



Software Defined Access (SD-Access)

Real-World Success Stories Powered by Cisco SD-Access!

Kanu Gupta | *Product Manager, Cisco*

Jacxine Fernandez | *VP Information Security, BIAL*

Joshua Hornig | *Network Administrator, Blum*

Ricardo Pinheiro | *Team Manager Infrastructure, Ikea Industry*

BRKENS-1803

Webex App

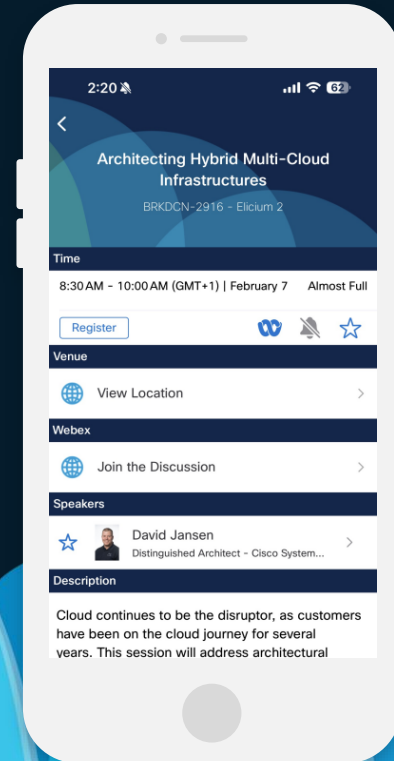
Questions?

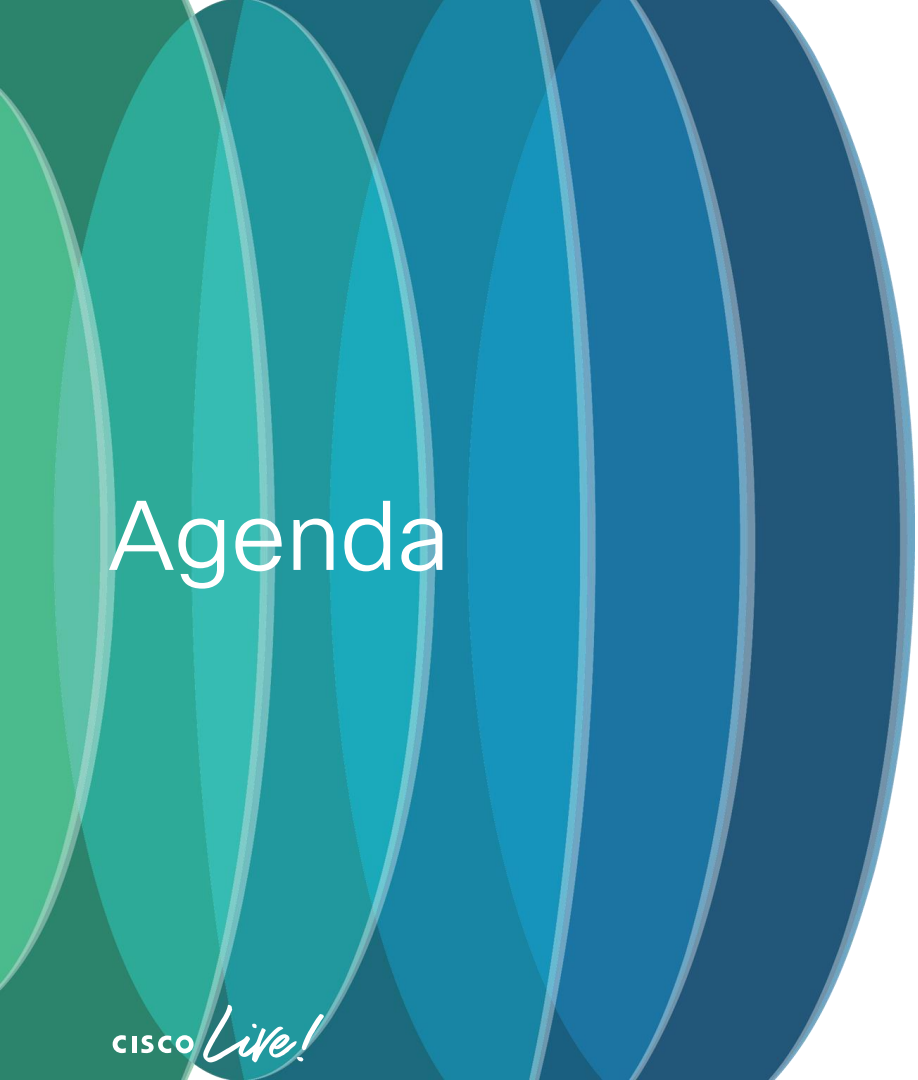
Use the Webex app to chat with the speaker after the session

How

- 1 Find this session in the Cisco Events 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 February 28, 2025.





