Real-World SD-Access Transformations!

How Rolls-Royce, KELAG & BMW Are Building Secure, Modern Campus Networks

Phillip Krebs, Branko Cerkuc, Gregor Geldhauser, Nico Armbruster, David Mayer, Bernhard Haring

BRKENS-1803

Rolls Royce Group Manufacturing

Phillip Krebs
Network Architect (RollsRoyce)

Branko Cerkuc
Product Owner Network (RollsRoyce)

Gregor Geldhauser
Senior Systems Engineer (NTS)

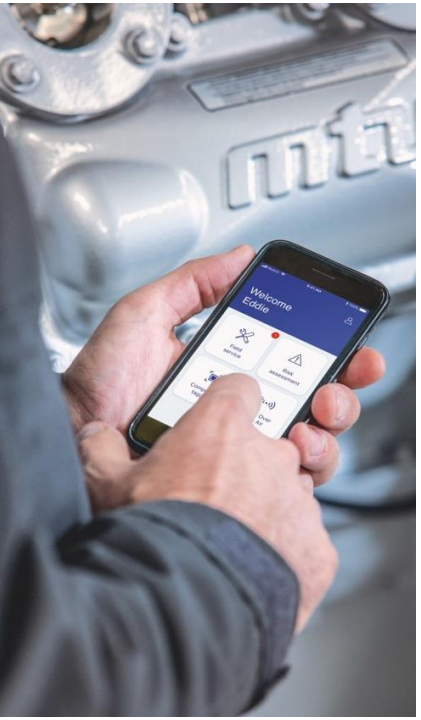
Nico Armbruster
Systems Engineer (NTS)

ROLLS-ROYCE POWER SYSTEMS

A world of solutions

A Rolls-Royce solution

Drive and energy



ROLLS-ROYCE GROUP

A world-class technology company, built on three strong and complimentary business units.

Civil aviation

35 types of commercial aircraft powered by us

13,000 engines in service around the world

18,300 total employees

9.04 billion (€ 10.69 billion) underlying revenue

Defence

160 customers in over 100 countries

16,000 engines in service around the world

12,000 total employees

4.5 billion (€ 5.32 billion) underlying revenue

Power Systems

> 40,000 customers in 13 different industries

8,000 engines sold per year

> 10,350 total employees

4.27 billion (€ 5.05 billion) underlying revenue

POWER SYSTEMS AT A GLANCE

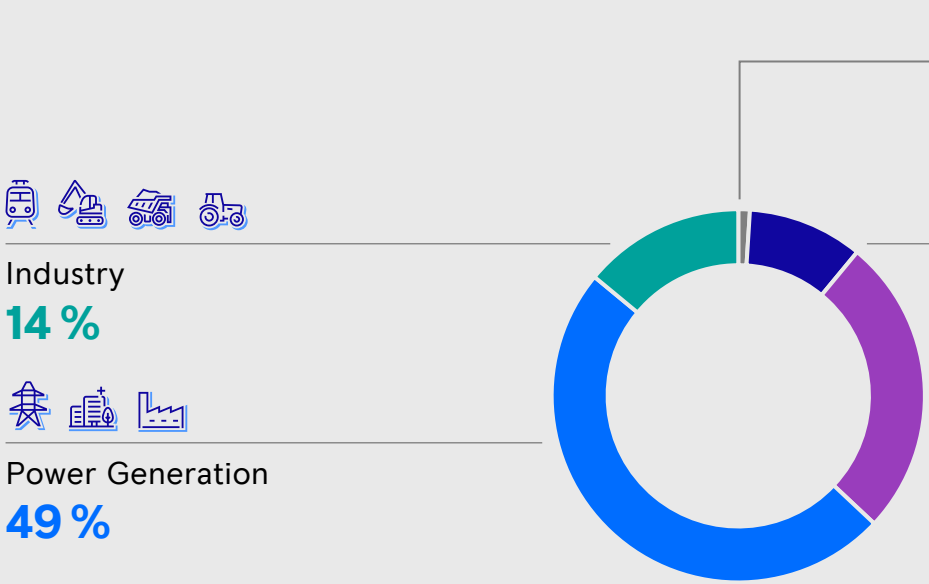
Turnover 2024

5.05 billion €*

(4.27 billion pounds)

Employees

> 10,350



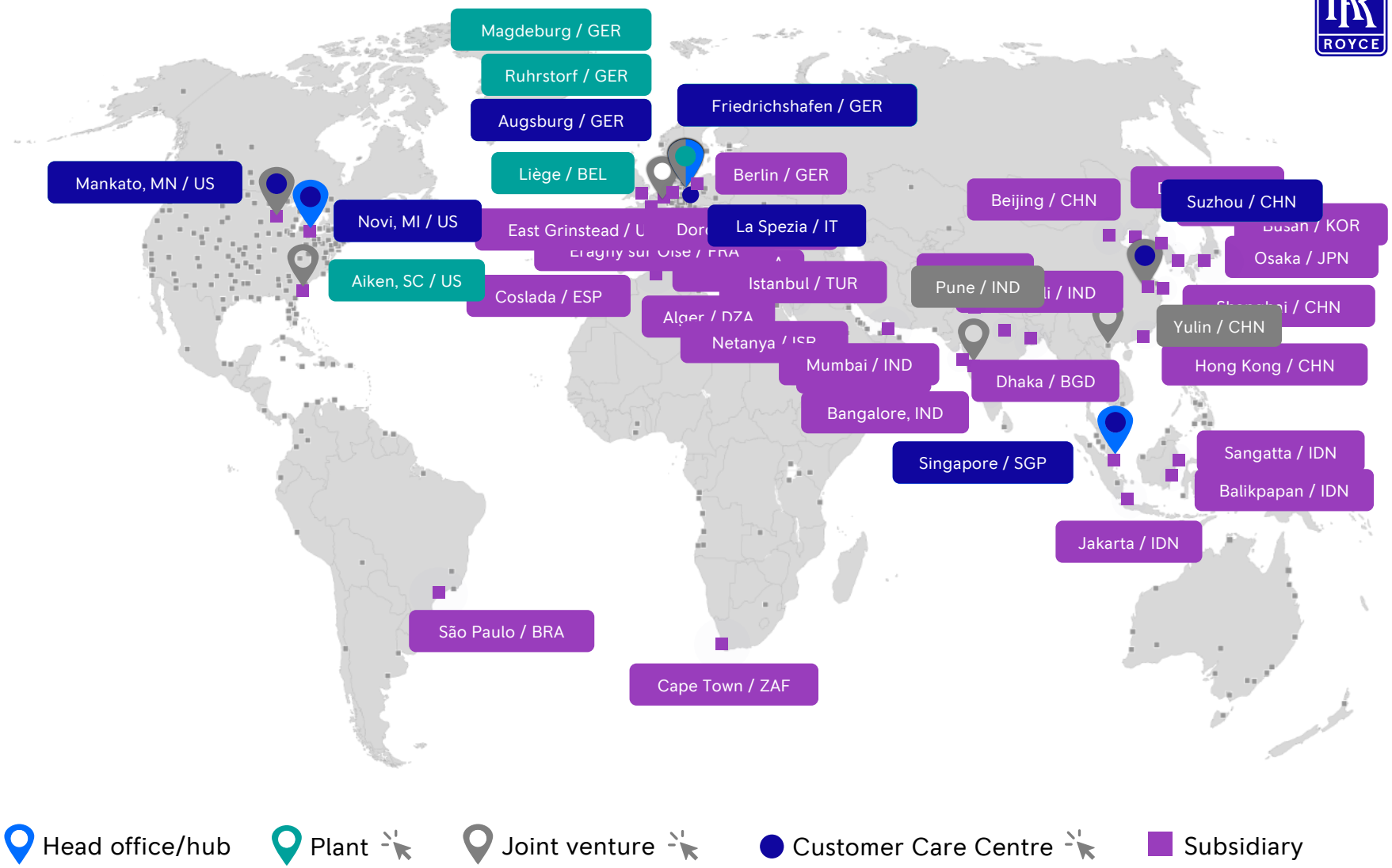
*The figures in British pounds are binding

GLOBAL PRESENCE

More than
420 **Sales and service partner**

Represented in over
175 **Countries**

More than
1,200 **Locations worldwide**



01

INFRASTRUCTURE UPDATE PROJECT

Project Name:
Rolls-Royce Power Systems **I**nterconnect **S**ystem **E**volution (RISE)

PROJECT TEAM SETUP

ROLLS-ROYCE POWER SYSTEMS

Phillip Krebs

Network Architect
Overall project architecture

Branko Cerkuc

Product Owner Network
Project Managed Service

NTS RELAX, WE CARE

Nico Ambruster

Systems Engineer
Overall project architecture
SDA-Project – Wired

Gregor Geldhauser

Senior Systems Engineer
SDA-Project - WiFi

PROJECT GOALS AND REASONS TO START WITH SDA

Challenges:

- Complete renew of old Hardware
- Create a Wireless first environment, with Voice ready Wireless.
- Issues with overlapping IPs in RR Group.
- Build an infrastructure that can be handed to an MSP
- Build an infrastructure that can handle current Business requirements and is “future prove”

