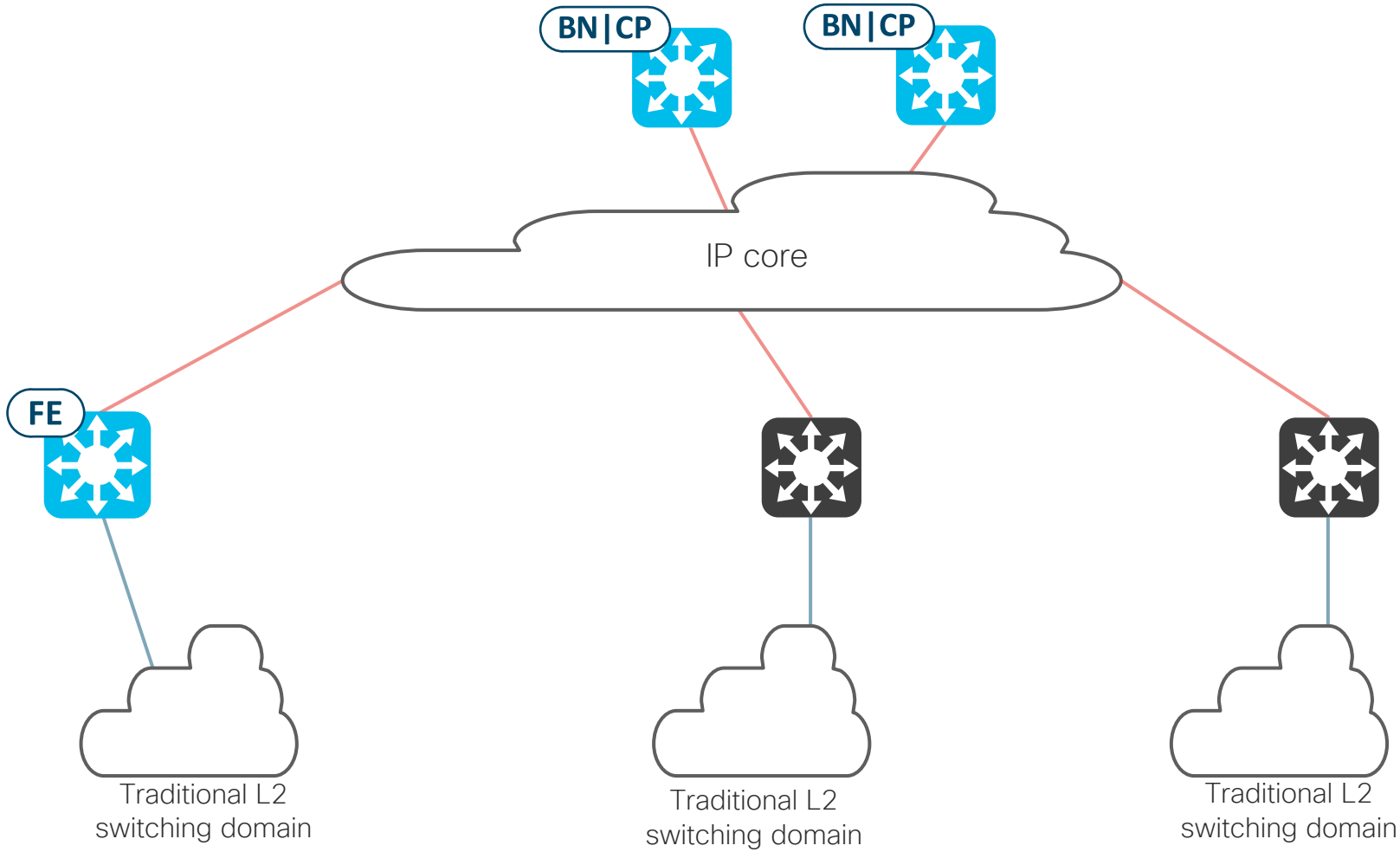
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Connecting L2 domains on Fabric Edge
Adding multiple L2 switching domains (2/7)



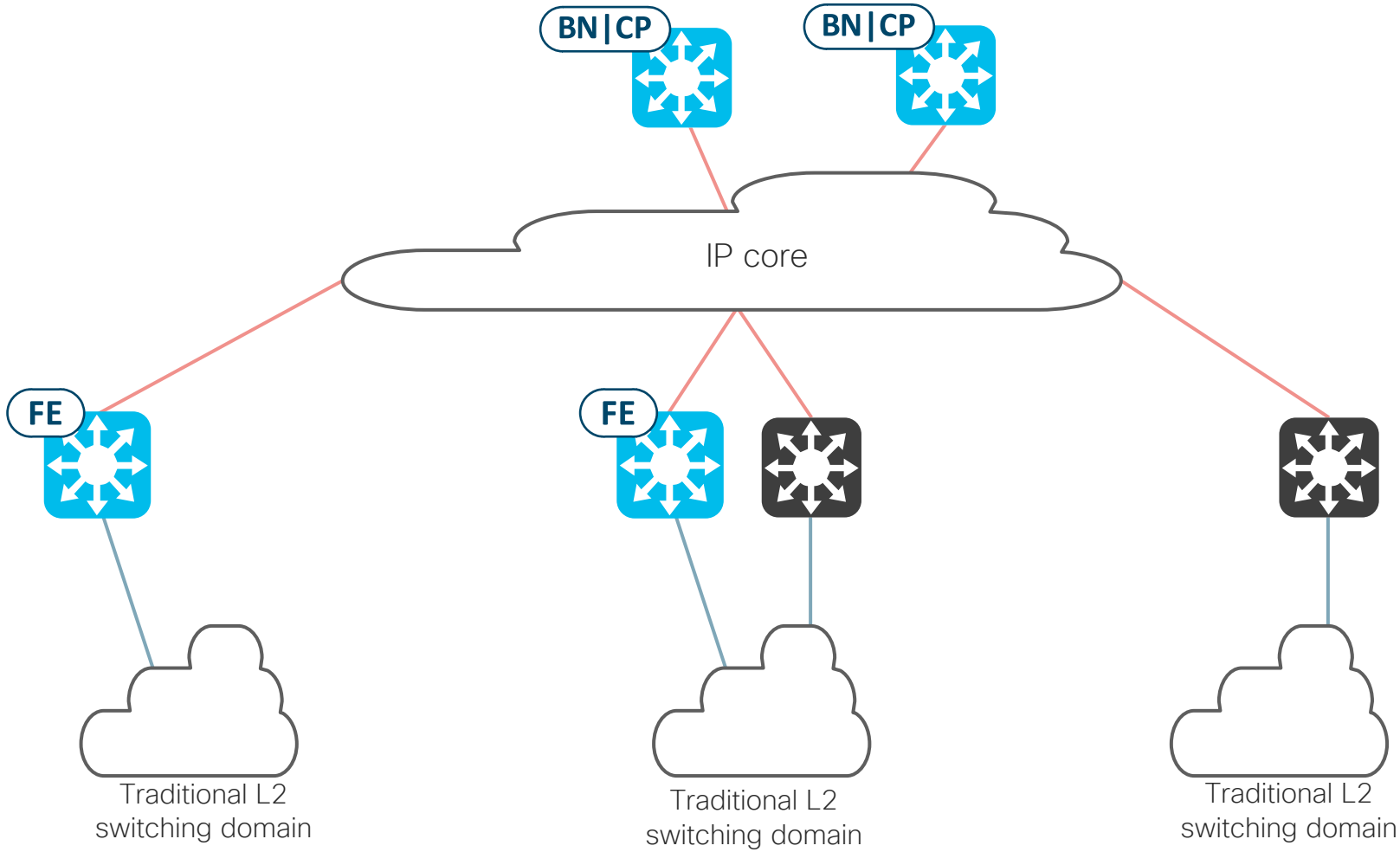
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Connecting L2 domains on Fabric Edge
Adding multiple L2 switching domains (3/7)



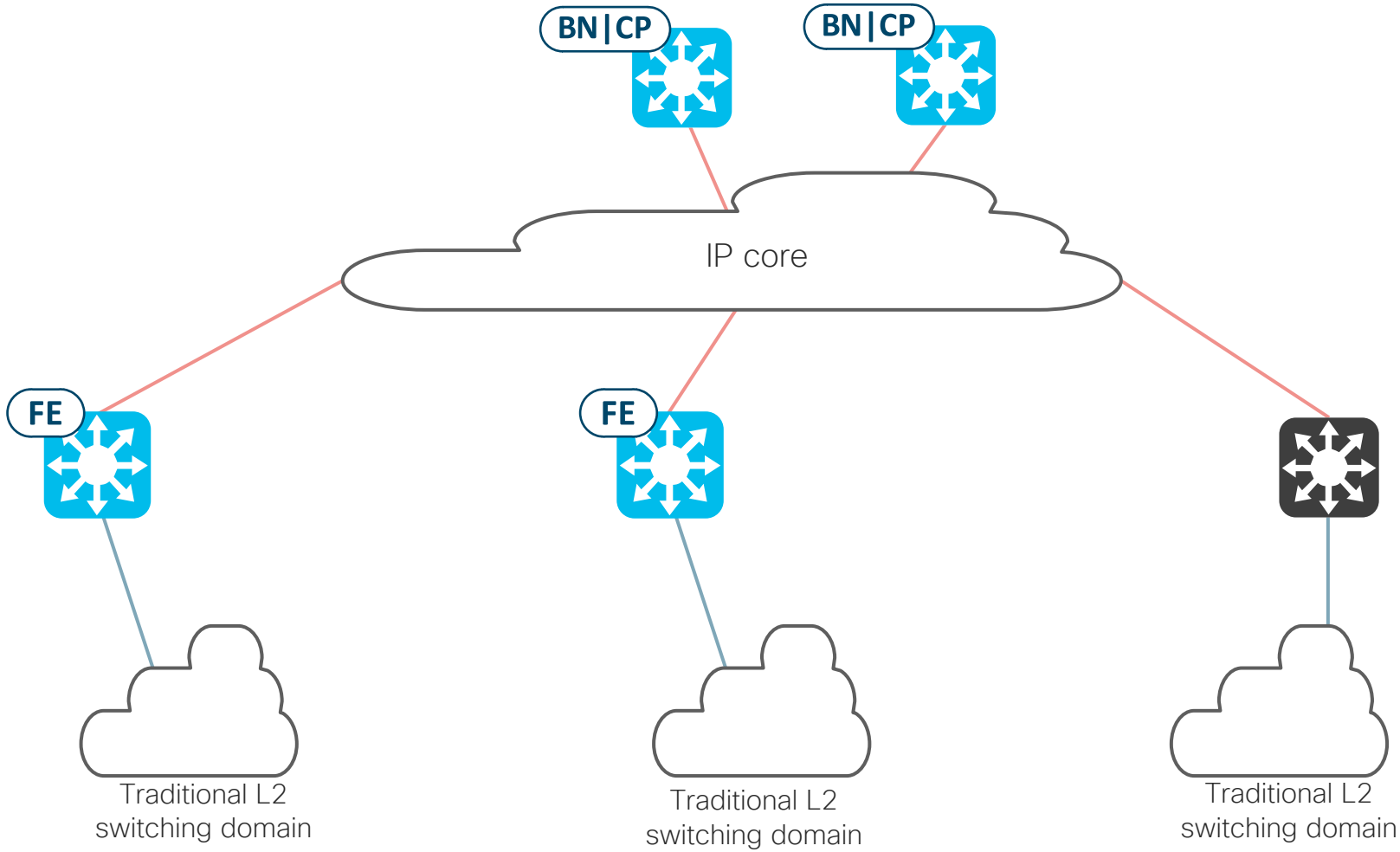
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Connecting L2 domains on Fabric Edge
Adding multiple L2 switching domains (4/7)



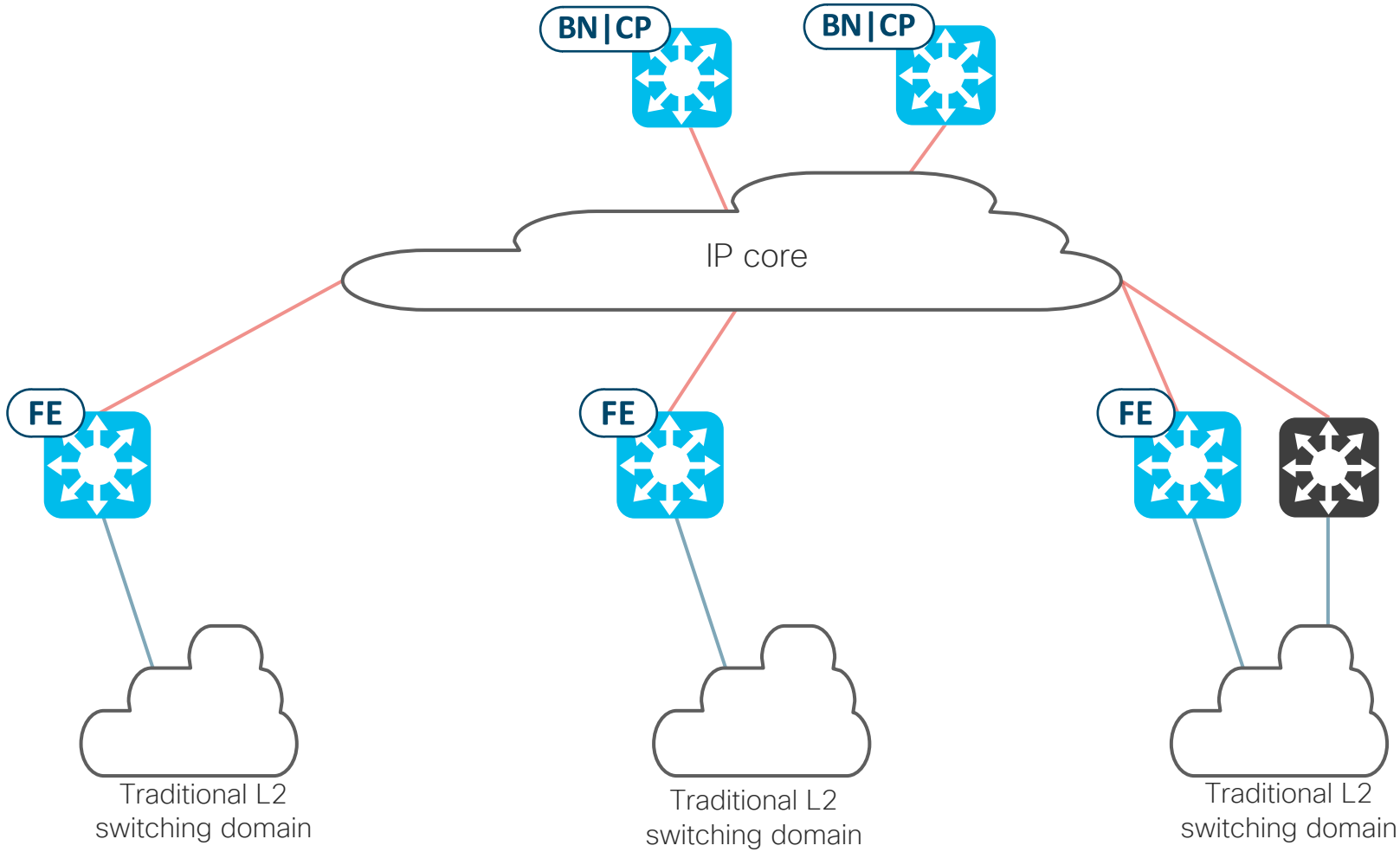
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Connecting L2 domains on Fabric Edge
Adding multiple L2 switching domains (5/7)



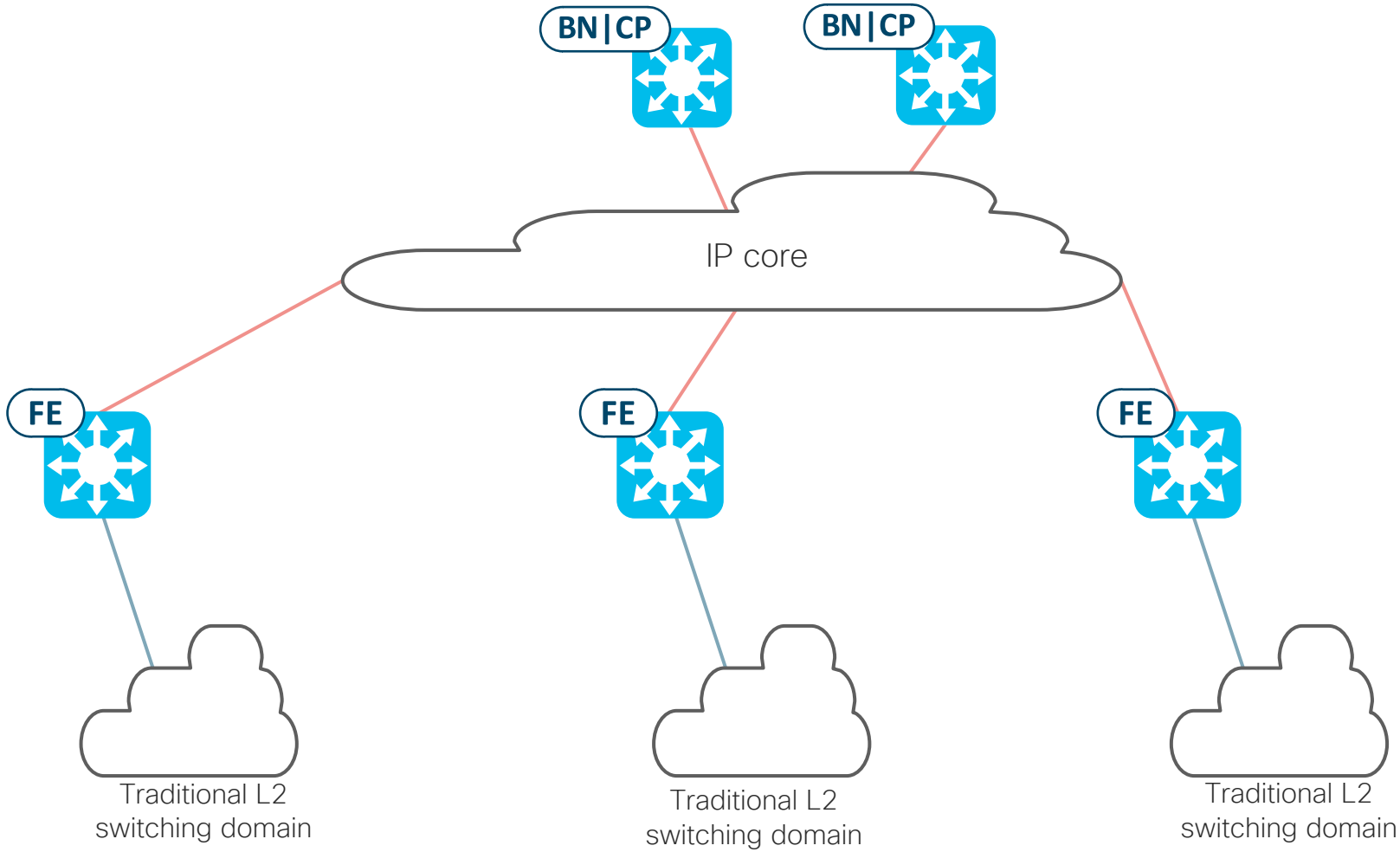
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Connecting L2 domains on Fabric Edge
Adding multiple L2 switching domains (6/7)



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

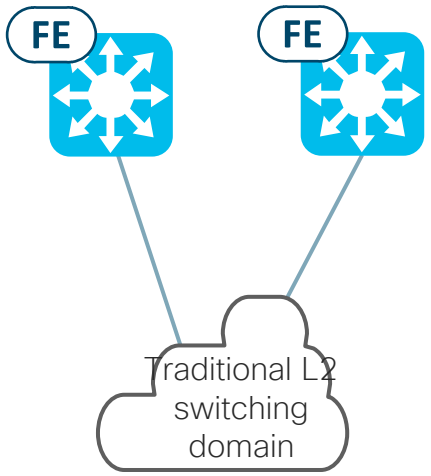
Connecting L2 domains on Fabric Edge
Adding multiple L2 switching domains (7/7)



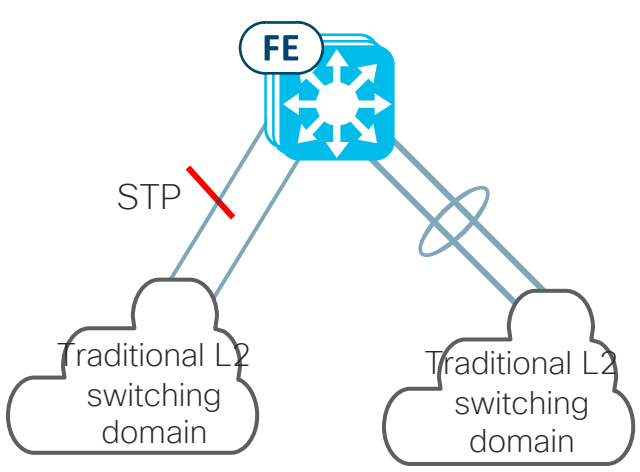
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

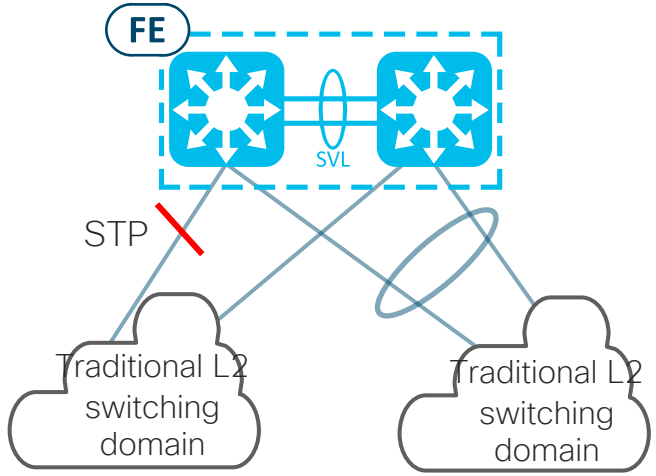
Connecting L2 domains on Fabric Edge
Important Considerations (1/6)

- 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.

