
cisco Live!
TURN
IT
UP
#CiscoLive

The bridge to possible

Where The Rubber Meets the Road

Customer Zero's Journey to Multi-Site SDA

Chris Tomazic, Customer Zero, Cisco IT
John Moe, Customer Zero, Cisco IT
Anjitha Shanmughan, Customer Zero, Cisco IT

BRKCOC-2008

Agenda

- Intro to Customer Zero
- CZ Production Fabric Topology
- Migration Strategy
- Challenges
- Best Practices
- Conclusion

Intro to Customer Zero

cisco Live!

About Customer Zero: Our Mission

Improve Quality	*Drive* Value	*Proof of* Scale
Engage BG/BU teams early in lifecycle to create value in design phase and improve solution quality once deployed	Demonstrate value of products and solutions through ROI and business cases including defining solution architectures	Prove solutions scale across the Cisco environment and transition to IT teams

Integrate solutions across BEs, share best practices & lessons learned, showcase outcomes

Customer Zero Outcomes

Accelerate Customer Adoption

Drive Value Through Integrated Solutions

Increase Delivery Velocity

Primary Value Drivers of SDA

Business Features

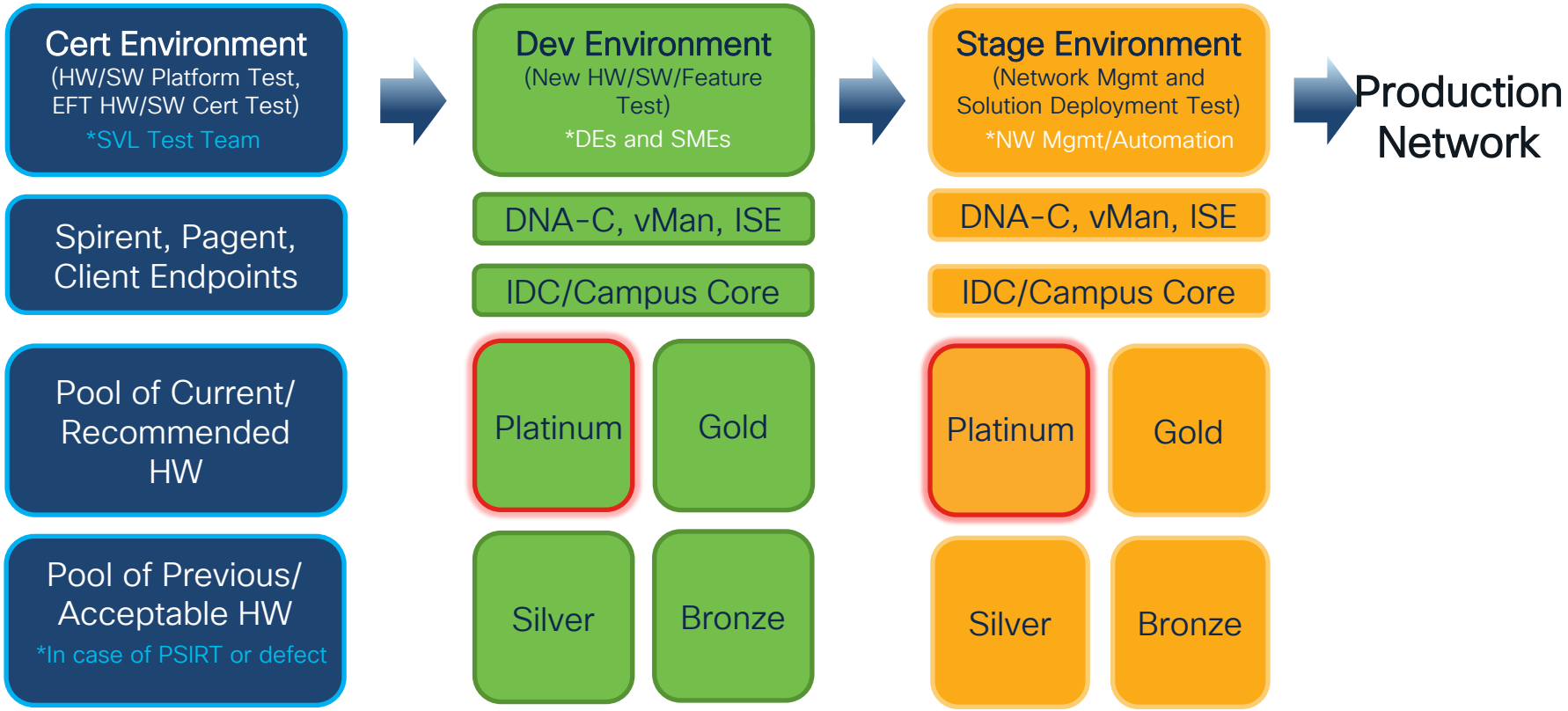
1. Cisco Trust Sec Segmentation
2. WiFi 6 refresh with C9800 eWLC
3. Additional bandwidth to edge (equal cost multipath load balancing)