Agenda

Success Stories

- Bangalore International Airport *Aviation*
- Blum *Manufacturing*
- IKEA Industry *Manufacturing*

My profile

Mr. Jaxine Fernandez is currently the Vice President – Information Security, ICT Governance and ICT Revenue at Bangalore International Airport Ltd., the leading airport in South India.

In this role, he is responsible for the enterprise cybersecurity program across IT, OT and IoT, ICT governance, partner management and budgeting and ICT revenue from various stakeholders at the airport.

He is an experienced cybersecurity and enterprise risk management senior executive with multi-geography experience across Asia, Middle East, and Africa. He has held previous roles as the Group CISO, Adani (Group) Enterprises, Group Enterprise Risk Director at Zain, a leading Middle East telecommunications service provider spread across 8 volatile markets and Group Head of Security and Compliance for airtel Africa (with operations in 17 countries), among others.

His expertise spans diverse industry sectors including aviation, telecommunications, ports & logistics, power, Oil & Gas, Defence, Public Utility and Media Communications.



TERMINAL- 2

IS DESIGNED AND BUILT ON 4 KEY
PILLARS:



TERMINAL
IN A GARDEN



TECHNOLOGY



SUSTAINABILITY



ART & CULTURE

BLR Airport : India's 3rd busiest airport

FY 2019

33.3_{mn}
passengers

380k_{MT}
Cargo

1 Terminal

CY 2024

40.7_{mn}
passengers

496k_{MT}
Cargo

2 Terminals

36

Airlines

13

Freighters

73

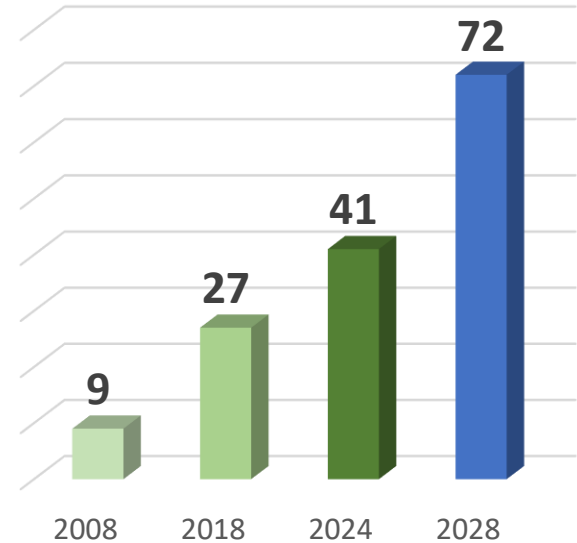
Domestic Destinations

31

International Destinations



Passenger Growth (in millions)



An ecosystem of ecosystems

Stakeholders



Airlines



Manufacturers, System Suppliers,
Service Providers



Governments and Regulators



Passengers / Customers



Other business units, cross border
stakeholders



Financial Institutions and other
stakeholders

Airport Operations

Air Traffic Control (ATC)

Physical Premises
Management

Technology

(Data Centers, applications, systems)

Supply Chain



2 Datacenters and 150+
Telecom/ IT Rooms



22,000+ Endpoints (incl. servers,
user machines, CCTVs, ACS, etc.)