Benefits only SDA can provide:

- Handling of moving OT-Endpoints
- Seamless wireless integration
- Easy implementation of segmentation
- Out-of-the-Box automation & standardization
- Bring in a „single plain of glass“ Management

TEAM SETUP

3rd Level Support (TAC / BU)
Ongoing development and improvement of new features for SDA
Special Support from Cisco SME Like
Peter Fuchs, Martin Rosensteiner, Stefan Honeder

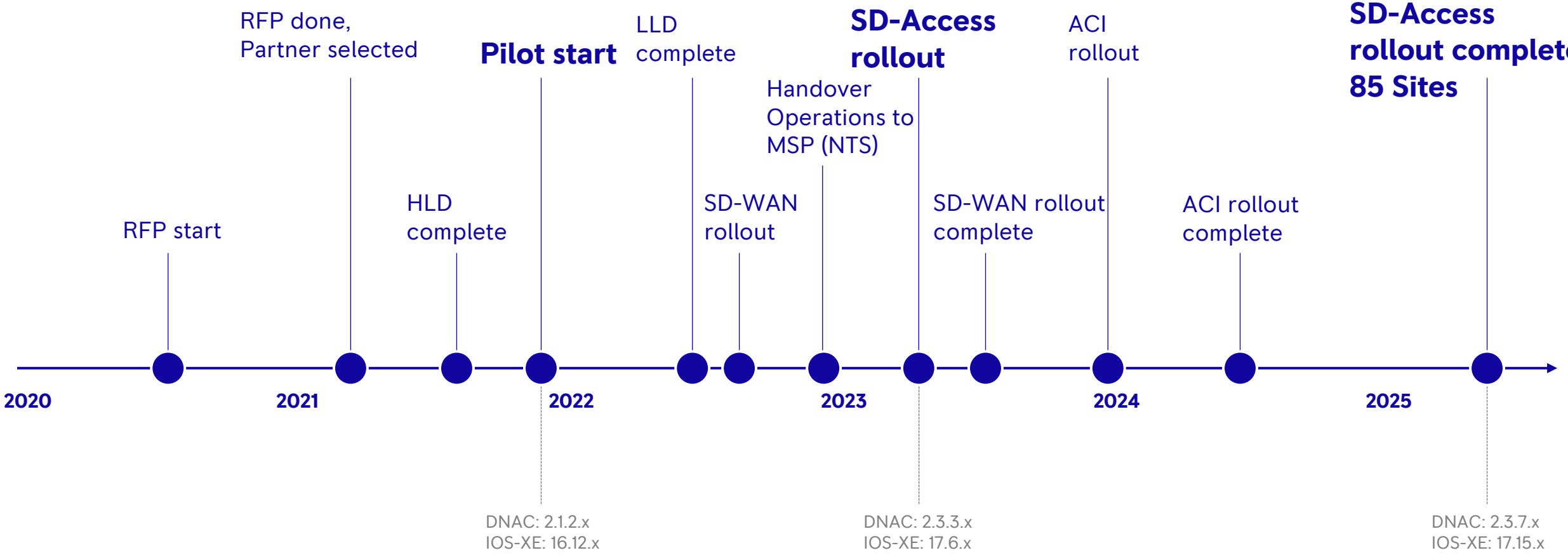
NTS RELAX, WE CARE

Project Integrator
Managed Service Provider
Cisco Center of Excellence (CoE)
Cisco multiple preferred Partner (Gold Partner)

ROLLS-ROYCE POWER SYSTEMS

Friendly Customer
Early Adopter

TIMELINE



02 TECHNICAL DESIGN

RISE

SIZE & HARDWARE

Switching

~ 1.150 Access

~ 150 Core & Distribution

85x Sites

Hardware:
- C9600
- C9500
- C9300(L)(X)
- C9200CX
- C3560CX

Wireless

~ 3500 AP

6x HW WLC
2x VM WLC

~ 140 Switch embedded WLCs

Hardware:
- C9800
- C9100
- AP2800

Network Management

6x Catalyst Center (3x DR)

15x ISE Nodes

1x Central Assets DB

Hardware:
- DN2-APL-L
- ISE-VM-K9

Clients

~ 11.000 IT-Clients

~ 18.000 OT/IoT Clients

~ 1.200 Monthly Guests

ACI

3x Datacenter complexes

~50 Leaf Switches

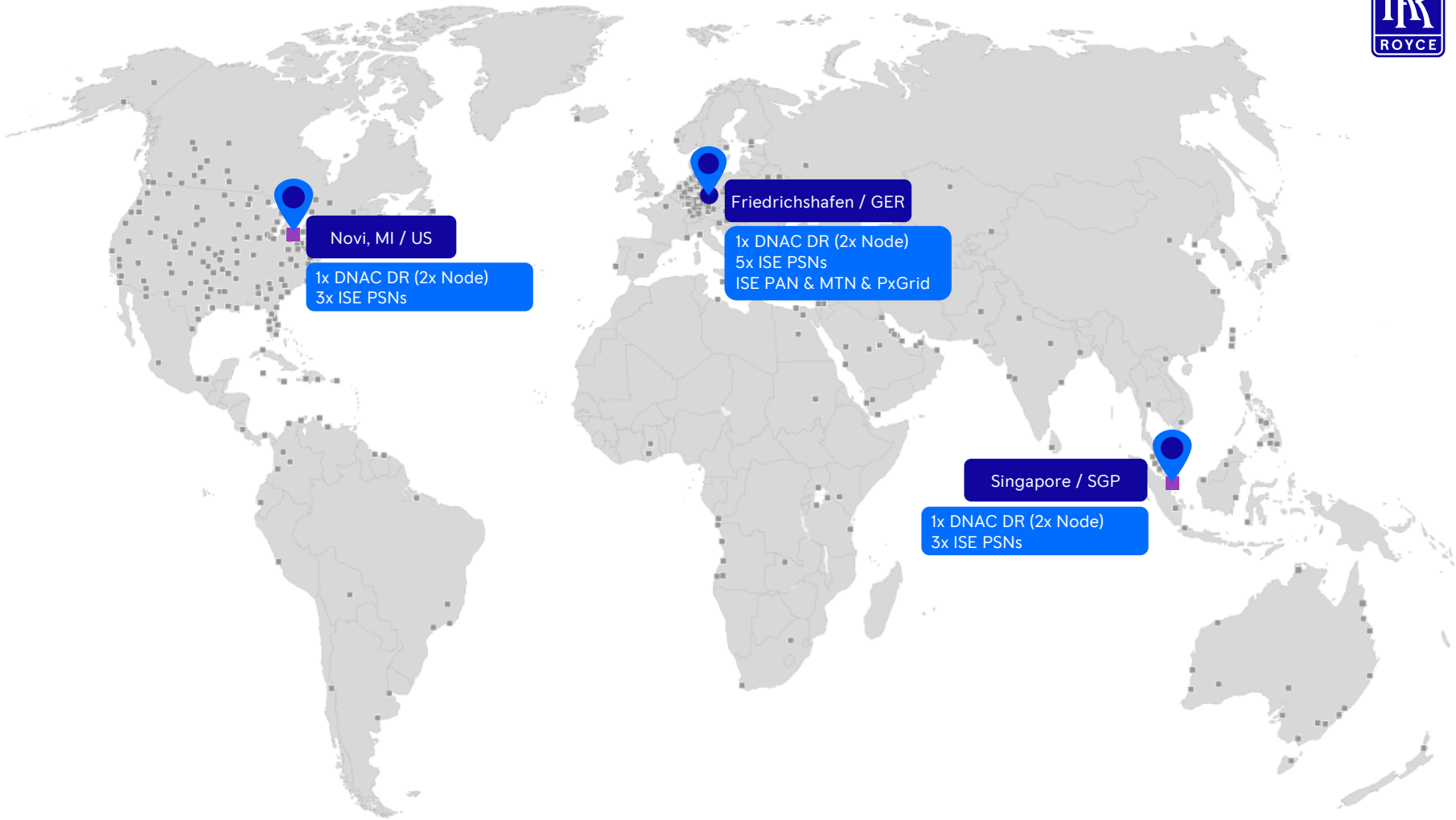
100G non-blocking DC

GLOBAL DATA CENTERS

More than
30K **Daily active Sessions**

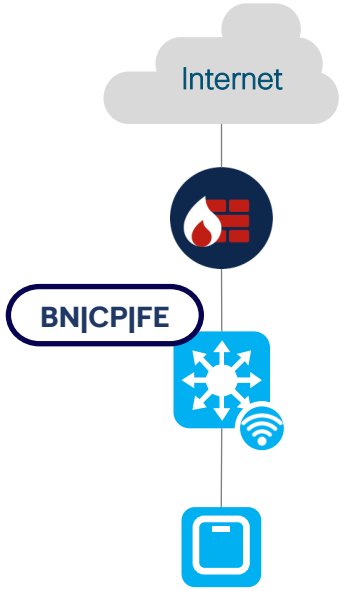
More than
500K **Daily TACACS+ Request**