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Connecting L2 domains on Fabric Edge
Important Considerations (2/6)

- 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

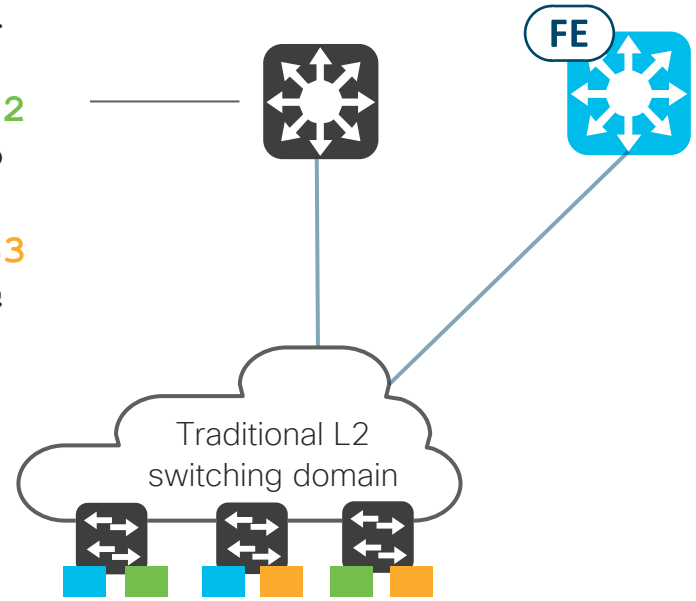
Wireless Deployment Type	Roam Pattern	Average Observed Roam Latency
FlexConnect OTT	APs connected to the **same** Edge Node	700-800 ms
FlexConnect OTT	APs connected to **different** Edge Nodes	700-800 ms
SD-Access Wireless	APs connected to the **same** edge node	70 ms
SD-Access Wireless	APs connected to **different** edge nodes	85 ms

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Connecting L2 domains on Fabric Edge
Important Considerations (3/6)

- 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
```



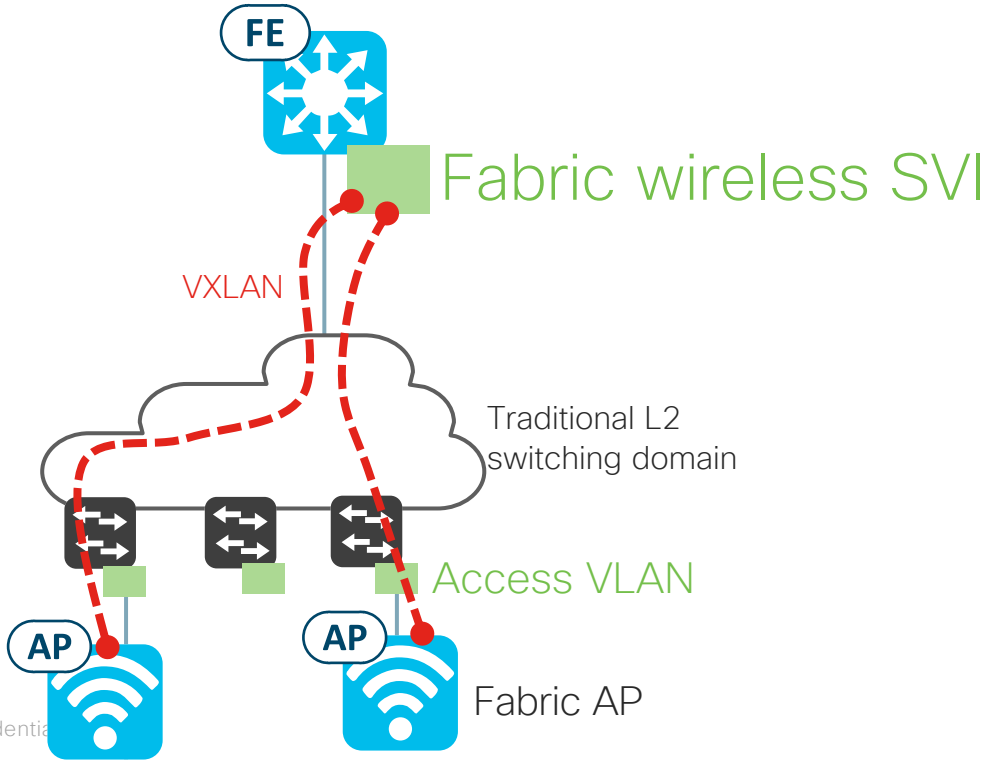