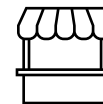
Users of IT
~30,000



70+ Applications
4 mobile apps



10+ Security
Solutions

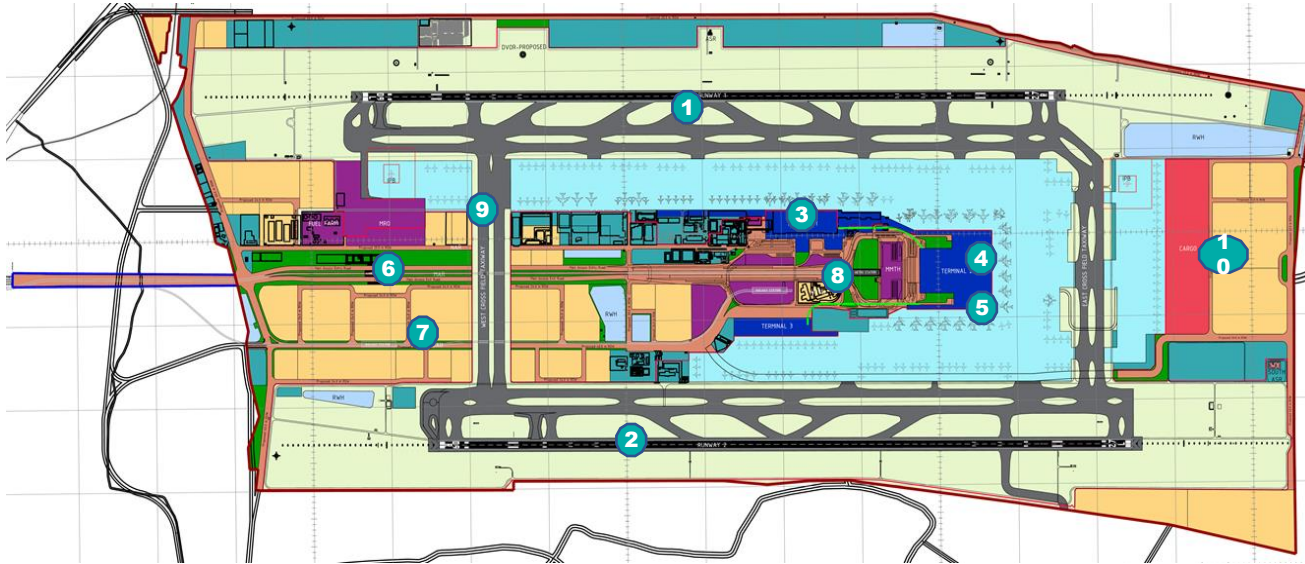


150+
Concessionaires



16 OT-Subsystems

Future Expansion Plans



- 1 Existing North Runway 09-27
- 2 New South Parallel Runway (NSPR)
- 3 Existing Terminal 1
- 4 Terminal 2 / Phase 1
- 5 Terminal 2 / Phase 2
- 6 Terminal Boulevard
- 7 South Secondary Access Road
- 8 Future Metro Station / MMTH
- 9 Future Western Cross-taxiway
- 10 Future Terminal 3 (T3)

Migration Accomplishments

SD-ACCESS

AIRPORT NETWORK - A NET

50 SWITCHES – 40 BOARDING/CHECK-IN GATES,
400 FIDS, AOCC

BUSINESS NETWORK - B NET

320 SWITCHES - BIAL Corporate, WLAN, Airline
Backoffice, Cargo, Concessionaires

SECURITY NETWORK - C NET

220 SWITCHES – 2300 CAMERAS, 500 Access
Control Systems, SOCC

PUBLIC ANNOUNCEMENT - PA NET

40 SWITCHES – Public Addressing,
Paging Stations & Speakers

FIREWALL

11 FIREWALLS

5 PHYSICAL, 6 VIRTUAL FIREWALLS

2 FIREWALLS

11 FIREWALLS MIGRATED TO 2 PAIRS
OF FIREWALLS

POLICY CONSOLIDATION

1000+ Policies -> 100's of Policies

ACI

SD DATACENTER

284 Physical & Virtual Servers
migrated including AODB

DC INFRA

4 SPINES, 41 LEAF SWITCHES
Deployed across NDC & MCR

RESILIENT DATACENTER

Application High Availability with
automation, security, and resiliency.