Operations Evolution

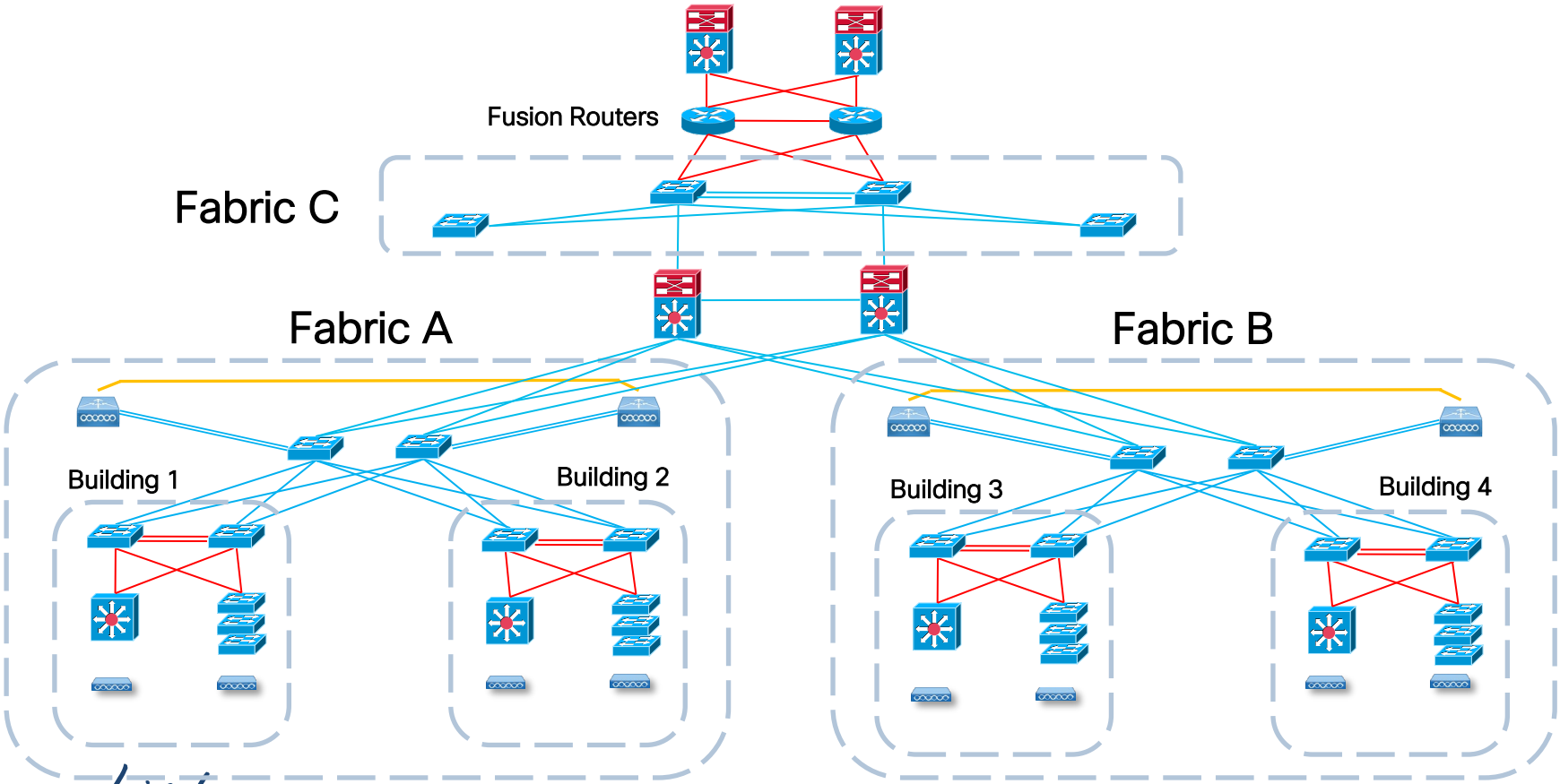
1. Guest ACLs only needed on border nodes
2. Address space simplification
3. Operational Standardization (DNAC config mgmt., DevOps workflows)
4. SWIM for IOS upgrades
5. Consistent network views from edges (PIM, LISP, etc.)
6. No more static IPs

