

Designing Highly Available Networks Using Cisco Catalyst 9000 Switches

cisco Live !

Minhaj Uddin
Leader, Technical Marketing

Session ID: BRKENS-2095

Cisco Webex App

Questions?

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

How

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

Webex spaces will be moderated by the speaker until 14 November 2025.

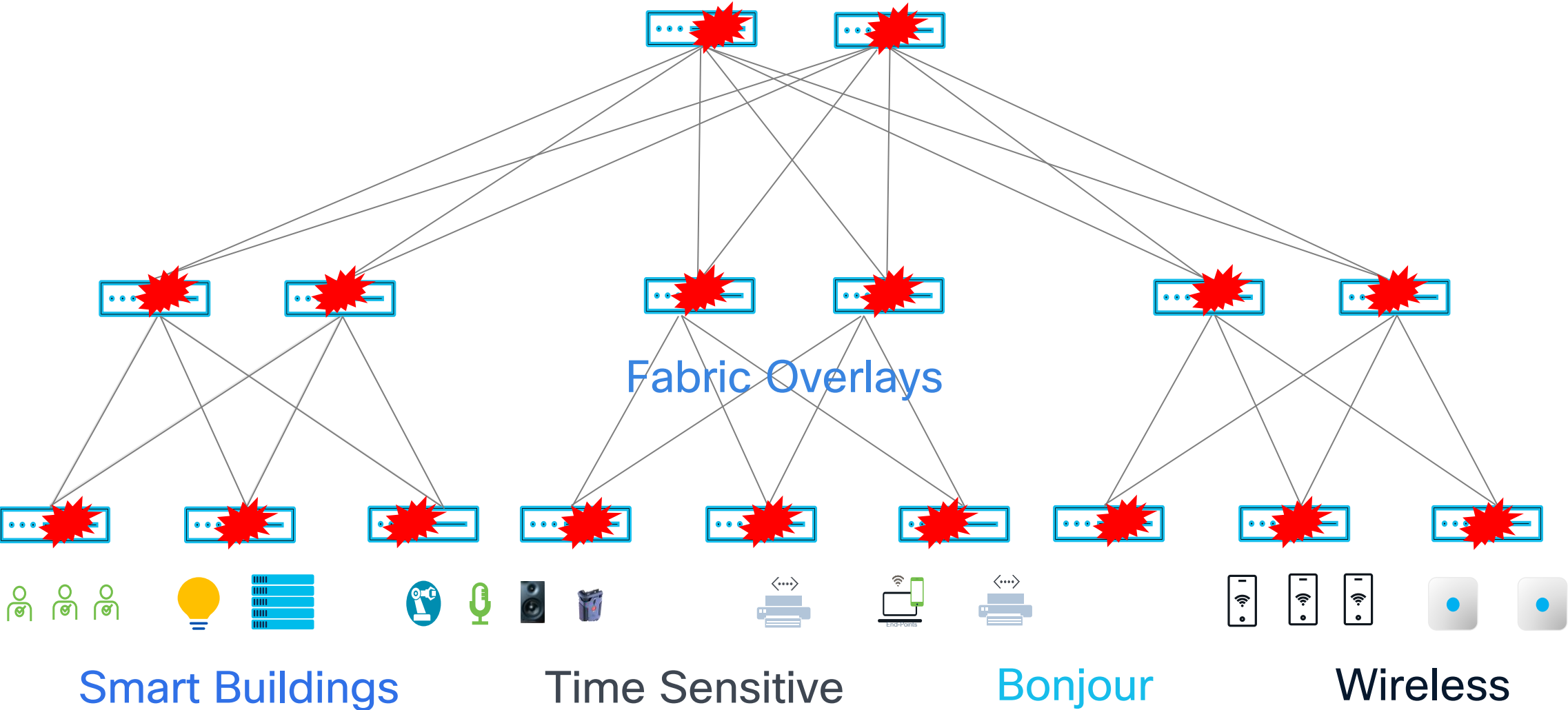


<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2095>

Agenda

- 01 Introduction
- 02 Platform & Design Redundancy
- 03 Software Redundancy
- 04 Customer Case Studies / Design Options
- 05 Conclusion

Traditional Enterprise Campus Network



99.999% *Availability*

Reliable Networks with Catalyst 9000

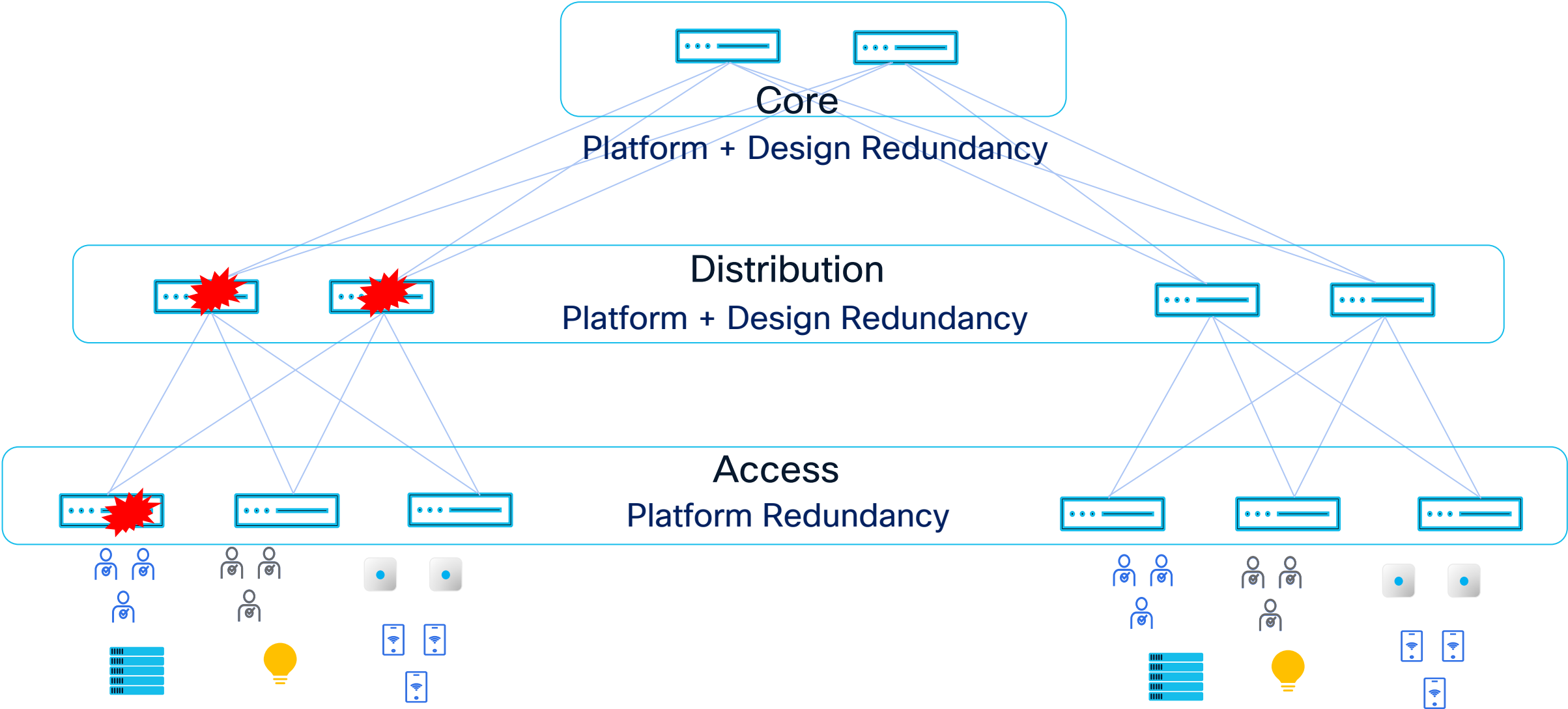
$$\text{Availability} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} = 99.999\% \text{ (5min/yr downtime)}$$

So, MTBF should be higher – Robust Platform

MTTR should be smaller – Redundancy

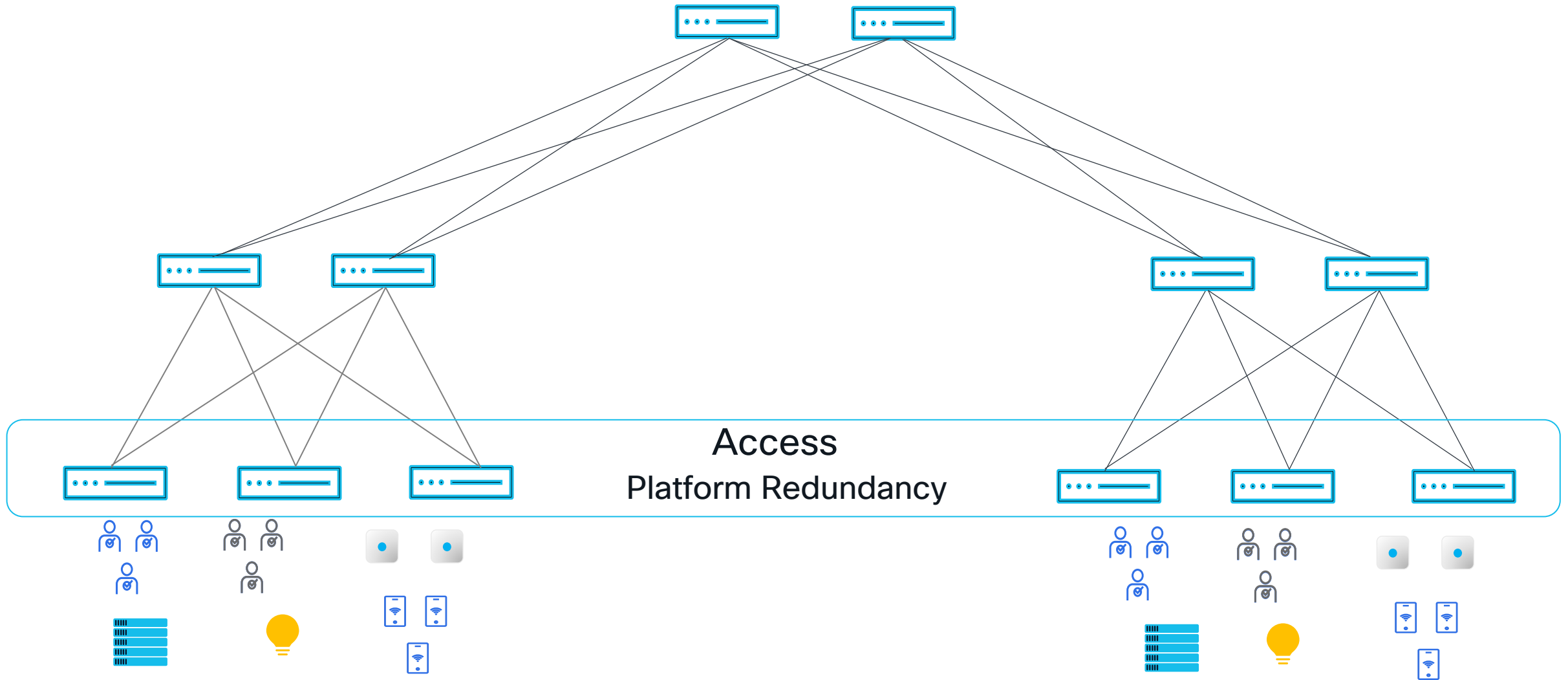
Key is to have Redundancy at every layer of the network

Traditional Enterprise Campus Network



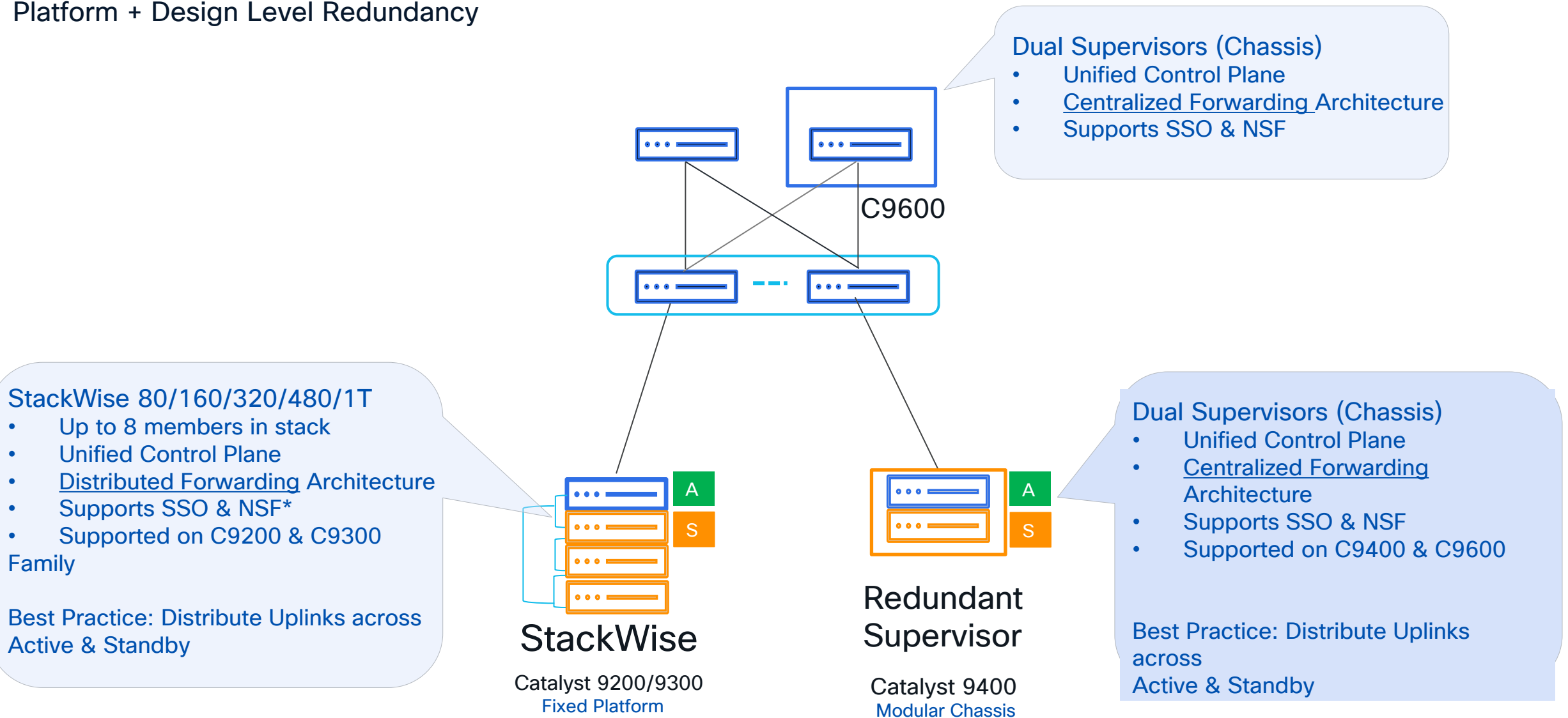
Redundancy at the Platform + Design Level