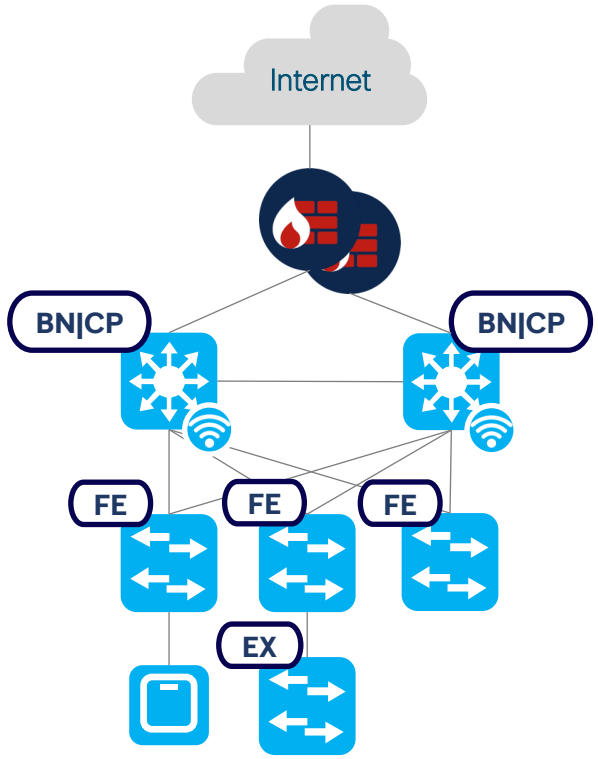
More than
3,2Mio **Daily Events**

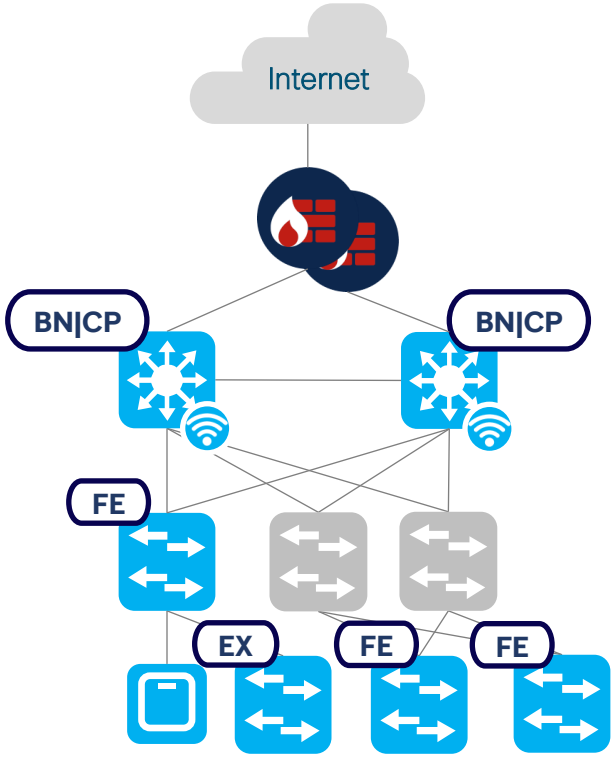


BRANCH DESIGN T-SHIRT SIZES

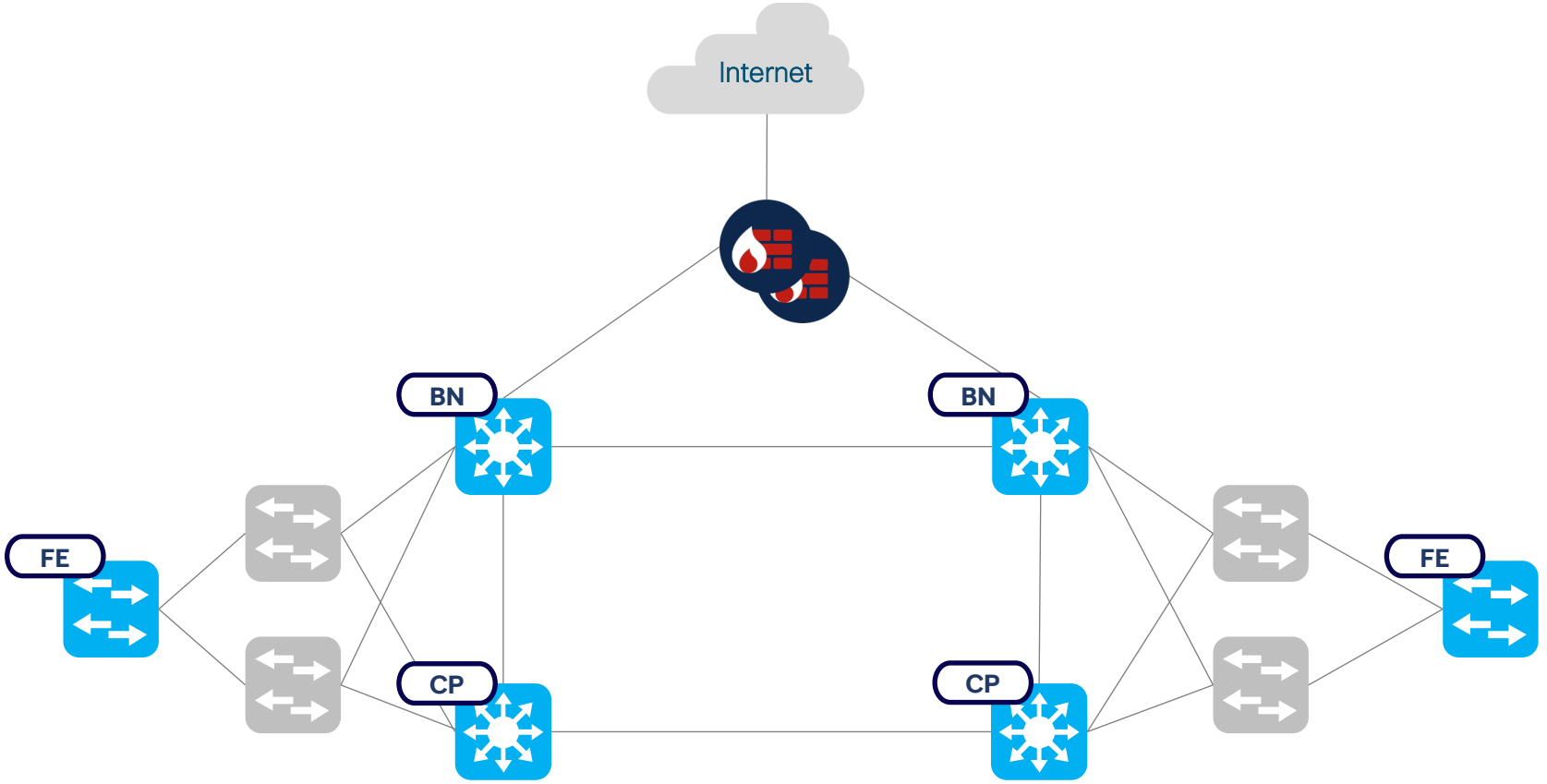
S	M	L







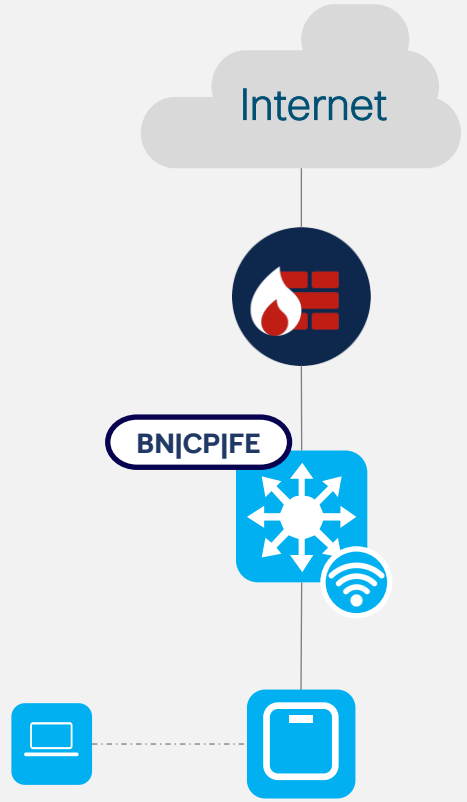
ROUTED ACCESS BENEFITS



Benefits:

- More flexibility
- Faster convergences
- Reduced cost
- Easier deployment & expansion

FABRIC EMBEDDED WIRELESS CONTROLLER



Ultra low-latency connection	No Backhauling, Local site roaming
Low wireless Footprint	No dedicated WLC needed; No Hardware No VM
Seamless integration into the Fabric	Small Config, Best roaming experience, Fully automated deployment

CHALLENGES WHILE IMPLEMENTING

Multi IP, one MAC	Build a custom workaround	Finally solved by a new feature in DNAC 2.3.5.x and IOS-XE 17.12.x	Improvements requested by Cisco (DHCP Support)
Silent Clients	Working with the device operator solved ~90% of issues	Workaround applied to the remaining ~10%	Improvement on the Roadmap with DNAC 3.2 (silent device tracking)
Proprietary DHCP clients	Build a custom workaround	Engaged with the business to replace the Devices	Project for device replacement in the works

03 LESSONS LEARNED

LESSONS LEARNED

Preparation and Planning is everything	Include business stakeholders	Analise switches / Wi-Fi in detail	Make sure to test uncertain devices	Build Migration runbooks for end-system groups
Stick to standards	Define standards that work in the field (not only on paper!)	Build standards that are flexible when needed	Everything needs to be a standard!	Challenge your Designs and Standards regularly
Everything can be migrated to SDA	If something seems to not work on SDA, take your time to find a solution	Include business stakeholders	Seek solutions beyond your immediate perspective	Should that system be on SDA?
Don't give up	SDA can be challenging	It´s a marathon, not a sprint	Sometimes talks can be hard – but necessary	You will be asked difficult questions

04

SO DID IT WORK?