CZ Production Fabric Topology

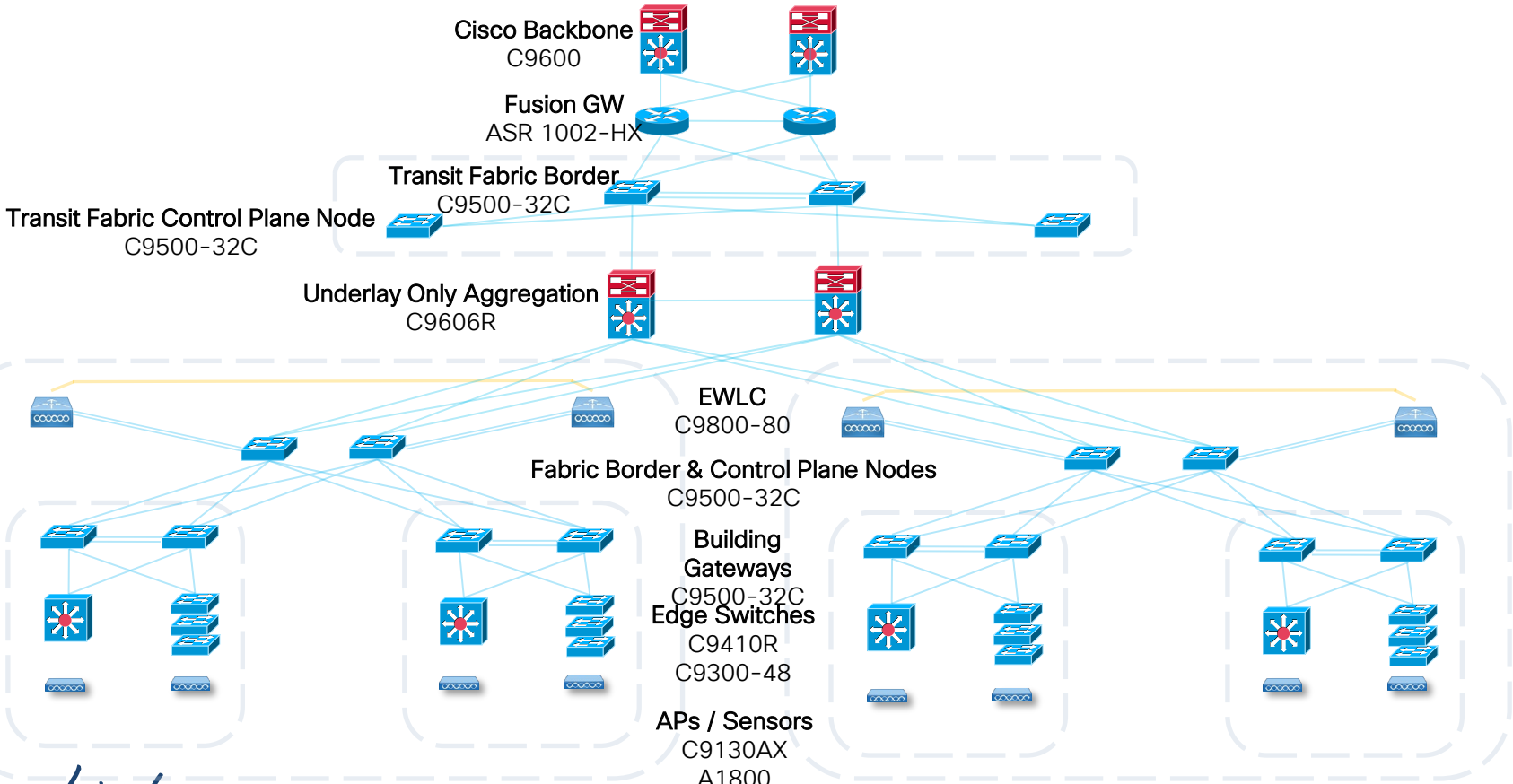
New SVL Test Environments and Testing Pipeline