Platform Resiliency in the Access Layer



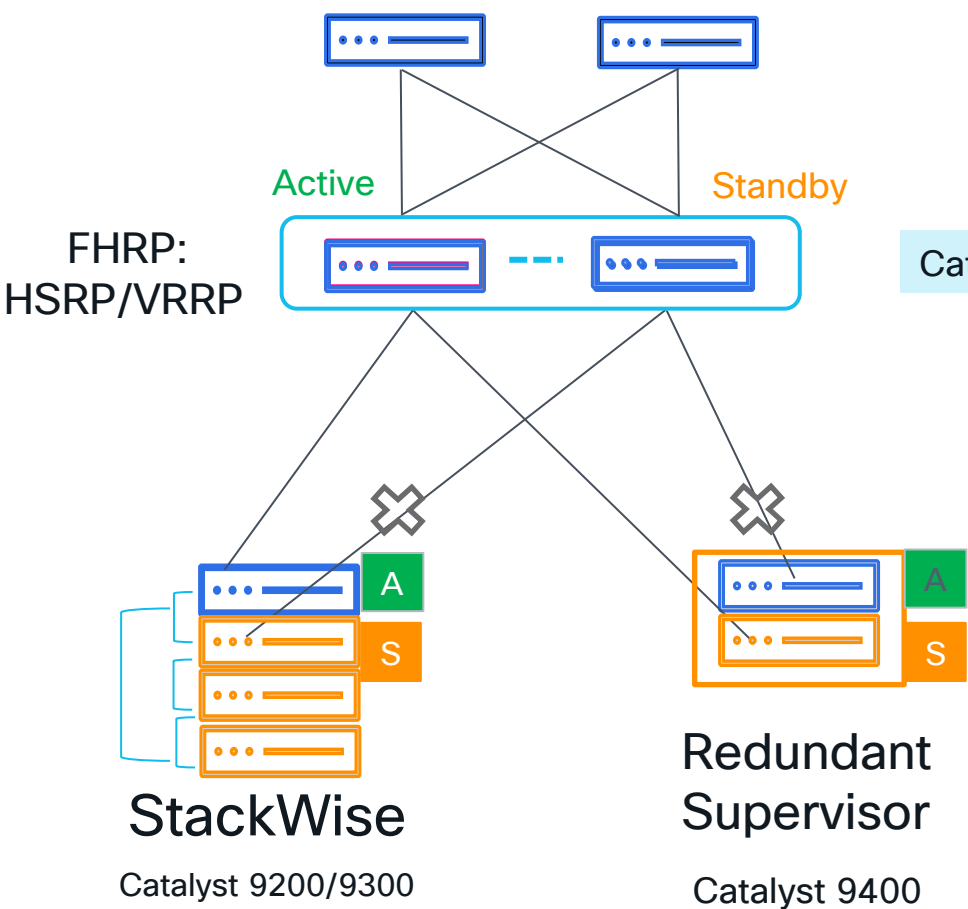
Enterprise Campus Network

Platform + Design Level Redundancy

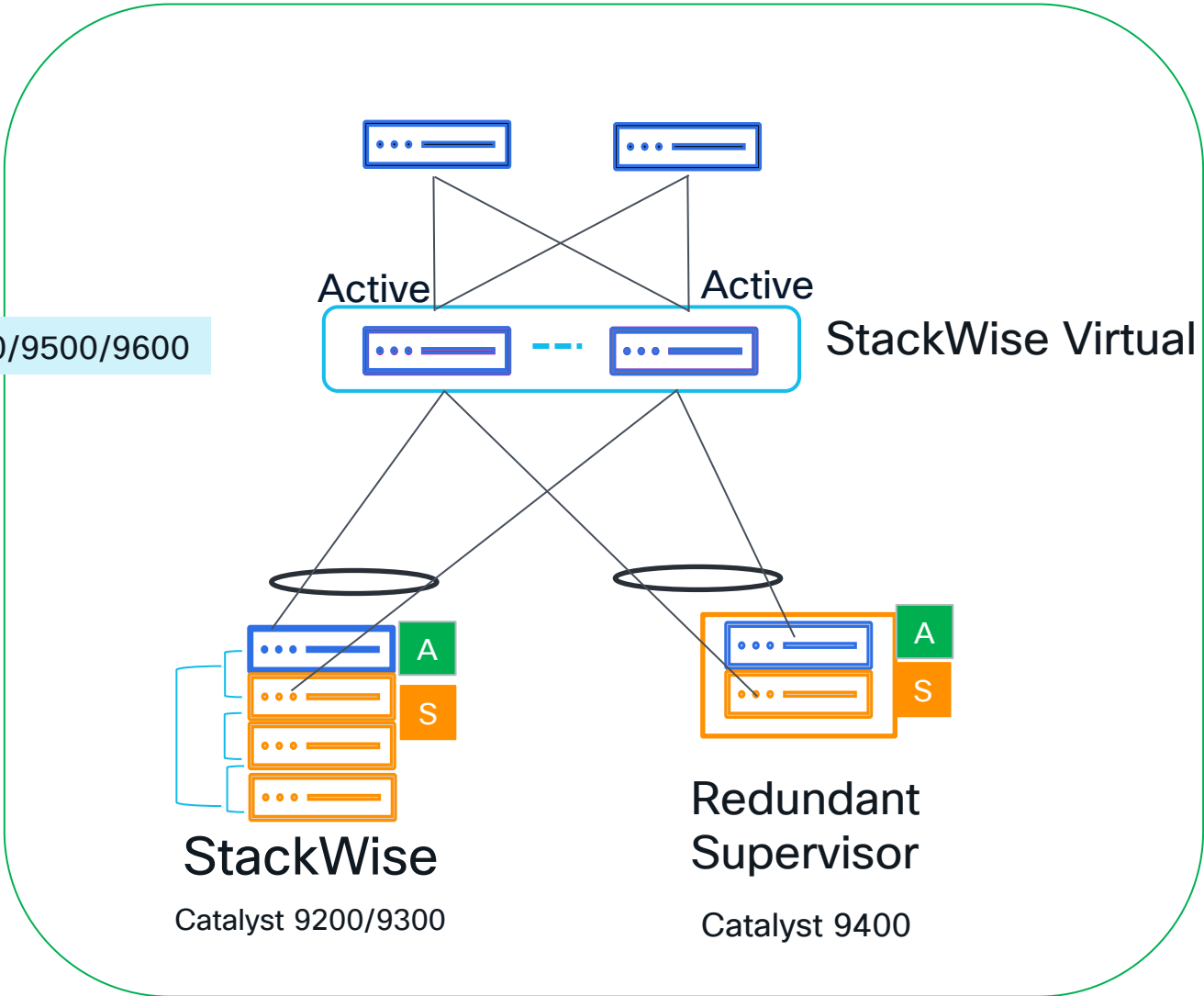


Enterprise Campus Network

Platform + Design Level Redundancy



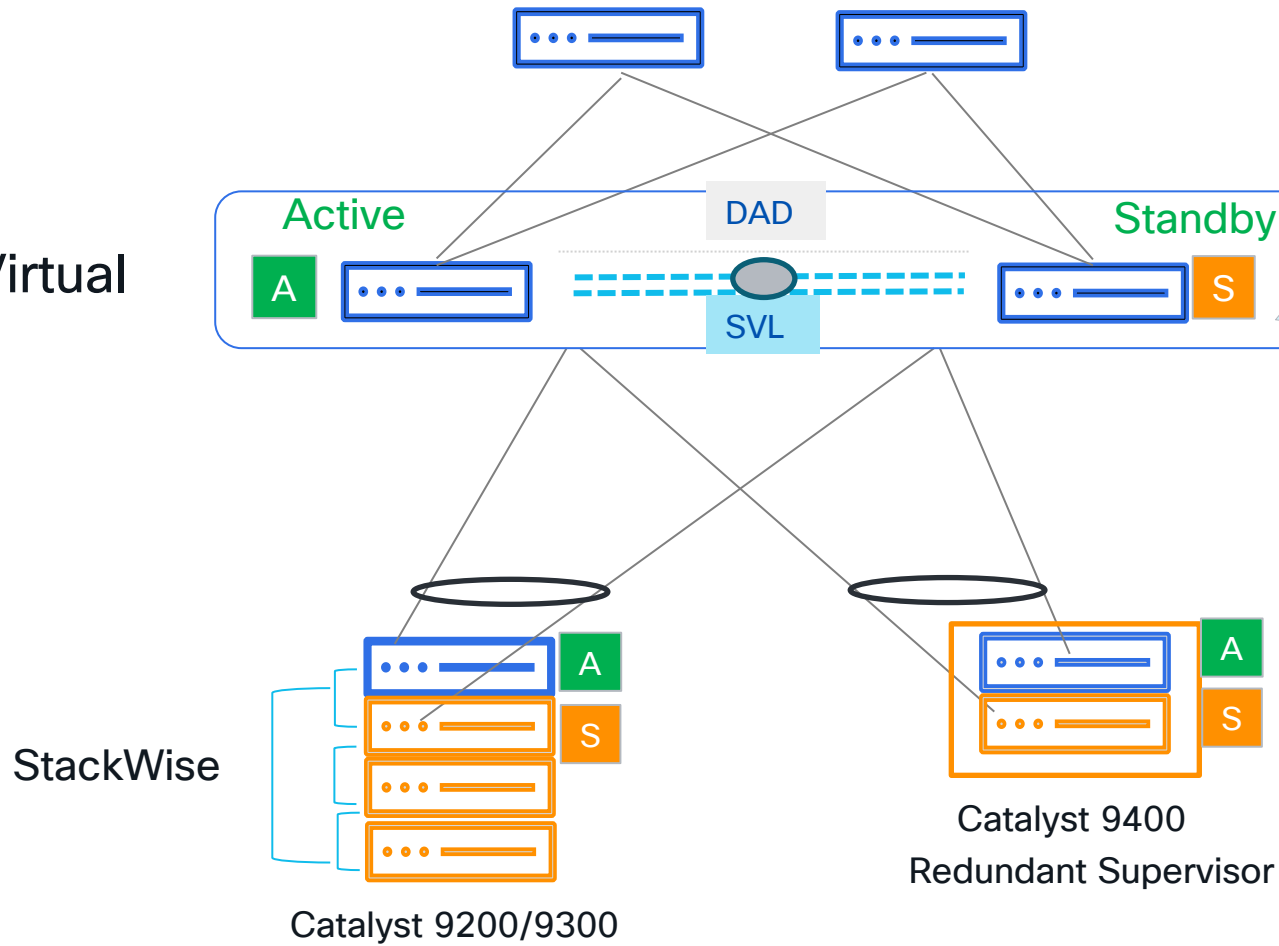
Recommended



Enterprise Campus Network

StackWise Virtual for Distribution and Core Layers

StackWise Virtual



StackWise Virtual

- Unified Control Plane
- Distributed Forwarding Architecture
- Supports SSO & NSF
- Supported on C9400, C9500 & C9600

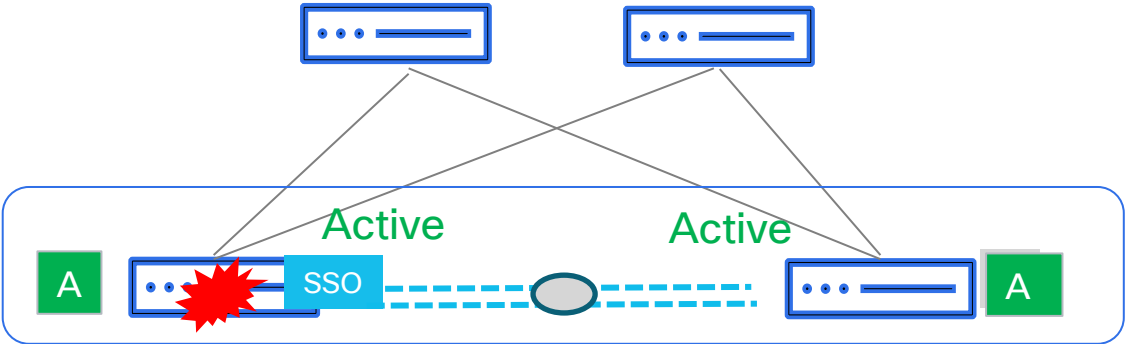
Best Practice:

- Have Redundant Links for SVL & DAD
- Dual-Homed Connections

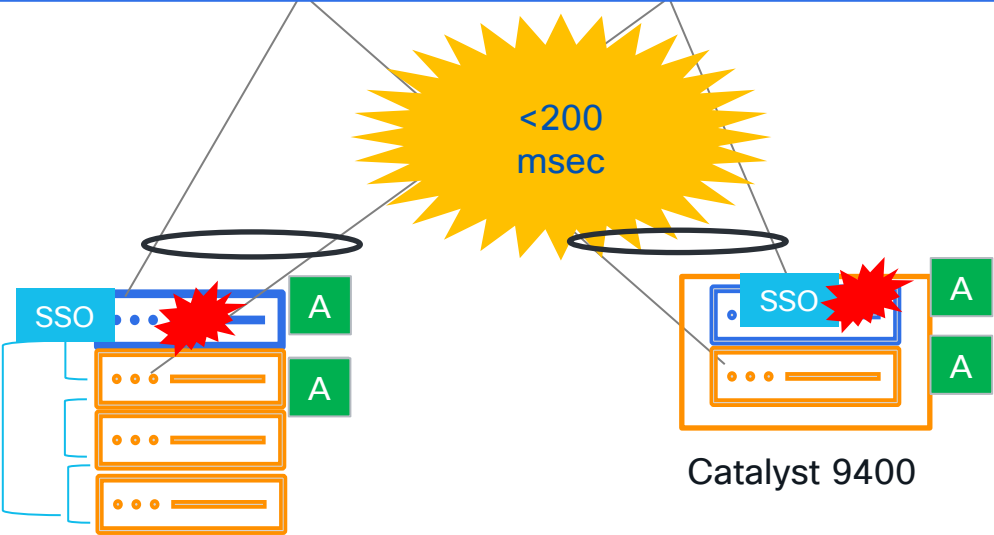
Enterprise Campus Network

Device Failures with Stateful Switchover (SSO)

StackWise Virtual



StackWise



Catalyst 9200/9300

Catalyst 9400

Redundant Supervisor

Stateful Switchover (SSO)