Did we reach our goals?

PROJECT GOALS AND REASONS TO START WITH SDA

Challenges:

- Complete renew of old Hardware
- Create a Wireless first environment, with Voice ready Wireless.
- Issues with overlapping IPs in RR Group.
- Build an infrastructure that can be handed to an MSP
- Build an infrastructure that can handle current Business requirements and is “future prove”

Benefits only SDA can provide:

- Handling of moving OT-Endpoints
- Seamless wireless integration
- Easy implementation of segmentation
- Out-of-the-Box automation & standardization
- Bring in a „single plain of glass“ Management

ADDITIONAL ACHIEVEMENTS

Cut time to deploy new infrastructure	Prior to SDA: >2 Weeks	Now: <1 Day
Increase availability (Access Level)	Prior to SDA: 98,15%	Now: 99,96%
Reduce amount of Incidences (per month)	Prior to SDA: 1215	Now: 423
Increase level of DayN Task automation	Prior to SDA: 5% of Tasks automated	Now: 85% of Tasks automated

05 ROADMAP

ROADMAP

More Segmentation (Microseg.)

CCGM (Catalyst Center Global Manager)

Expand the Network

06 WISHES FOR THE FUTURE IN SDA

WISHES FOR THE FUTURE IN SDA

Device Management

- Move Switches & WLCs from one Building to another (like with APs)

Wired Fabric

- Dual-homing support for fabric clients
- Moving extended node support (moving from one FE “Uplink Port” to another)

Assurance & reporting

- Create manual reports

Wireless Fabric

- Improve the Switch embedded eWLC (scale)
- Support for one WLC in multiple fabric sites

mtu A Rolls-Royce solution

kelag

YOUR ENERGY IS OUR NATURE

About the KELAG Group

GENERATION (KELAG)

100 hydropower plants
9 wind farms with 49 wind turbines
46 photovoltaic systems
960 megawatts of generation capacity

POWER DISTRIBUTION NETWORK (KNG)

~ 18.700 km system length
~ 7.500 transformer stations
50 substations

GAS DISTRIBUTION NETWORK (KELAG)

32 reduction stations
~ 820 km system length

HEAT (KELAG Energie & Wärme GmbH)

83 district heating networks
36 biomass heating plants
~ 840 heating stations
~ 983 kilometers of district heating network

FIBER OPTIC NETWORK (KELAG)

~ 1.800 km fiber optic network
~ 2.000 km empty conduits
~ 14.400 customers

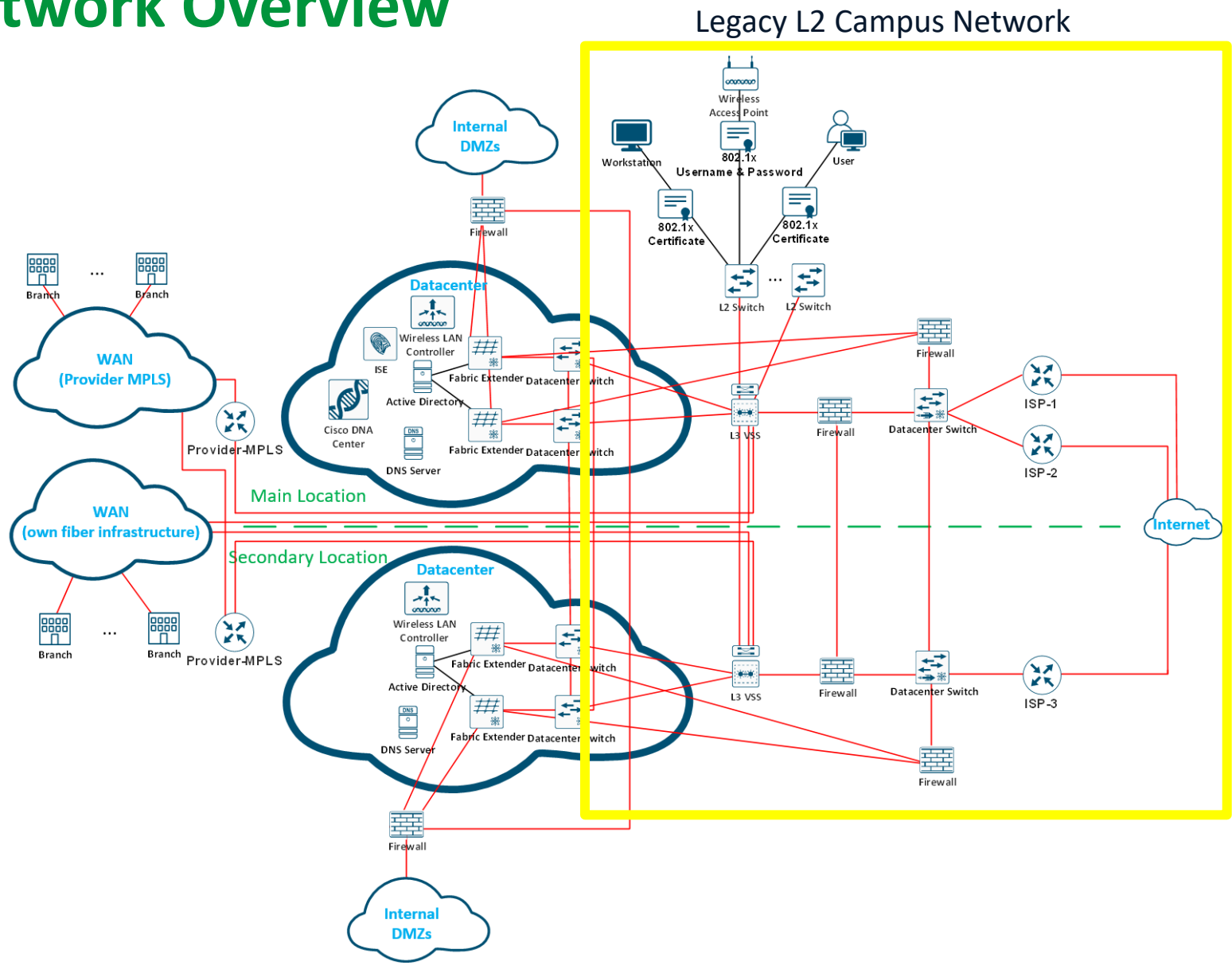
KELAG Group

~ 2.011 employees
1.979 million euros net revenue in 2024
One of Austria's ten largest companies in the energy sector

IT Environment – KELAG Group

334 Switches	4 ISE Nodes	2 DC Locations (4 Spines & 43 Leaves)
450 AP’s	3 Catalyst Center Nodes	75 IT Sites
2 WLC’s	15 Firewall Clusters	3.062 Active Clients

Legacy IT Network Overview



The Need for Change

Hardware lifecycle reached

Current implementation
no longer state-of-the-art

New legal regulations
(e.g. EUGDPR & NISG)

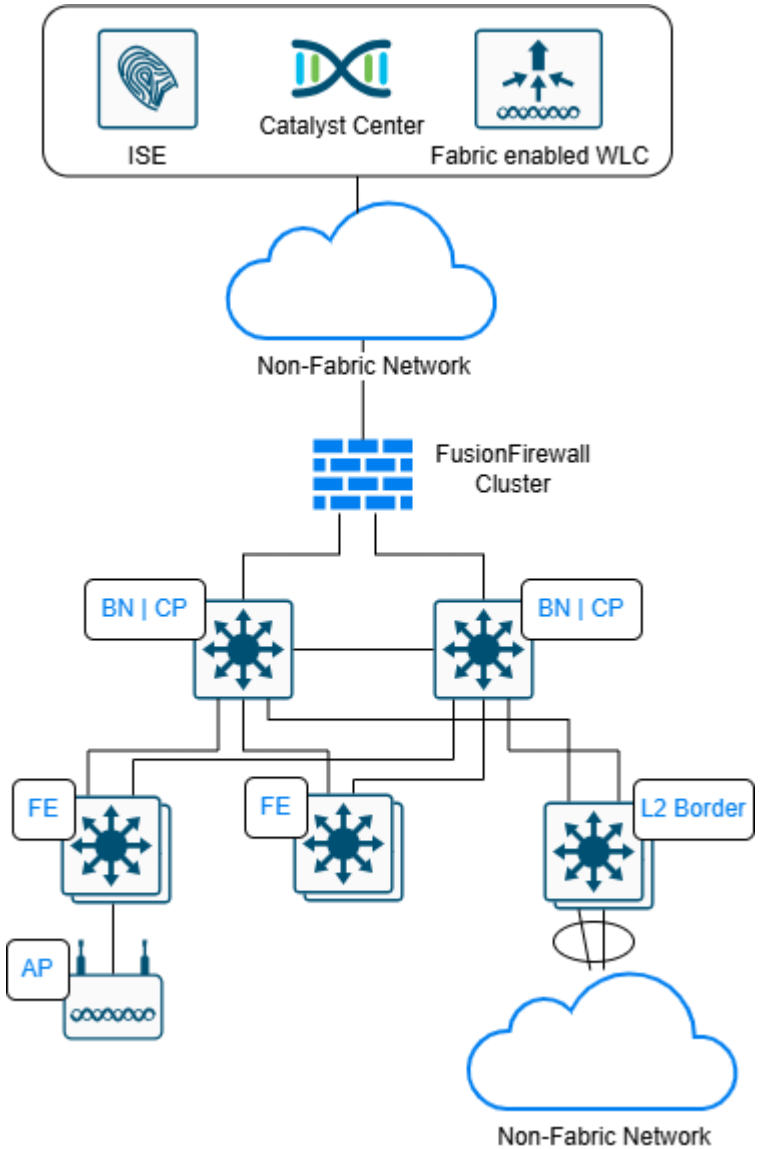
Compliance frameworks to fulfill
(e.g. ISO/IEC 27001 & ISO/IEC27019)