SJC20-25 Logical Fabric Topology



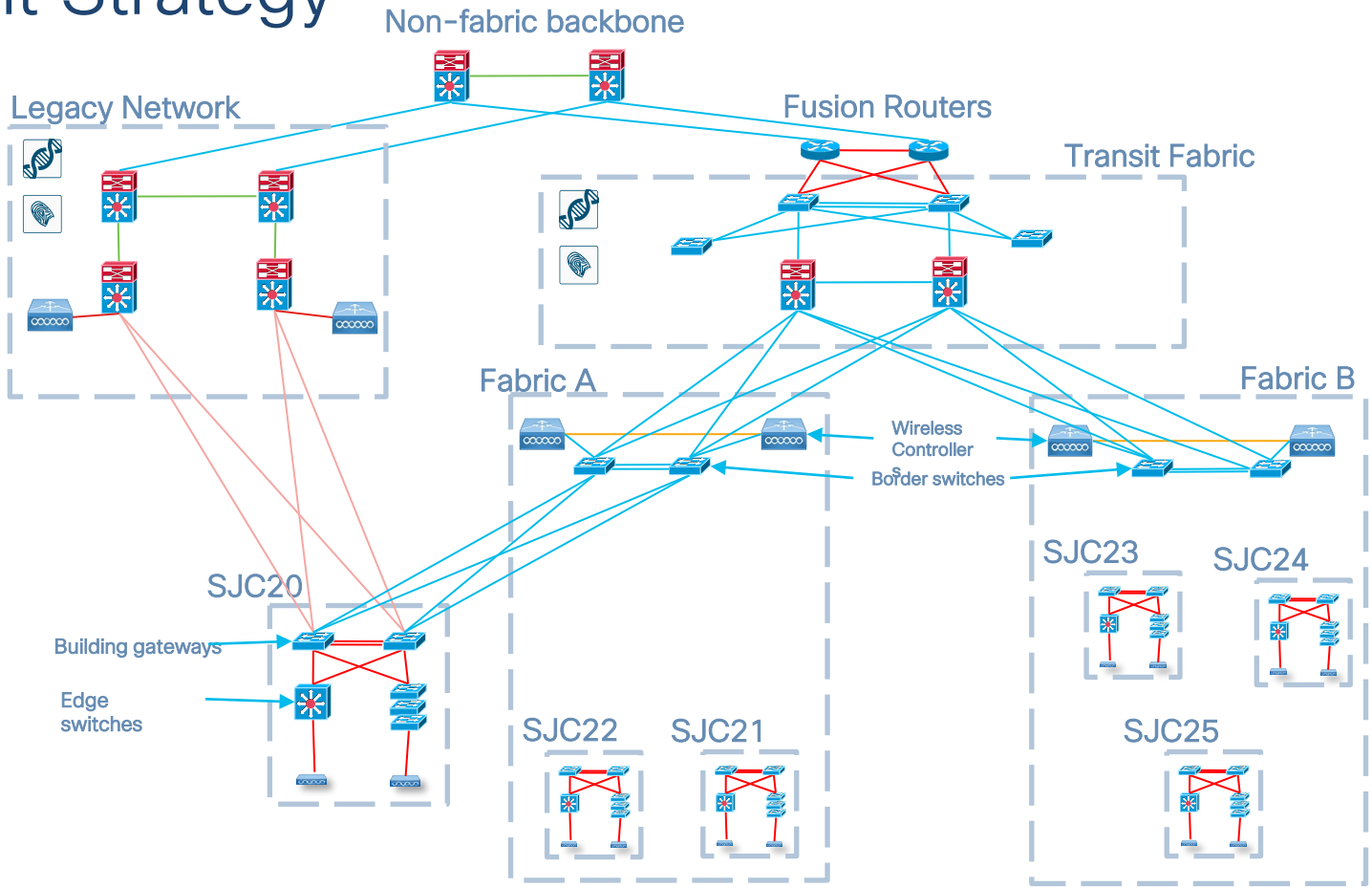
SJC20-25 Physical Fabric Topology Roles



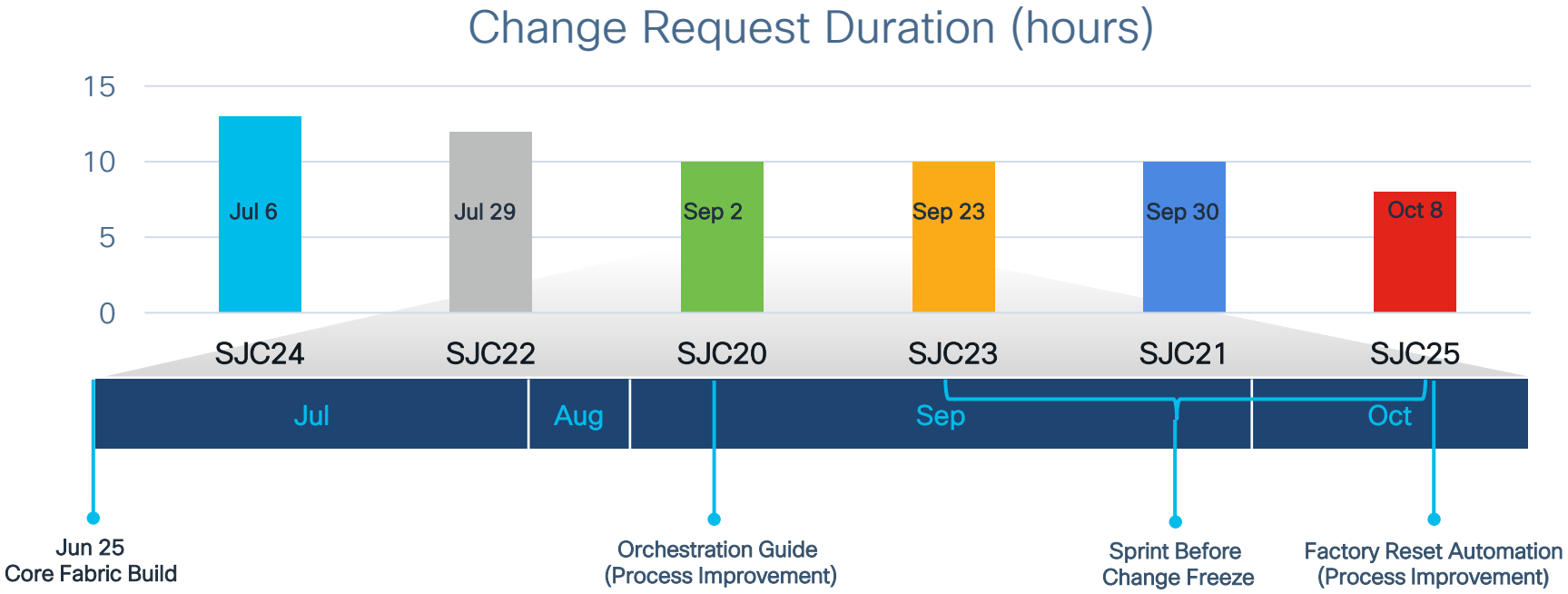
Migration Strategy

Deployment Strategy

1. Deploy Transit Fabric and Fabric A & B borders
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



Fabric Migrations Improved Over Time



Challenges

Customer Zero's approach to challenges...

- Work with products early and aggressively
- Find gaps and functionality issues
- Then work tightly with product developers to get them addressed

Edge Switch Blocks End-User Switchports

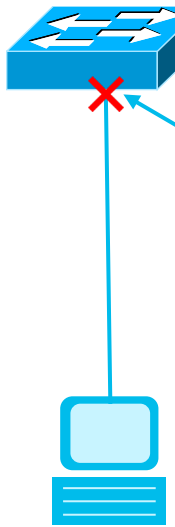
Still under investigation

SYMPTOMS

- Ports get stuck in terminal MAB/dot1x failed state after edge switch reboots
- Switchport should restart authentication, but does not
- Seems to be a corner case

SOLUTION

- Manually find and bounce the port.