WIRELESS & ISE

360 Access Points

Seamless Migration of 360
Aruba AP to Cisco

Identity Services Engine

44K Endpoints Authenticated on
the Network

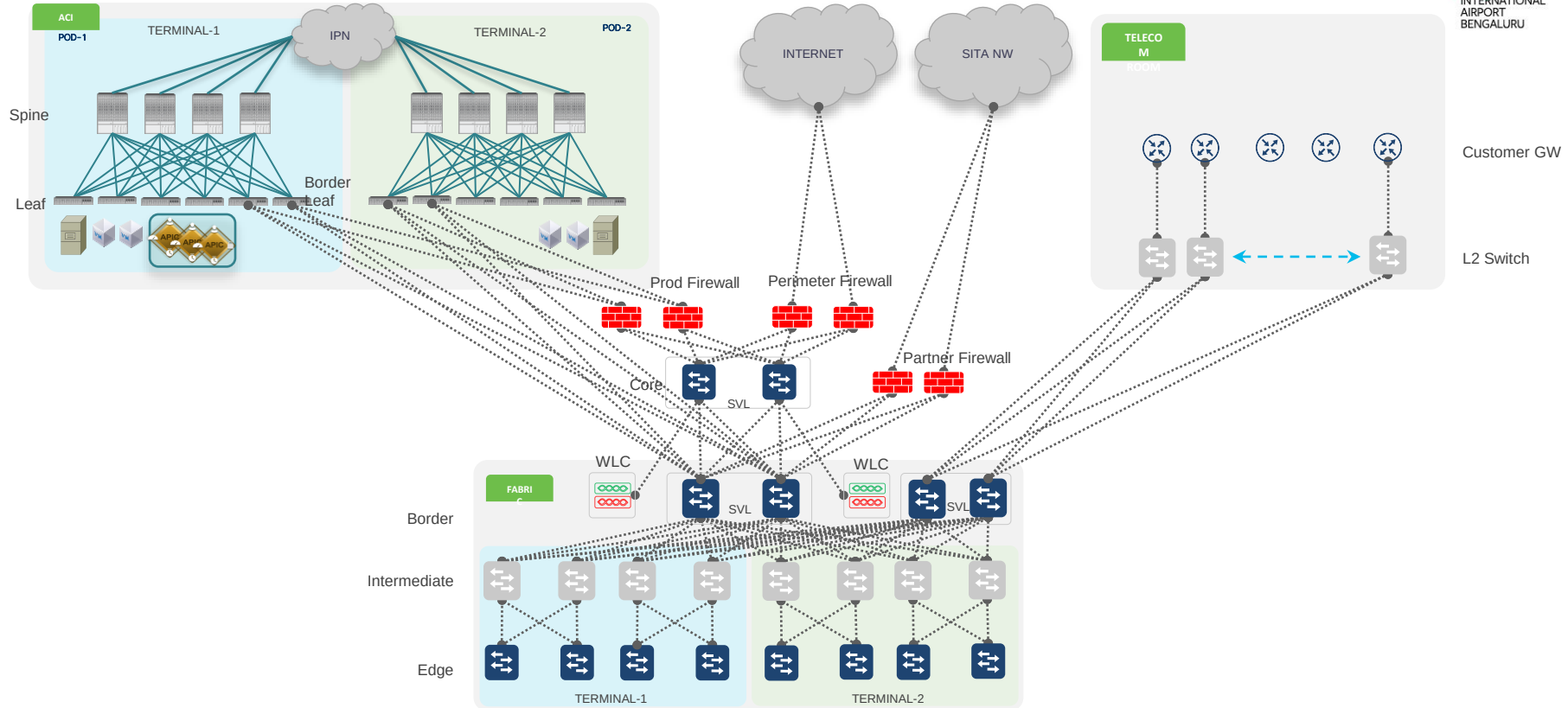
WIRED

SECURITY

DATACENTER

WIRELESS

BIAL Indicative Network Architecture & Design



Operational Gains

Category	Traditional Network (Pre-SDA)	Software-Defined Access (Post-SDA)	Improvement Metrics
Network Management	Manual VLAN management, complex configurations, high admin overhead	Automated policy-based network segmentation, centralized management via Cisco DNA Center	50%+ reduction in admin effort & network configuration time
	Manual device configuration, inconsistent policies across network domains, decentralized management	End-to-end automation with Cisco DNA Center, consistent policy enforcement, unified network visibility	50%+ reduction in manual network operations, faster policy updates, enhanced network agility .
Operational Efficiency	Time-consuming onboarding, slow troubleshooting	Automated device onboarding, AI-driven network analytics for proactive issue resolution	40% faster service provisioning & incident resolution . AI-driven network analytics for proactive issue resolution partially used.
	Reactive troubleshooting with limited network visibility, high Mean Time to Resolve (MTTR), manual ticket handling	AI-driven analytics for predictive maintenance, automated ticket resolution, real-time network health insights	50%+ reduction in troubleshooting time, 70% improvement in network issue detection
User Experience	Inconsistent connectivity, high latency, service disruptions	Seamless, secure access with optimized bandwidth, improved QoS for critical apps	30%+ improvement in network uptime & performance.
Sustainability & Cost Savings	Higher power consumption, extensive cabling, high cooling costs	Reduced hardware footprint, lower cooling and energy consumption, optimized infrastructure	

Airport Systems

Digi Yatra & Self Check-in Kiosks



Concept:

DigiYatra, core concept, 'My Face is my ID – **seamless single token**'

Central identity management system to facilitate DigiYatra enrolment, authentication, consented and limited profile sharing by passenger



Kerb to Boarding gate journey with automated passenger validation across various touch points through "Biometric Framework"



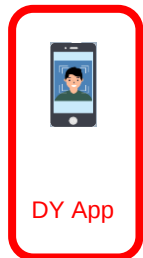
Technology:

Biometric technology for paperless, Contactless and Digital travel experience at the Airport.

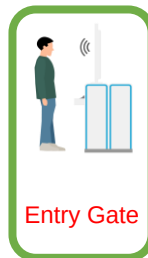
Need not show tickets, boarding passes or physical Identity cards at various check points at the Airport



Reduced queue waiting times, faster processing times, Contact-less, safer and simpler processes