SSO Aware Applications

Forwarding Information Base

IEEE 802.1x

PAgP / LACP

...and more

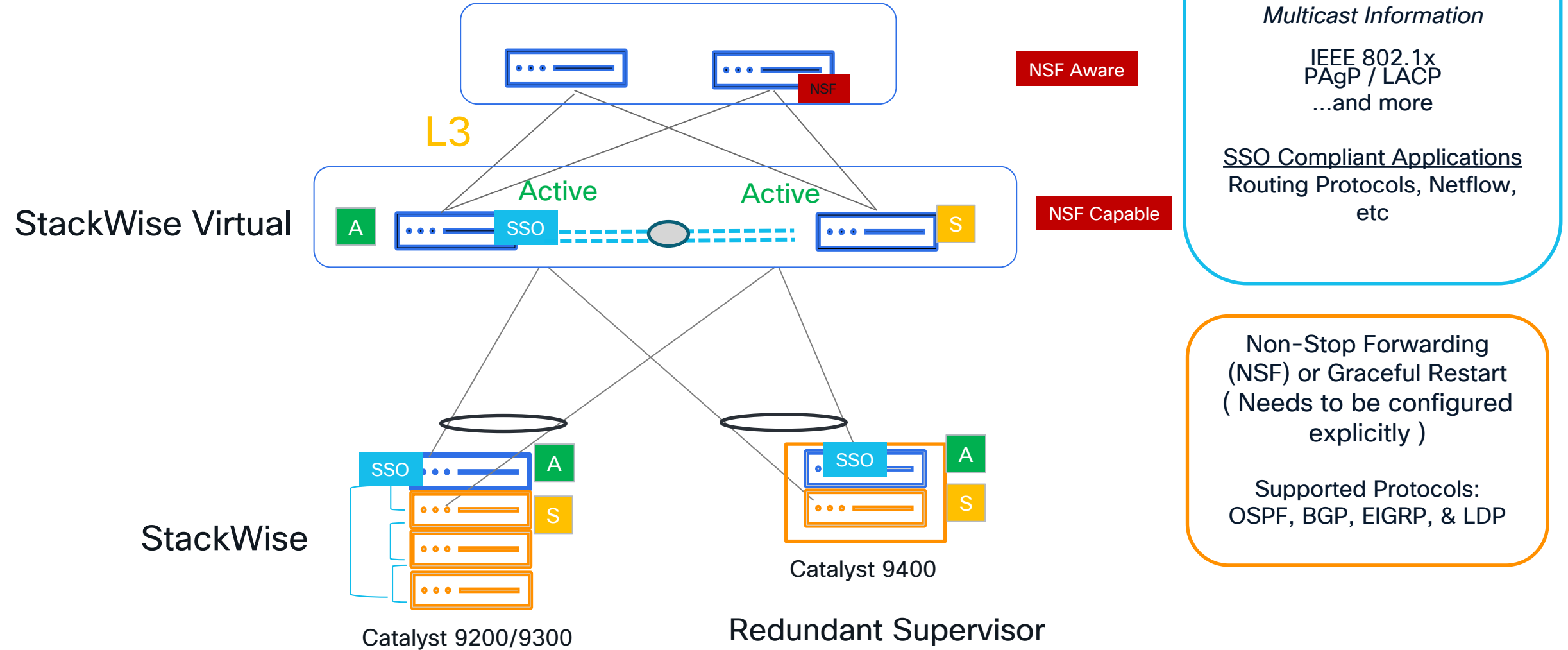
SSO Compliant Applications

Routing Protocols, Netflow, etc

FIB Table	
Prefix	Next HOP
10.1.1.1	aabbcc:ddee32
10.1.1.2	adbb32:d34e43
192.168.0.0	aa25cc:ddee8

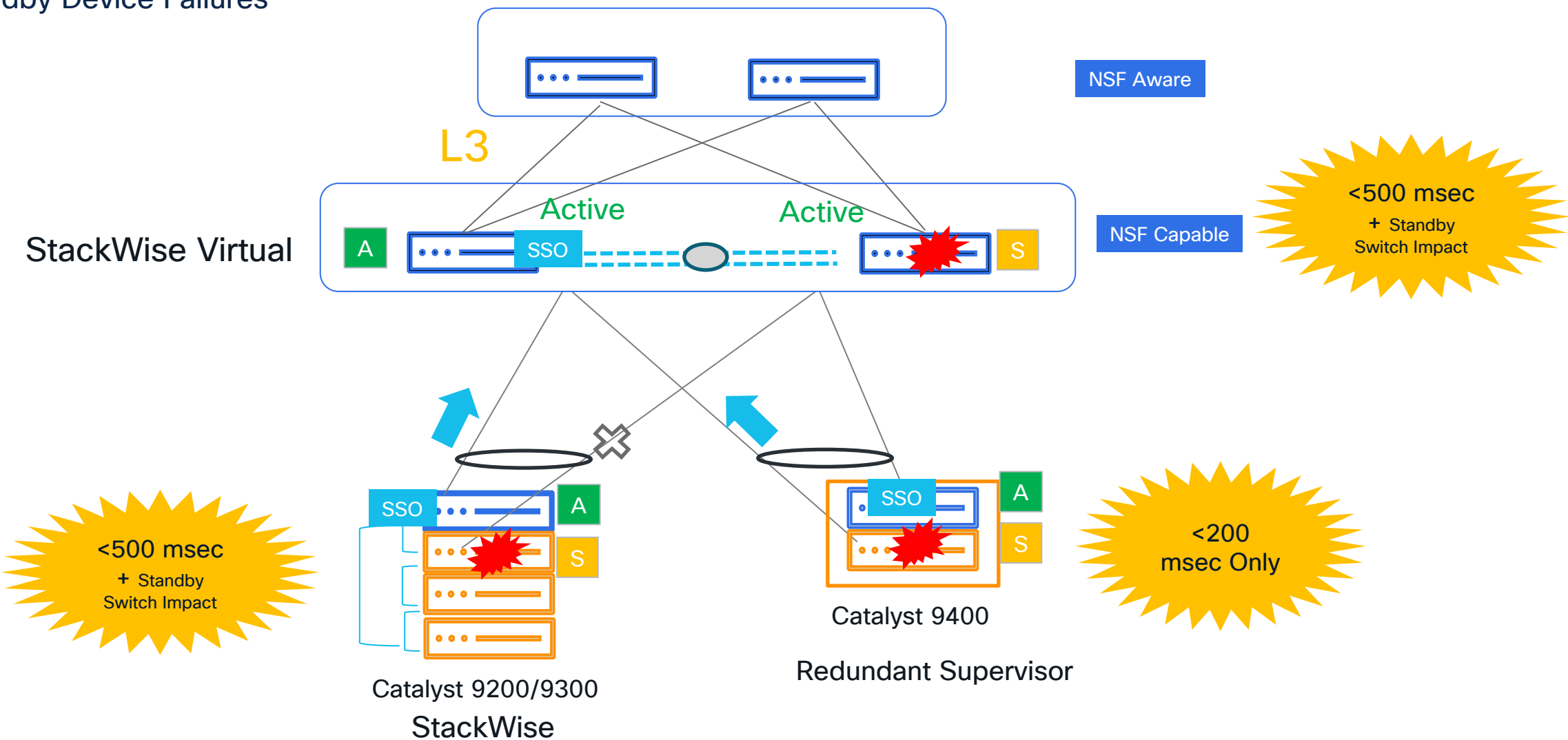
Enterprise Campus Network

Non-Stop Forwarding for L3



Enterprise Campus Network

Standby Device Failures

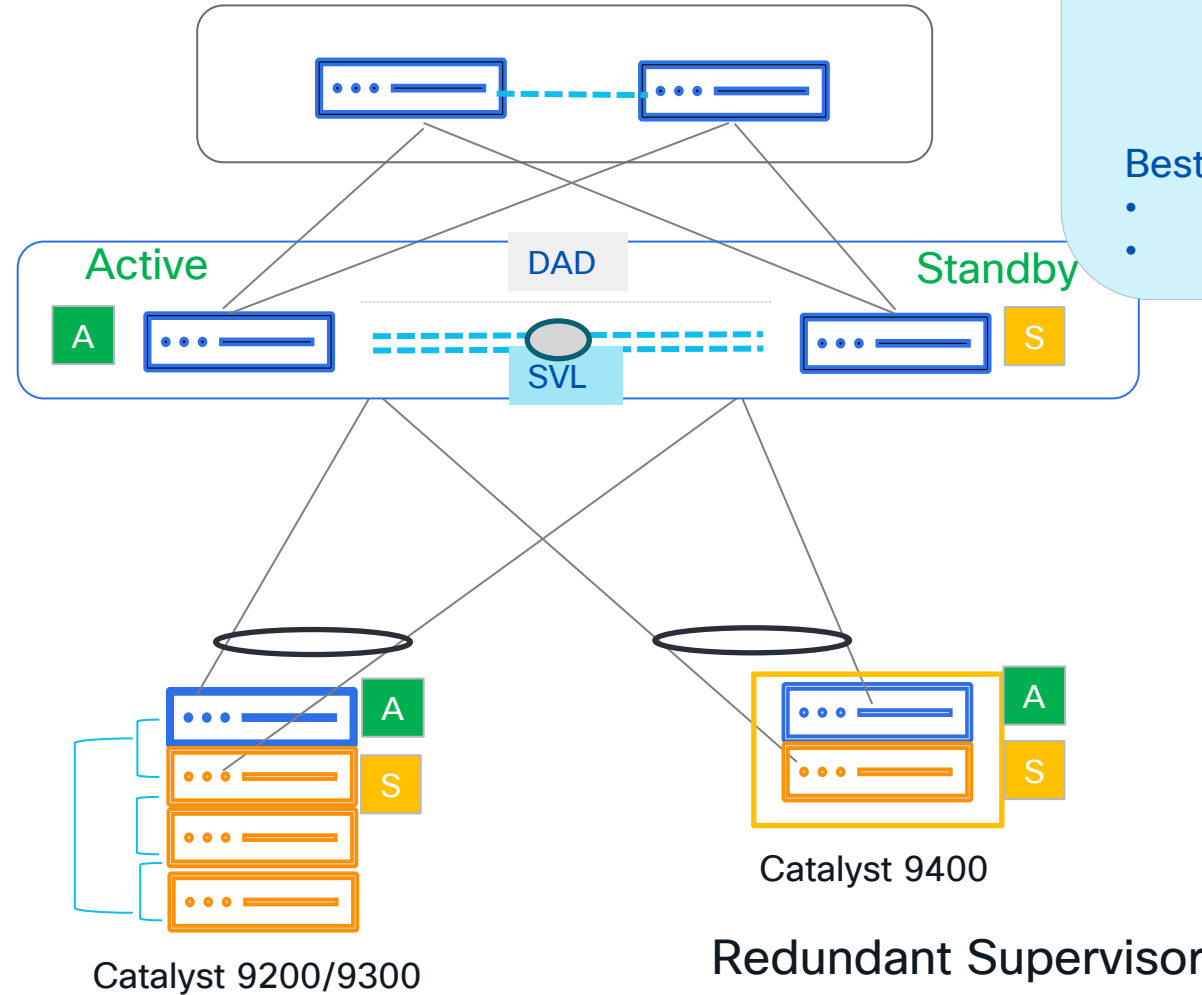


Enterprise Campus Network

StackWise Virtual for Distribution and Core Layers

StackWise Virtual

StackWise



StackWise Virtual

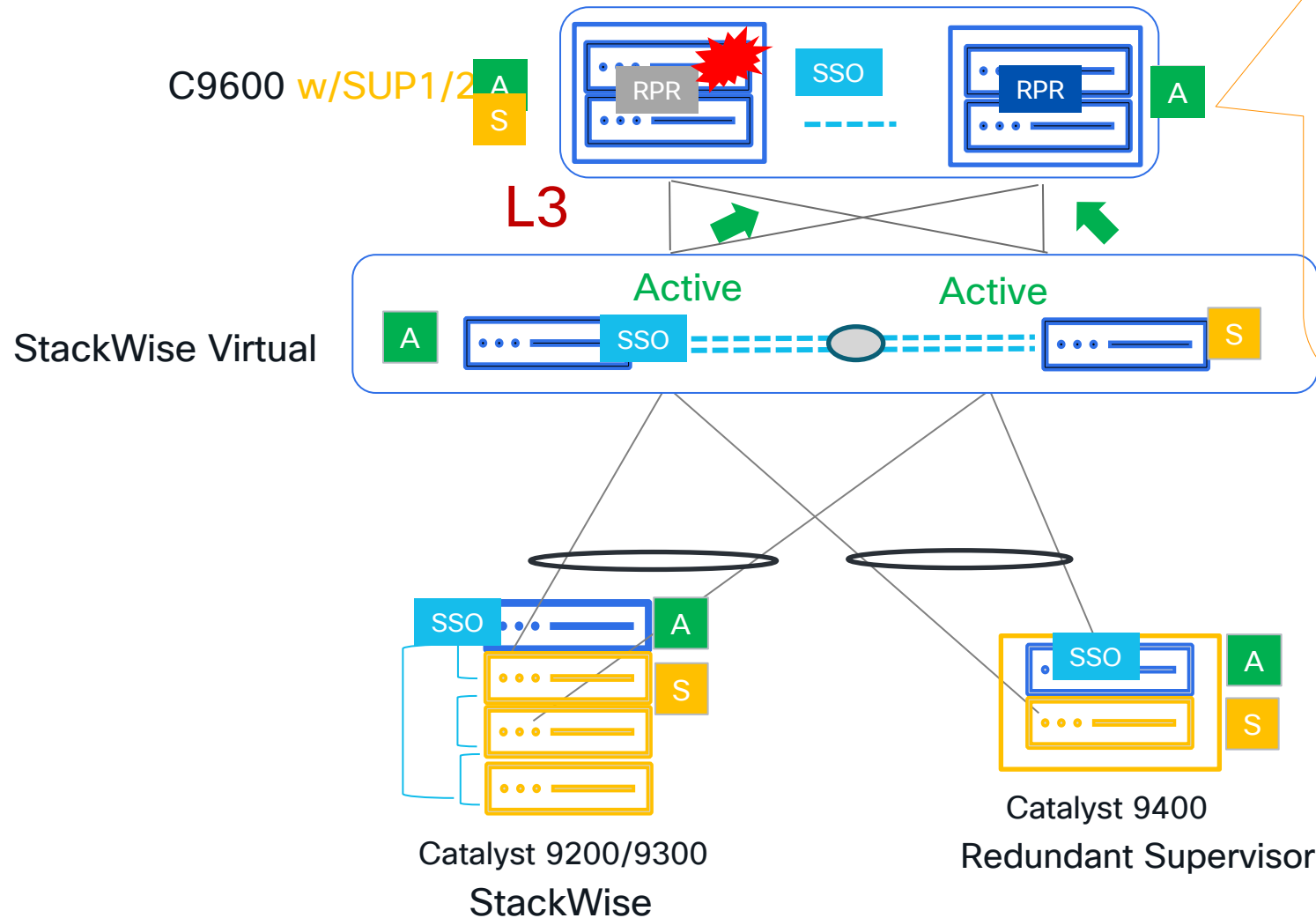
- Unified Control Plane
- Distributed Forwarding Architecture
- Supports SSO & NSF
- Supported on C9400, C9500 & C9600

Best Practice:

- Have Redundant Links for SVL & DAD
- Dual-Homed Connections

Enterprise Campus Network

StackWise Virtual Quad SUP RPR for Core



StackWise Virtual with Quad Sup

- SVL with Dual Supervisors in each chassis (Supported on 9600 SUP1* only)
- RPR (Route Processor Redundancy) within Chassis & SSO between the chassis