Higher security requirements
due to changed threat landscape

Lack of well-trained
employees for network operation

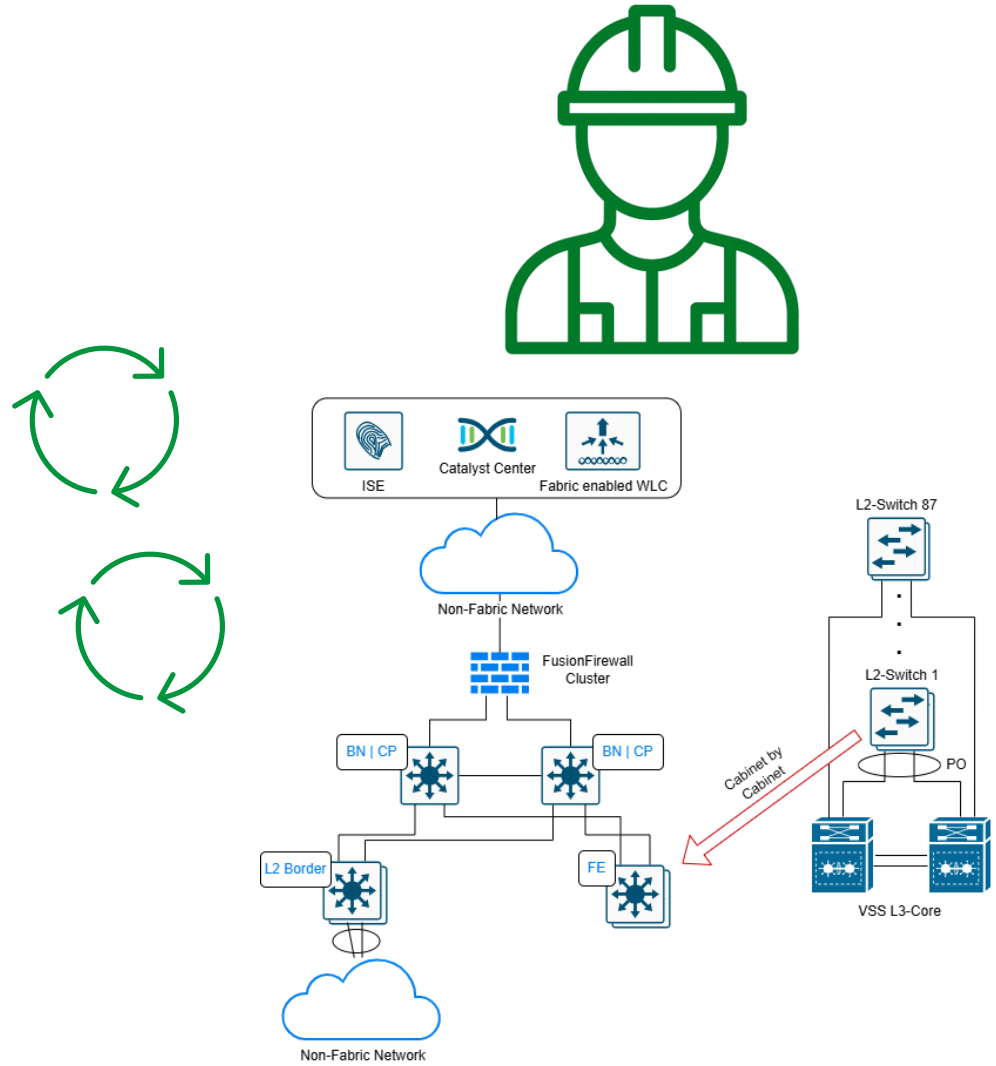
High Level SD-Access Design

- Standard SDA network design
- Hardware based on Catalyst 9k Series
- MACSec between network devices
- L2-Border for migration purposes
- SGT aware Fusion Firewall Cluster
- Enhanced Monitoring & Testing with Thousand Eyes
- Closed Authentication Fabric wide



Migration Steps - Brownfield

1. HW-Refresh with SDA ready components
2. Building up central fabric components
3. Planning of needed VN‘s and Micro-Segmentation Policy
4. Testing Phase
5. Implementing of special use cases (e.g. Scripts, Templates, …)
6. Testing Phase
7. Planning maintenance window
8. Migration of non-SDA cabinet into SDA Fabric
9. 2-3 Days of hyper care



Encountered Challenges

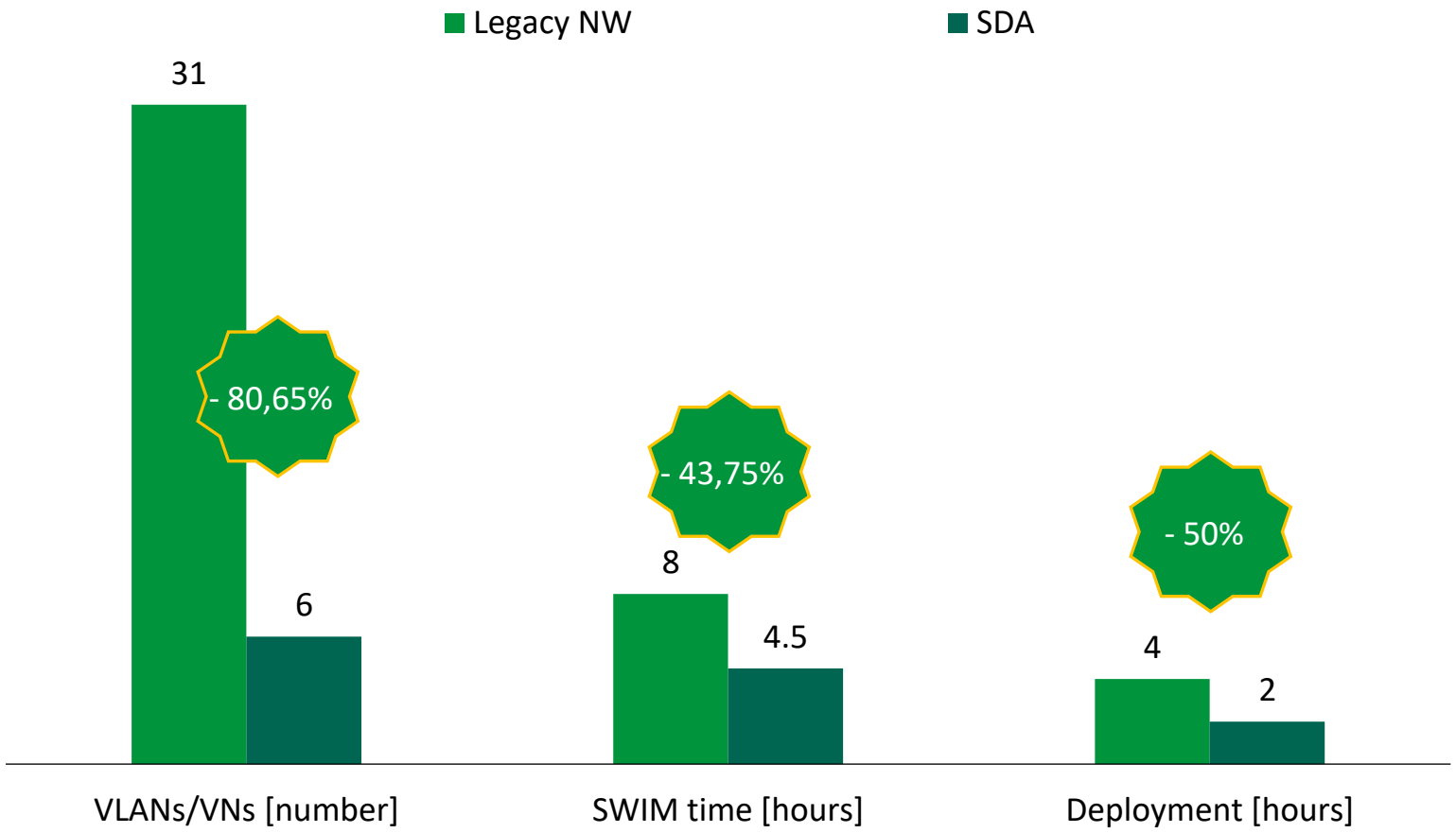
- Tight maintenance windows
- Operation must not be disrupted
- Many different departments
- Not only a switch to SD-Access, but also to a new firewall
- Solutions for specific use cases (e.g., emergency telephony, voice recording, CIS hardening)
- Software changes during rollout
- Long sync time for stacked switches (has already been improved)
- Software Bugs