DY App



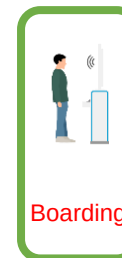
Entry Gate



Self Bag Drop



Pre-Security



Boarding

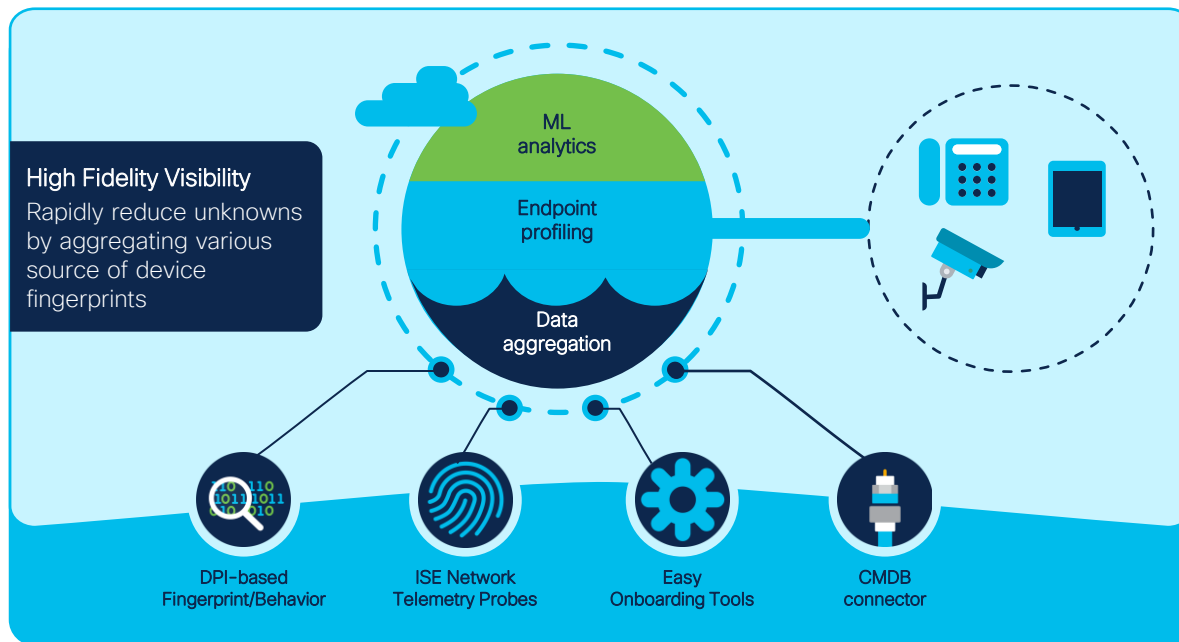


DigiYatra

Biometric

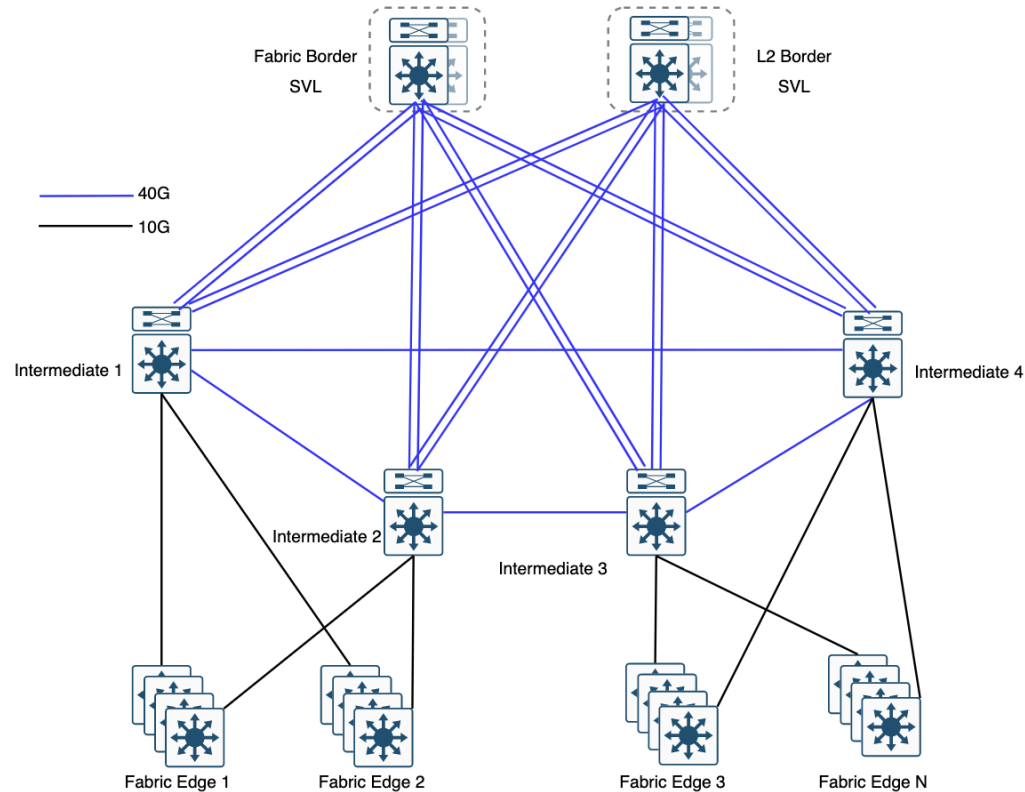
Airport Systems

Next-generation endpoint visibility with Cisco AI End Point analytics powered by network driven deep packet inspection