- Configure Critical VLAN to help trigger re-auth



```
Edge_switch#show run | sec PMAP_DefaultWiredDot1xClosedAuth_1X_MAB
PMAP_DefaultWiredDot1xClosedAuth_1X_MAB
<snip>
  40 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authentication-restart 60
```

```
Edge_switch#show access-session int Te1/0/1 detail
            Interface:  TenGigabitEthernet1/0/1
          MAC Address:  aabb.ccdd.eeff
               Domain:  UNKNOWN

Method status list:
       Method           State
        dot1x           Stopped
          mab           Authc Failed
```

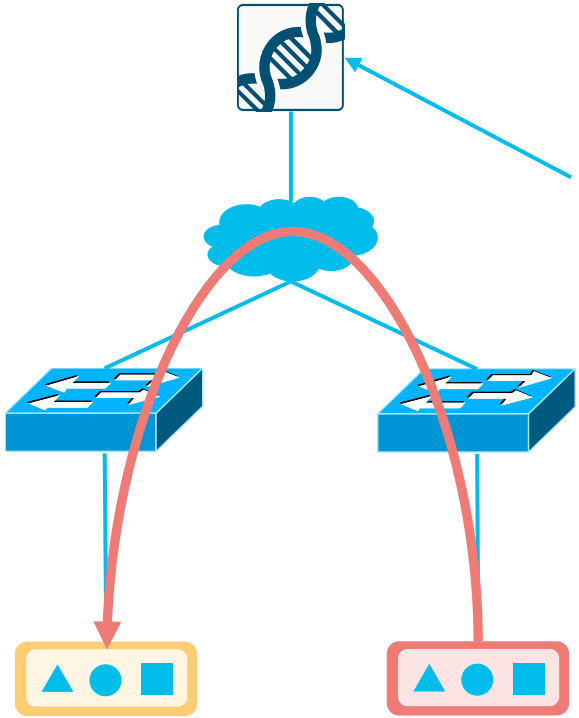
BMS Devices May Need L2 Flooding Enabled

SYMPTOMS

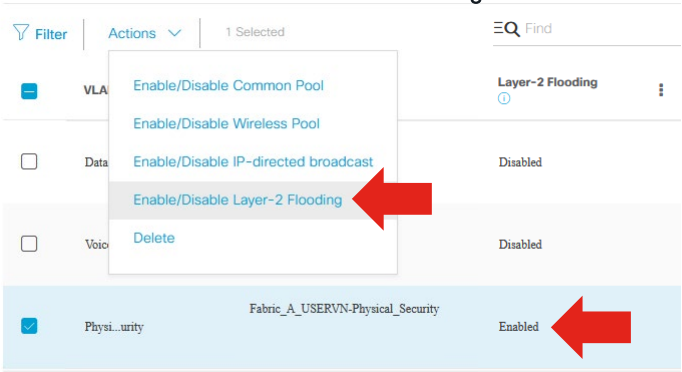
- Building Management Systems (BMS) go offline
- “Child” systems (red) find “parent” systems (yellow) via L2 broadcast
- SDA drops L2 broadcasts without explicit config