Success Highlights

- Quick and easy rollout of micro-segmentation via SGTs
- VN-wide multicast configurations with just a few clicks
- Easy-to-use QoS rollout across the entire fabric
- Possibility of L2Border for connecting non-fabric networks
- Automated switch provisioning via LAN automation

SD-Access Benefits

- Micro-Segmentation & SGT’s
- Simplified operation
- Mobility of Users & Devices
- Compliance
- Scalability
- Empowering the Help Desk



Conclusion

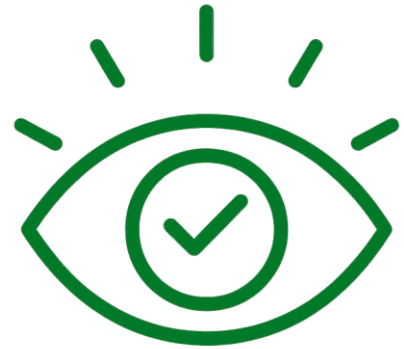
Basic Requirements:

- Check whether SDA is a suitable solution and covers all necessary use cases
- Automation means standardization
- DevOps skills required (e.g. for particular use cases and templates)

Success Factors:

- Working closely with the departments to identify all use cases
- Extensive testing is crucial
- Don't get stuck in old patterns - Think in new ways
- Collaboration between CANCOM Austria (Partner) and Cisco

What We'd Like to See



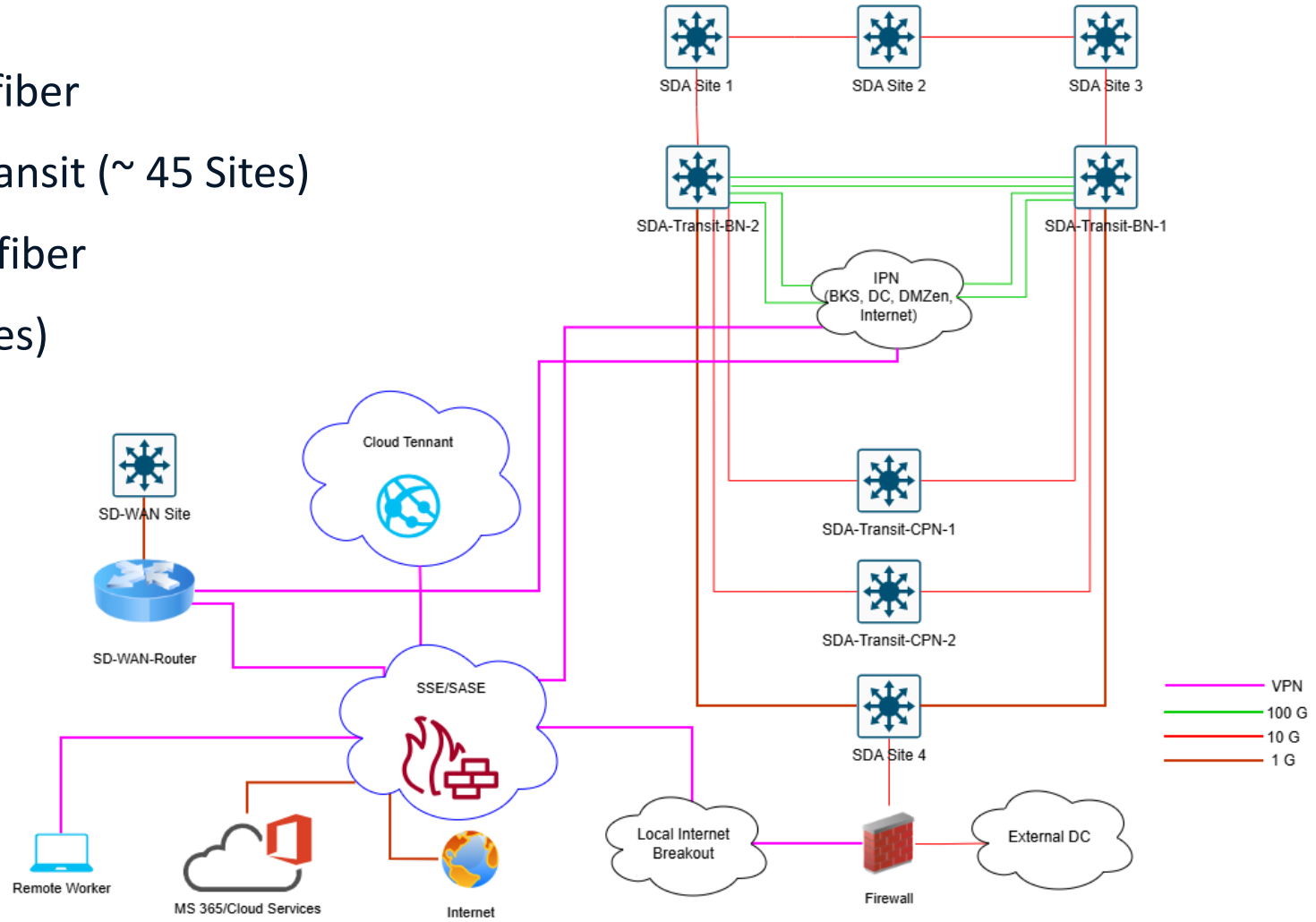
- Possibility to share WLC across sites (> 4 sites)
- Improved topology overview and more customizability
- Automated creation of match patterns for security advisories

How the Journey Will Continue

- Implement SDA-Transit for sites with own fiber
- Migrate site for site to SDA and the SDA-Transit (~ 45 Sites)
- Implement SD-WAN for sites without own fiber
- Migrate sites to SDA and SD-WAN (~ 30 Sites)
- Implementation of SSE/SASE solution
- Activation of Adaptive Network Control

Micro- & macro-segmentation through the whole IT network

Commissioning of all sites possible via LAN automation



THANK YOU

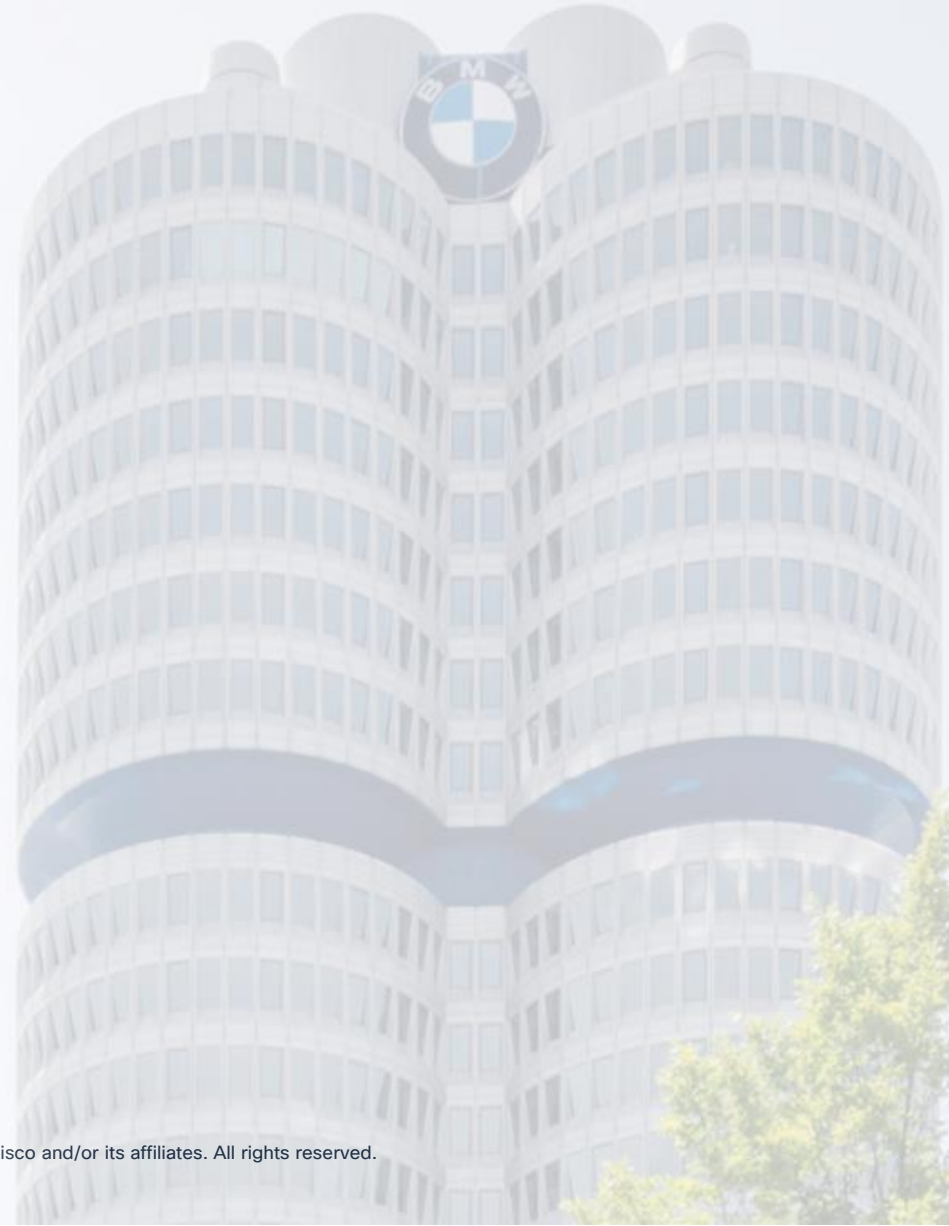
kelag

Cisco SD-Access @ BMW Group

cisco Live !