```
interface VLAN111
  vrf forwarding CORP
  ip address aaa
  no shutdown
interface VLAN222
  vrf forwarding CCTV
  ip address bbb
  no shutdown
```

*introduced in 2.2.2.x

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Connecting L2 domains on Fabric Edge
Important Considerations (4/6)

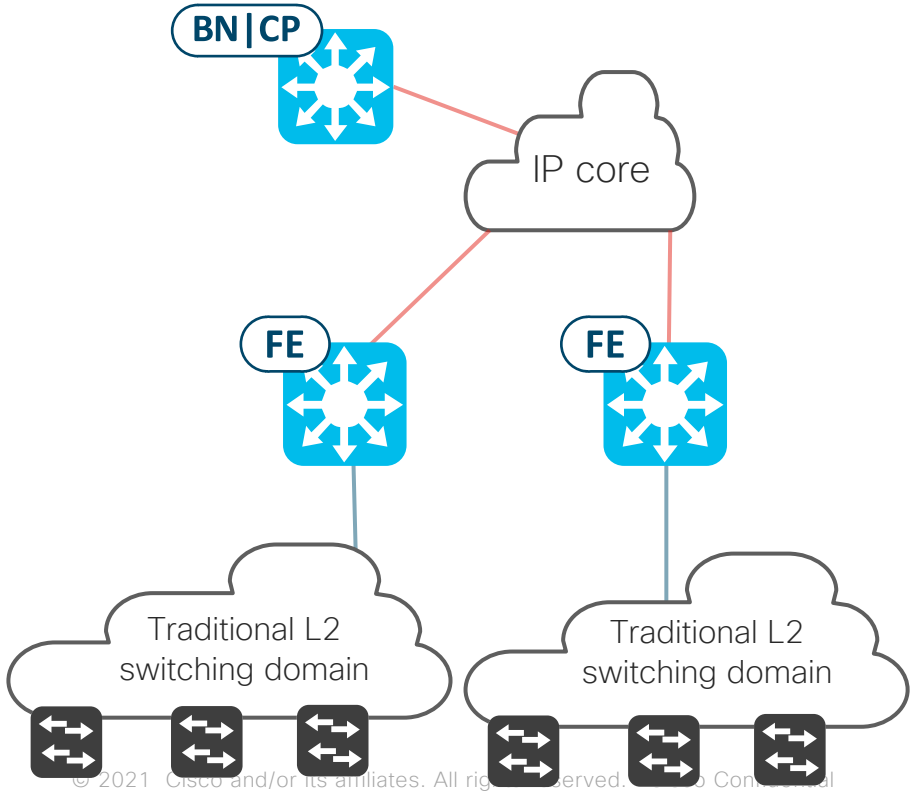
- Fabric APs connected to traditional L2 switching domain are already supported.
  - This enables a rapid realization of the benefits of Fabric-Enabled Wireless (SGT, Automation, Assurance, wireless data plane switched locally on Edge Node, etc.)



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidentia

Connecting L2 domains on Fabric Edge
Important Considerations (5/6)

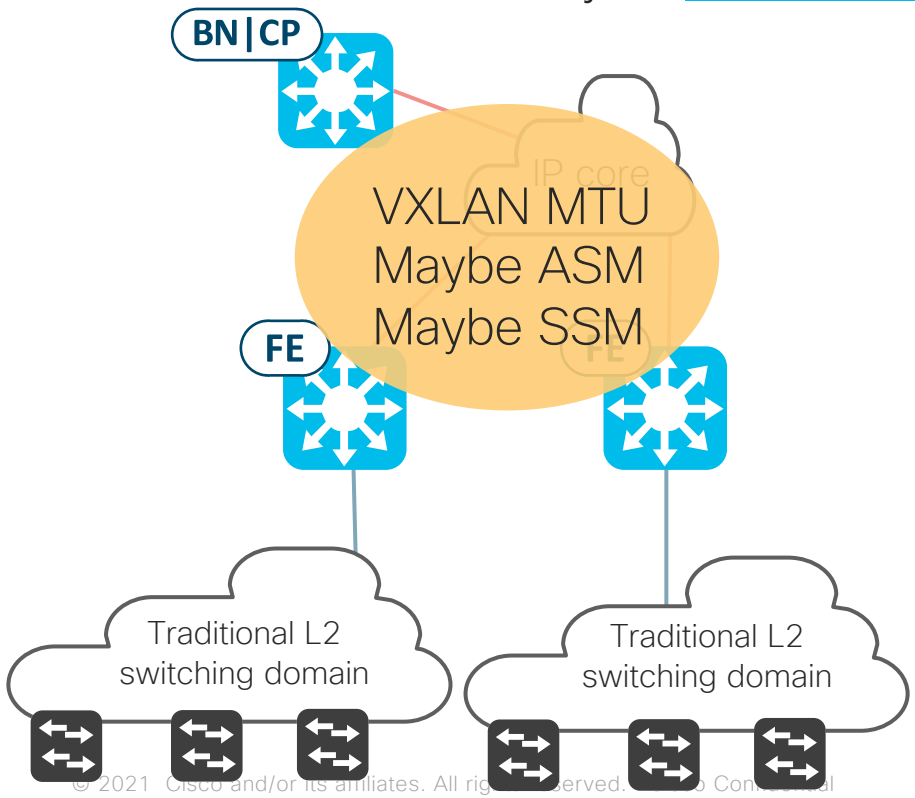
- The IP core may need to support multicast and jumbo MTU (depends on size of overlay packets).
  - Covered heavily in DGTL-BRKENS-3822. But in short:



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Connecting L2 domains on Fabric Edge
Important Considerations (6/6)

- 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.

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

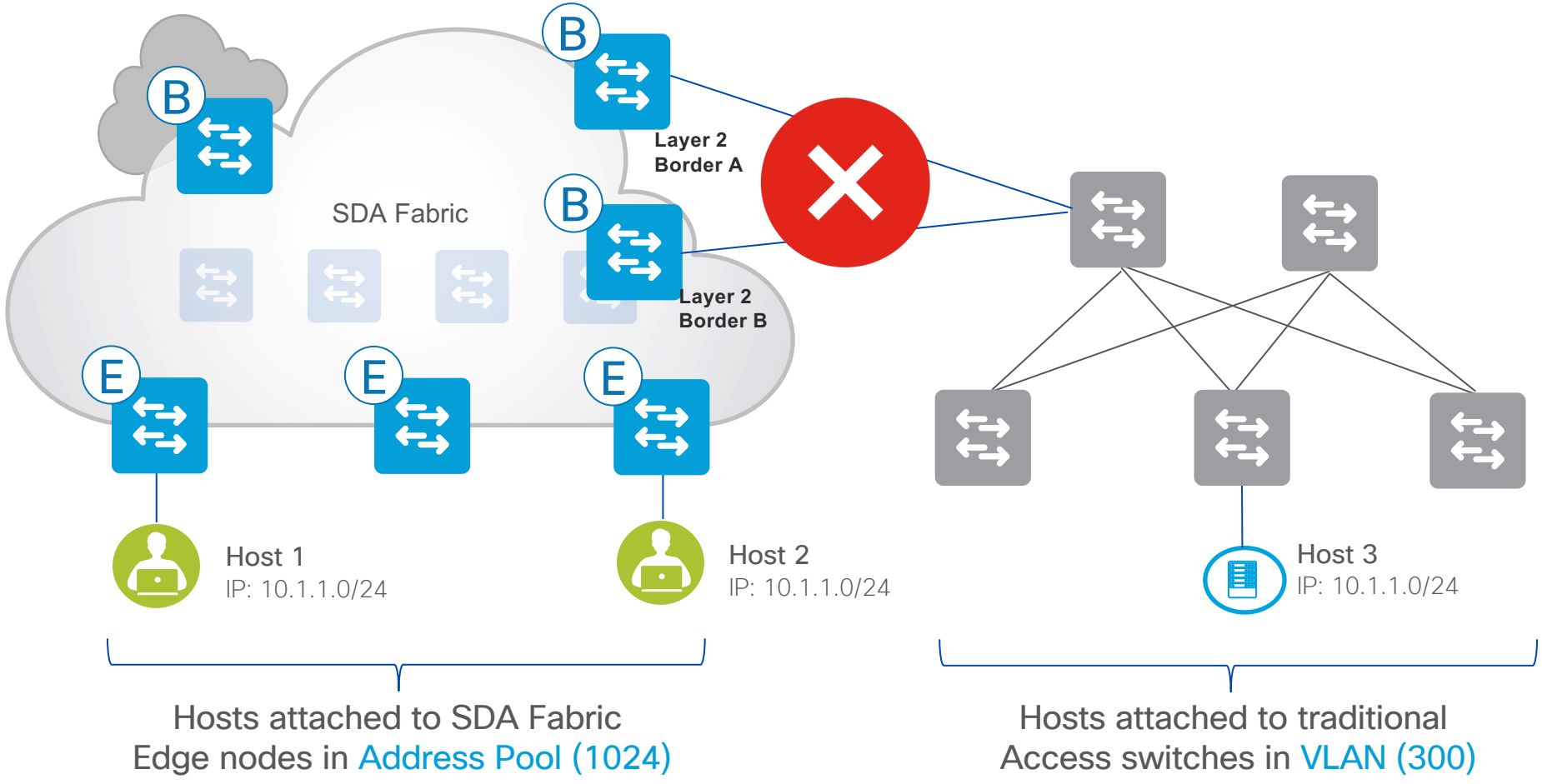
Cisco SD-Access Migrationsszenarien

1. Connecting L2 domains on Fabric Edge
2. Connecting L2 domains on L2 Border
3. Phased migration
4. L2 Border migration
5. Cisco SJC migration

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

L2 Border – Deployment Model

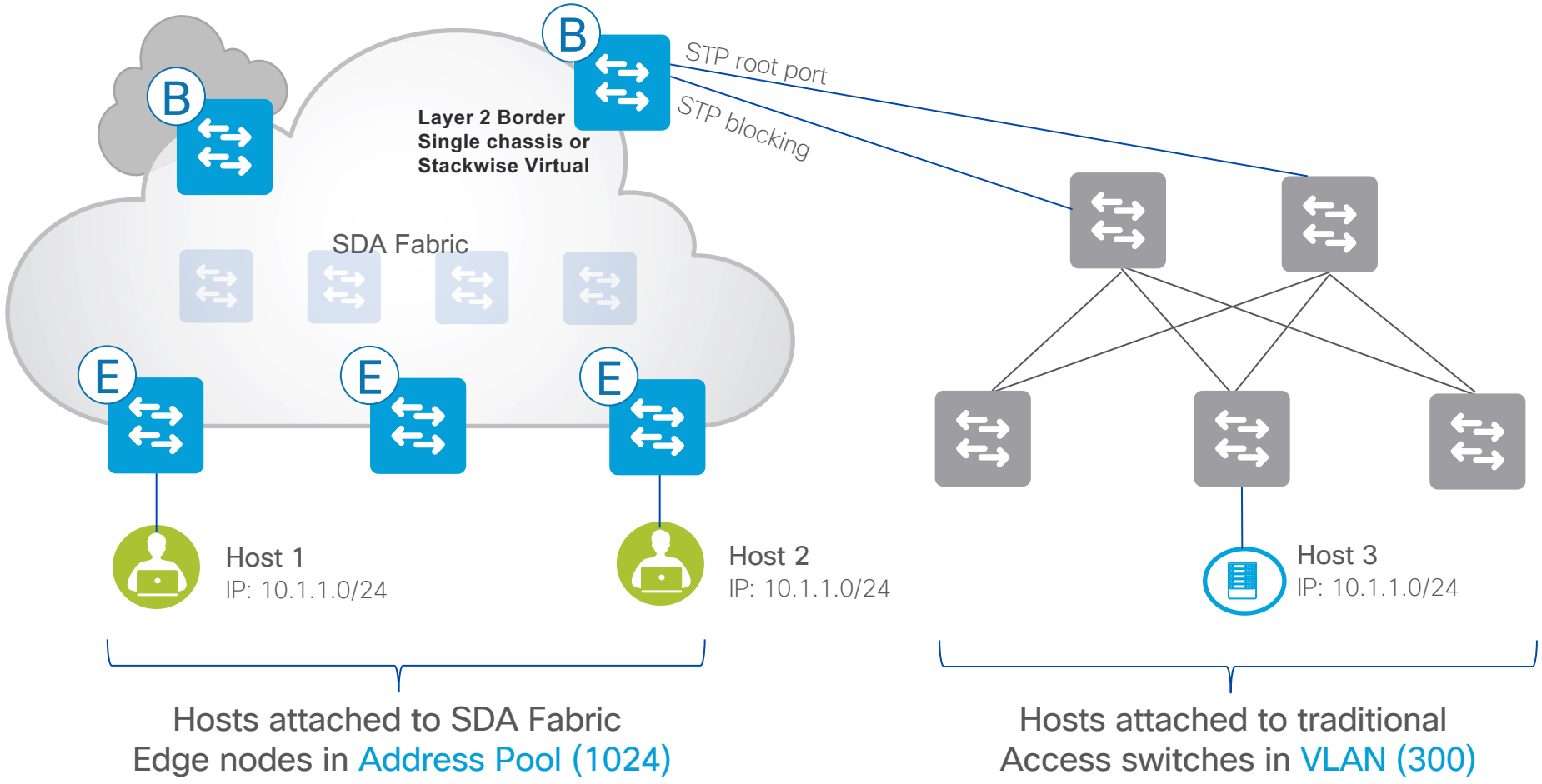
Same VLAN on two borders not supported



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

L2 Border – Deployment Model

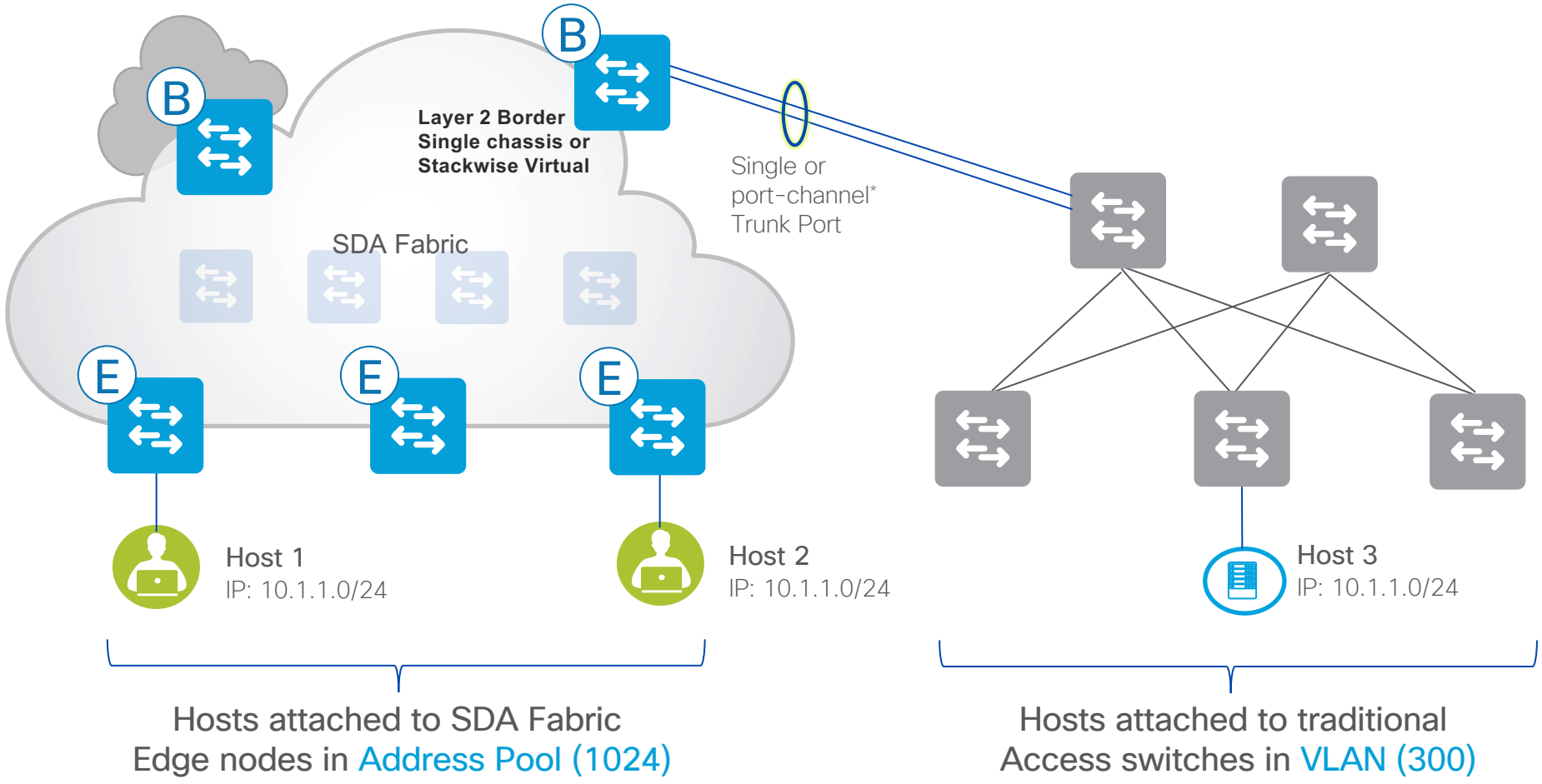
Supported



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

L2 Border – Deployment Model

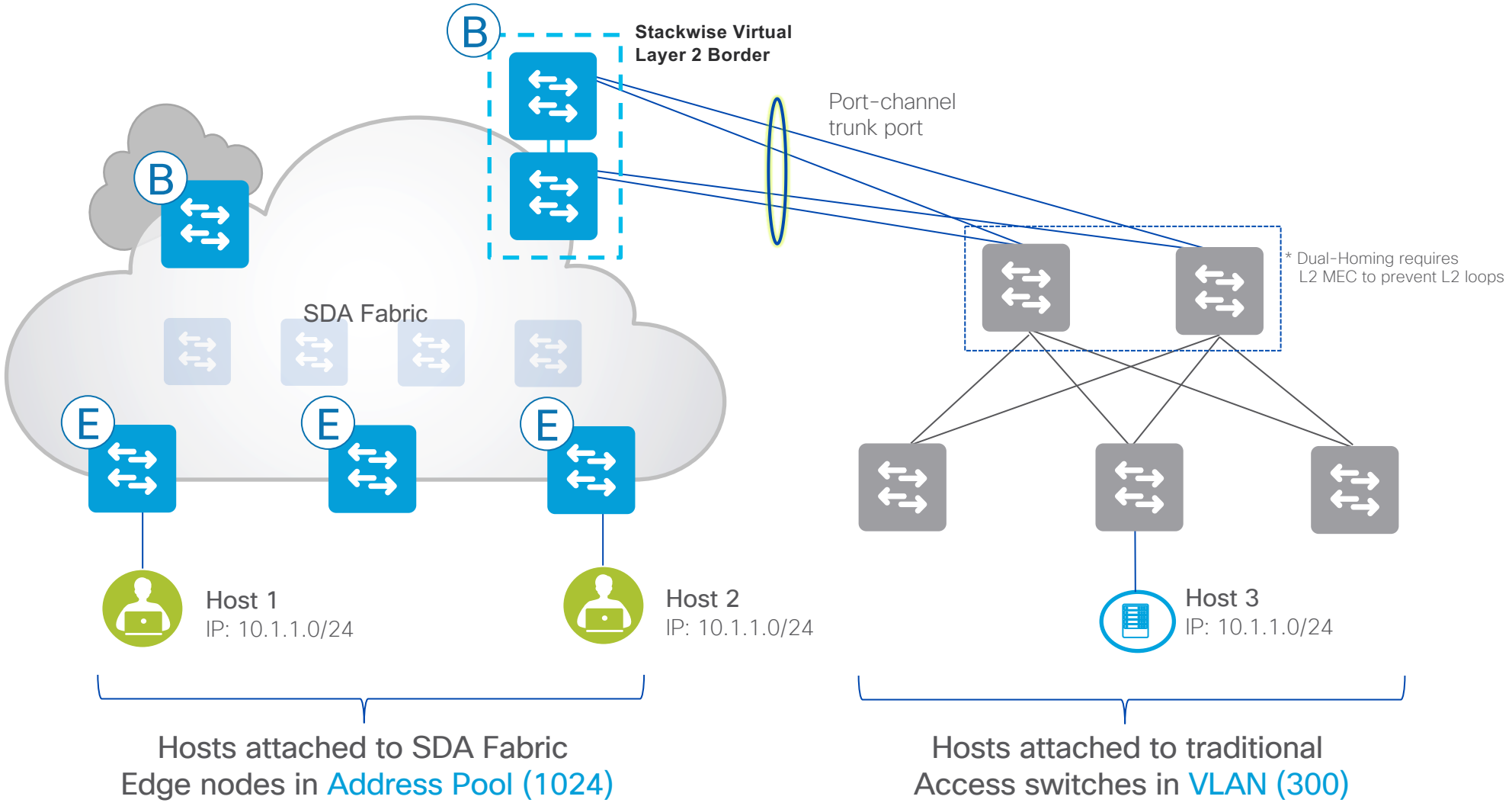
Supported



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

L2 Border – Deployment Model

Stackwise Virtual 9500 and 9500H



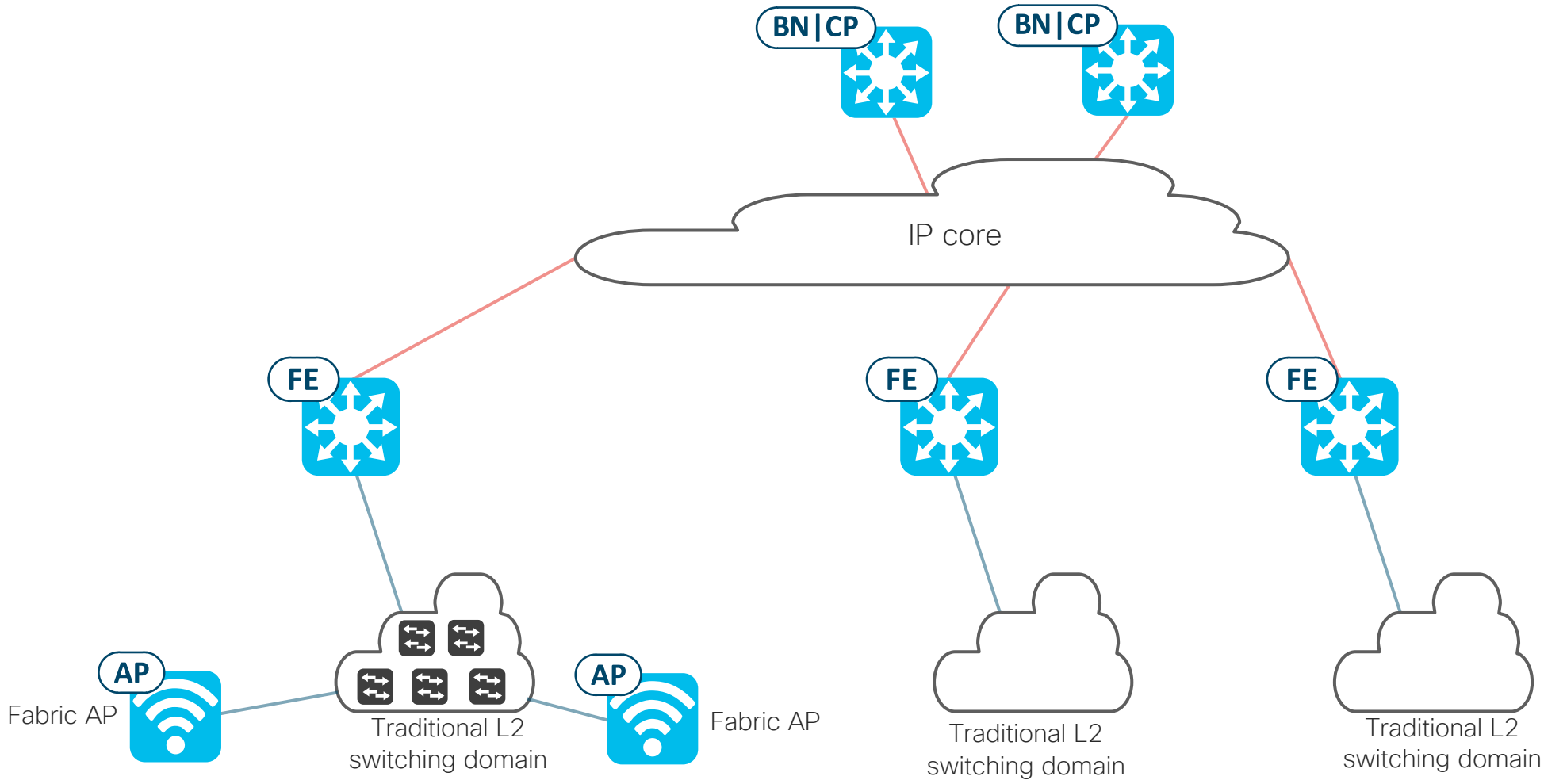
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco SD-Access Migrationsszenarien

1. Connecting L2 domains on Fabric Edge
2. Connecting L2 domains on L2 Border