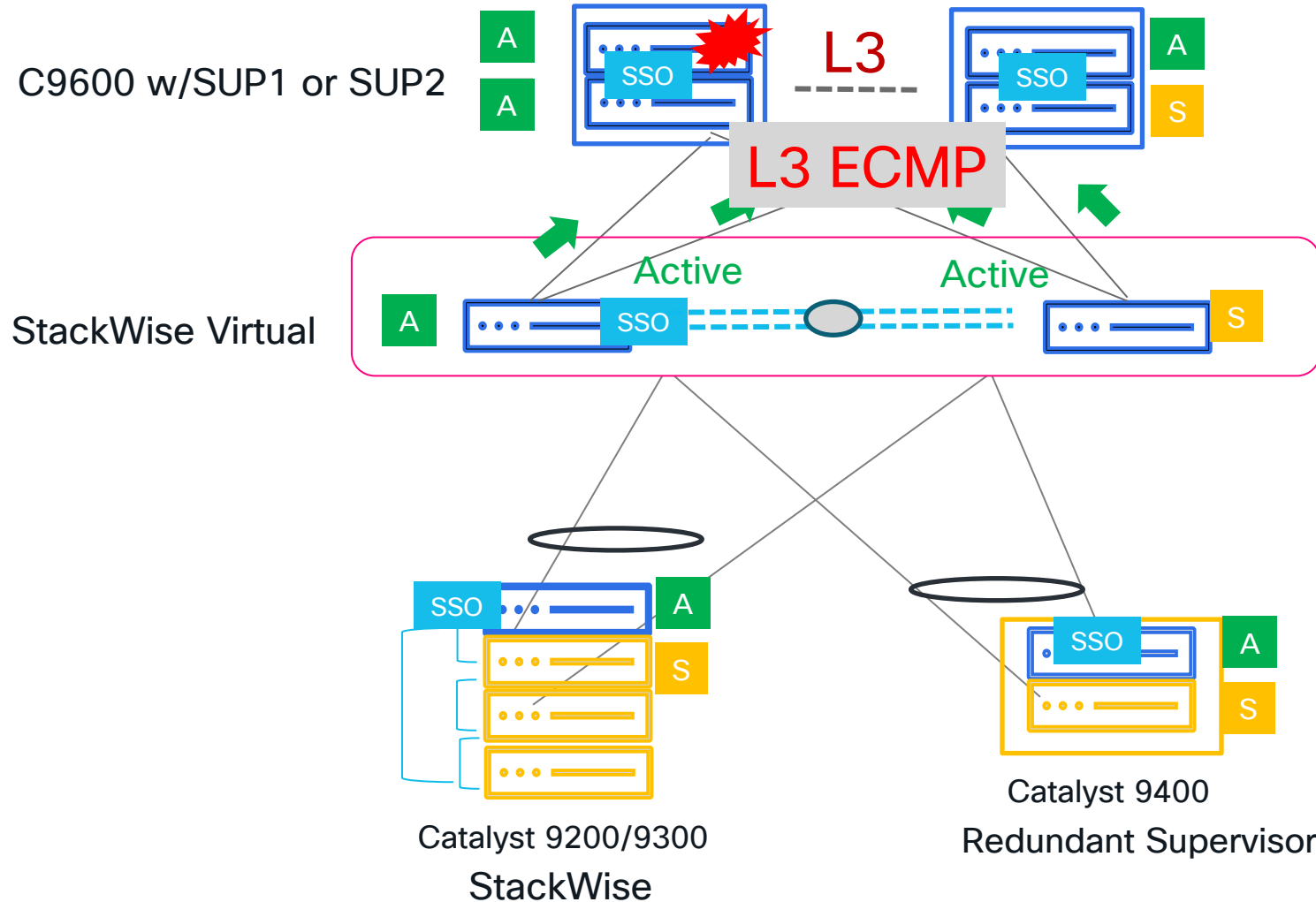
Best Practice:

- Have Redundant Links for SVL & DAD
- Dual-Homed Connections

<200 msec Only
+ 6-8 min for
ICS to become
Standby

Enterprise Campus Network

L3 with Dual Sup for Core



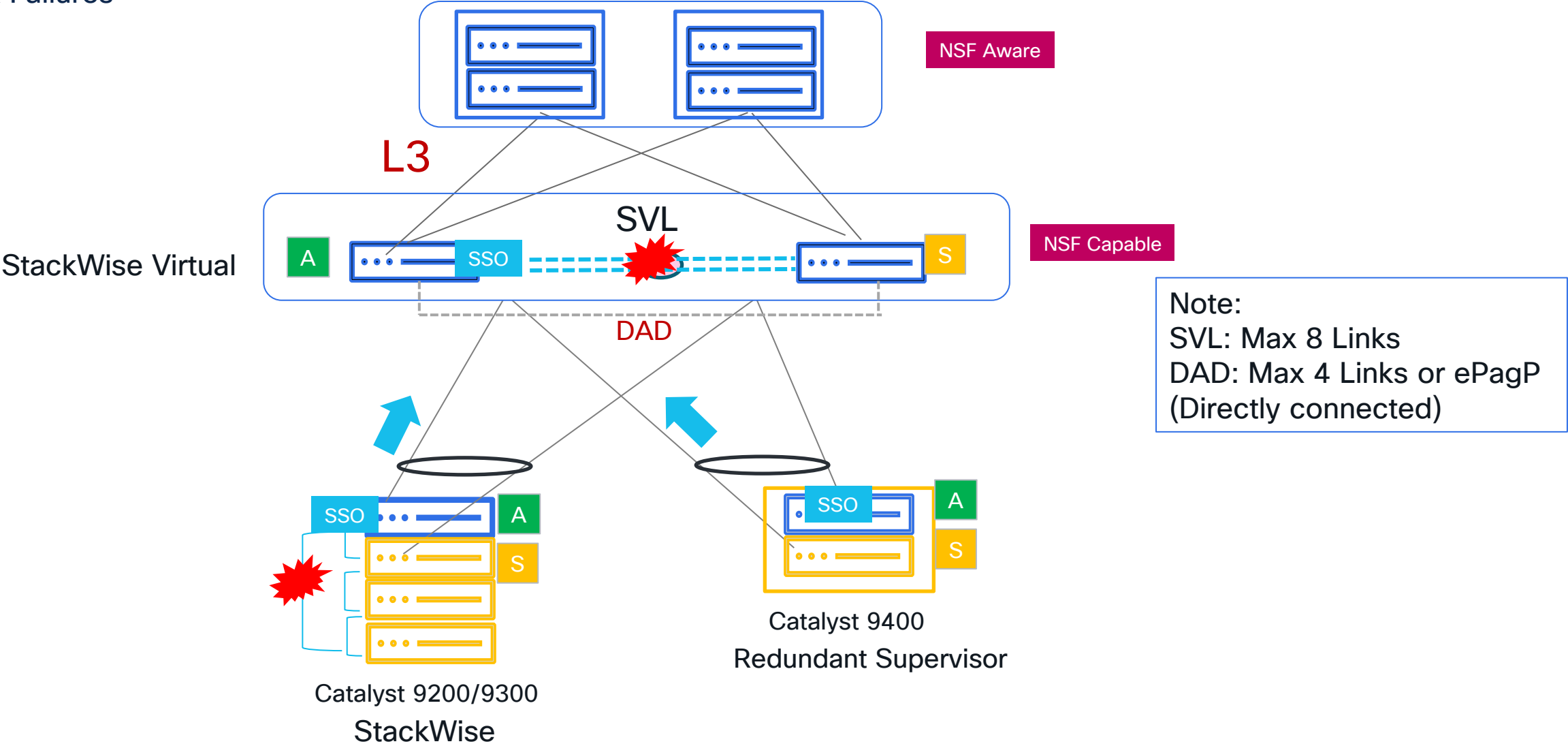
Standalone Deployment with L3 ECMP

- Leverage Dual Supervisors
- Traffic impact < 200msec

<200 msec
Only

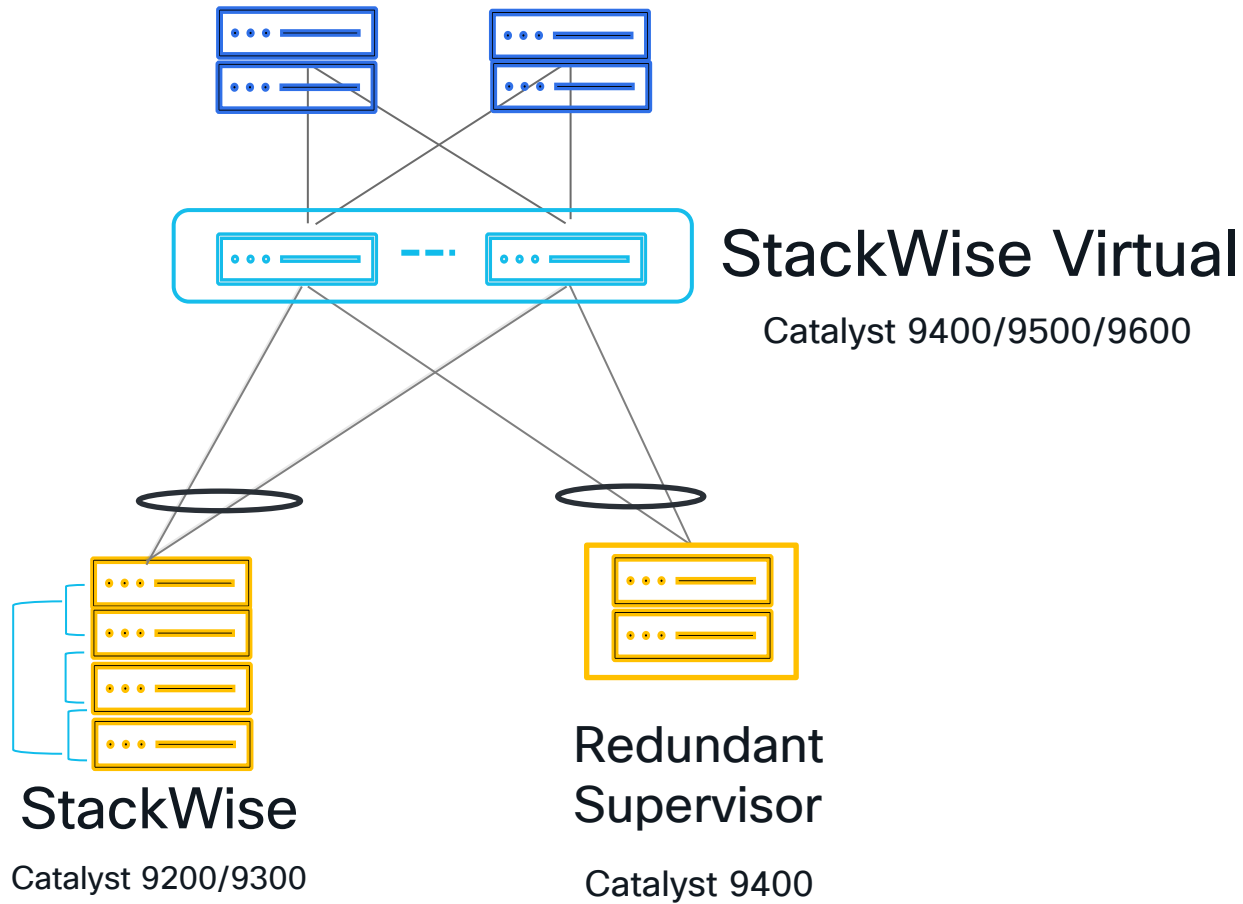
Enterprise Campus Network

Link Failures

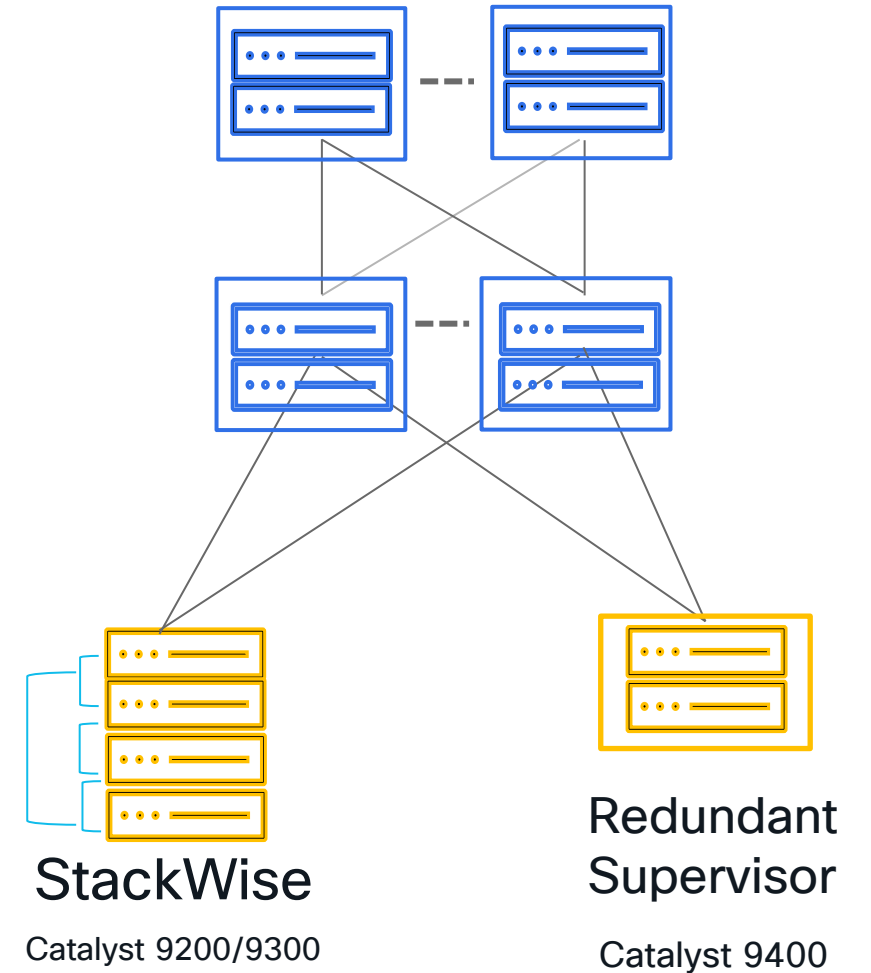


Enterprise Campus Design Options

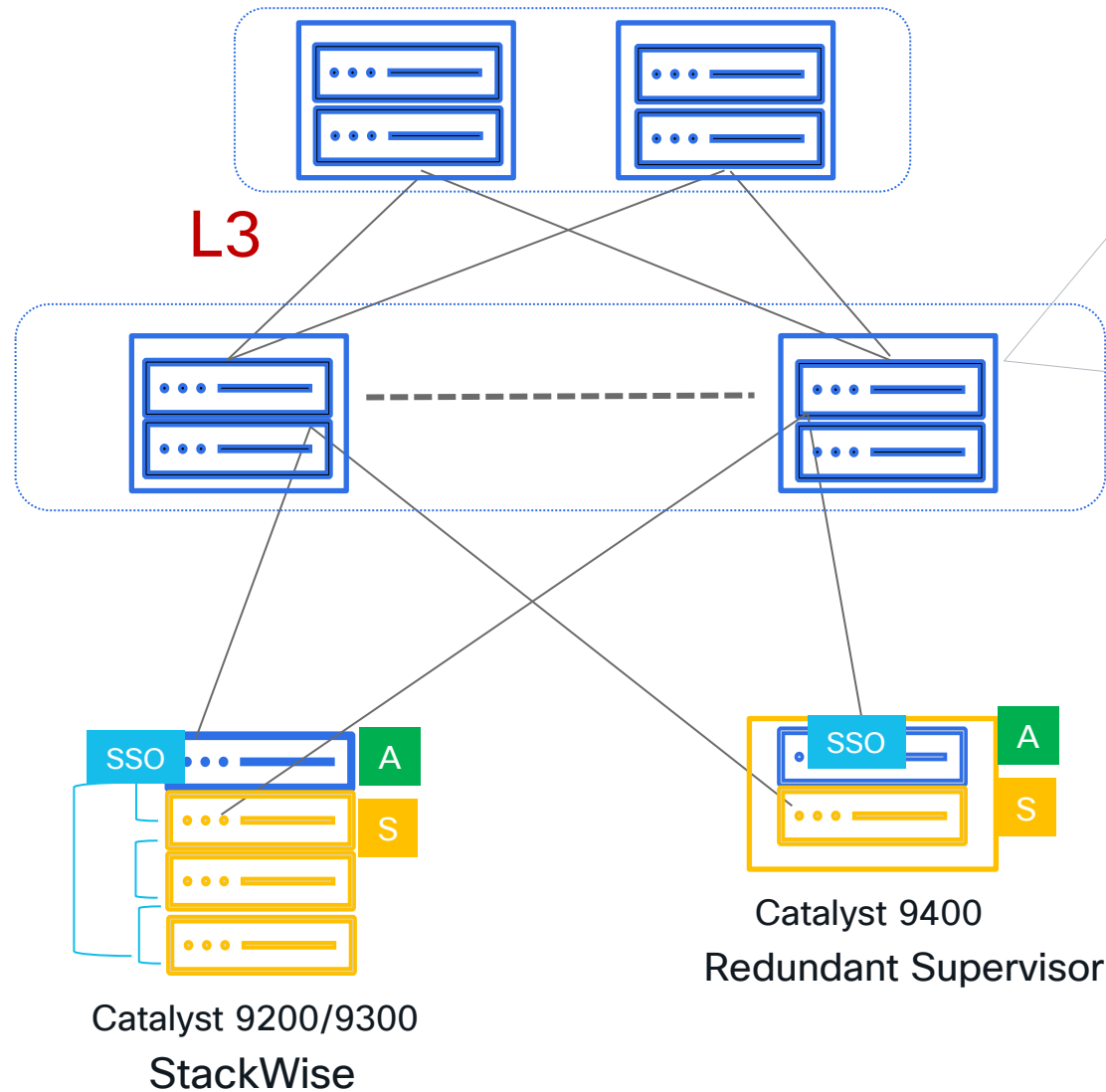
L2 + L3 Design



Routed Access Design – L3

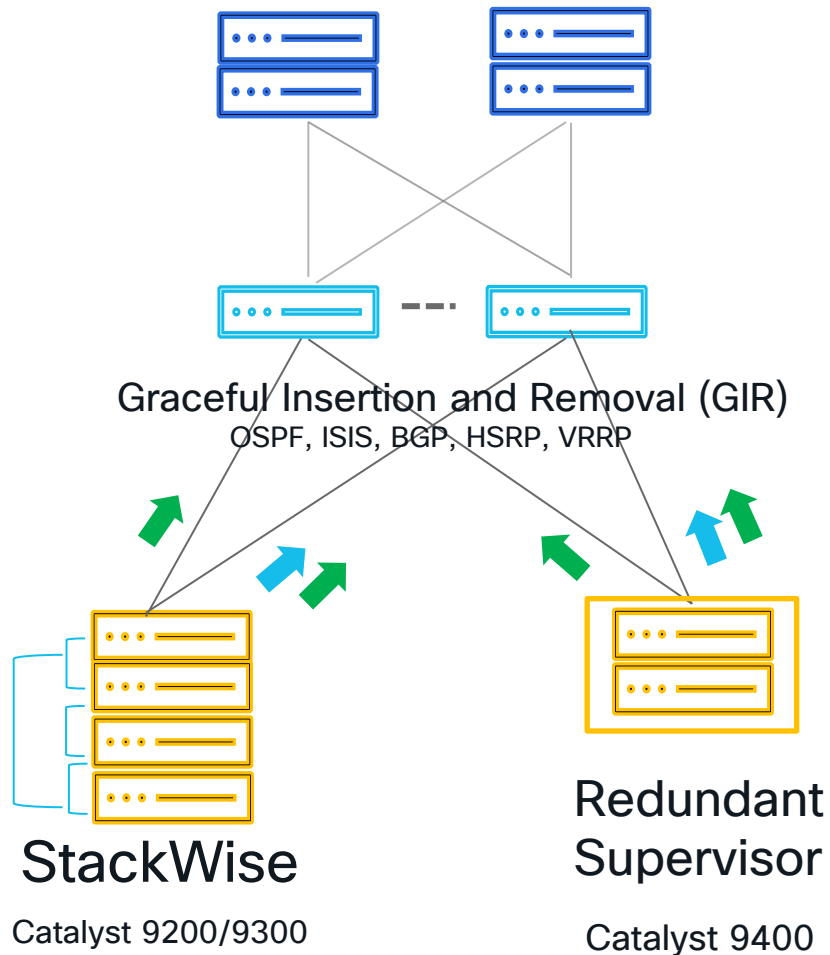


Network Resiliency with GIR



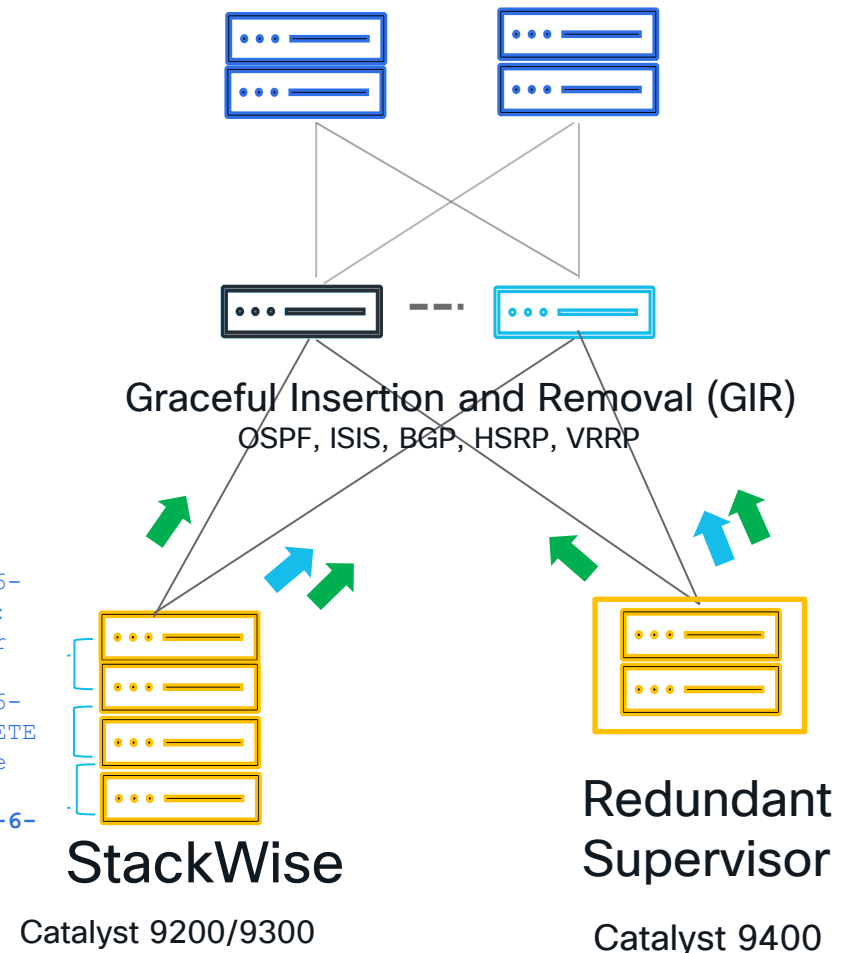
Enterprise Campus Design Options

Routed Access Design with GIR



```
9300#start maintenance
Template default will be
applied.
Do you want to
continue?[confirm]
*Mar 25 17:43:20.162: %MMODE-6-
MMODE_CLIENT_TRANSITION_START:
Maintenance Isolate start for
router isis 1
*Mar 25 17:43:50.213: %MMODE-6-
MMODE_CLIENT_TRANSITION_COMPLETE
: Maintenance Isolate complete
for router isis 1
**Mar 25 17:44:20.214: %MMODE-6-
MMODE_ISOLATED: System is in
Maintenance
```

Routed Access Design with GIR



Operational Failures via Power Supply

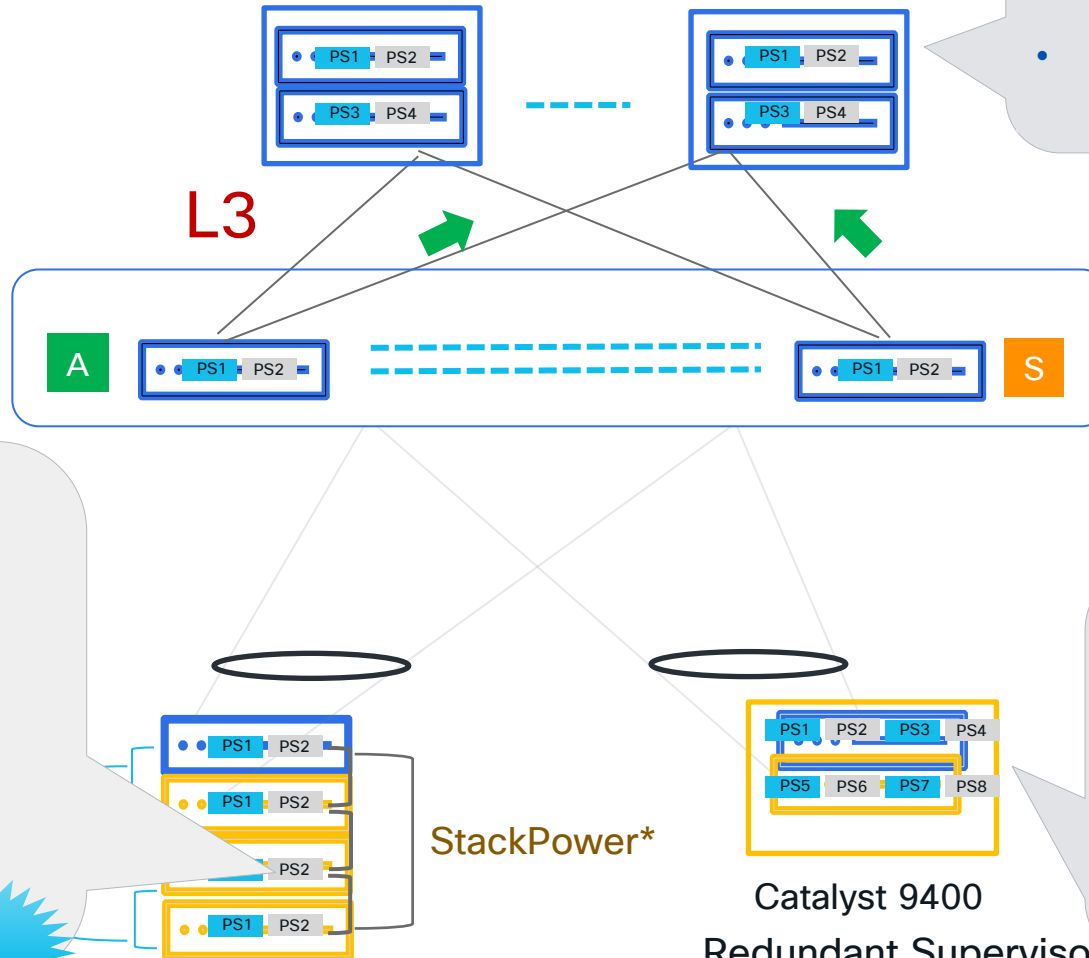
Enterprise Campus Network

Power Supply Failures



L3

C9500



Power Redundancy with StackPower

- Combined mode supported by default
- Redundant mode configurable with N+1
- Helps in reducing the carbon footprint and achieve better sustainability
- Intelligent PS activation and deactivation

New

Catalyst 9200/9300

*Supported on 9300

Power Redundancy

- Combined mode supported by default
- Redundant mode configurable with N+1

Power Redundancy

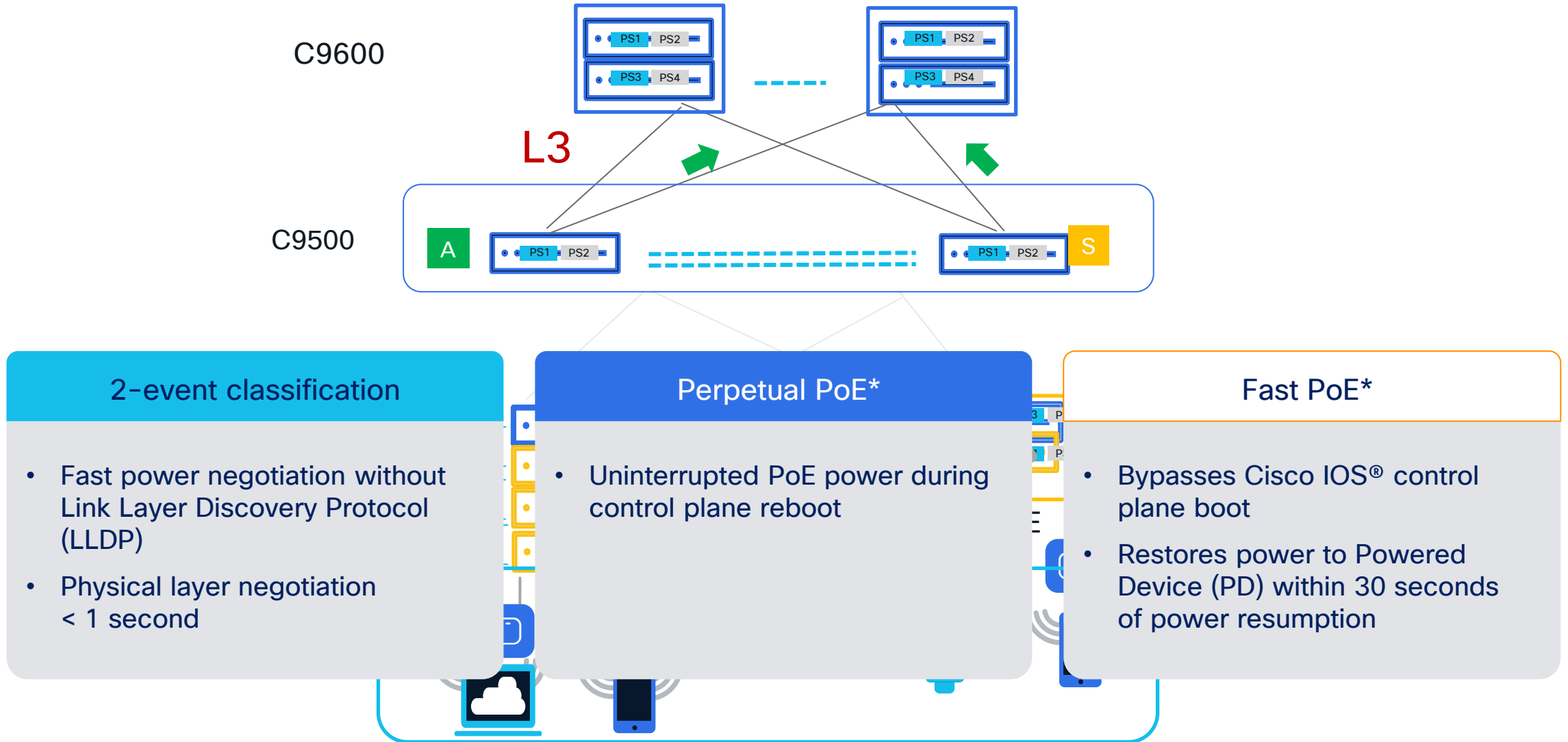
- Combined mode supported by default
- Redundant mode configurable with 1+1