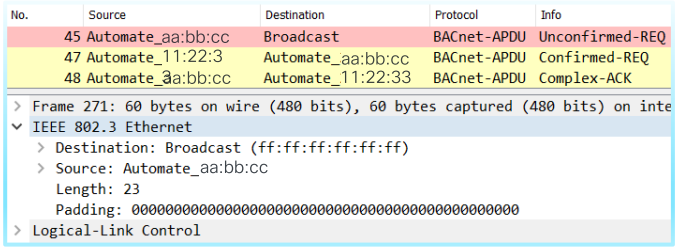
SOLUTION

- Behavior is dependent upon controller age and model
- Confine BMS controllers to one Virtual Network
- Enable L2 Flooding on the VN



Provision > Fabric > Host Onboarding > Virtual Networks





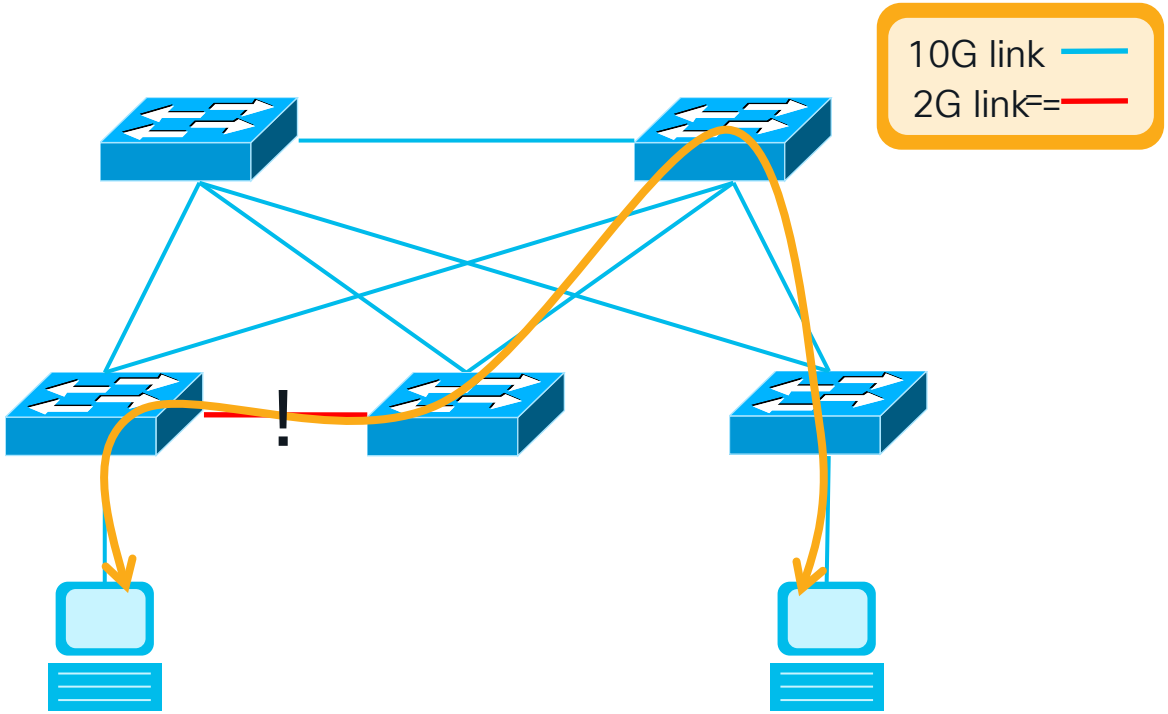
Links Between Edge Switches Become Routable Links

SYMPTOMS

- Sub-optimal routing
- Edge-to-edge links were undiscovered before factory reset and LAN Automation
- Became routable IS-IS links after LAN Automation

SOLUTION

- Improve auditing before maintenance window
- Manually remove unwanted IS-IS interface config
- Follow CSCvw23495 for DNAC enhancement to automate removal of LAN Automated L3 link



Excessive Device Resyncs Indicate Network Problem

SYMPTOMS

- DNAC resyncs a device very frequently (every few minutes)
- This is typically due to link flaps, AP disassociations, or config changes

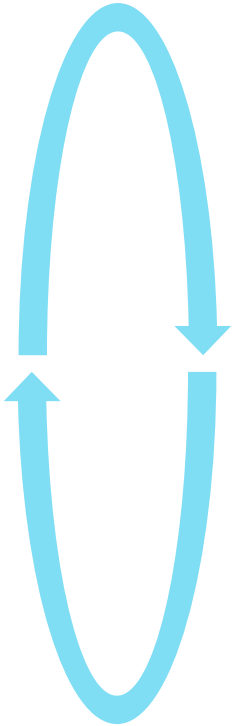
SOLUTION

- CZ generates alerts to Webex Teams for excessive resyncs
- Resync behavior is hardened in later DNAC versions
- Note: if using “aaa accounting commands”, excessive resyncs can create lots of TACACs logging