3. Phased migration
4. L2 Border migration
5. Cisco SJC migration

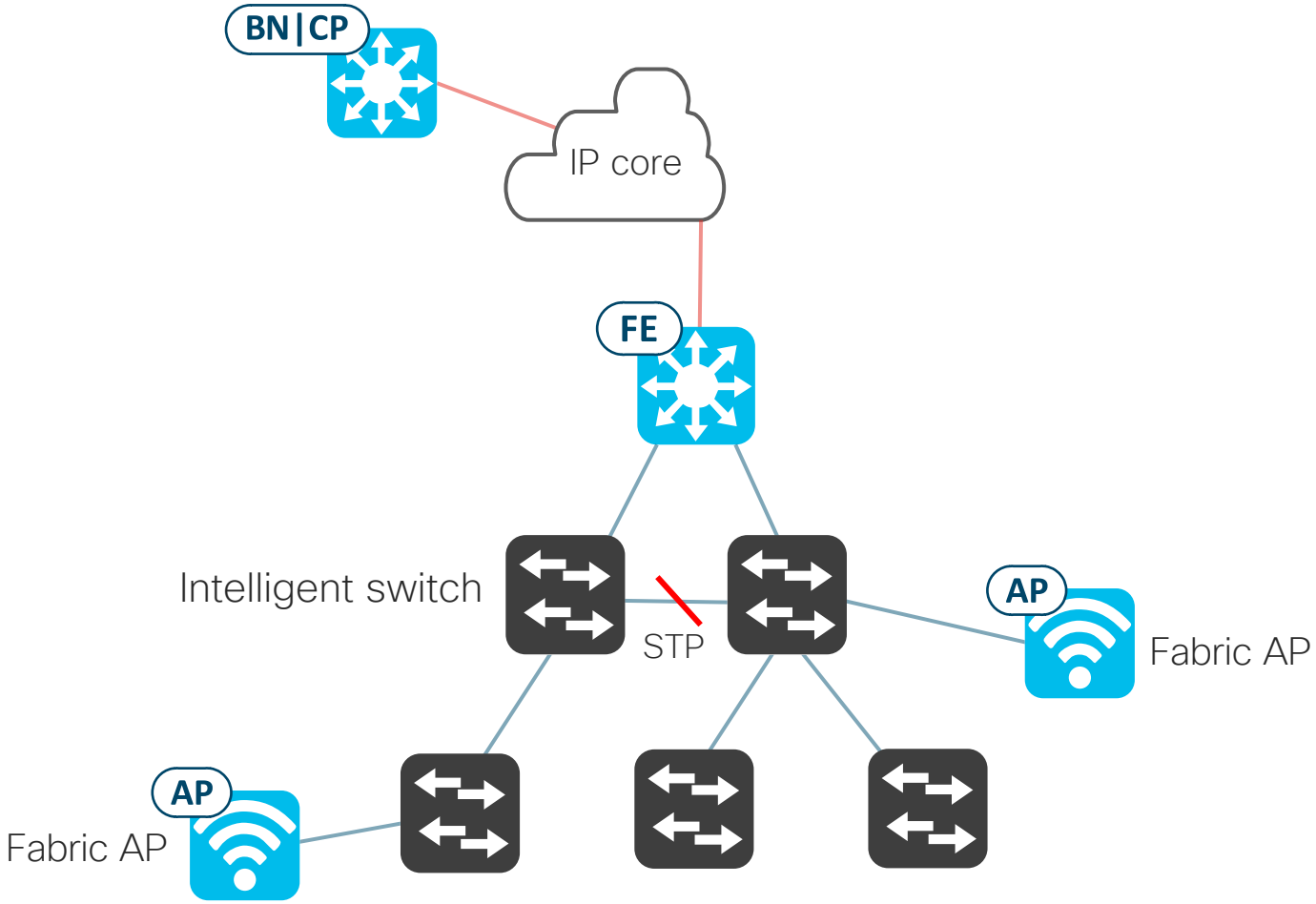
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Starting point for phased Migration
Traditional L2 switching domain connected to FE



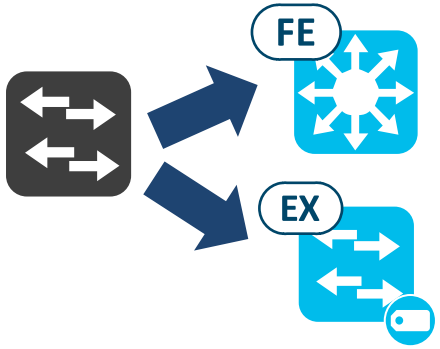
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Traditional Layer 2 Switching Domain Connected to Fabric Edge



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Convert a Traditional Switch to Cisco SD-Access Mode

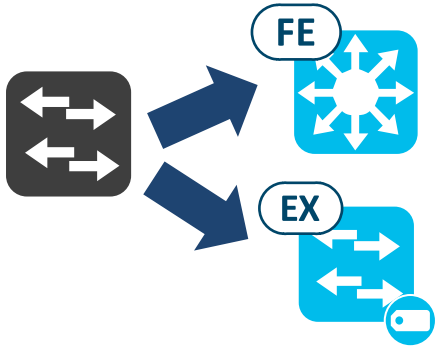


© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.



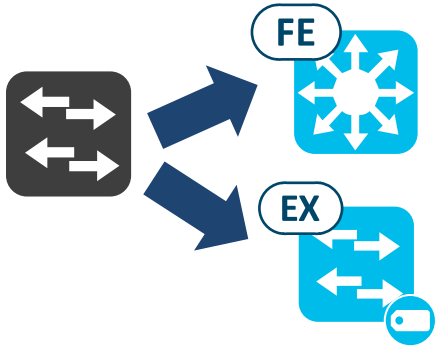
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

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.

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

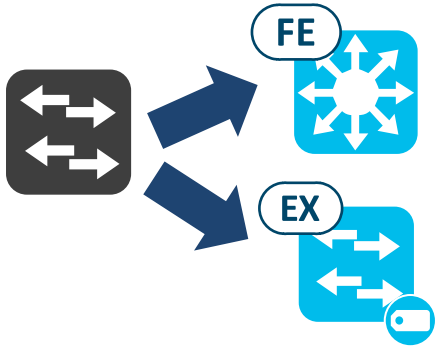
Convert a Traditional Switch to Cisco SD-Access Mode

Rebuild the switch:

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

LAN Automation or Extended Node Onboarding

Manual conversion to Fabric Edge Node

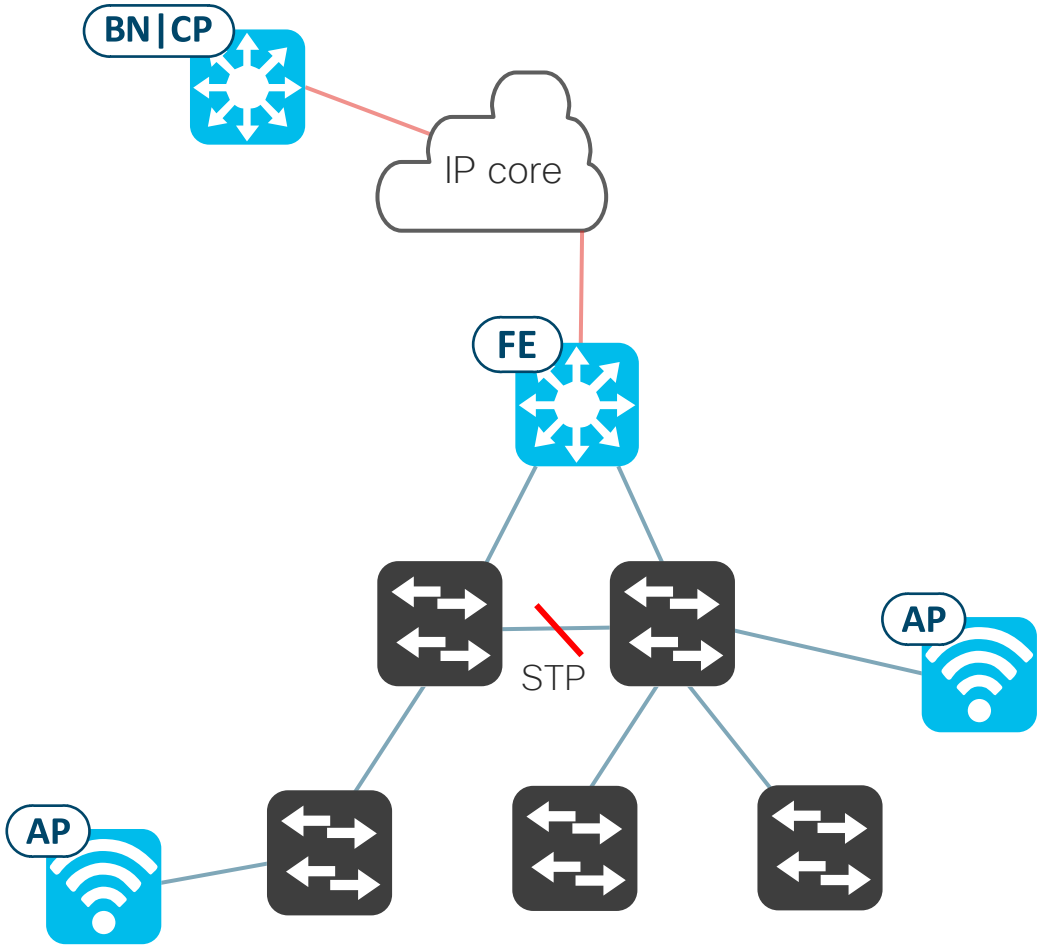


3. Factory reset the switch as per LAN Automation Deployment Guide.
4. Execute LAN automation or Extended Node onboarding.
5. Add to Fabric Site as Edge Node or Extended Node.
6. Provision Edge Node ports in Host Onboarding.

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

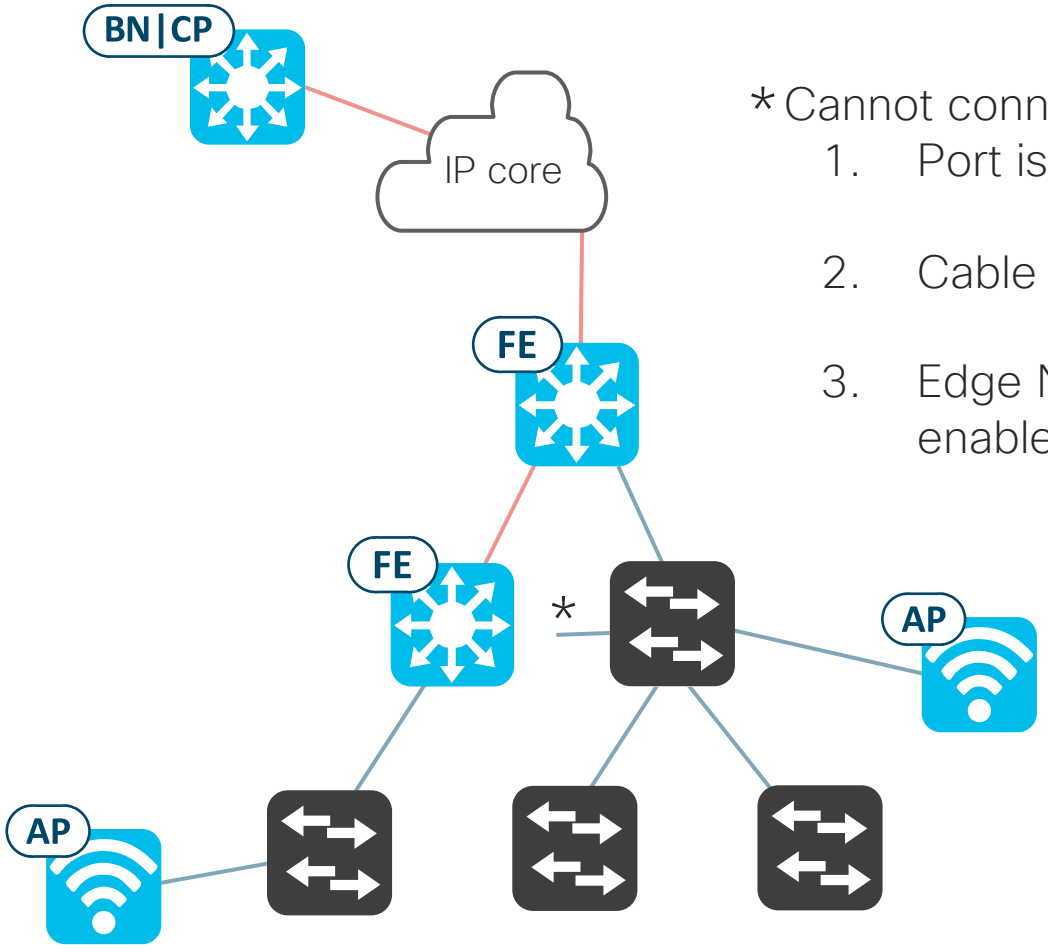
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Traditional Layer 2 Switching Domain Connected to Fabric Edge



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Traditional Layer 2 Switching Domain Connected to Fabric Edge

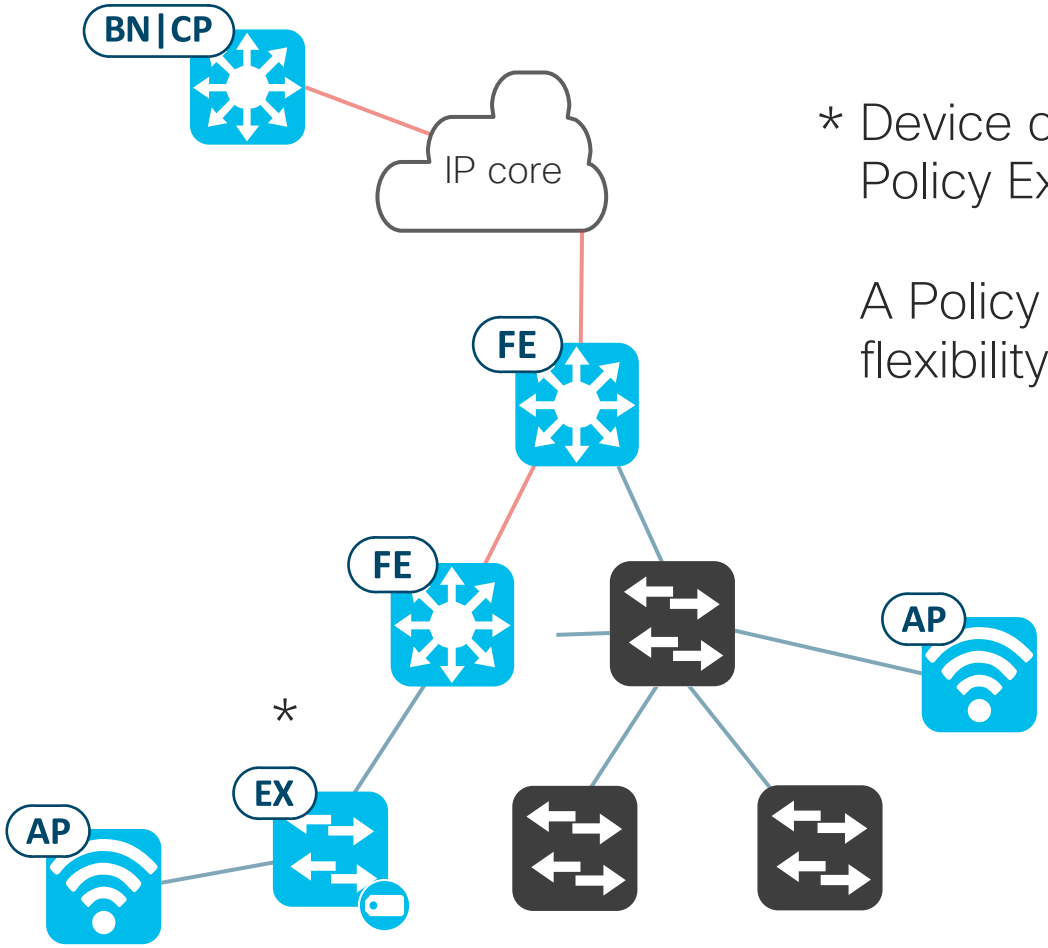


* Cannot connect same Layer 2 domain to two Edge Nodes. Thus:

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

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Traditional Layer 2 Switching Domain Connected to Fabric Edge

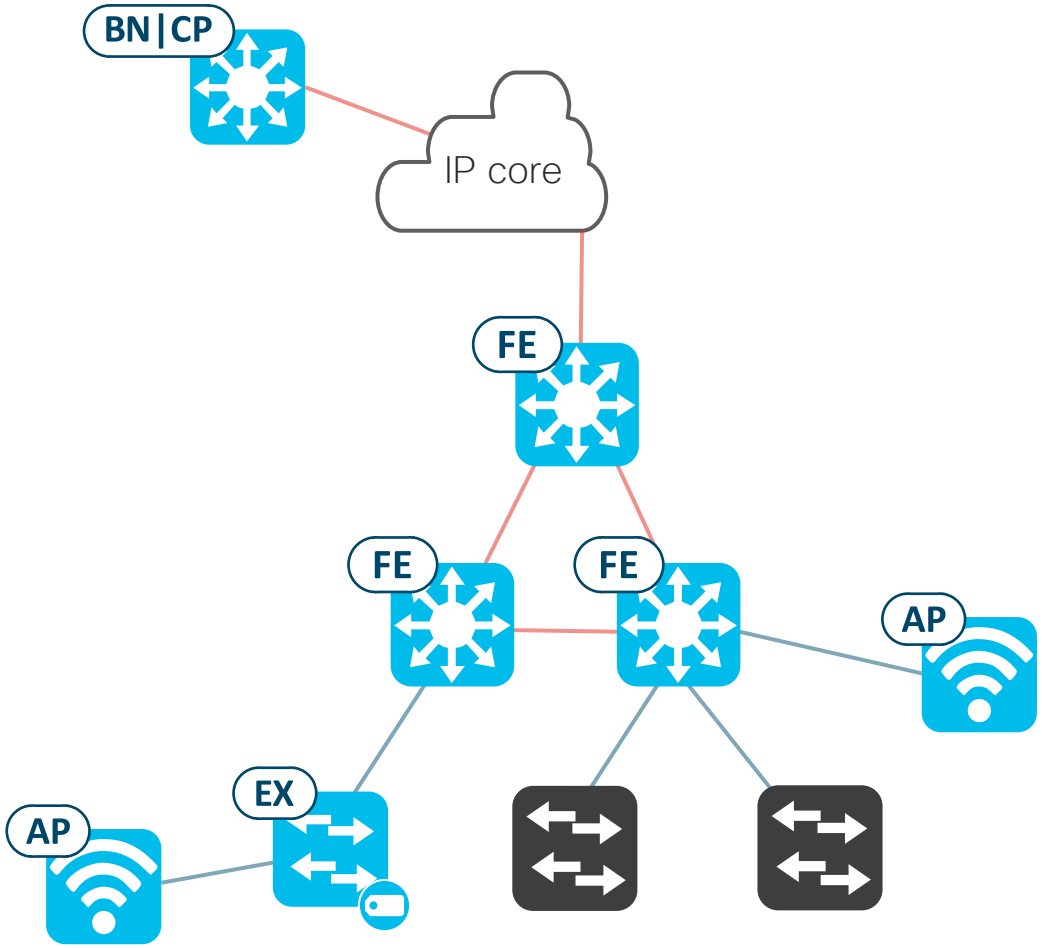


* Device could be provisioned as an Edge Node or Policy Extended Node.

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

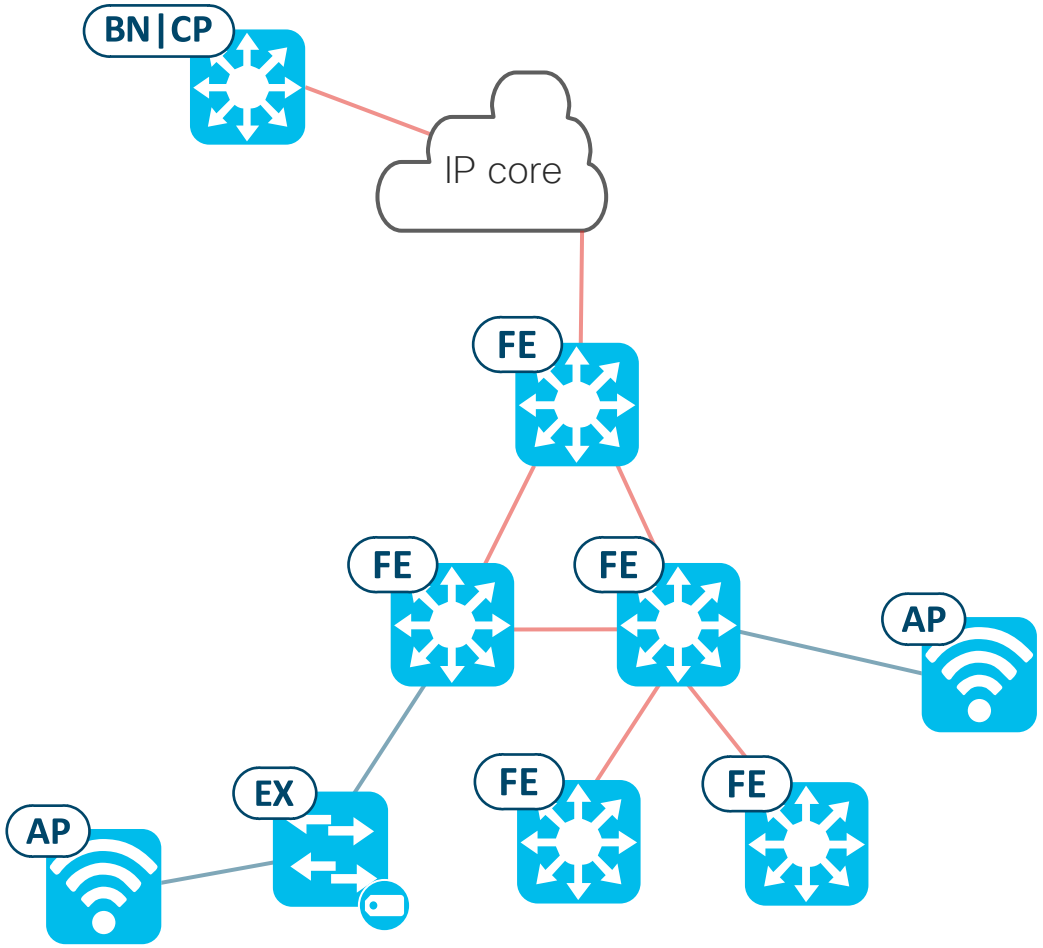