Bernhard Haring
Network Architect
CCIE #8265

Agenda



01 BMW Group

02 Key business drivers

03 Journey to SDA

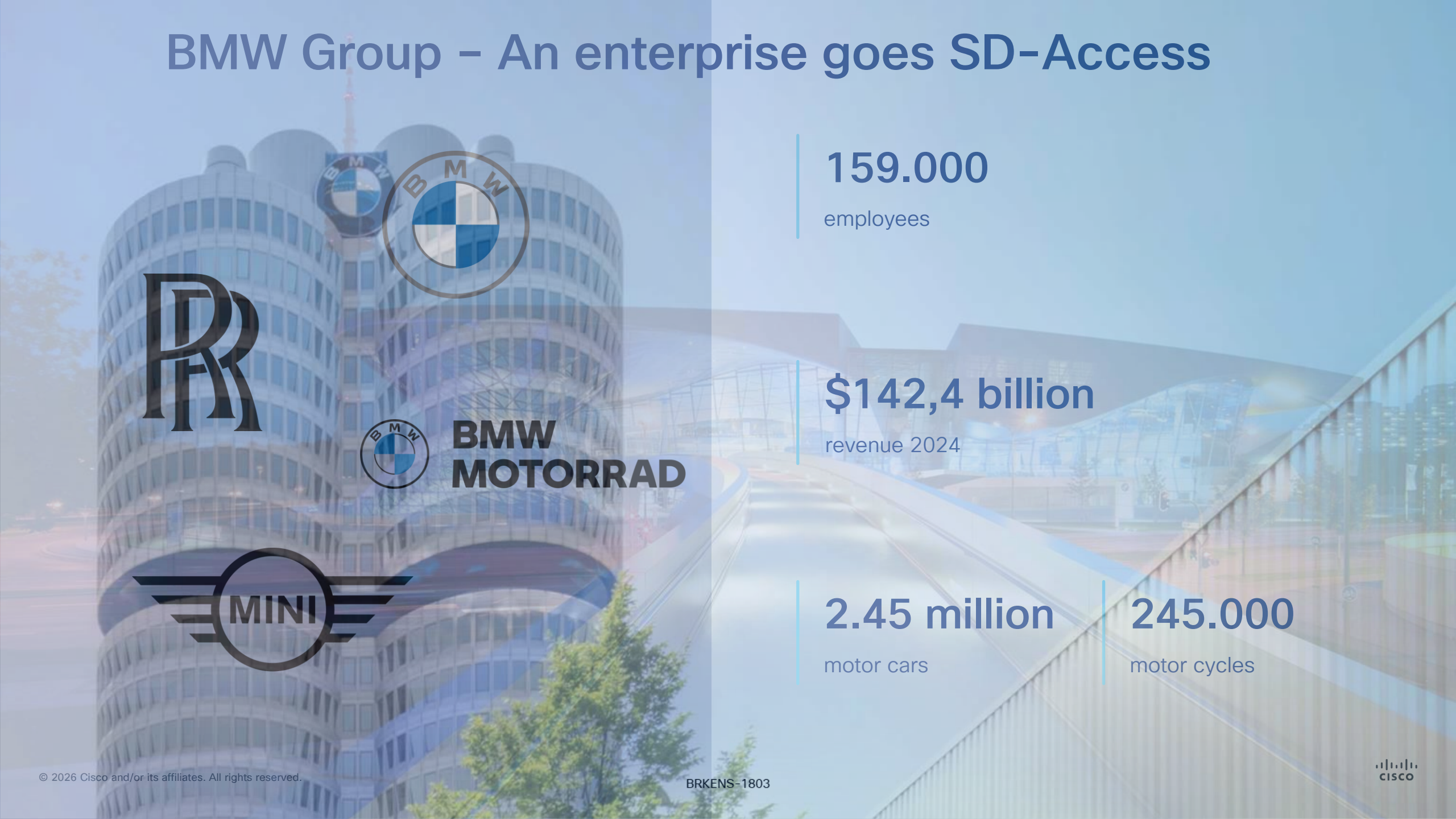
04 Lessons learned

05 Operational changes

06 Expansion and roadmap

cisco

BMW Group – An enterprise goes SD-Access



159.000
employees

$142,4 billion
revenue 2024

2.45 million
motor cars

245.000
motor cycles

BMW Group


MÜNCHEN
DINGOLFING
REGENSBURG
LEIPZIG
BERLIN
LANDSHUT
IRLBACH-STRASSKIRCHEN
WACKERSDORF
EISENACH
SPARTANBURG
SAN LUIS POTOSÍ
DEBRECEN
OXFORD
GOODWOOD
STEYR
HAMS HALL
SWINDON
MANAUS
ARAQUARI
ROSSLYN
CHENNAI
RAYONG
DADONG
TIEXI & LYDIA
SHENYANG

BMW Group

- Over 30 production sites
- More than 400 locations in > 140 countries
- ~ 12.500 LAN Switches
- ~ 25.000 Access Points
- ACI in most of the production sites
- Thousands of Applications
- Centralized and highly standardized IT

Key business drivers for SDA at BMW Group?

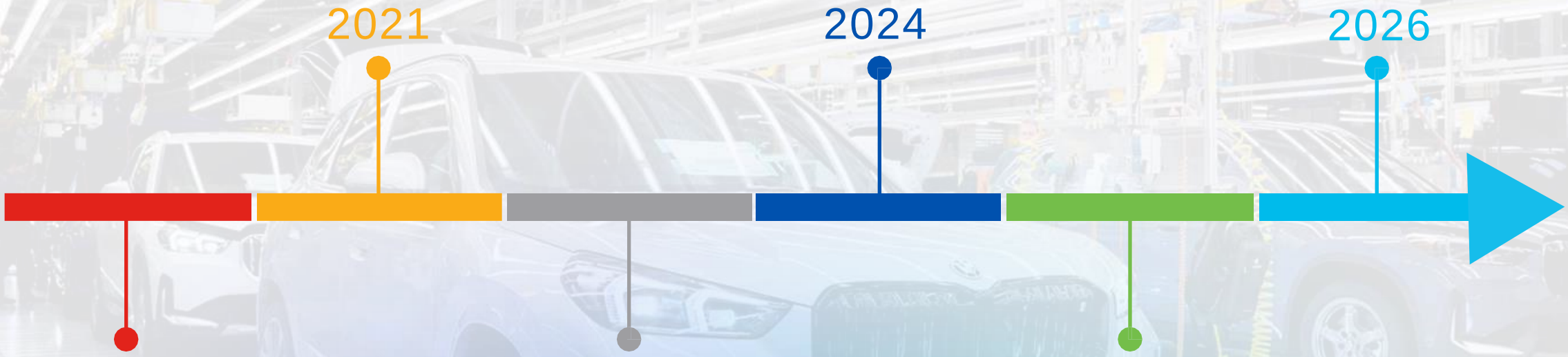
AS-IS:

- Highly standardized network environment
  - Standardized and BMW released hardware / software / configuration
  - Compliance is difficult
- Network Automation with different tools
- No Zero touch installation
- Lifecycle process
- New requirements for security and internet access → segmentation not easily possible in routed access environment

TO-BE:

- Automated configurations, no human errors, 100% compliance
- Up to 100% automation with Catalyst Center
- LAN Automation is standard
  - For 20 Catalyst 9400: time reduction from 40 hours to 4 hours
- Segmentation is standard

Journey to SDA



2020

Technical and Business
Use Case Evaluation

2021

Consulting with CX
SDA design for BMW group
CPoC
Work in Lab

2022

First pilot site
- 48 Catalyst 9400 as Edge
- 4 Catalyst 9500-48Y4C &
- 6 Catalyst 9600 as B/C and intermediates, 2 fabrics

Close collaboration with Catalyst Business Unit
→ show stoppers and critical feature requests

2024

Second and third pilot sites
(today 120 Catalyst switches
> 9000 users)

2025

Change IP Transit to SDA Transit in global design, preparation for global rollout (Office only, no production for now), Onboarding Rollout Provider, Automation (API), Migration plan, fine tuning...