Power Redundancy

- Combined mode supported by default
- Redundant mode configurable with N+1 & N+N

Enterprise Campus Network

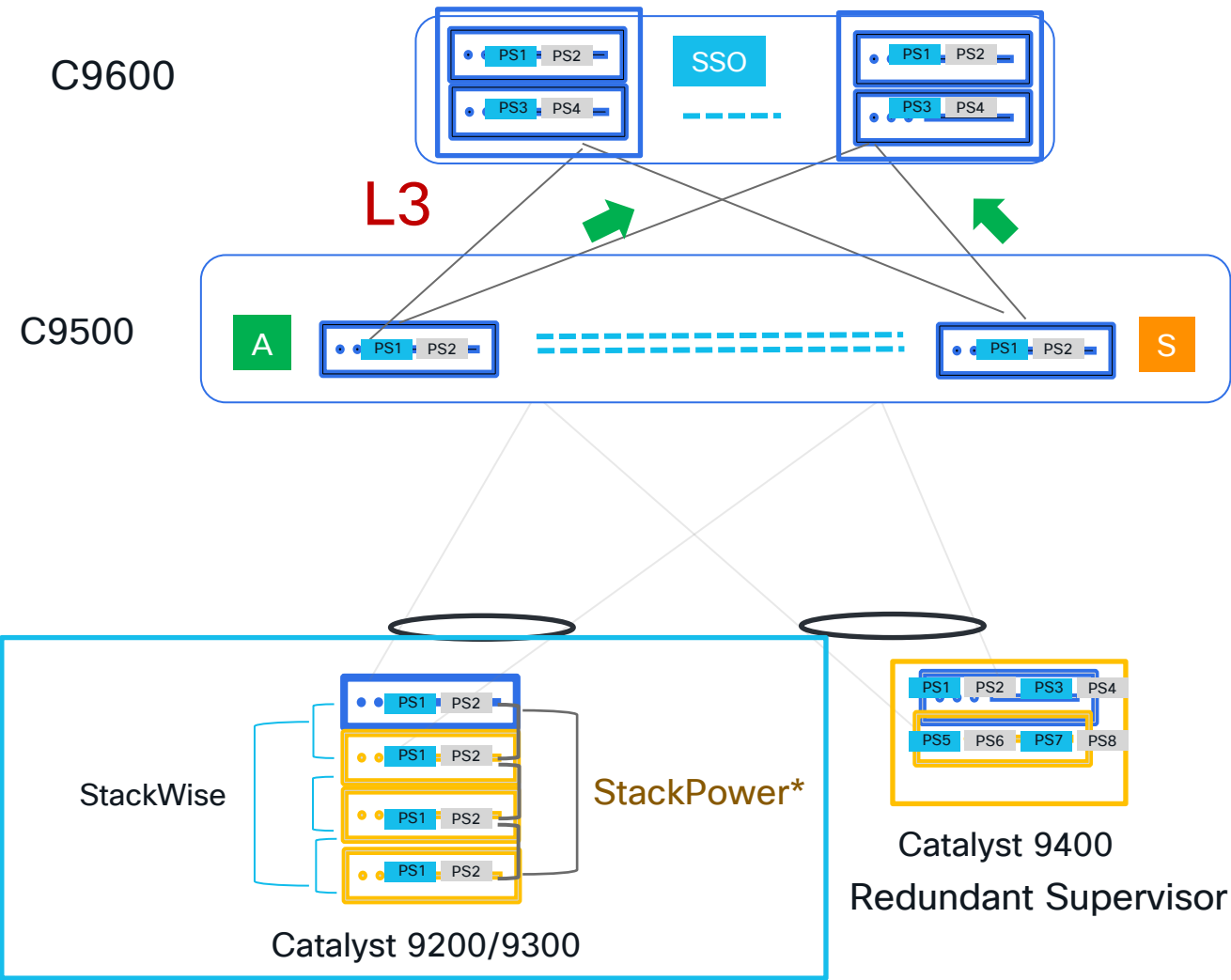
Power Over Ethernet High Availability



Operational Failures via Software Upgrade

Enterprise Campus Network

Software Upgrades on Catalyst 9300



*Supported on 9300

Operational Resiliency with Extended Fast Software Upgrade

C9300- 17.3.2

C9300X-
17.7.1

Catalyst® 9300/9300X standalone



9300# install add file image activate xfsu
commit

Catalyst 9300/9300X stack



9300# install add file image activate xfsu
commit

Control plane

Data plane

< 5 seconds
From 17.15.2*

< 30
seconds of
traffic
impact

Active control plane

Data plane

< 30 seconds
of traffic impact
for all ports in
the stack

Features/Protocols: L2, L3 (OSPF, ISIS, BGP), IGMP, LACP, etc.

Statistics Tools

Statistics

Data

Formula / Alerts

Design

Clear All Statistics

Customize Traffic View

Drill Down

Ingress/Egress Statistics

Stat View Profiles

Add to New

Add to Existing

Take Snapshot

More Actions

Overview

Statistics

Host Directory

Quick Connection

Disconnect

Scroll Back as Window

Clear Scroll Buffer

Show Data Stream Viewer

C9300

About these Buttons

Unix Commands

Run Sample Script

Call Host from Host Directory

Select Views...

L2-L3 Test Summary Statistics

Traffic Item Statistics

User Defined Statistics

Back

Traffic Item

Source/Dest Value Pair

	Source/Dest Value Pair	Tx Frames	Rx Frames	Frames Delta	Loss %	Packet Loss Duration (ms)	Tx F
1	192.168.100.9-2.0.0.9	797	797	0	0.000	0.000	
2	192.168.100.8-2.0.0.8	797	797	0	0.000	0.000	
3	192.168.100.7-2.0.0.7	797	797	0	0.000	0.000	
4	192.168.100.6-2.0.0.6	797	797	0	0.000	0.000	
5	192.168.100.5-2.0.0.5	797	797	0	0.000	0.000	
6	192.168.100.4-2.0.0.4	797	797	0	0.000	0.000	
7	192.168.100.3-2.0.0.3	797	797	0	0.000	0.000	
8	192.168.100.2-2.0.0.2	797	797	0	0.000	0.000	
9	192.168.100.21-2.0.0.21	796	796	0	0.000	0.000	
10	192.168.100.20-2.0.0.20	796	796	0	0.000	0.000	
11	192.168.100.19-2.0.0.19	796	796	0	0.000	0.000	
12	192.168.100.18-2.0.0.18	796	796	0	0.000	0.000	
13	192.168.100.17-2.0.0.17	796	796	0	0.000	0.000	
14	192.168.100.16-2.0.0.16	796	796	0	0.000	0.000	
15	192.168.100.15-2.0.0.15	797	797	0	0.000	0.000	
16	192.168.100.14-2.0.0.14	797	797	0	0.000	0.000	
17	192.168.100.13-2.0.0.13	797	797	0	0.000	0.000	
18	192.168.100.12-2.0.0.12	797	797	0	0.000	0.000	
19	192.168.100.11-2.0.0.11	797	797	0	0.000	0.000	
20	192.168.100.10-2.0.0.10	797	797	0	0.000	0.000	

1/1 (total rows: 20)

All

Loss

Throughput

Latency

Telnet

Xterm

Zmodem

ZOC2409_C93000119.log

00:00:22

89x34

xFSU Implementation Scenarios & Support

FYI

L2 Access Node

Layer 2 Protocol	Stack	Standalone
STP	✓	✓
STP with RSTP and MSTP	✓	✓
Per VLAN Spanning Tree (PVST)	✓	✓
Static L2 Port Channels (Mode on)	✓	✓
UDLD	✓	✓
Link Aggregation Control Protocol (LACP)	✓	✓

L3 Routed Access Node

Layer 3 Protocol	Stack	Standalone
Open Shortest Path First - OSPFv2 or OSPFv3	✓	✓
IS-IS	✓	✓
BGP (IPv4 and IPv6 address families)	✓	✓



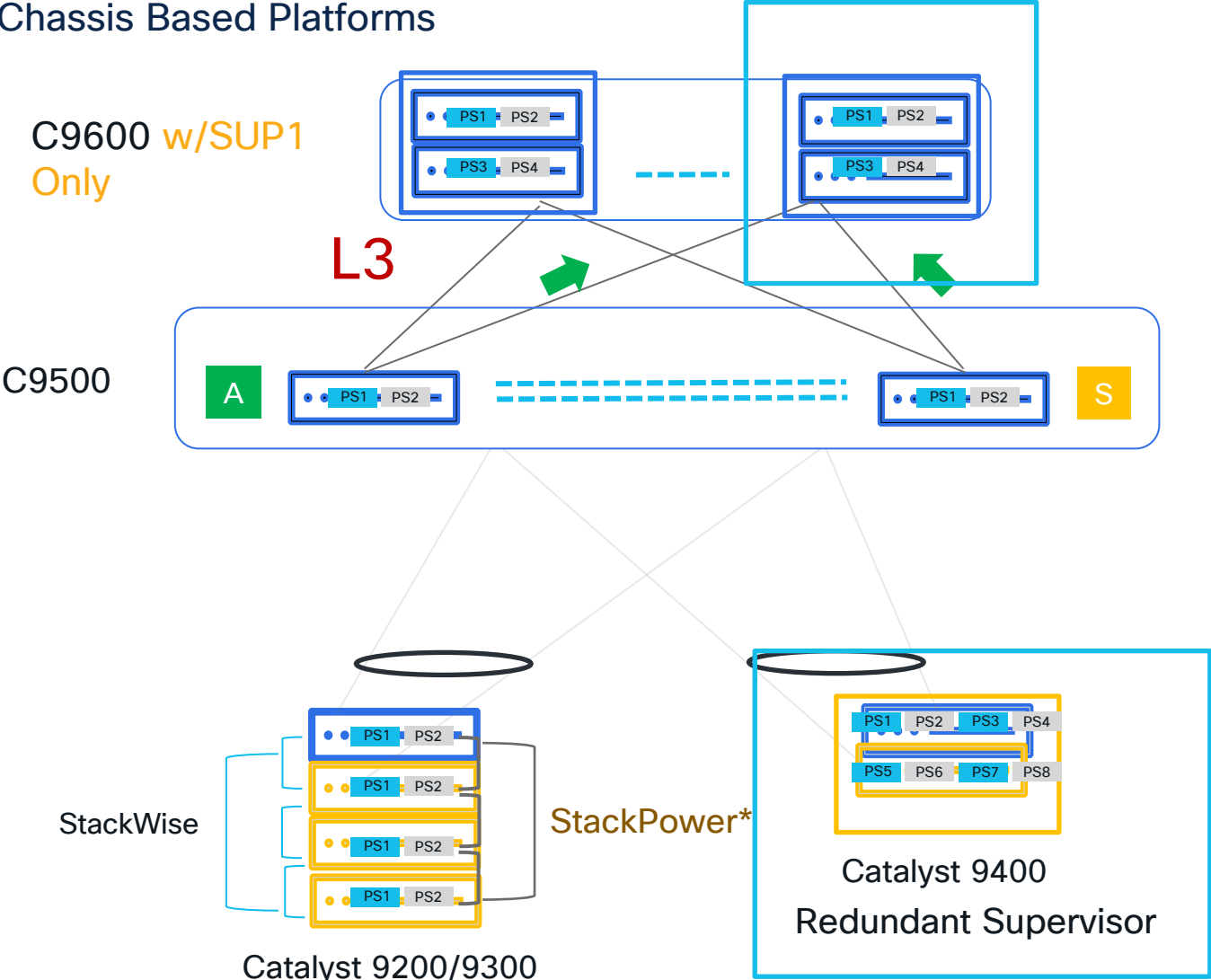
L2 ACCESS
>60% campus deployments across different verticals still have traditional L2 topologies