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Traditional Layer 2 Switching Domain Connected to Fabric Edge



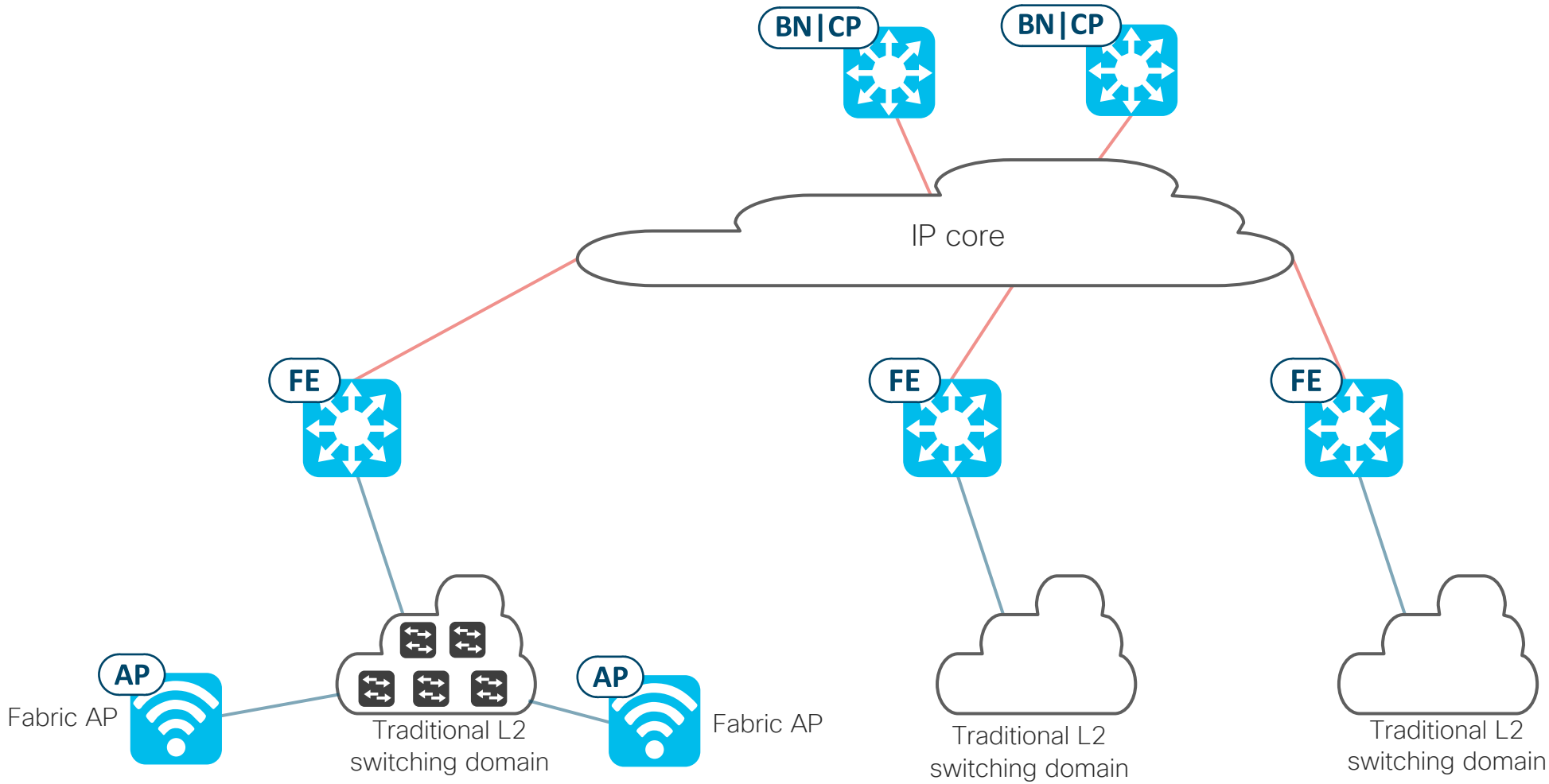
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Traditional Layer 2 Switching Domain Connected to Fabric Edge



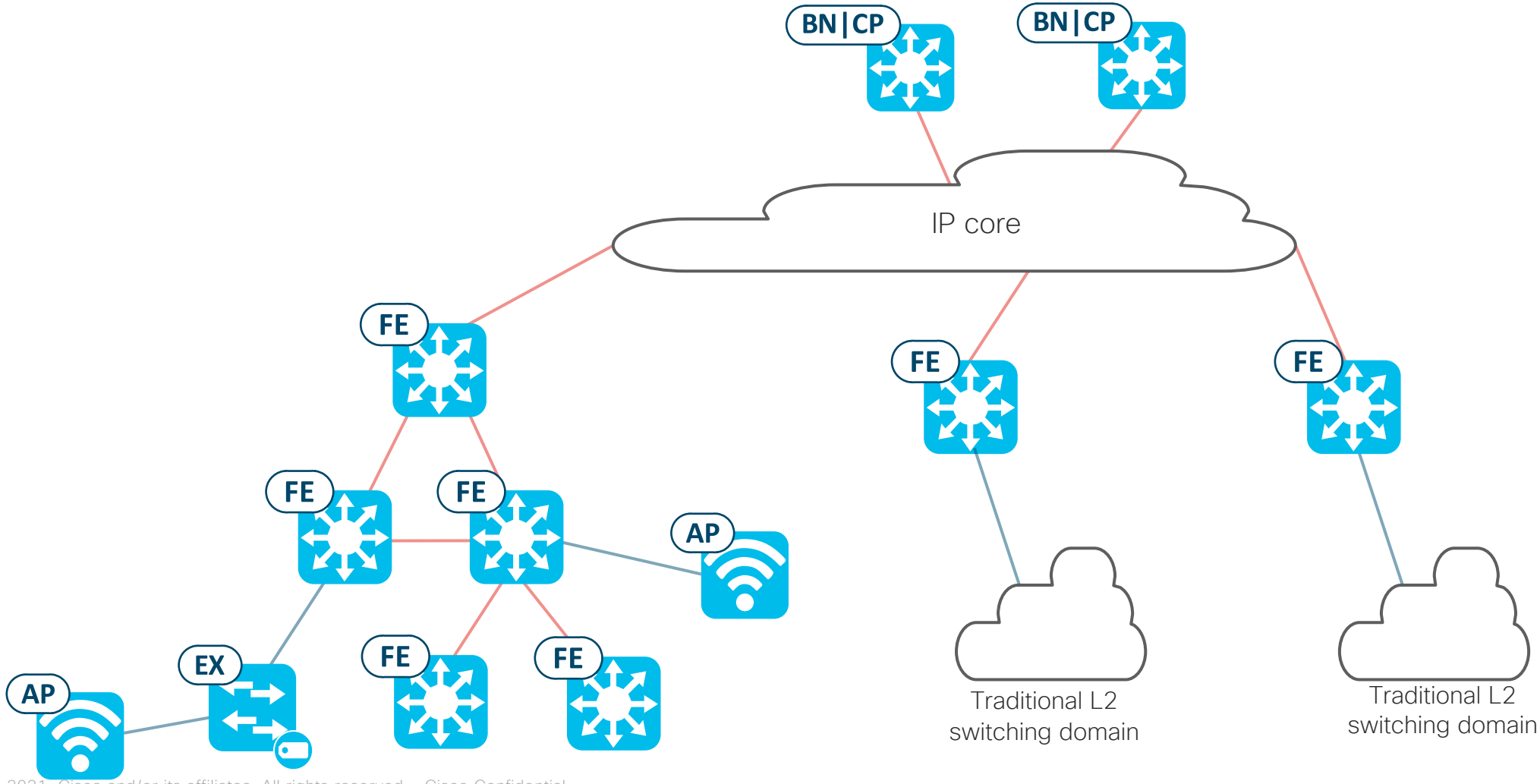
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Starting point for phased Migration
Traditional L2 switching domain connected to FE



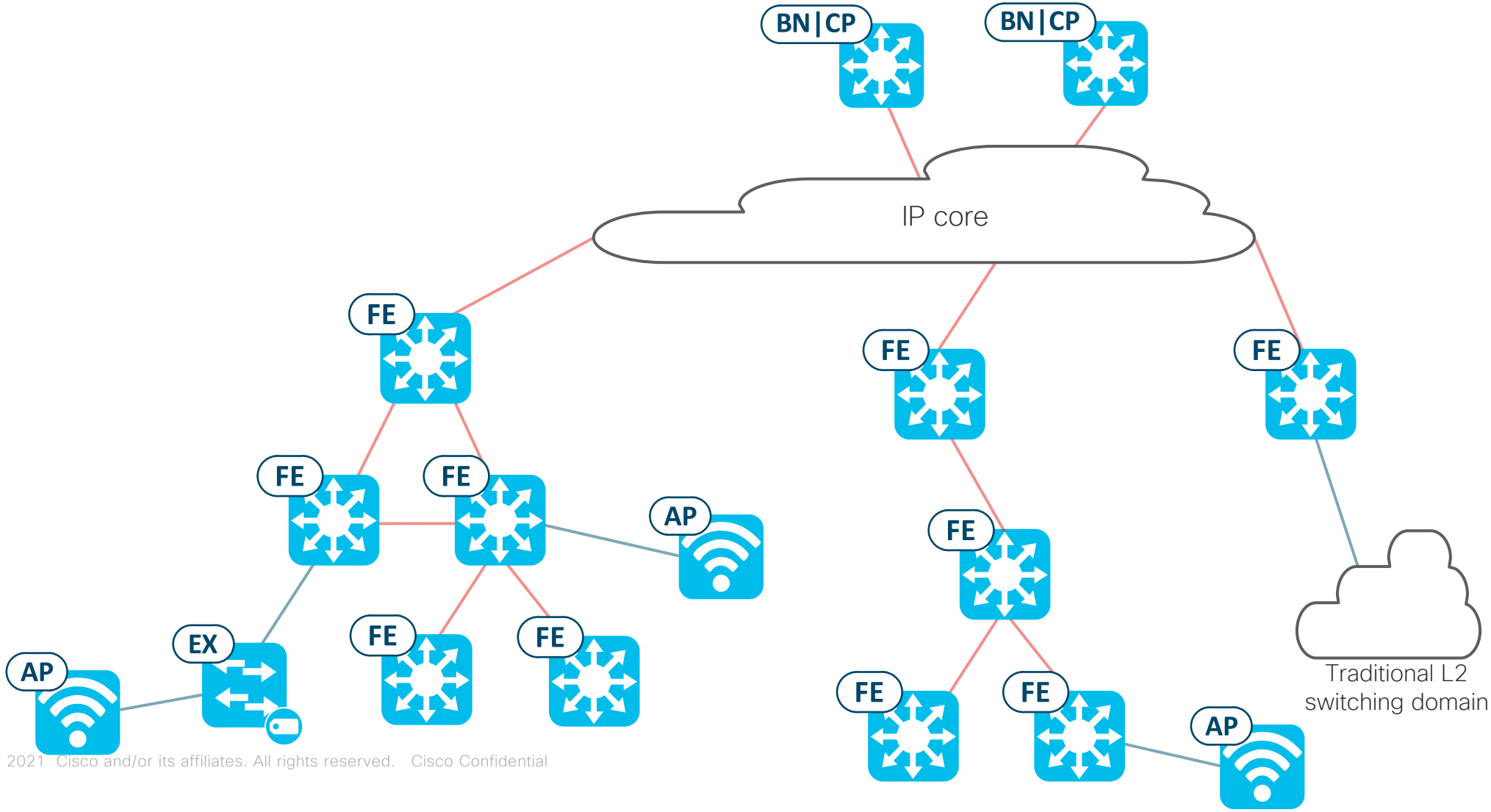
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Phased Migration over time
Traditional L2 switching domain connected to FE



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

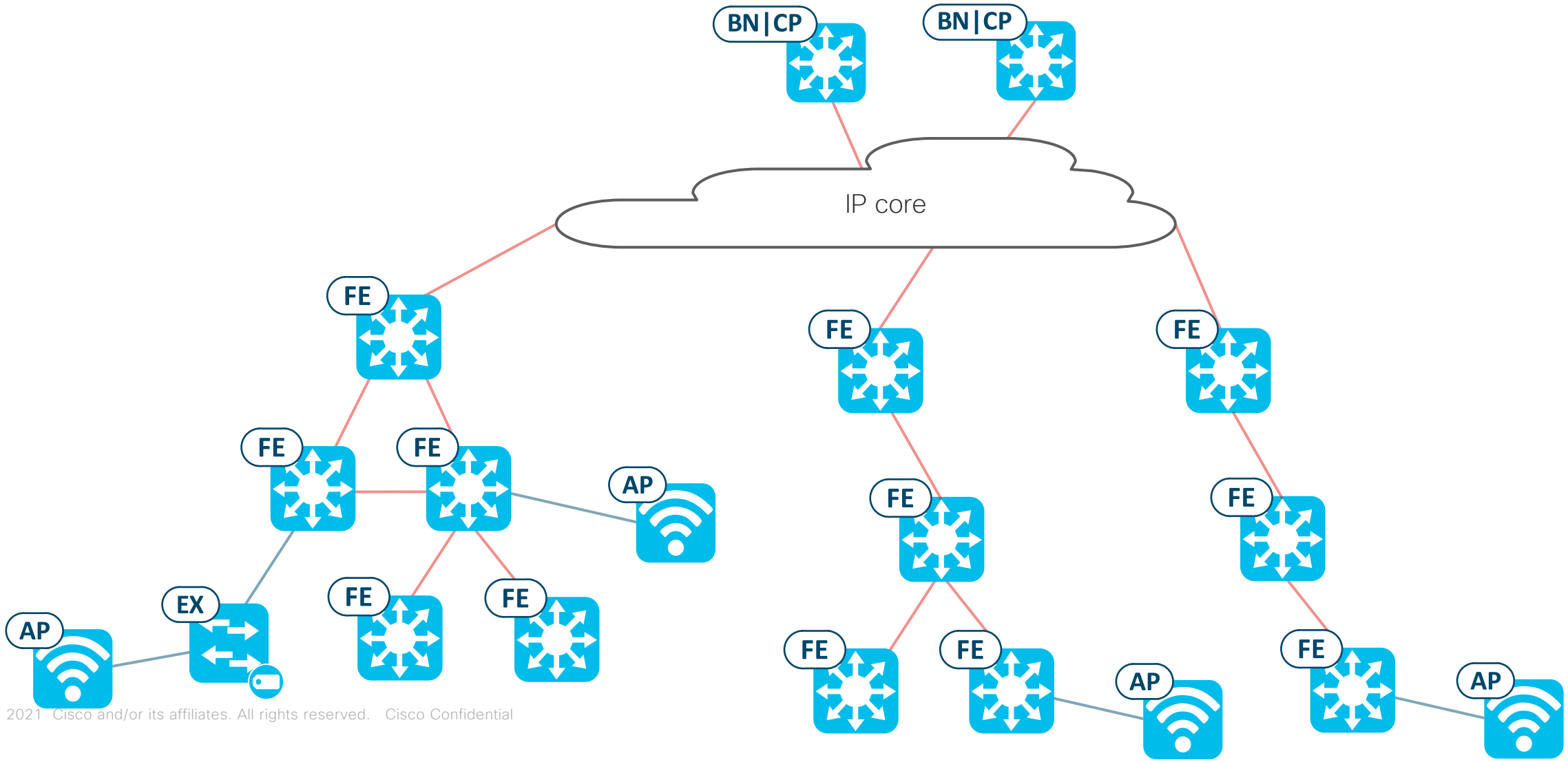
Phased Migration over time
Traditional L2 switching domain connected to FE



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Phased Migration over time

Traditional L2 switching domain connected to FE



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

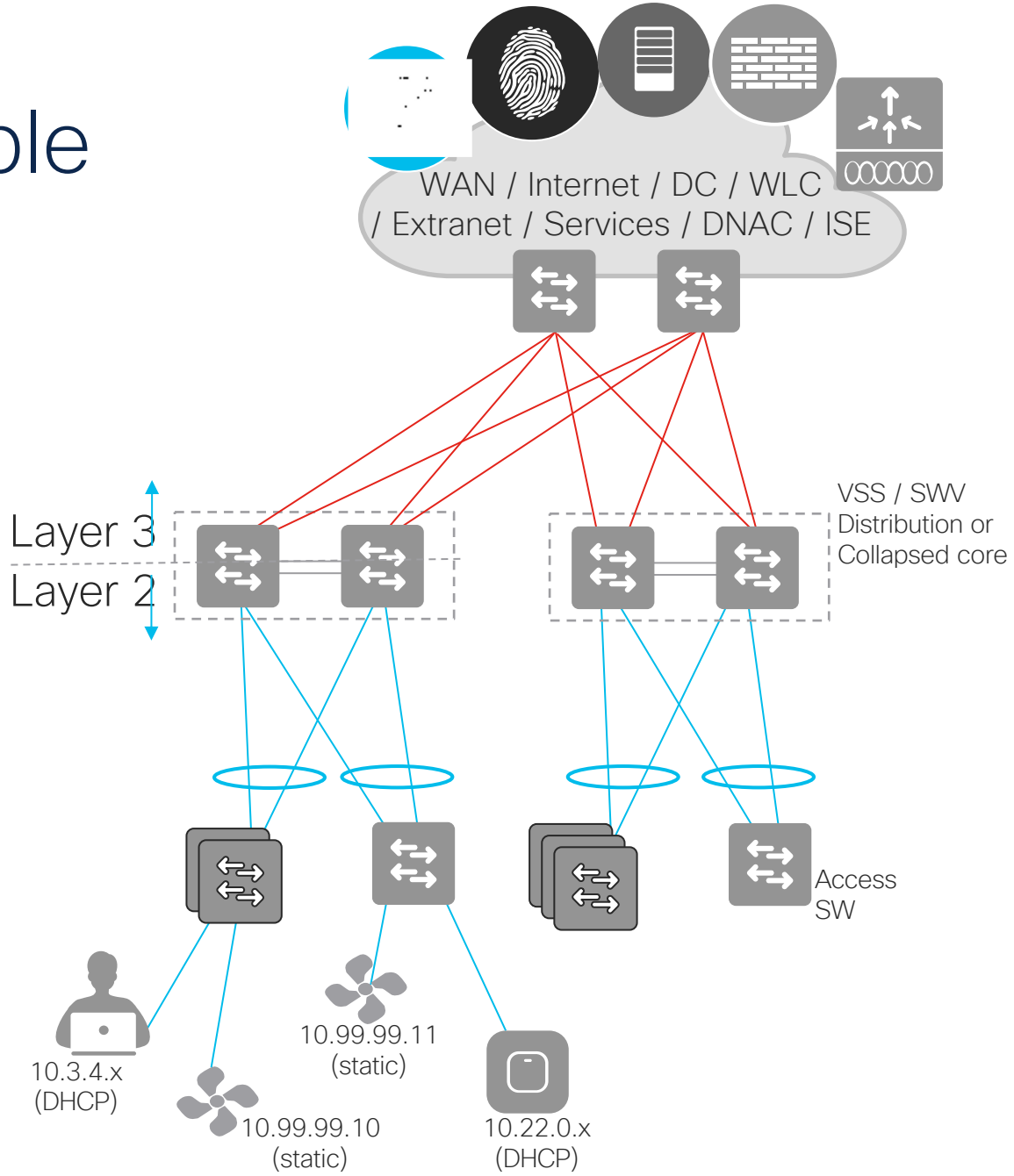
Cisco SD-Access Migrationsszenarien

1. Connecting L2 domains on Fabric Edge
2. Connecting L2 domains on L2 Border
3. Phased migration
4. L2 Border migration
5. Cisco SJC migration

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

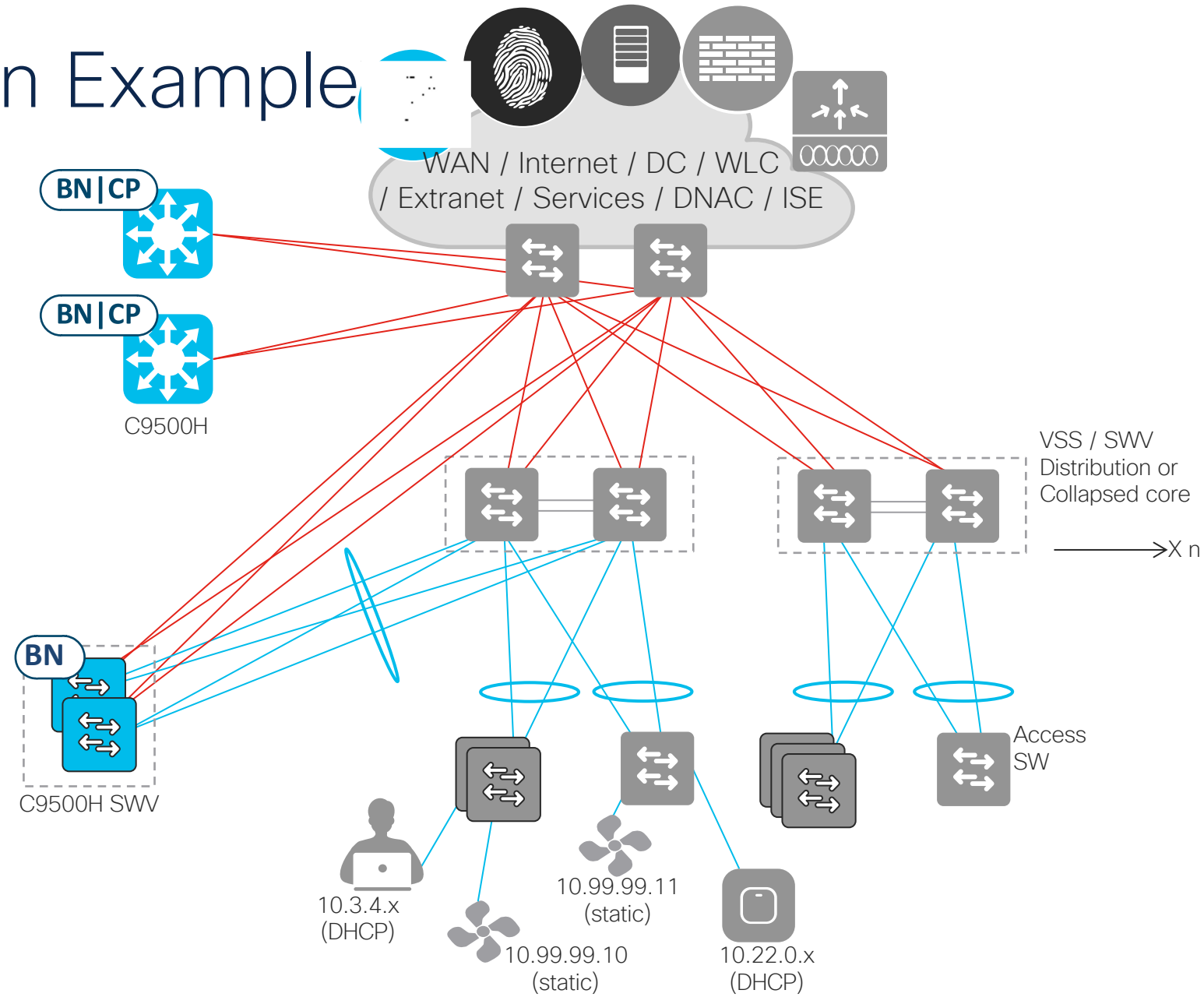
L2 Border Migration Example

- Brownfield Routed/Switched to SD-Access fabric Migration
- L2 Access with L3 Distribution/Core Layer
- IOT devices cannot change IP address (static)
- Corporate endpoints have DHCP enabled
- No cabling changes to existing brownfields network
- Access Layer HW is already SD-Access capable
- Keep wireless OTT design



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

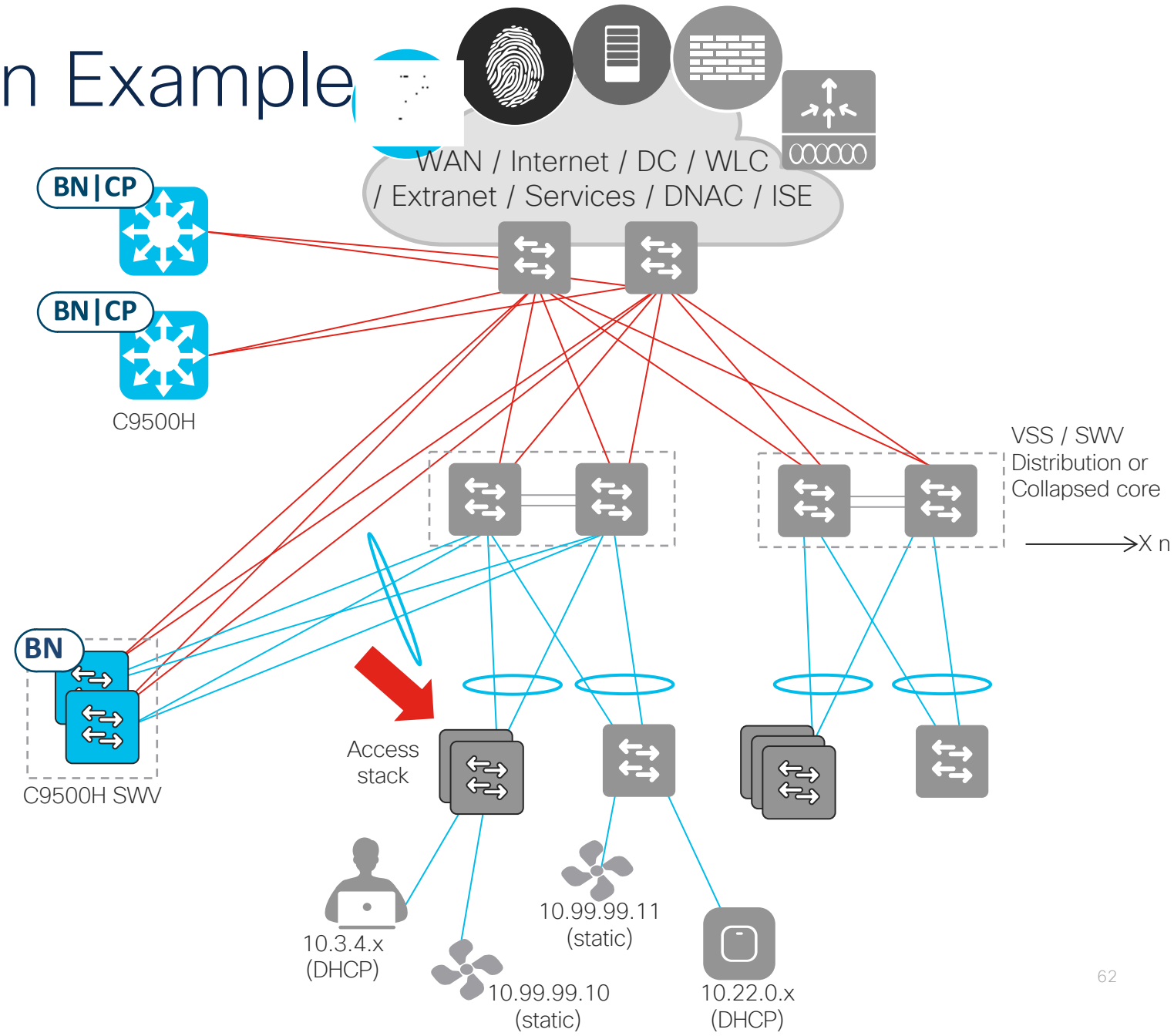
L2 Border Migration Example



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

L2 Border Migration Example

1. Connect L2 border to legacy L2 domain, shut down SVI in legacy domain and create SVI on L2 border
2. Confirm correct licenses and SDA certified IOS-XE version on access stack
3. Replace startup config on access stack and reload
4. Convert SWV downlinks to P2P L3