3. After receiving enough traps, DNAC resyncs device.

2. Switch sends Link Up/Down traps to DNAC.

1. Un-provisioned 1800 sensor can’t reach DNAC. It causes port flaps.

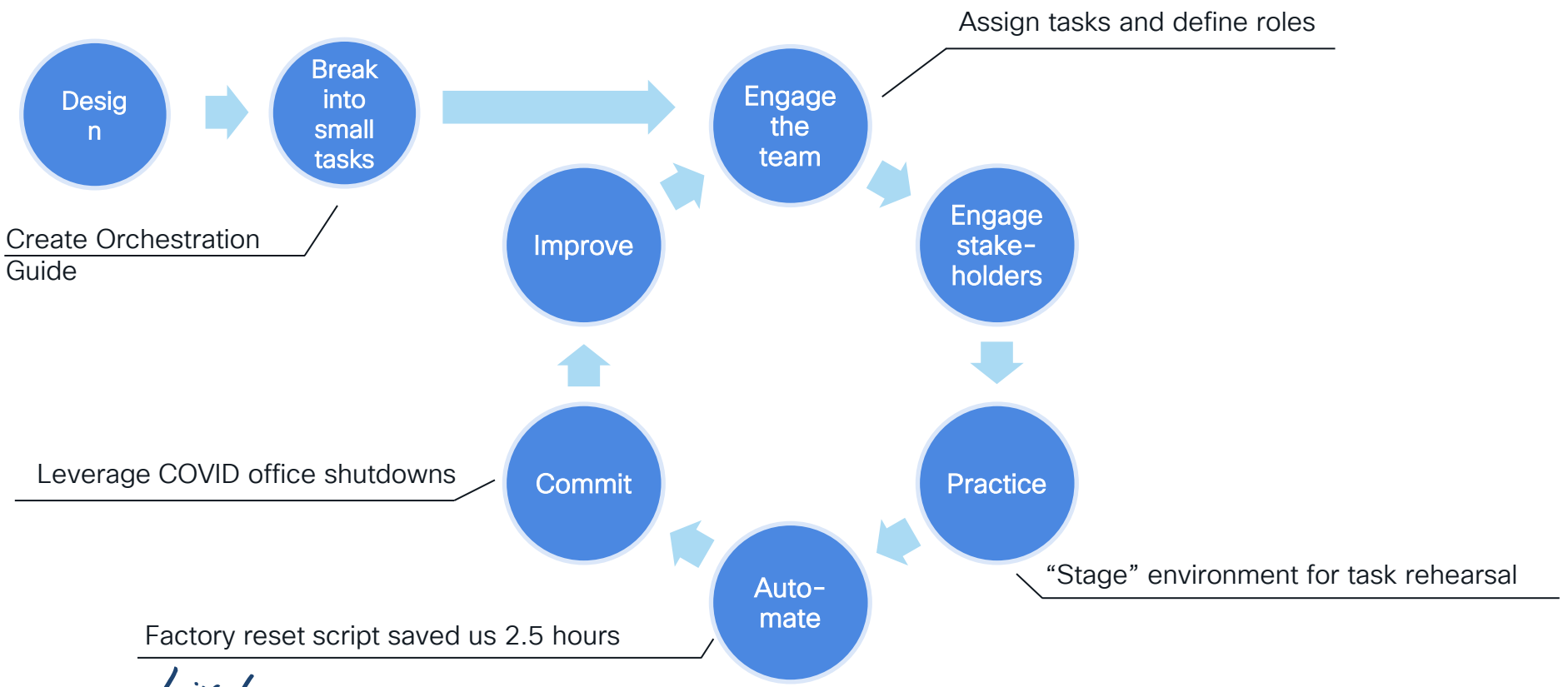


Best Practices

Customer Zero Best Practices

1. SDA requires technical competency plus agile organization … NetDevOps can help manage both
2. Trust DNAC to configure your fabric
3. Know DNAC's limitations
4. Understand the technical skills required for SDA (both traditional skills and new)
5. Engage TAC before you need them

1 Find your NetDevOps cycle



2 & 3 What workflows does DNAC support?

Before

- Audit the network ✗
- Build documentation ✗
- Work with stakeholders ⚠ ✗
- Open CR ✓
- SWIM Upgrade

During

- Notify stakeholders ✗
- Factory reset switches ✗
- Physical uplink mov ✓
- PnP / LAN automatio ✓
- Underlay/Overlay conf ✓
- Wireless AP conf ✓
- Validate ⚠

After

- Interface descriptions ✗
- Add switch license ⚠
- DNS and DHCP updates ✗ ⚠
- DNA Spaces ma ✓ update
- Day 2 monitoring