STACKED ACCESS
>50% Cisco's campus deployments are stacked deployments

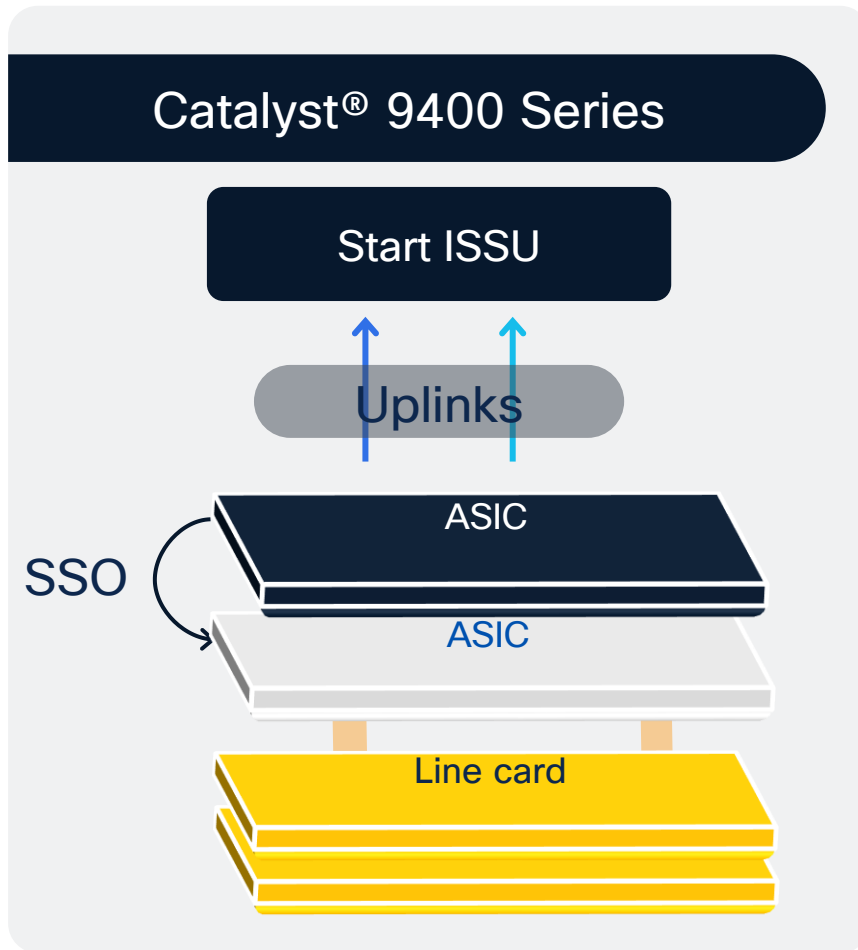
Enterprise Campus Network

Software Upgrades on Chassis Based Platforms



ISSU process

Dual supervisors

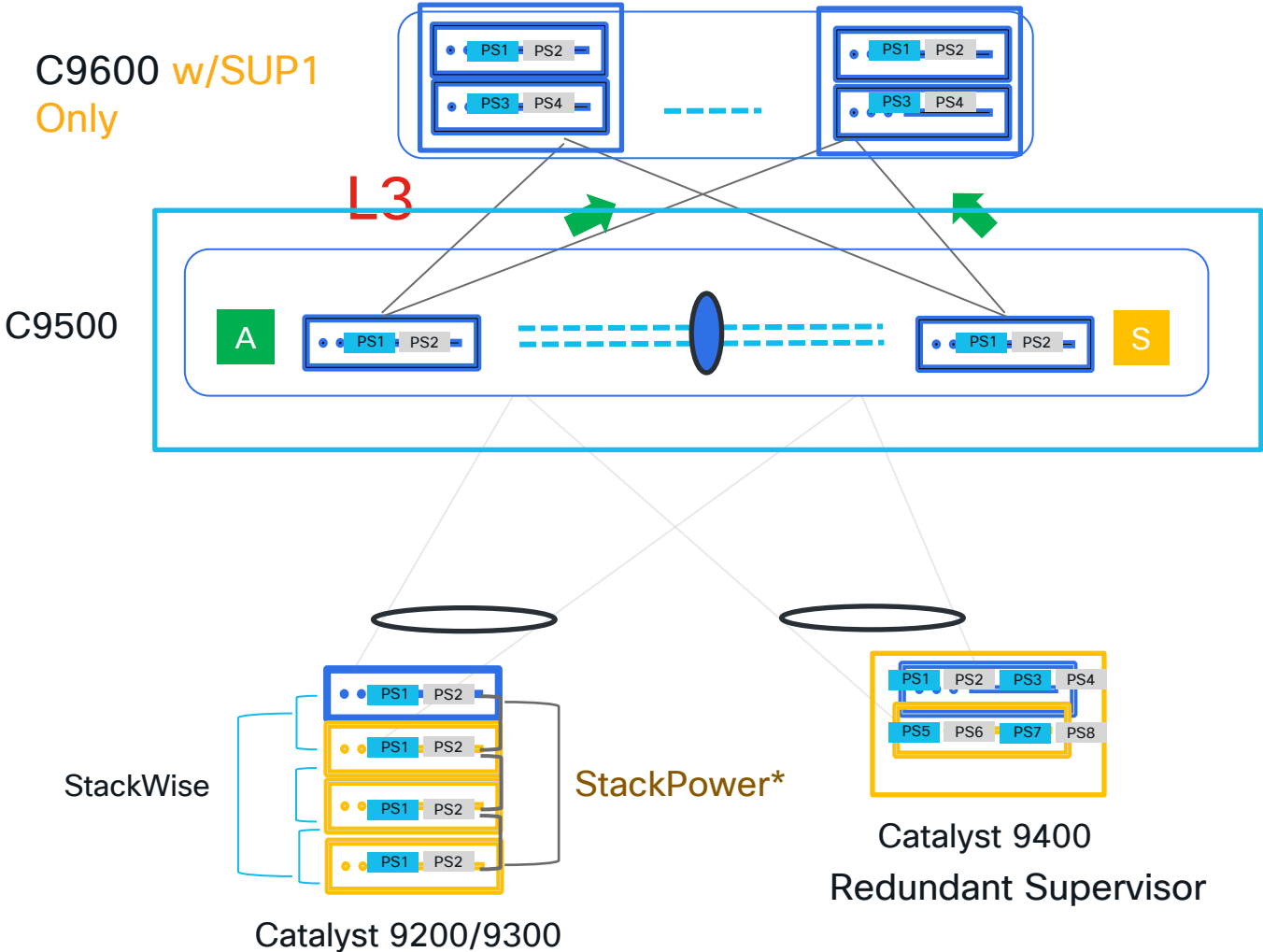


Active supervisor

Standby supervisor

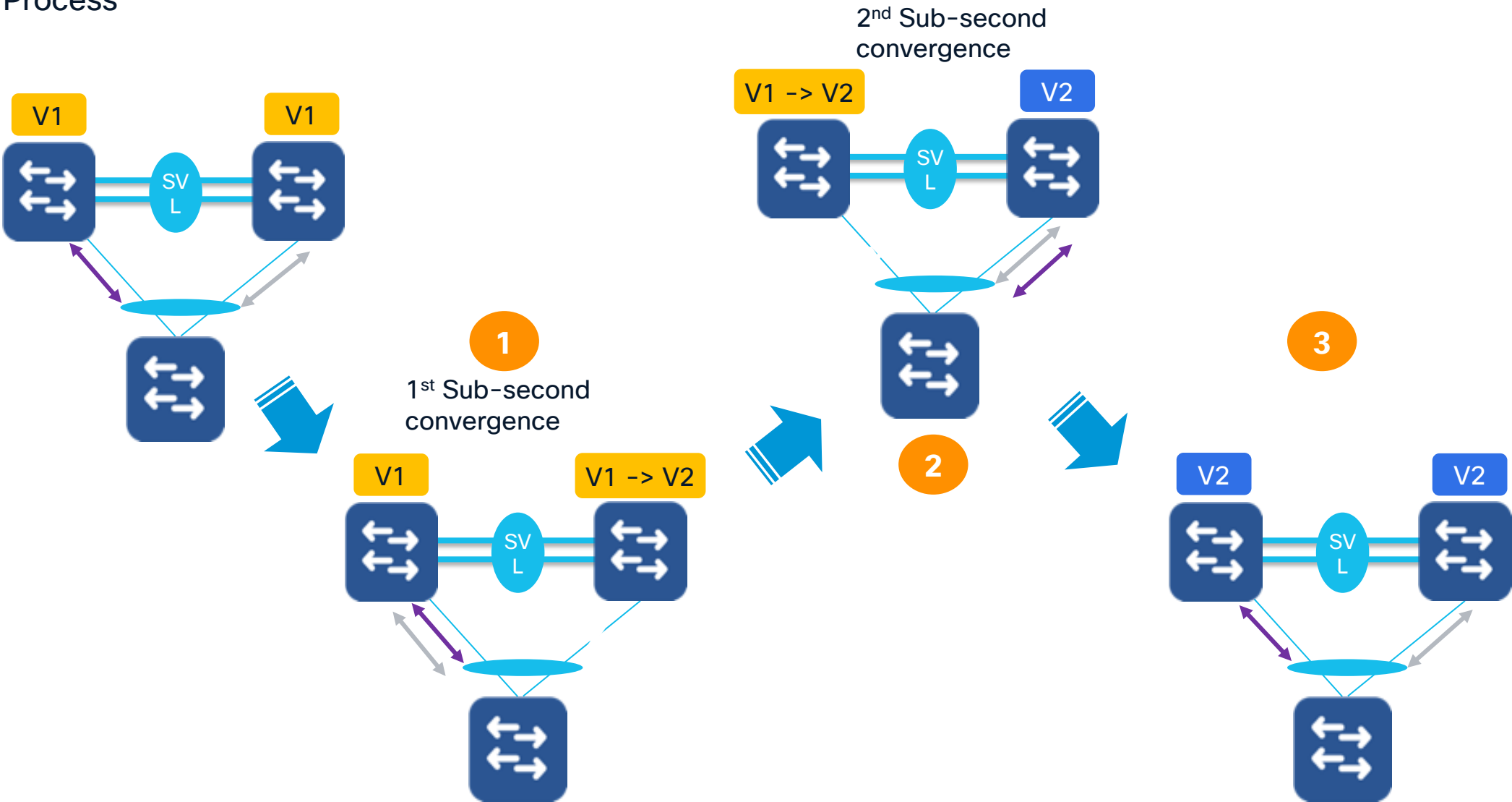
- Uplinks on both Active and Standby supervisors are forwarding traffic
- Convergence takes less than 200 ms during the switchover

Enterprise Campus Network

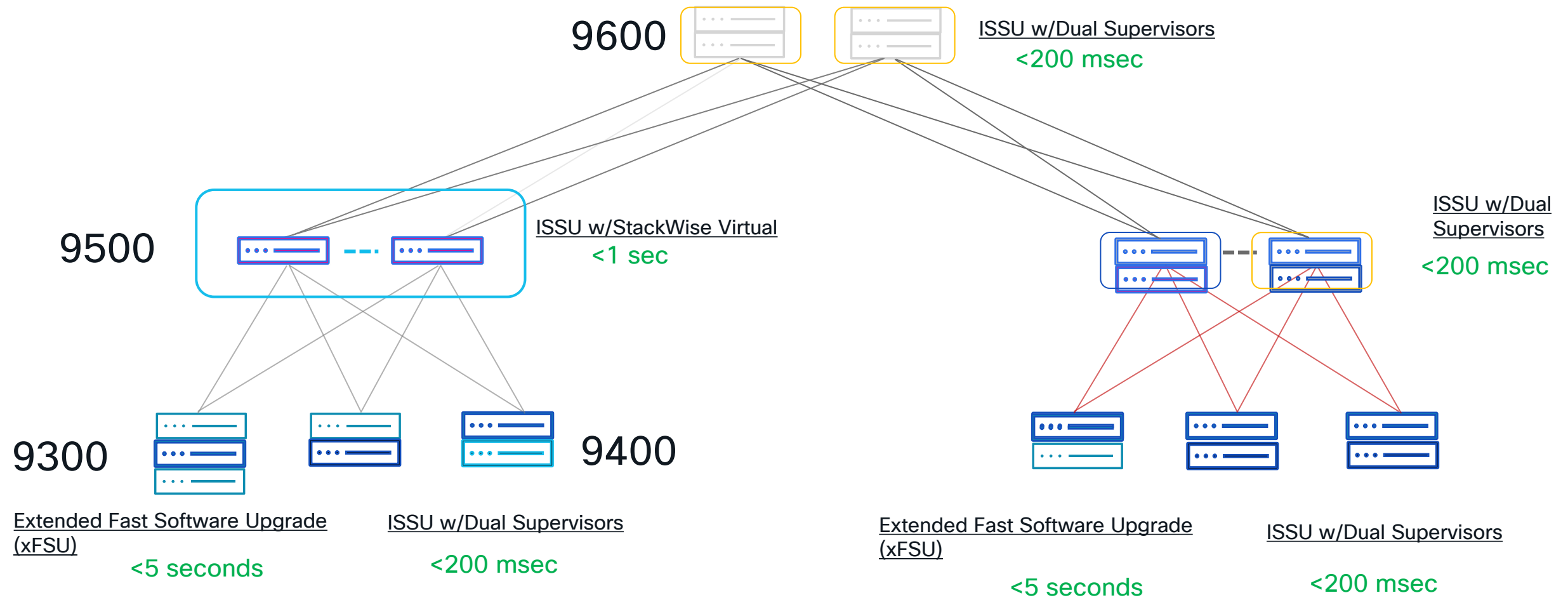


Stackwise Virtual ISSU

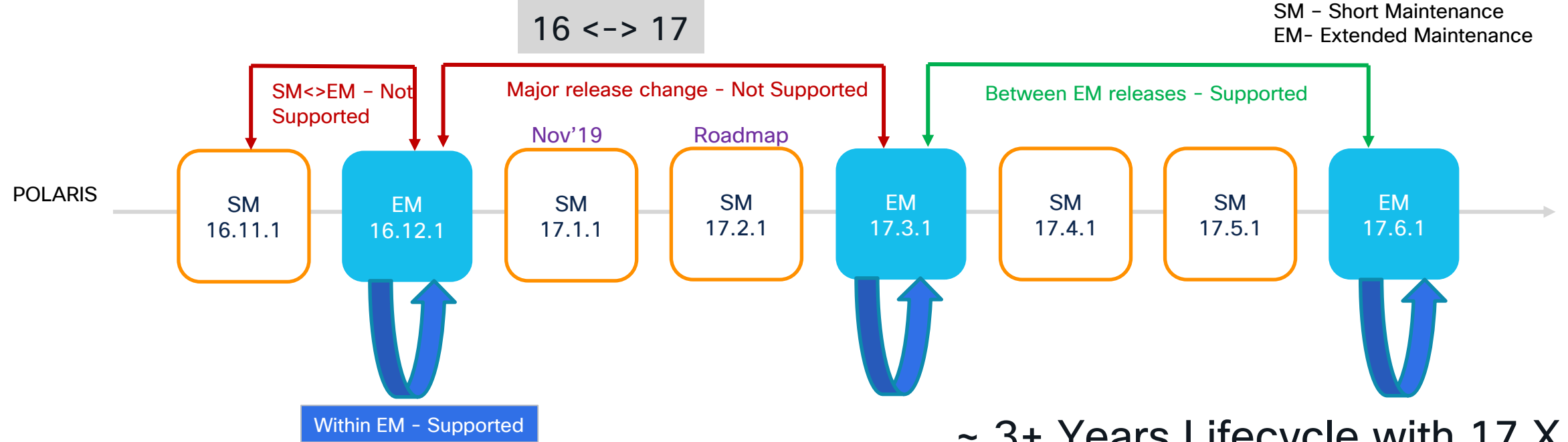
ISSU Process



Software Upgrades with Catalyst 9000 Platform



ISSU/xFSU Release Guidelines



~ 3+ Years Lifecycle with 17.X EM

Supported

- Within EM Release - Any to Any within the EM Release (16.12.X <-> 16.12.X)
- Between EM Releases but within major releases [within + 2 EM releases]

Not Supported

- SM to EM or EM to SM.(16.11.X <-> 16.12.x)
- Within SM Release - (16.11.1 <-> 16.11.2)
- Beyond the + 2 EM Releases.
- When there is a major release change.
 - For example 16.x.x to 17.x.x

* Downgrade is not supported via ISSU method



Software Maintenance Upgrade

SMU is a package that can be installed on a system to provide a fix or a security resolution to a released image.