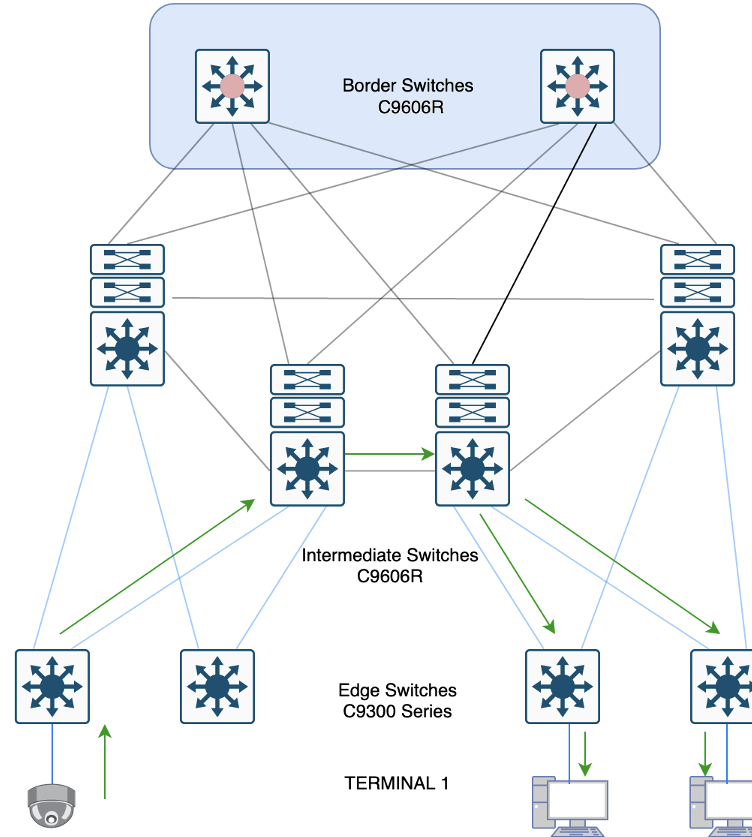


Using machine learning, DPI, and integrations, Cisco AI Endpoint Analytics provides **fine-grained endpoint identification and labelling** not previously possible.

L2 VNI Network for External Connectivity



Multicast for CCTV Network





Cisco SD-Access @ Blum

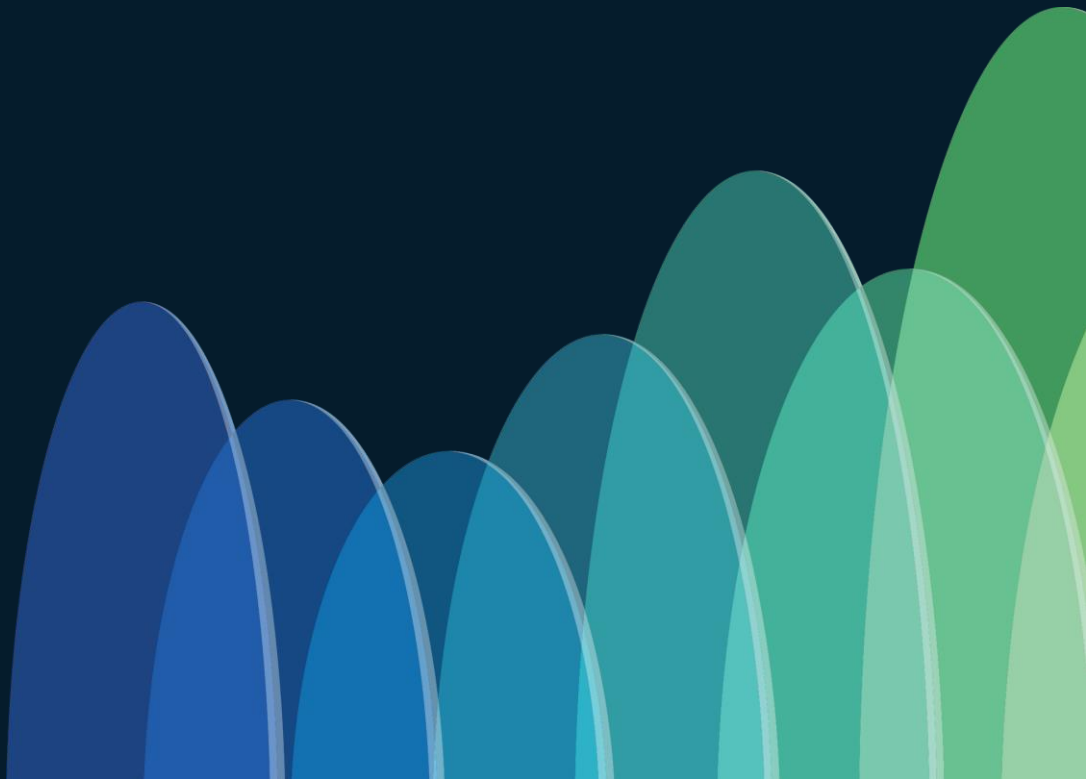
Joshua Hornig
Network Administrator



Agenda

- Who is Blum
- Our network before SD-Access
- SD-Access Project Overview
- Deploying SD-Access
- Conclusion