✓ = Supported ✗ = Unsupported ⚠ = Not supported at time of CZ migrations

2 & 3 Filling the gaps: Roles and Orchestration Guide

1. Create Orchestration Guide → 2. Define Roles → 3. Assign Tasks → 4. Follow the Leader

1

	A	B	C	D
1	**Task**	**Expected start time**	**Owner**	**Notes**
26	On-site Engineer arrives	+2 hours		
27	Building Distribution Gateway Physical Fiber Move (from Legacy Aggregation Distribution Gateway to Fabric Borders)			
28	Update IT Partner Stakeholders (All Stakeholders Webex Room)			
29	Find two open ports on the Borders for the Building Distribution Gateways			
30	Open consoles to Building Distribution Gateways and Borderss			Monitor the up/down status of the interfaces to ensure the correct fibers are
31	Migrate Building Distribution Gateways uplinks to Primary Border			
32	Drive to other buidling with Secondary Border			
33	Remove Stackwise Virtual Config and Reload Building Distribution Gateway's			SVL has been removed. Building Distribution Gateways are now two standalon
34	Remove 3rd cross link (Hun 1/0/5) interface cable between the Building Distribution Gateways			This is the dual-active-detection link.
35	Migrate Building Distribution Gateways uplinks to Secondary Border			
36	Factory Reset Building Distribution Gateways			
37	Update IT Partner Stakeholders			
38	Clear PnP List in DNAC			
39	Trigger re-sync of the Fabric Borders			This should pick up the new connections to the building Building Distribution G
40				
41				
42	While starting LAN Automation in DNAC - (PnP)	+3 hours		
43	Trigger LAN Automation			
44	Use the CSV File with new switch hostnames and SNs			
45	Open Console to All Switches and Monitor PnP Progress			
46	If any issue get TAC involved			
47	Update IT Partner Stakeholders about status and if TAC involvement is required			
48	Switch Loopbacks			
49	Export new switches inventory from DNAC			
50	Update audit sheet with new loopback ip address and new switch names			

Important Info | Before Fabric CR | During Fabric CR | After Fabric CR

2

Ops Team

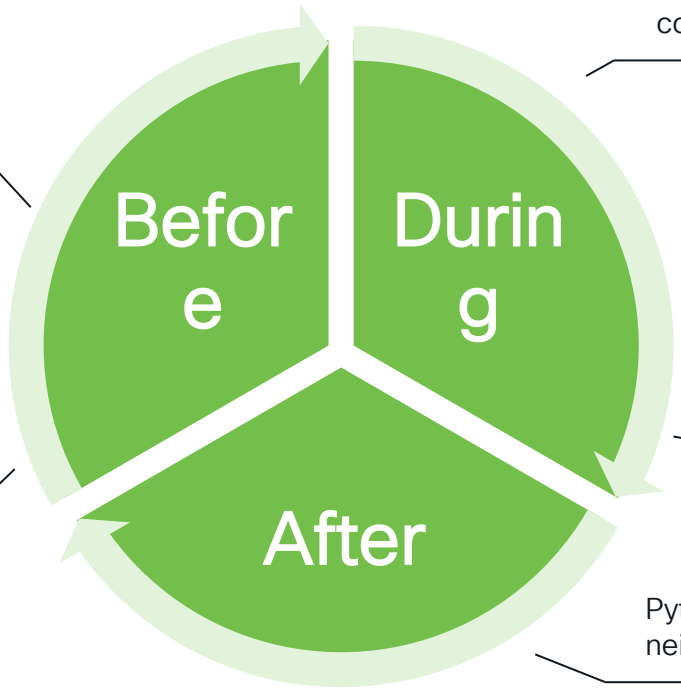
4

Orchestrator

3

Task Owners

2 & 3 Filling the gaps: Scripting



Python script that audits CDP neighbor info and interface MAC entries

"Command Runner" – Push any command(s) to a list of devices

Prep for PnP Script – factory reset switches

Ansible scripts to confirm SDA network element config

Python to backup configs

Python script to copy CDP neighbors to interface descriptions.

4 Understand the engineer skills needed

Existing Skills

- Cisco TrustSec
- DNAC
- Enterprise route/switch
- Wireless
- PIM-SM
- Knowledge of encapsulation protocols
- Python

New Skills

- Critical VLAN
- LAN Automation
- Native DNAC config vs. templates
- DNAC order of operations
- IS-IS
- ECMP
- LISP message flows
- Changes to ARP and L2 Broadcasts
- Tags and Profiles
- Broadcast/multicast handling
- VXLAN
- Custom tools

5 Engage TAC early and efficiently

- Open a proactive TAC case
  - Attach DNAC RCA logs before and after the migration
- Select SDA as the technology
- Keep WebEx Team room open with TAC
- What you expect from the case determines resolution time
  - “I want a workaround as soon as possible.”
  - “I want to troubleshoot this to root cause and file a bug, if needed.”
  - “I want to update documentation, so it is easier to understand.”
  - “I want to file an enhancement request to change the behavior.”

Conclusion

Conclusion

- Cisco's Customer Zero team deployed multisite fabric in the production network
- By using our Orchestration Guide and NetDevOps execution cycle, the deployments became faster and less painless over time
- CZ distilled its best practices in this slide deck for other customers to use

Questions?

- Contact us at cz_sda_ext@cisco.com

The bridge to possible

Thank you


cisco Live!
TURN
IT
UP
#CiscoLive