- **Hot Patching** - does not require explicit reload after installation to get activated. (*not traffic-affecting*)
- **Cold Patching** - requires a system reload after installation to get activated. (*traffic-affecting*). The 9200 family supports only this.

- **Bundle SMU** - One single SMU file containing and applying multiple SMU fixes on the backend.
- **Independent SMU** - One single SMU file tailored to address a specific bug or vulnerability.

Patching can also be performed using Cisco DNAC

C9300-Access.cisco.com (172.26.192.131) Image Update

Date: Mar 16, 2023 12:15 PM Duration: 4 minutes 20 seconds Status: ● Successfully Activated cat9k_iosxe.17.03.04.SPA.bin cat9k_iosxe.17.03.04.CSCwa53947.SPA.smu.bin

DNAC Version: Guardian 2.3.3
License Level : DNA Advantage

Operations Checks

> ● SMU Distribution 1 minute 51 seconds

✓ ● SMU Activation 2 minutes 27 seconds

SMU Activation of image: cat9k_iosxe.17.03.04.CSCwa53947.SPA.smu.bin on device: 172.26.192.131 completed successfully

> ● Pre Activation Script Execution 1 second

> ● Activation 2 minutes 26 seconds



Reduces time and scope of testing



Self-sufficient and reliant bug fix solution for **PSIRT, CFD & IFD**

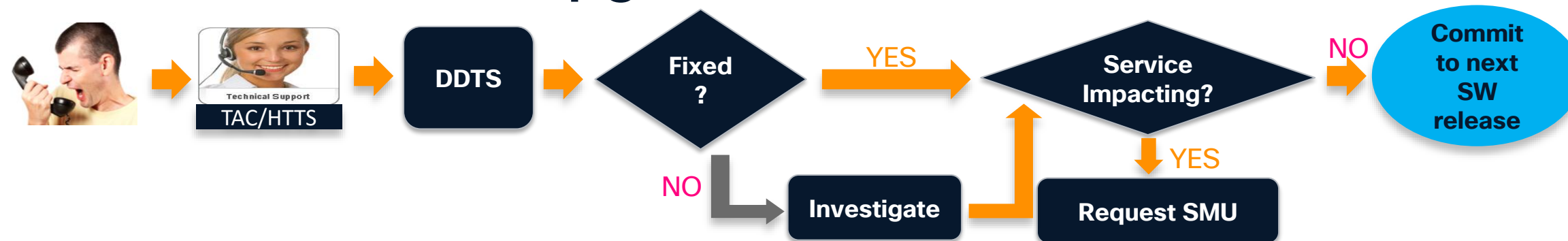


Hot Patching



EMR Releases with **371** SMU files available

Software Maintenance Upgrade Customer Use Case



CDETS	Bugs & Vulnerabilities	SMU Fix File
CSCwb16232	SNMP Engine High CPU when NVE interface is Configured	cat9k_iosxe.17.06.03.CSCwb16232.SPA.smu.bin
CSCwd92655	Cat9k switch hangs during bootup after power-cycle	cat9k_iosxe.17.06.03.CSCwd92655.SPA.smu.bin
CSCwa85257	VXLAN Encapsulated Unicast DHCP ACK packet, after arriving at Fabric Edge is silently dropped	cat9k_iosxe.17.06.03.CSCwa85257.SPA.smu.bin
CSCwc85207	Umbrella SMU for critical defects on 17.6.3	cat9k_iosxe.17.06.03.CSCwc85207.SPA.smu.bin

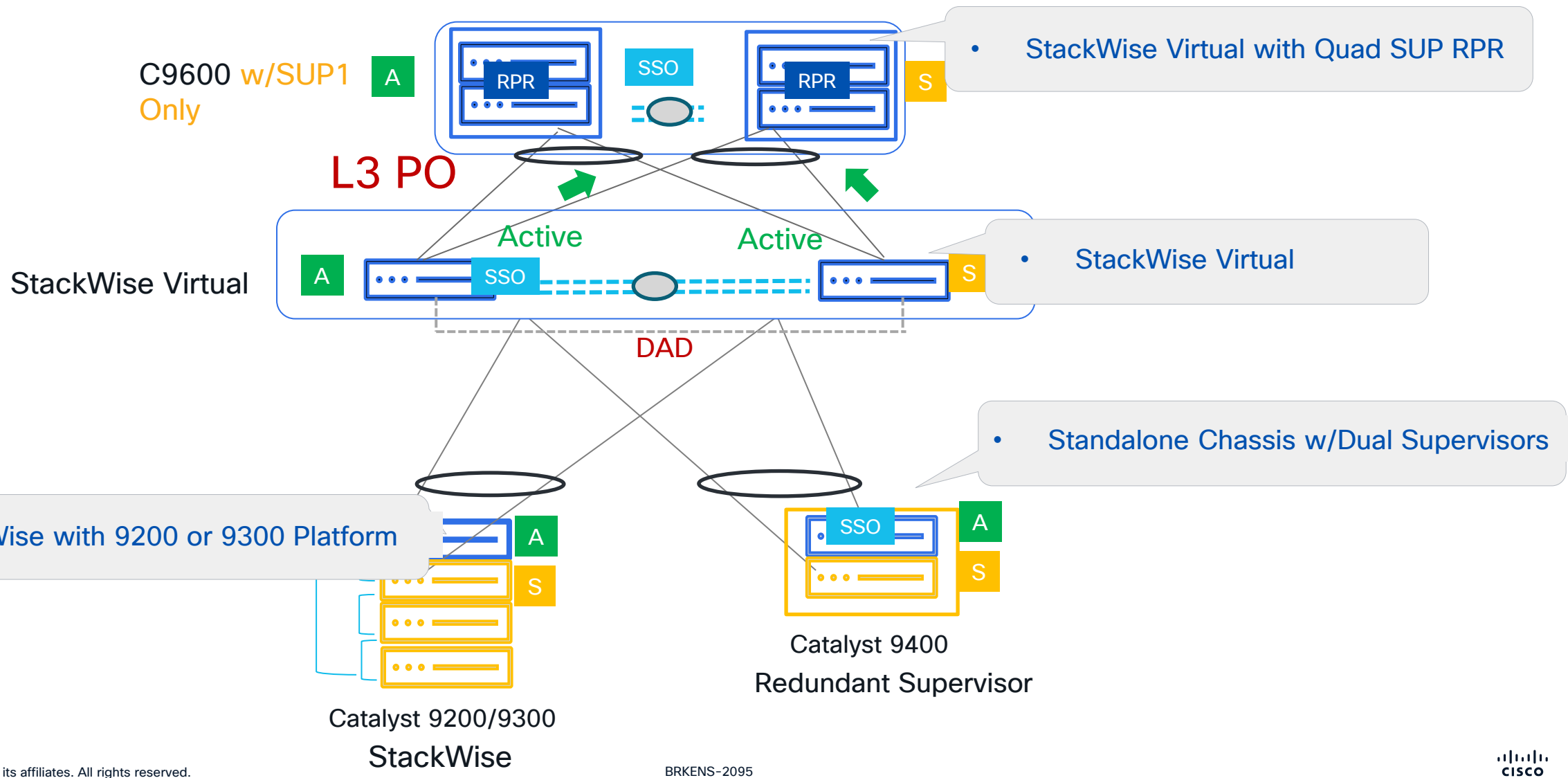
Hot Patched!
This Bundle SMU resolved two issues

- CSCwb25610 - IPv6: Switch may reload due to a memory allocation error by SISF - Occurs on a scaled environment
- CSCwb70411 - C9300 - Critical software exception crash - iosd core - No specific trigger

Customer Profiles

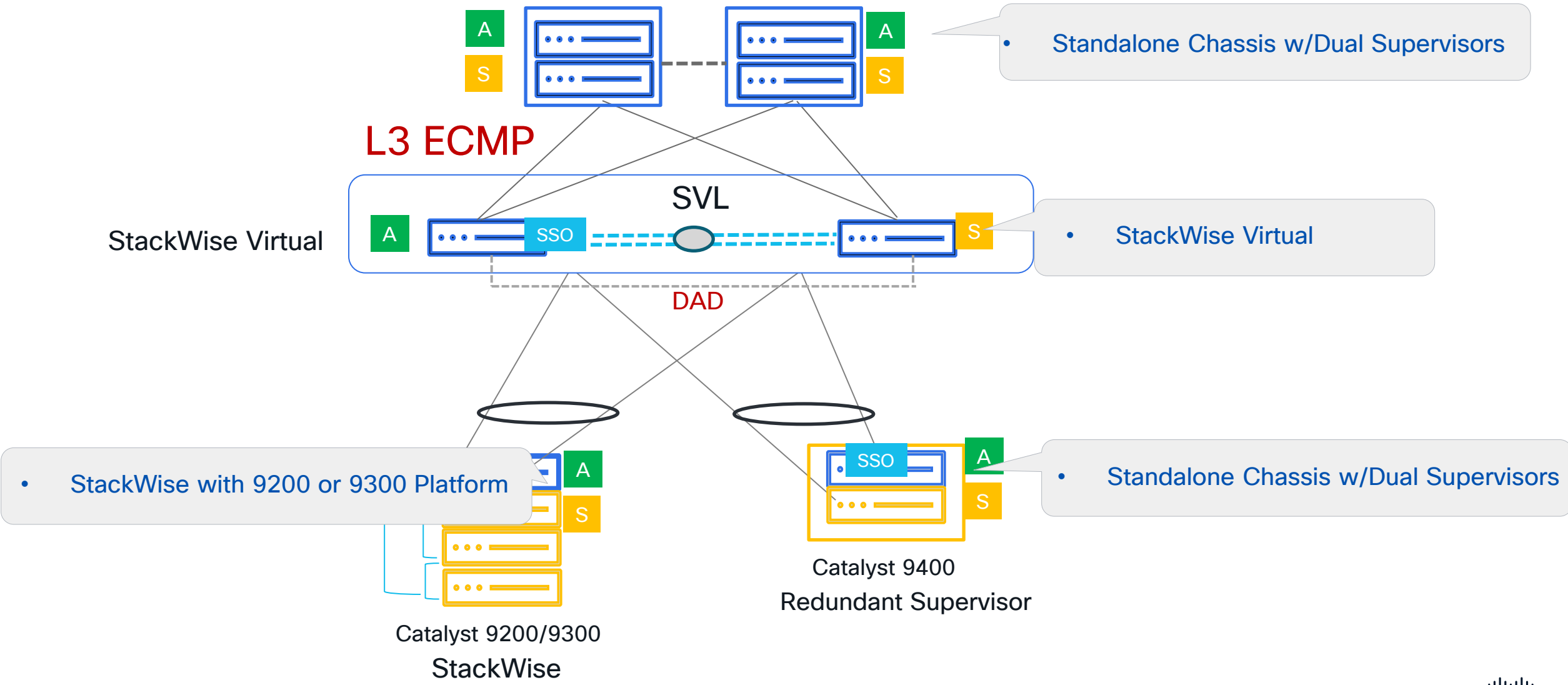
L2 + L3 Design with StackWise Virtual

Customer Profile 1



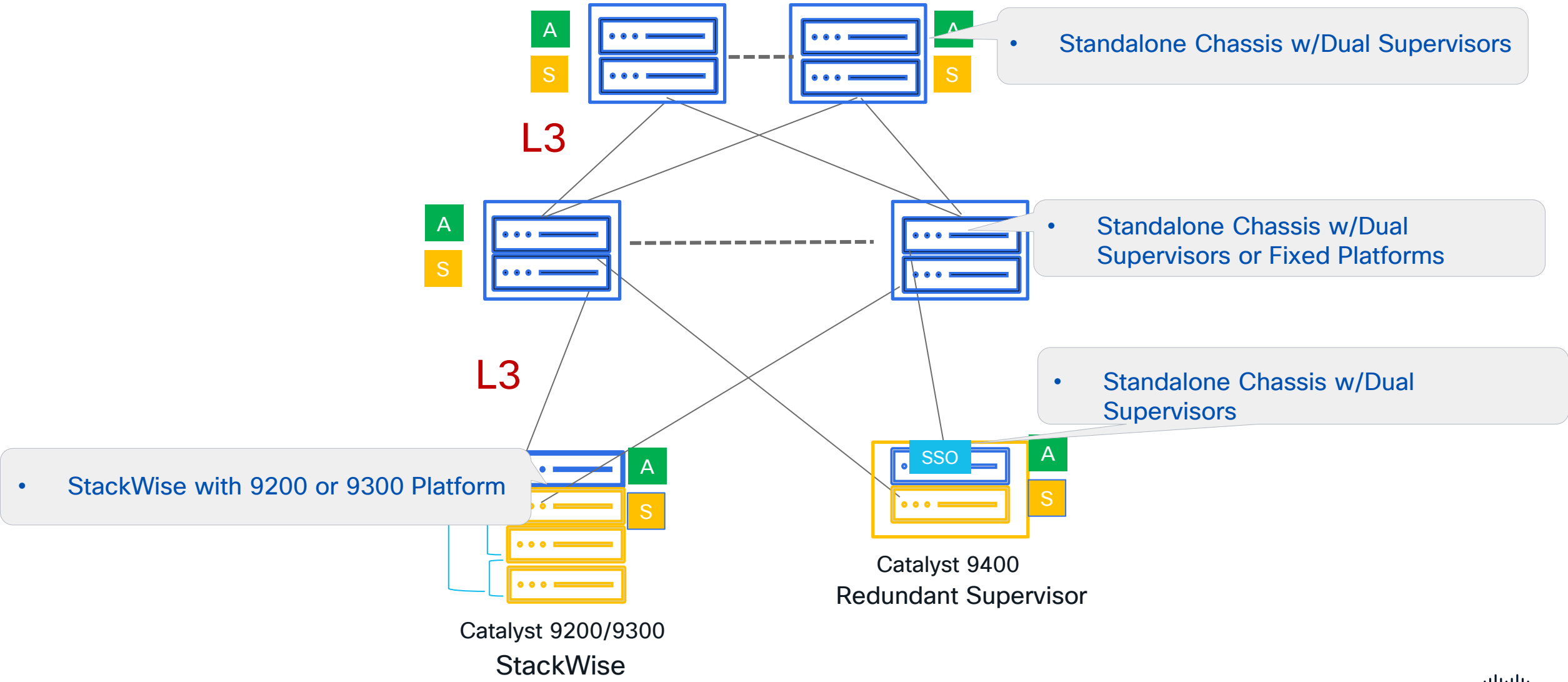
L2 + L3 Design with StackWise Virtual & ECMP

Customer Profile 2



L3 Routed Access Design

Customer Profile 3



Catalyst 9000: Redundancy at every layer



Sub-second Traffic Impact across all layers of Redundancy

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn 800 points per survey completed and compete on the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

CISCO Live !