Who is Blum



Blum employees



9300

employees in the
Blum Group

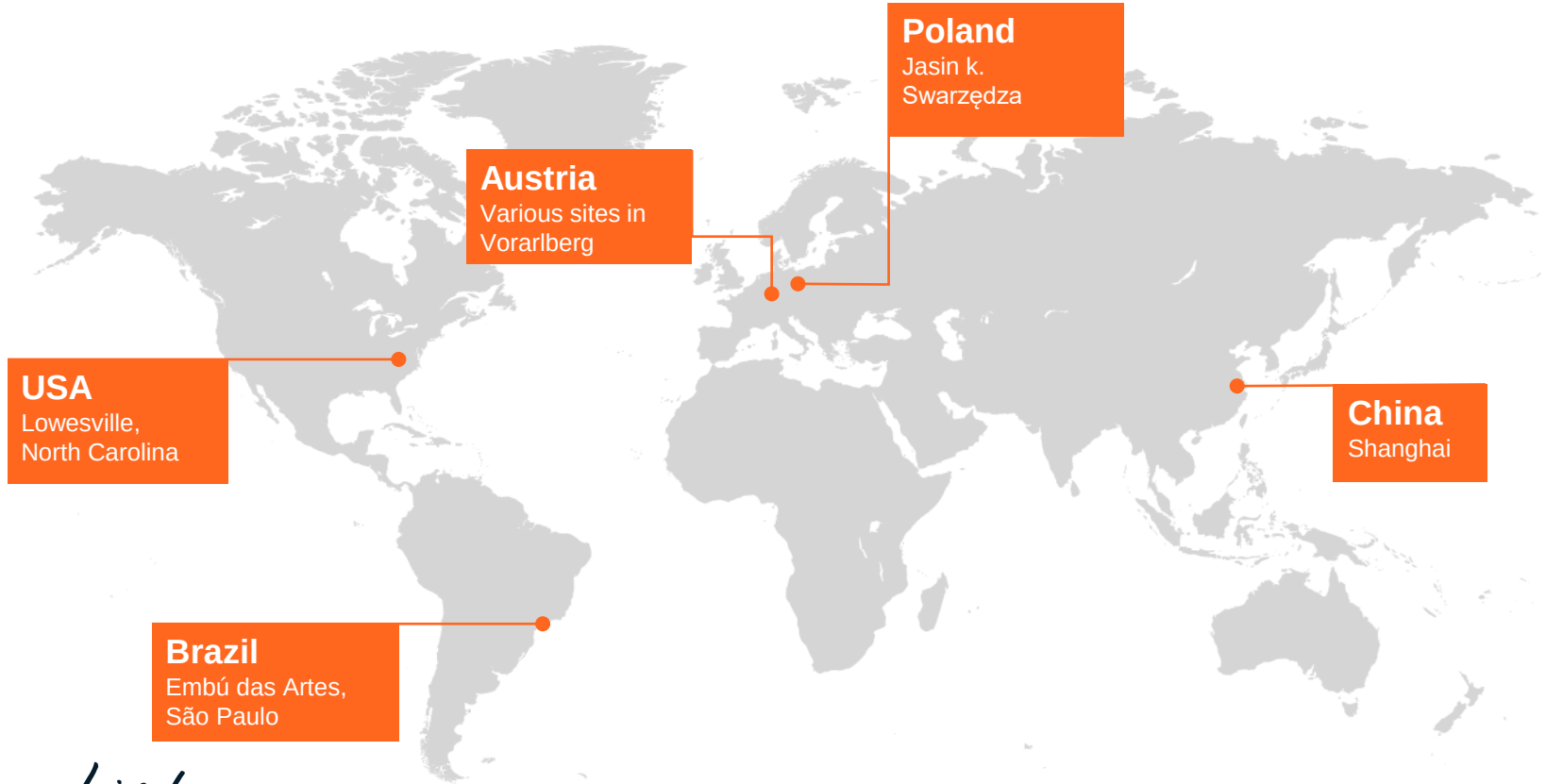


6600

of these employees are based
in Austria

(As of 1 July 2024)

Our production sites

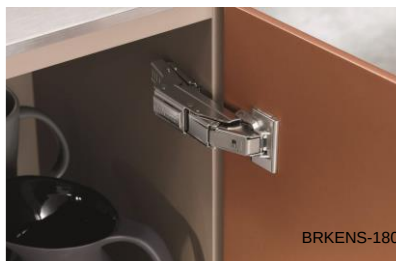
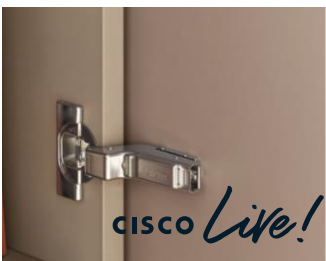


Hinges



For a wide range of applications

- Wood, glass and aluminium frame doors
- Thin or thick doors
- Special solutions such as blind corner and angled applications
- Hinges in onyx black



Lift systems

AVENTOS HKi



Exceptional design
is a given with the AVENTOS HKi
integrated lift system.