5. Discover and provision as FE
6. Assign new FE ports to VNs/Pools

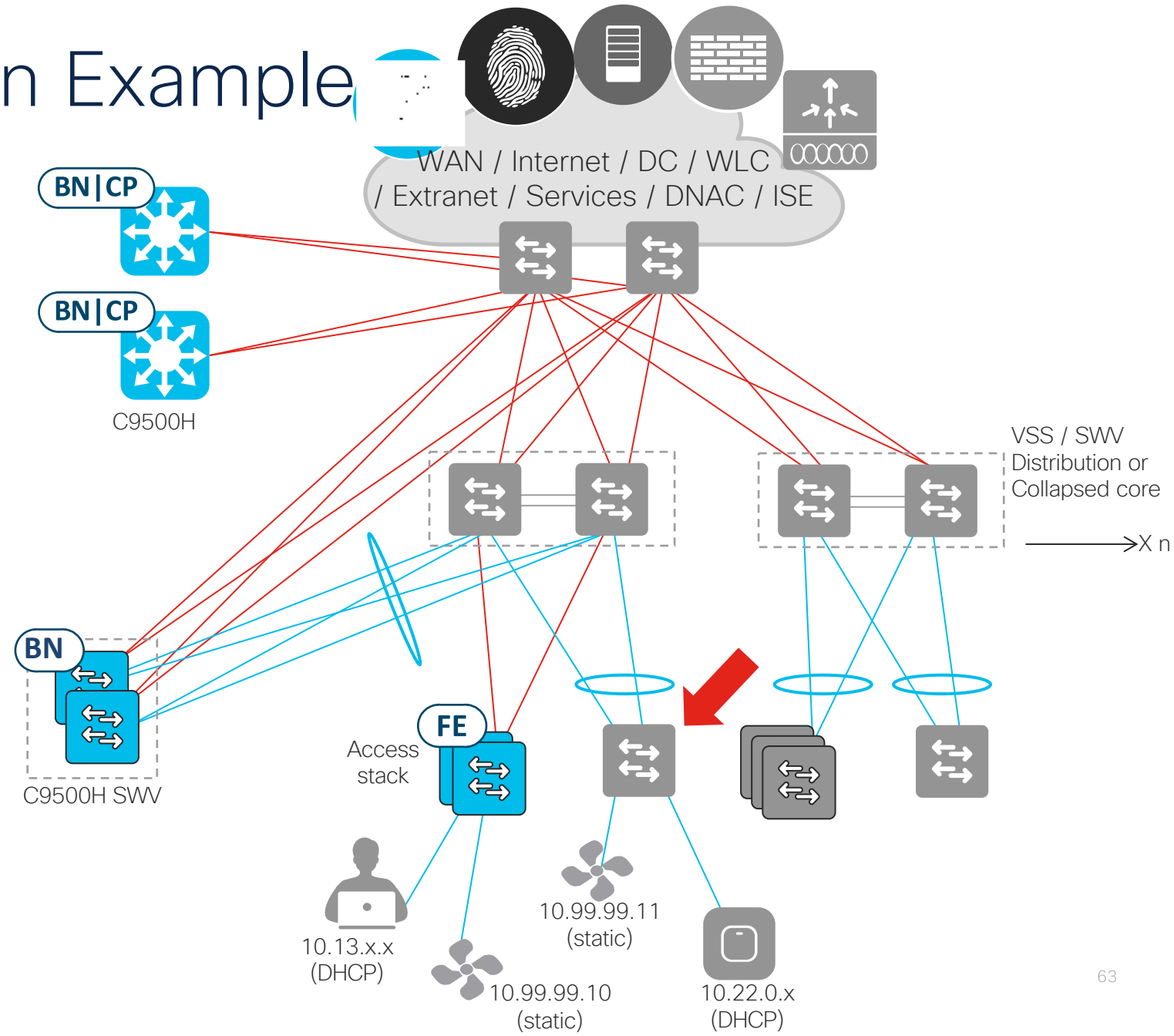


© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

L2 Border Migration Example

7. DHCP client IP address changed
8. For IOT devices, IP address stays same

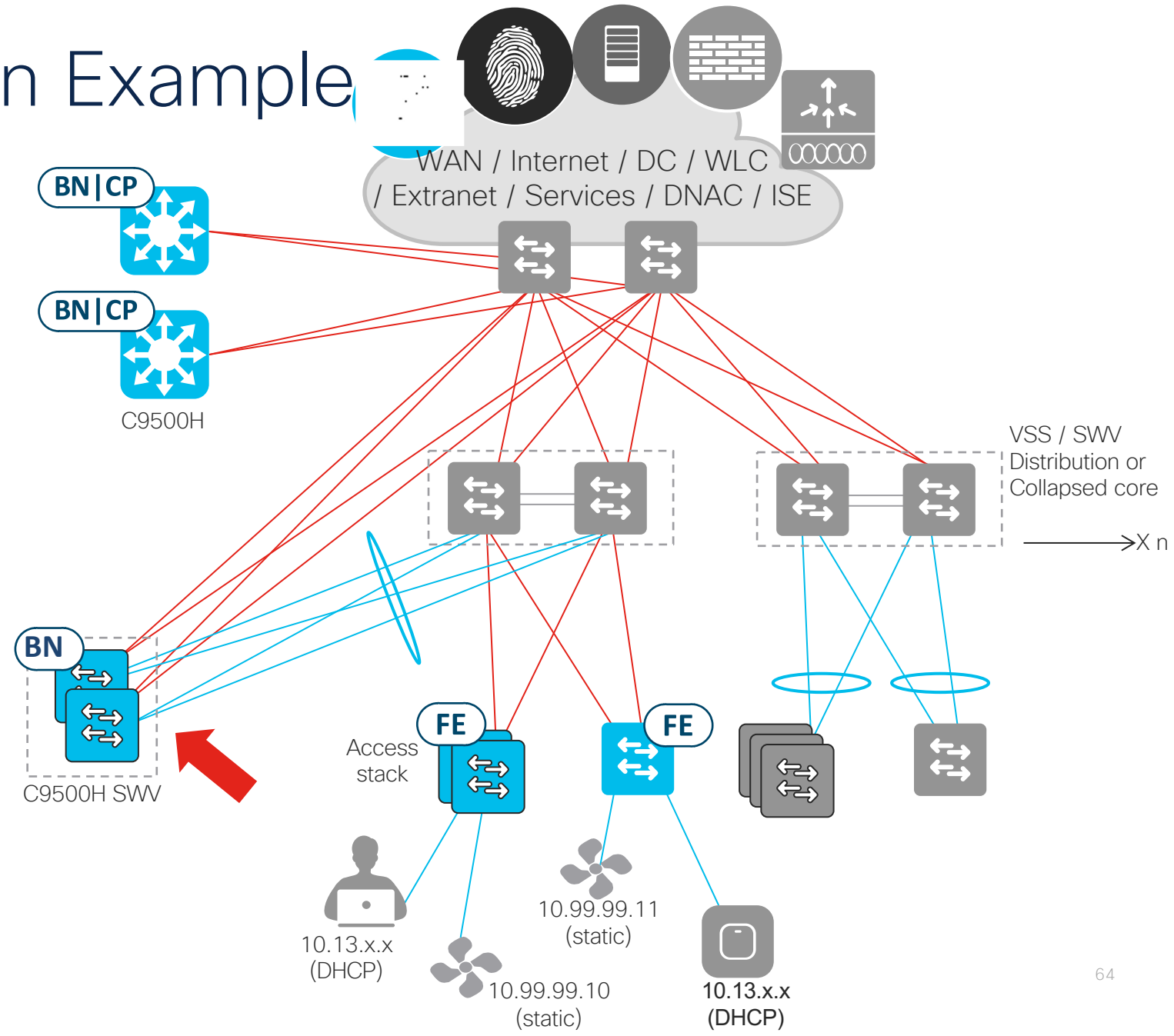
9. On next next access stack confirm correct licenses and SDA certified IOS-XE version on access stack
10. Replace startup config on access stack and reload
11. Convert SWV downlinks to P2P L3
12. Discover and provision as FE
13. Assign new FE ports to VNs/Pools



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

L2 Border Migration Example

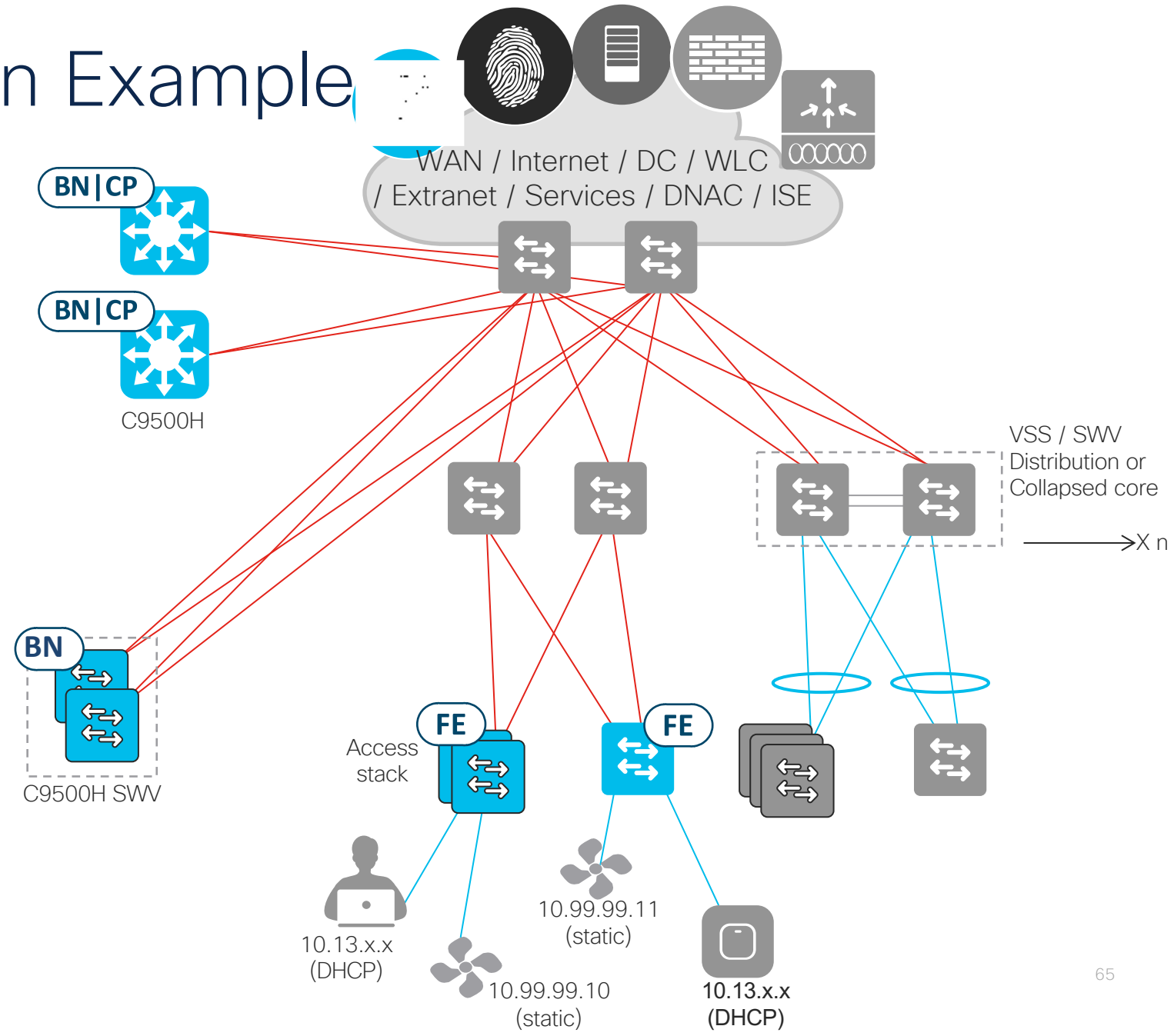
12. Remove L2 handoff from L2 border
13. Disconnect L2 border from legacy L2 domain



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

L2 Border Migration Example

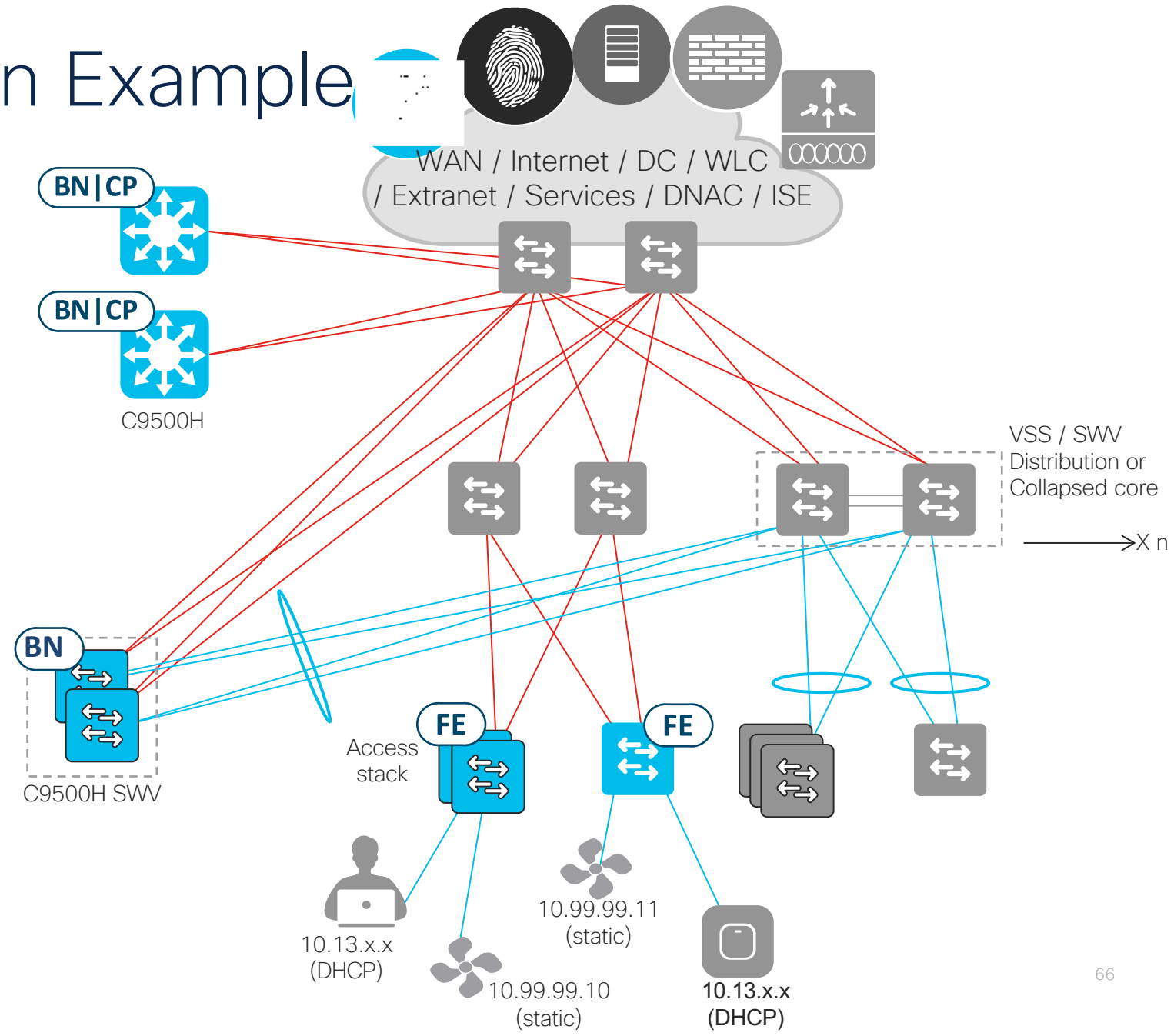
(For completeness: Repeat procedure per L2 domain, or if ambitious, convert entire L2 domain in one change window)



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

L2 Border Migration Example

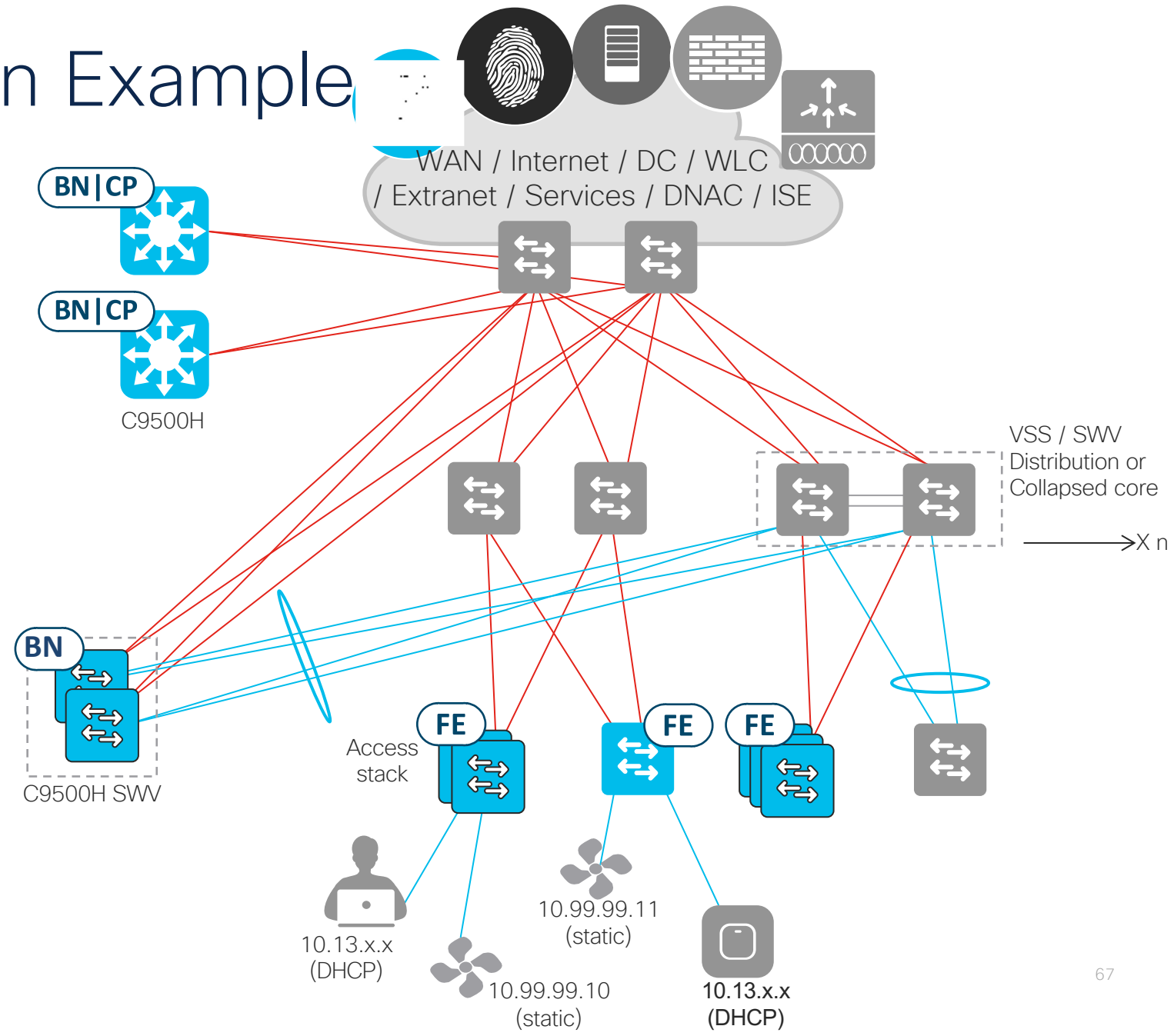
(For completeness: Repeat procedure per L2 domain, or if ambitious, convert entire L2 domain in one change window)



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

L2 Border Migration Example

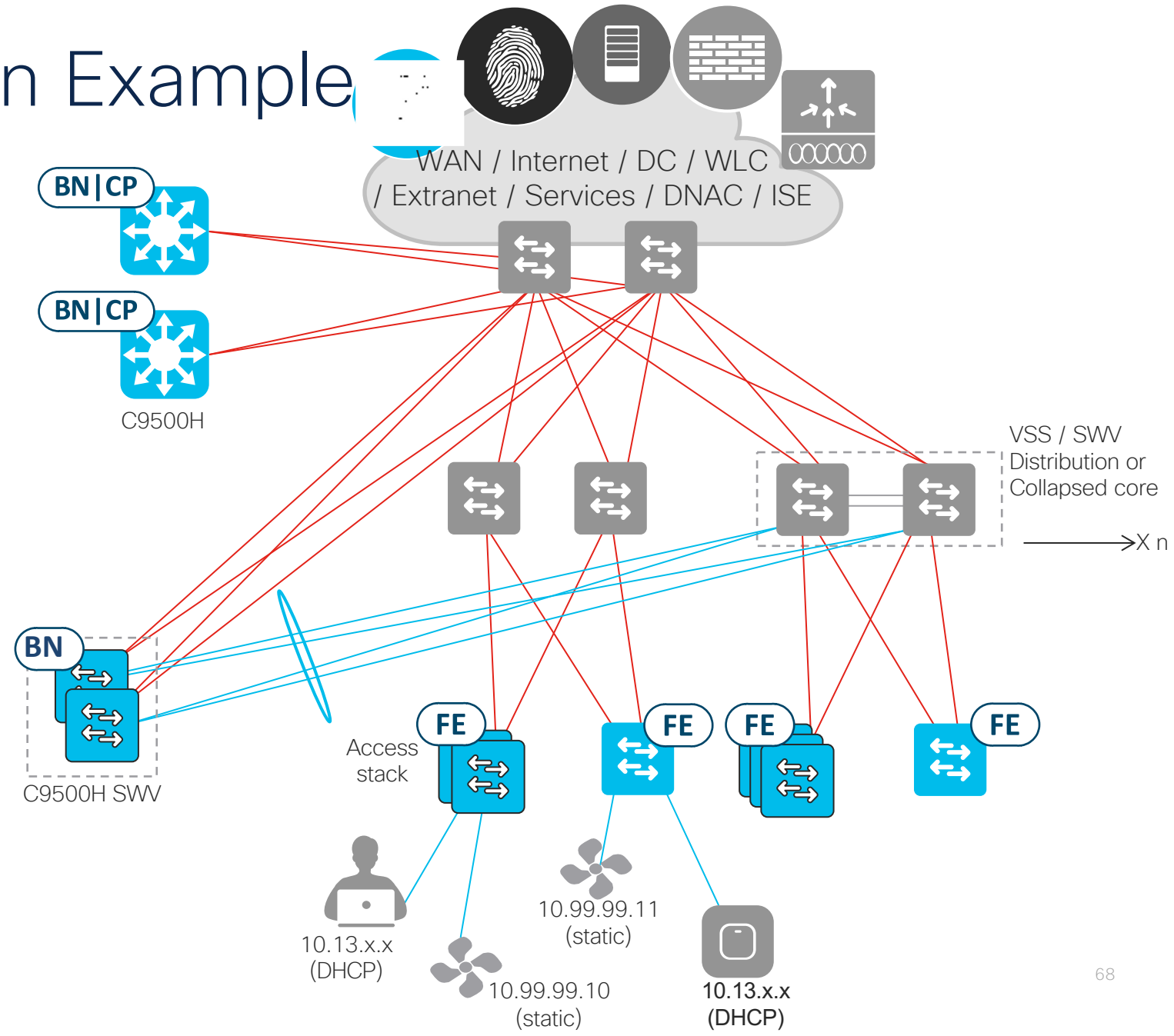
(For completeness: Repeat procedure per L2 domain, or if ambitious, convert entire L2 domain in one change window)



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

L2 Border Migration Example

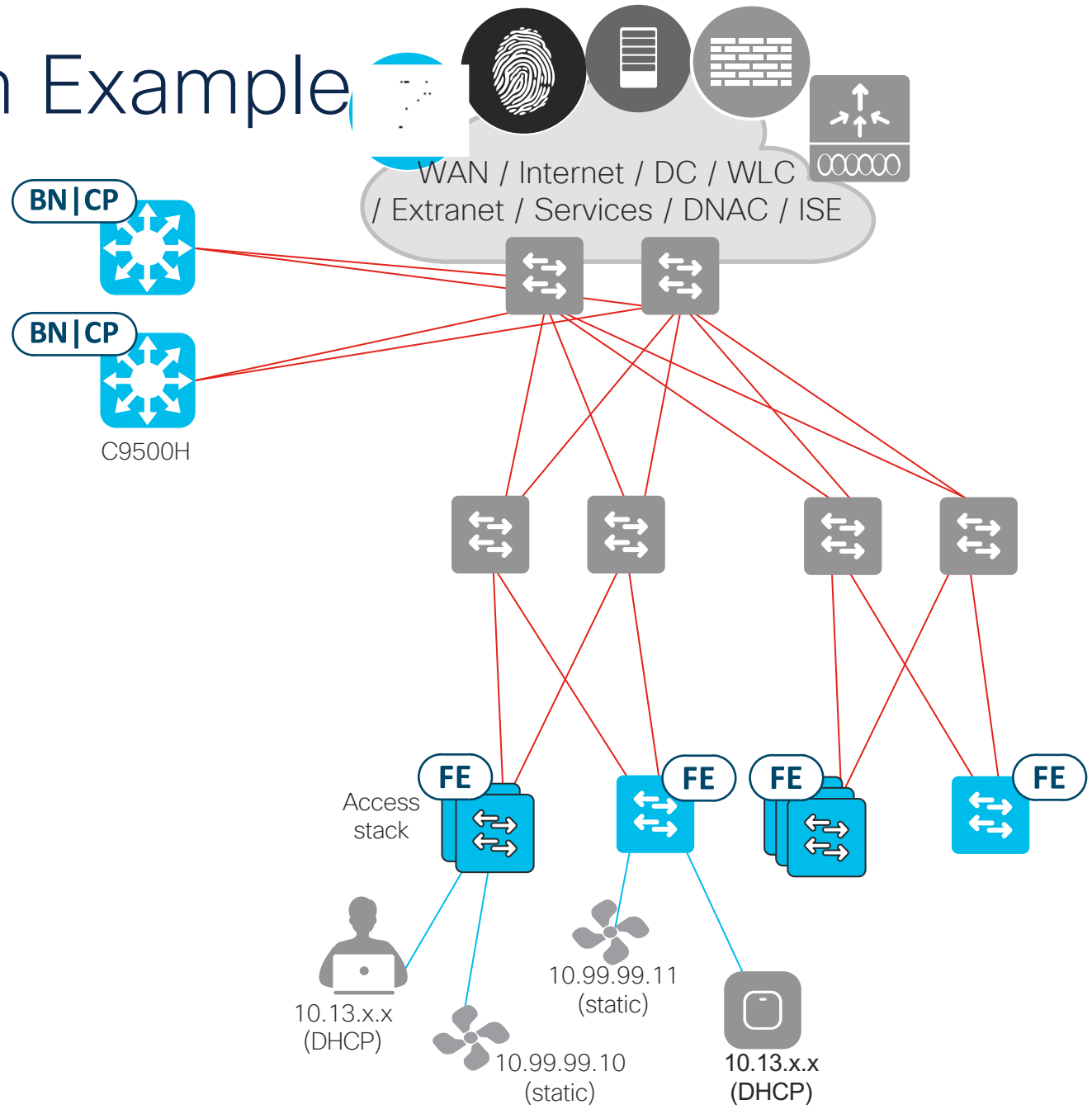
(For completeness: Repeat procedure per L2 domain, or if ambitious, convert entire L2 domain in one change window)



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

L2 Border Migration Example

(For completeness: Repeat procedure per L2 domain, or if ambitious, convert entire L2 domain in one change window)



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco SD-Access Migrationsszenarien

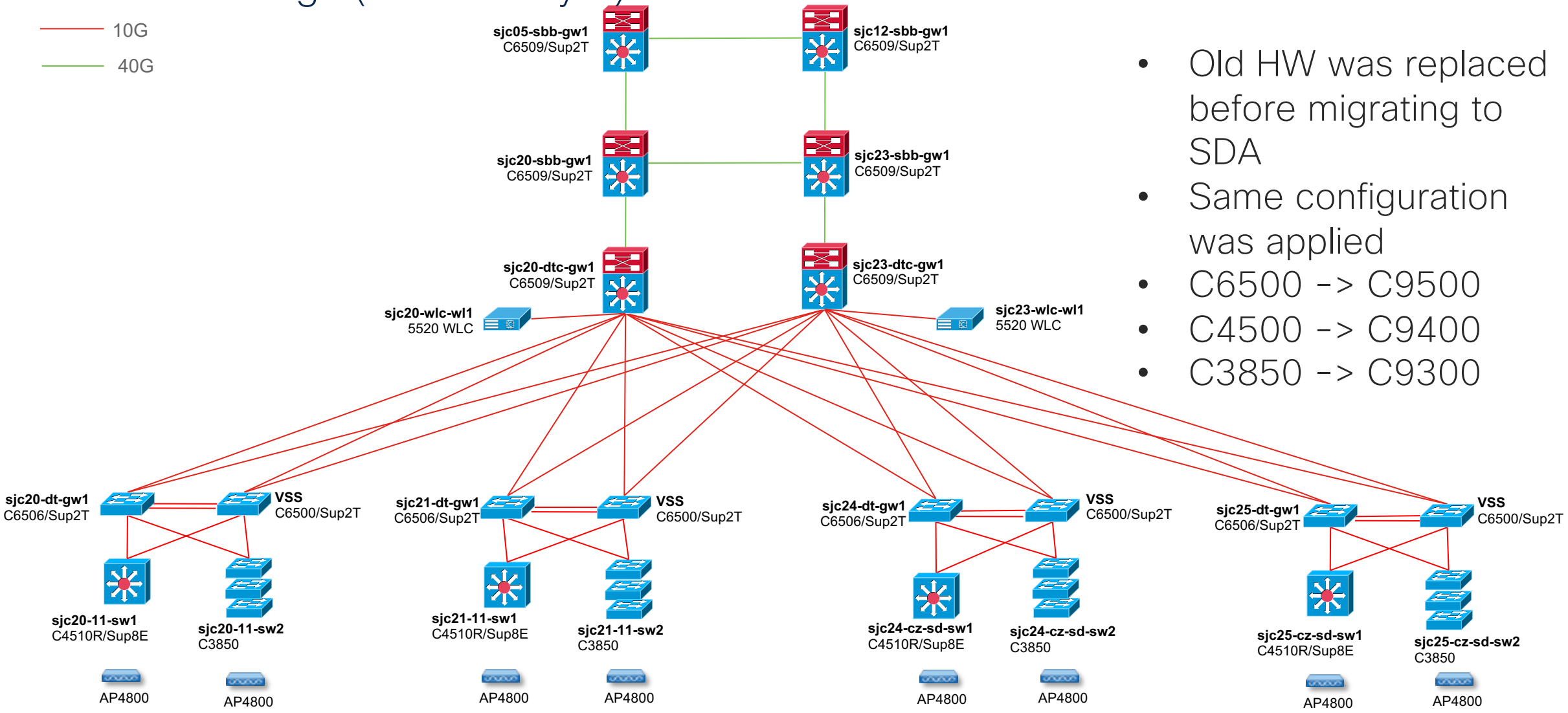
1. Connecting L2 domains on Fabric Edge
2. Connecting L2 domains on L2 Border