2026

Start of global rollout

Flagship Use Cases & Lessons learned

Show stoppers found in initial and current installations

- Simultanous LAN automation
- Silent hosts

Operational issues

- Compliance checks

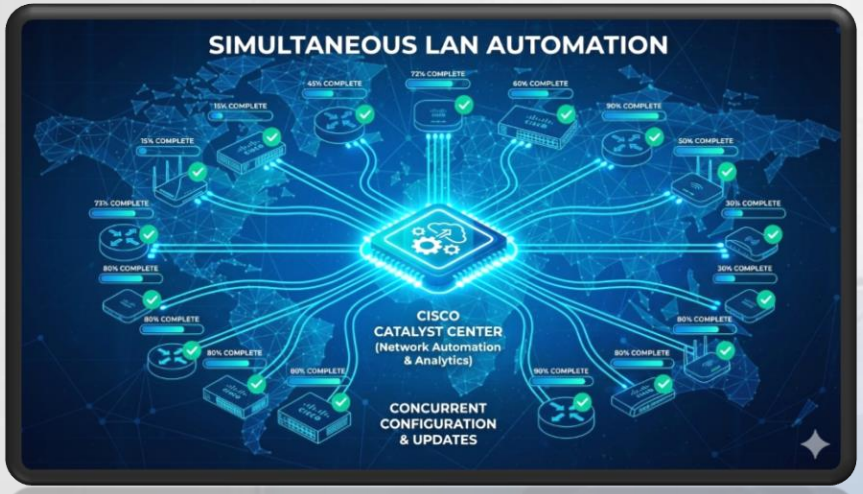
Preparation effort

- Comprehensive Lab-tests and participation in Early Field Tries EFT

Great Collaboration with Cisco Catalyst BU

cisco

Simultaneous LAN Automation



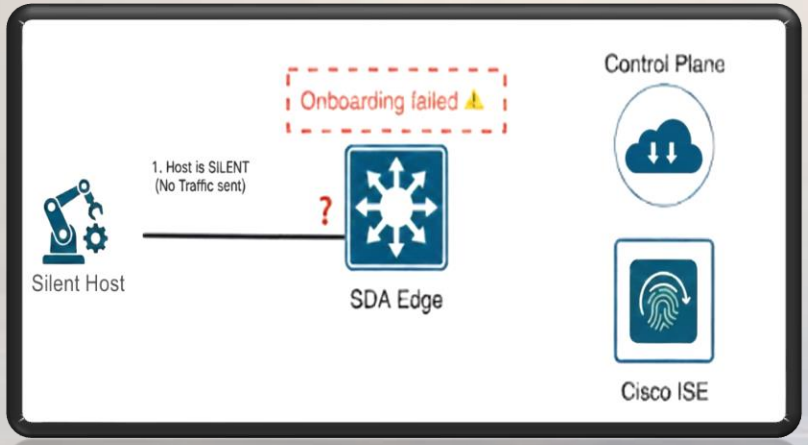
LAN automation essential for
- Migration
- New installations
- Lifecycle process

One XL-Cluster for EMEA and ZA
- 20 production Sites / ~200 locations
- Approx. 4500 switches

Different operational teams
- Need to work in parallel
- Only one LAN Automation was possible

Issue discovered in 2021 as show stopper
Collaborate with BU
New Feature available in Cat Center Version 2.3.5, 2023

Silent hosts



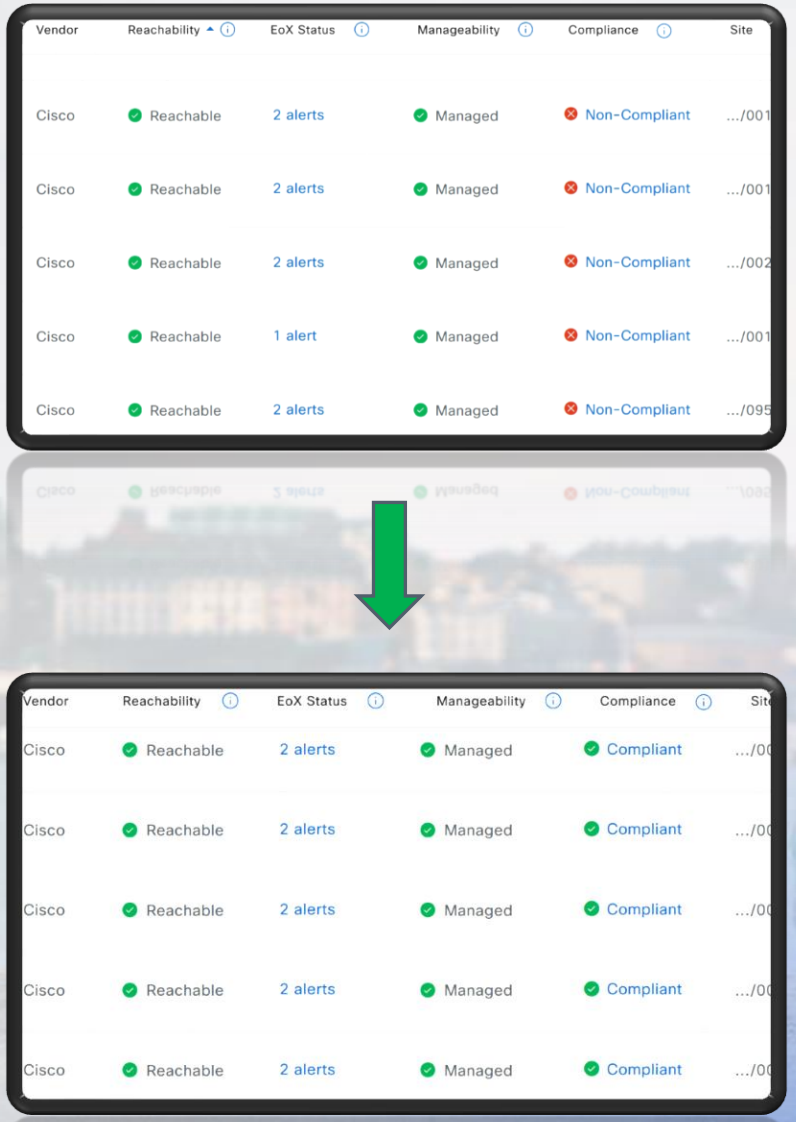
Unauthenticated silent hosts are member of default vlan1
Dynamic VLAN assignment for authenticated hosts

Challenge: how to achieve that silent client uses MAB (MAC authentication bypass)
→ in combination with multiple VNs and huge networks (/19, no broadcast flooding) and other features

Issue discussed with BU on Cisco Live EMEA 2024
- Identified as show stopper
- Co-invention BMW / Cisco
- Feature will be available in 2026

→ in time for planned BMW rollout

Compliance checks



Compliance at BMW Group

- Software
- Hardware
- Security Advisories
- Configuration (extremely complex in traditional environments)

Compliance within Catalyst Center evolved significantly over the versions

Operational issue:

- Special configuration pushed via Day-N template
- Hundreds/Thousands false positives are generated by executing a Day-N template
- Needed to be acknowledged individually on each and single switch
- Feature Request “Bulk selective acknowledge” in 2025
- Committed for 3.2.1

“ Migration needs time “

For migration "wr erase", "reload", LAN Automation and configuration is needed
Maintenance window with few hours of downtime
Migration of a location only on weekend / sunday
Maximum 2 locations per week

Migration means much work:

- Pre-Work
  - Planning (Overlay IP, IPv6, MTU size, AP (static to DHCP), ...)
- Change
  - Quite easy, only a few hours per location
- Post-Work
  - IP renumbering -> Static IPs / DHCP reservations, AP (DHCP to static)... very time consuming

Operational changes & conclusion

- Standardization
  - Even though IT standardization is extremely high at BMW Group today, it will be further improved with SDA
- Since 2022 no incident related to SDA in all fabrics with more than 120 switches / 9000 end systems
- Stability is the goal
- Comprehensive high time reduction staging or lifecycle process
  - For 1 Catalyst 9400: time reduction from 4 hours to 1 hour
  - For 20 Catalyst 9400 in parallel: time reduction from 40 hours to 4 hours
- Partnership with Cisco
  - All show stoppers and critical Feature Requests implemented before BMW rollout
  - Amazing Co-invention BMW / Cisco

Expansion and roadmap

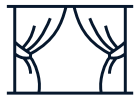
- Global rollout 2026 and beyond
- 100% SDA in office environments
  - 20 production sites / ~300 locations
  - More than 5000 switches
- SDA in production environments will follow in a later phase
  - 20 production sites
  - Approx 4000 switches
- Segmentation as base for ZeroTrust
  - Common policy
    w/ SDA and ACI in planning

Complete your session surveys

Complete your surveys in the Cisco Events App.

Complete a minimum of 4 session surveys and the overall event survey to receive a unique Cisco Live t-shirt.
(from 11:30 on Thursday, while supplies last)

Continue your education



Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Visit the Technical Solutions Clinics to discuss your technical questions

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

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

Thank you

cisco Live !


CISCO