3. Phased migration
4. L2 Border migration
5. Cisco SJC migration

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Real-world Migration Cisco Campus in San Jose (SJC) Multi-Site SDA fabric

SJC20-25 Original Hardware and Topology

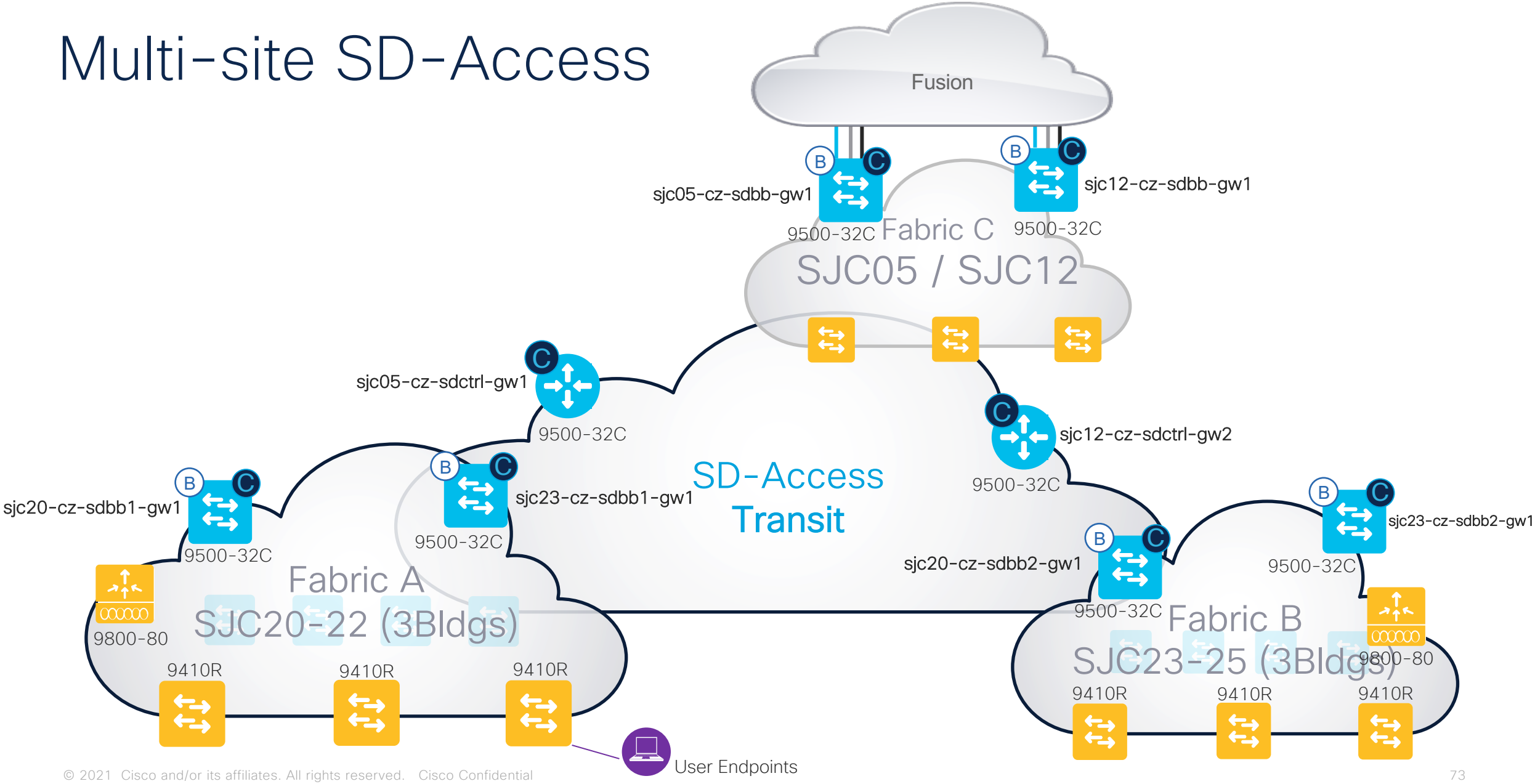
Total of 6 Bldgs (shown only 4)



- Old HW was replaced before migrating to SDA
- Same configuration was applied
- C6500 -> C9500
- C4500 -> C9400
- C3850 -> C9300

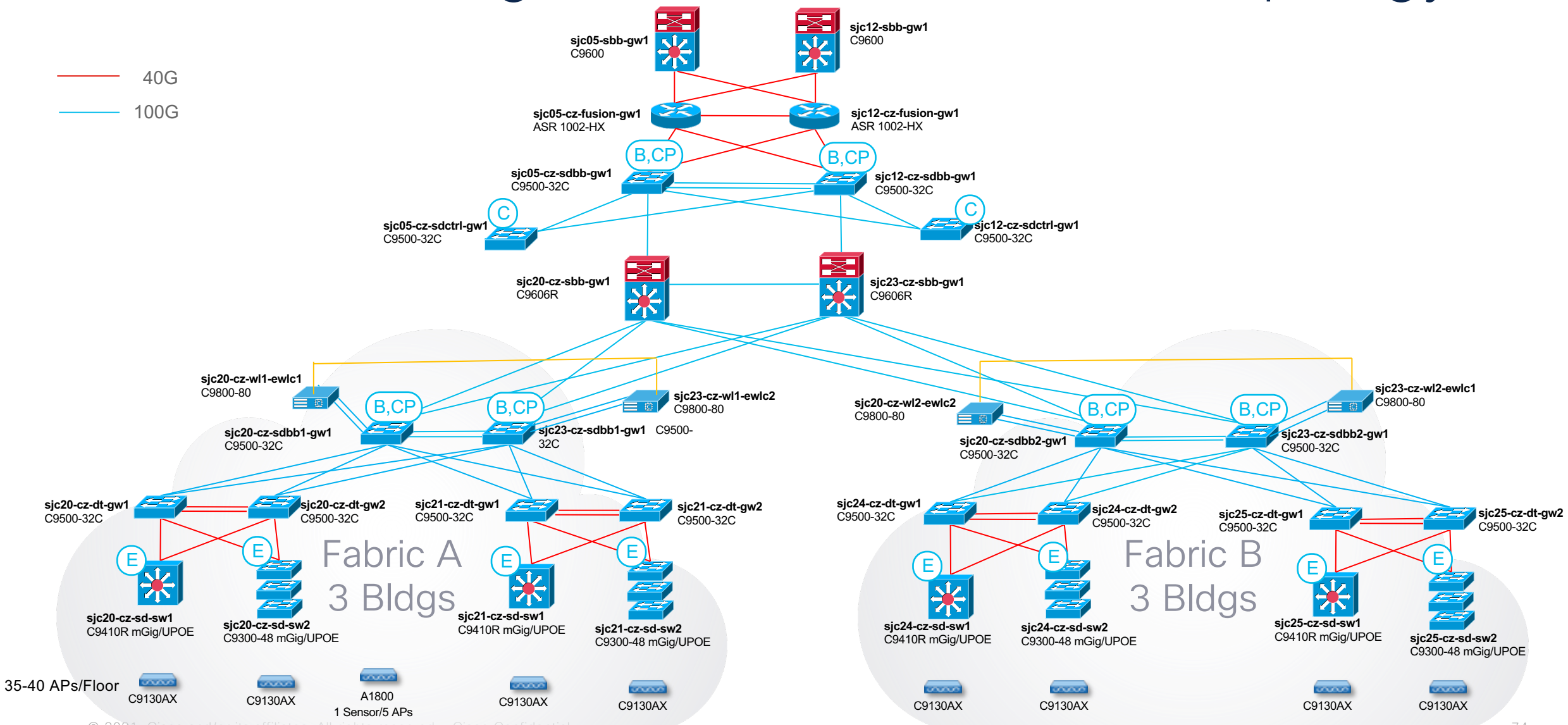
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Multi-site SD-Access



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

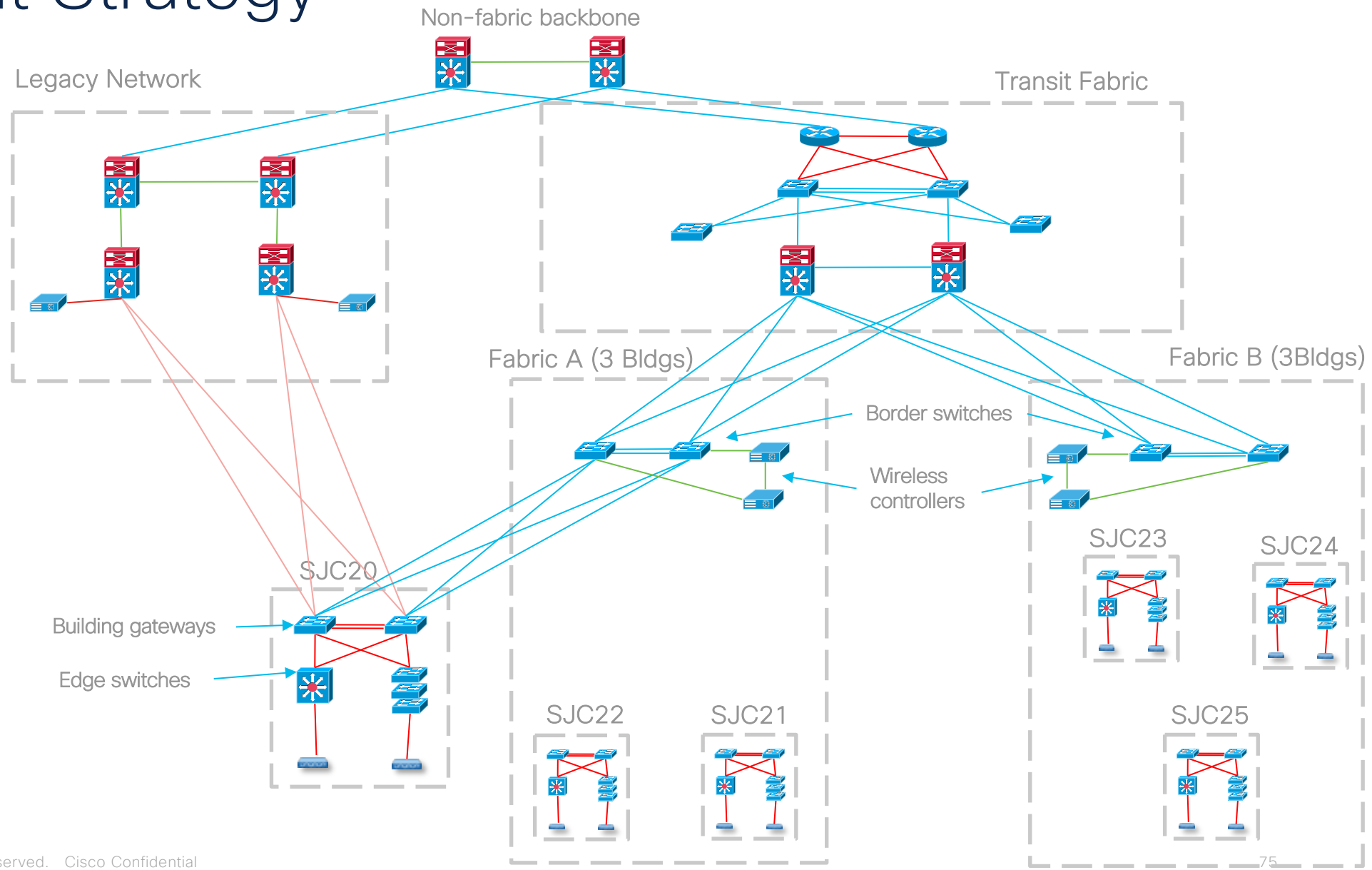
SJC20-25 Target State Hardware and Topology



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

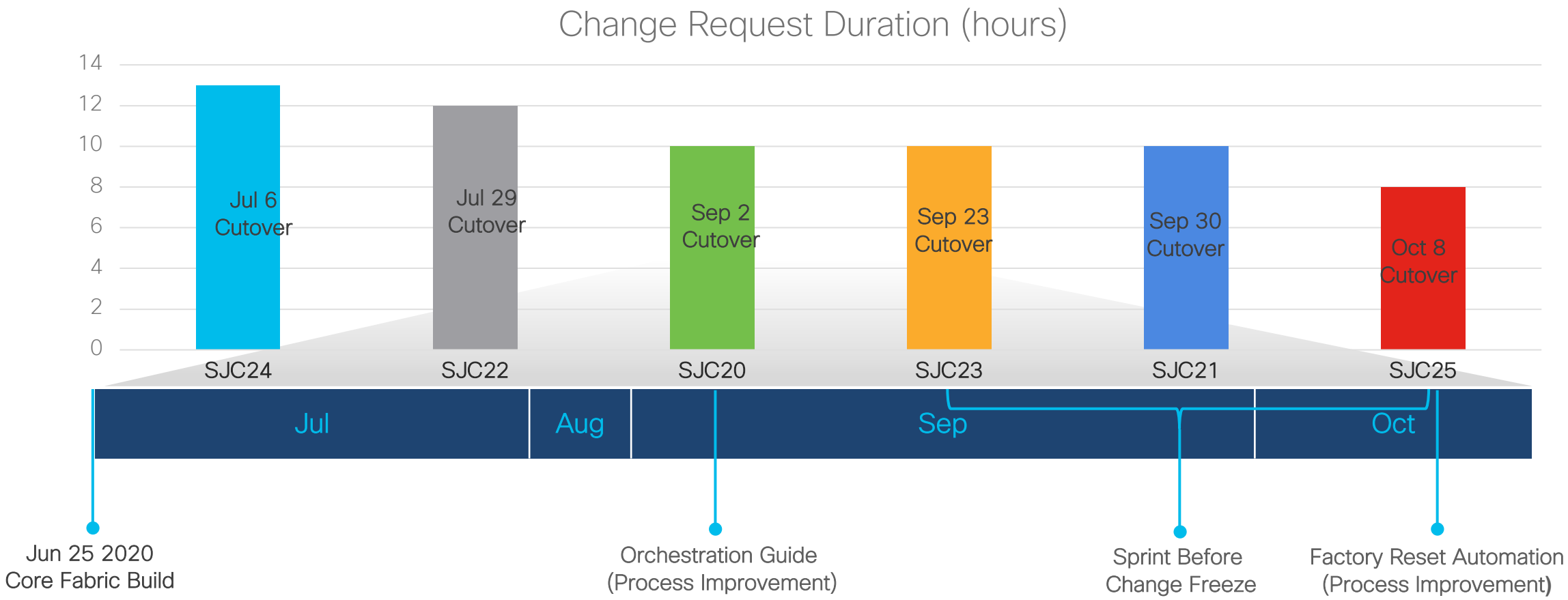
Deployment Strategy

1. Replaced old HW in Bldgs. Deploy Transit Fabric and Fabric A & B building aggregation
2. Prepare for a building migration
   a) Audit the building network
   b) SWIM Upgrade
3. Migrate each building, one at a time
   a) Factory reset edges
   b) Physical uplink move
   c) Factory reset building gateways
   d) Fabric configuration: LAN automation, underlay/overlay config, wireless AP config
   e) Network cleanup
4. Repeat for other buildings



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Fabric Migrations Improved Over Time



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Sample of Orchestration Guide

File Automation Forms — Remaining fabric migrations

Grid View · Filter · Arial · 10

	Task	SJC23 - Owner	SJC23 - Status	SJC23 - Timeline	SJC23 - Notes
3	**CR Date**				**Sept. 23, 2020**
4	Link to Fabric Deployment Guide				Link to Fabric Deployment Guide
5	SWIM CR Link				SWIM CR: https://rfc/CHG0519780
6	Fabric cut-over CR link				Fabric CR: https://rfc/CHG0519612
7	Project Folder link (Sharepoint)				SJC 23 Project Folder
8	End-user DHCP Migration List				End-user DHCP Migration List
9	TAC Case Link				Pro-Active TAC Case - 689971003
10	Site Audit Sheet				Site Audit Sheet
11	ITE Network Automation Tool				
12	ARBAC Tool				
13					
14					
15	Before		Completed		
94	During		Completed		
95	Tasks before starting LAN Automation in DNAC		Completed		
145	While starting LAN Automation in DNAC - (PnP)	Asad	Completed	11:00 AM PDT	
159	After LAN Automation (Underlay + Overlay)		Completed		
160	Finish Underlay deployment		Complete		
161	Stop LAN Automation	Asad	Complete		
162	Wait for all up-link interfaces to be configured as L3	Asad	Complete		
163	Verify status of devices in DNAC is in managed state	Asad	Complete		
164	Follow the guide and update network settings (via tags)	Asad	Complete		
165	Follow Post-Underlay Checklist	Lance	Complete		
166	Use Lance's script				
167	Validate one Edge node	Lance	Complete		
168	Validate DT GW	Lance	Complete		
169	~~Validate border nodes~~	Lance	Complete		

Each task is a small step with an owner

© 2021 Cisco and/or

Sample slide from our Deployment Guide

Kicking off LAN Automation

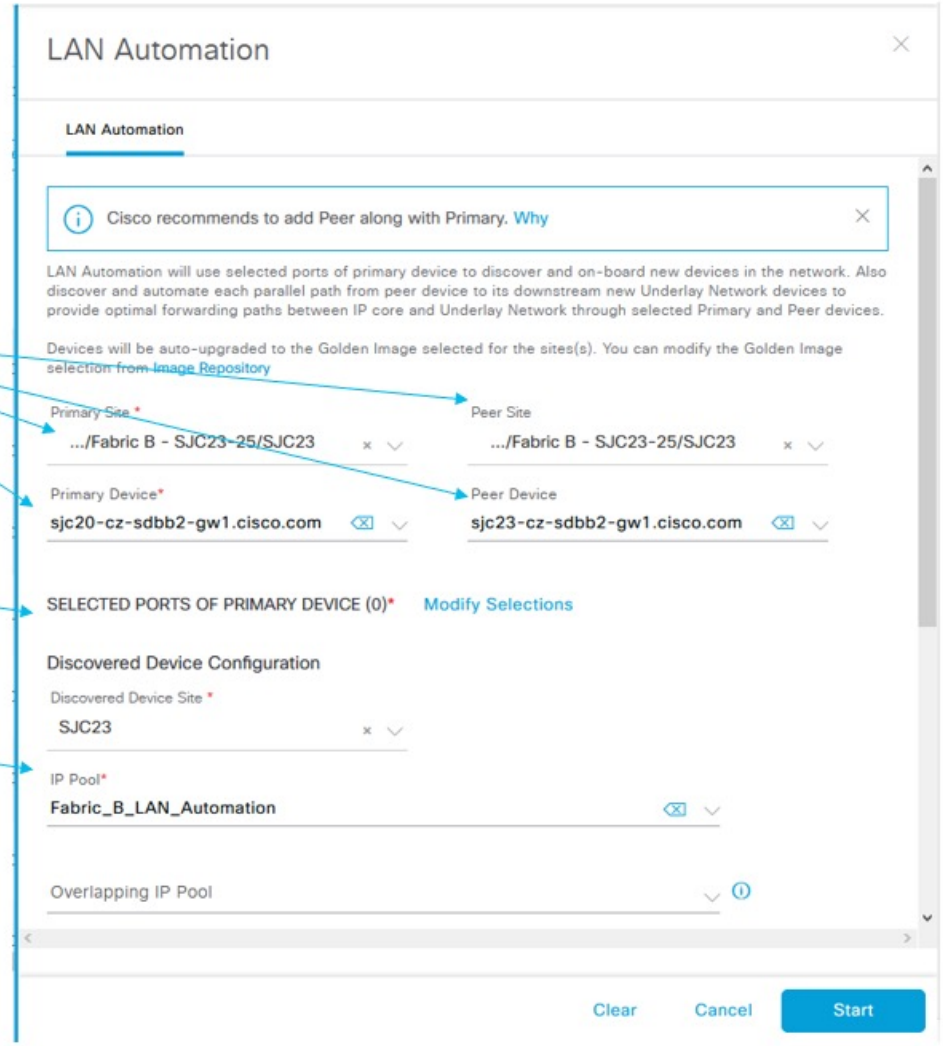
Select Primary and Peer Sites and Devices
Fabric A Site = SJC20
Fabric B Site = SJC23
Primary = sjc20-cz-sdbb[1/2]-gw1
Peer = sjc23-cz-sdbb[1/2]-gw1

***Due to a limitation in DNA-C, Fabric A SDBBs both live in SJC20, and Fabric B SDBBs live in SJC23.**

Primary Device Ports = downlinks to DT-GW
Depending on which Building is being cutover, select the downlinks to the respective DT-GWs.

All buildings in Fabric A use the same LAN Automation IP Pool. There is another pool that is shared by all buildings in Fabric B as well.

The site the switches are being installed at. Use the building, NOT the floor.



© 2021

Fragen?

👉 Now it’s time to play the game!

Please use a real name as nickname. Win nice Prices!

Join at **www.kahoot.it**
or with the **Kahoot! app**
Game Pin: 498 7744

1st Price
Cisco Headset HS730

3rd Price
Coffee Cup

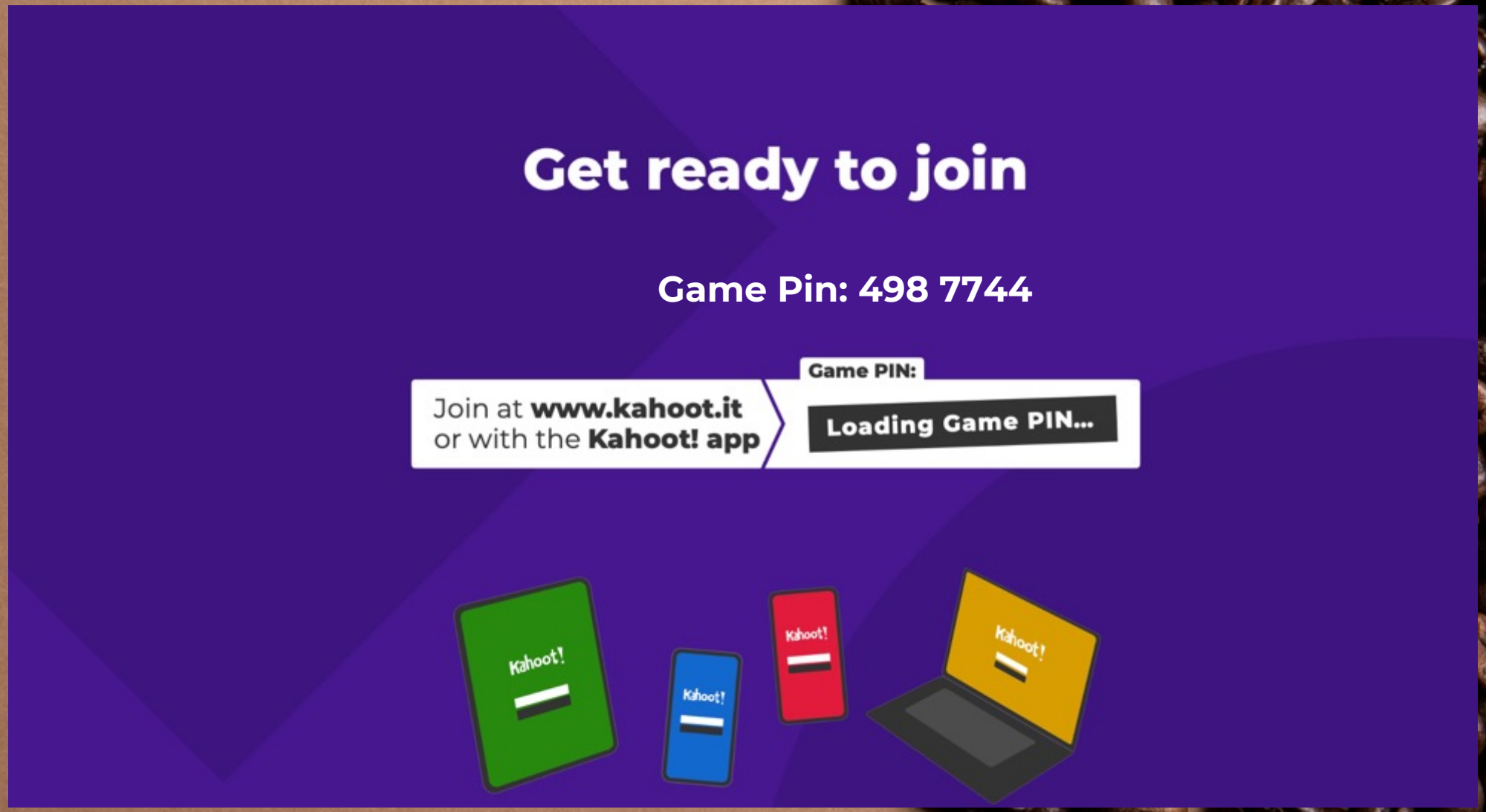
2nd Price
Thermo Bottle

OUTLOOK Upcoming Virtual Espresso

- Blog: https://gblogs.cisco.com/ch-de/tag/virtual-espresso/
- Topics:
  - 12. Januar 2022: Wie funktioniert eigentlich NetDevOps?

Join the game at **www.kahoot.it**
or with the **Kahoot! app**
Game Pin: 498 7744

...so then - let the games begin...



dankä villmal
grazie mille
merci beaucoup
grazia fitg
thank you