AVENTOS HF top



AVENTOS HS top



AVENTOS HL top



AVENTOS HK top



Be it for fronts that fold up, swing up and
over, lift up or pivot up – enhanced ease of
use is guaranteed.

AVENTOS HK-S



AVENTOS HK-XS



We have the right
solution, even for the
smallest of cabinets.

BRKENS-1803

Box systems



LEGRABOX

Turn your inspiration
into a reality

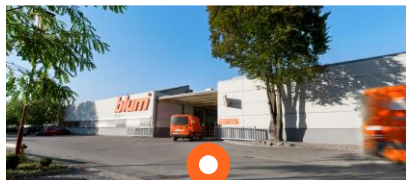
MERIVOBX

Let's create –
The box platform
for your ideas

TANDEMBOX

Efficient and simple

Plants in Austria



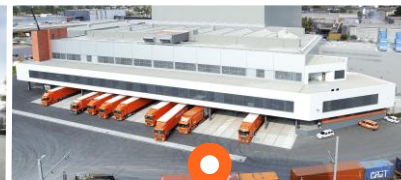
Plant 1
in Höchst



Plant 3
in Höchst



Plant 5
in Fussach



Plant 7
in Dornbirn



Plant 2
in Höchst



Plant 4
in Bregenz

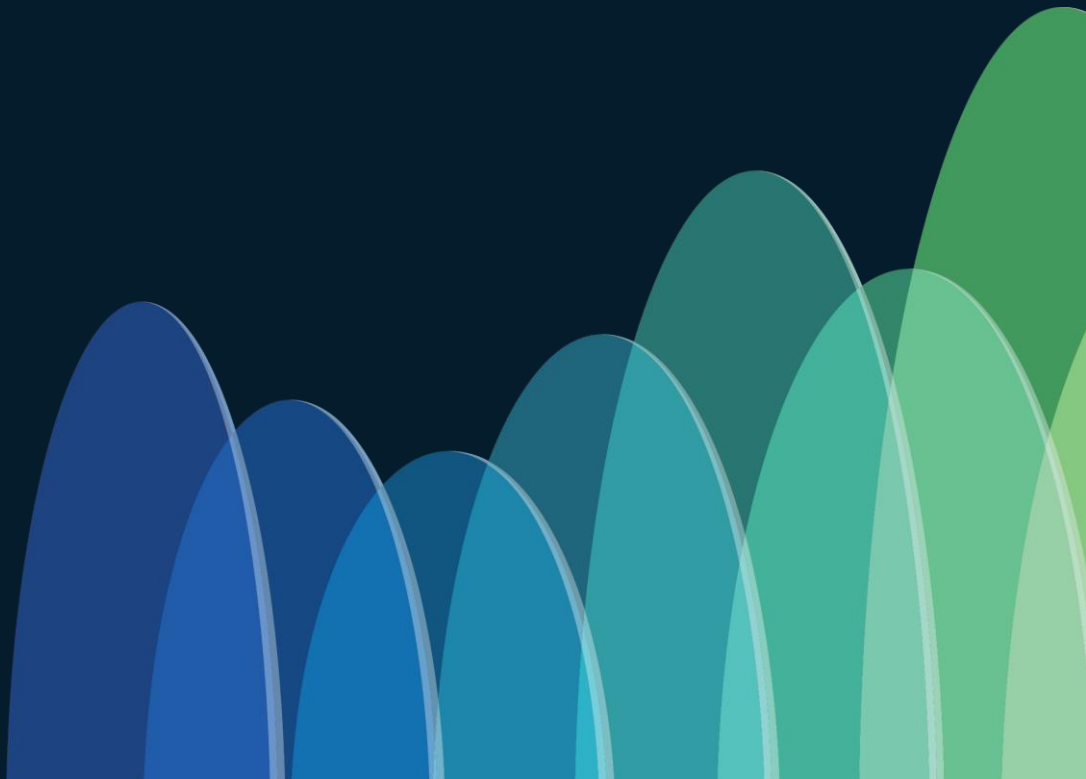


Plant 6
in Gaissau



Plant 8
in Dornbirn

Our network before SD- Access



Our Environment

70+ Sites

432 Switches

1683 AP's

6 WLC

7 ISE Nodes

10,000 Managed
MAC Addresses

16,500 Active
Wired Clients

7,500 Active
Wireless Clients

4 Network
Engineers

Clients in the Network

10,000
Windows Clients

1,000 Zero
Clients

650 Production
Machines

6,000 Industrial
Clients

850 Warehouse
Clients

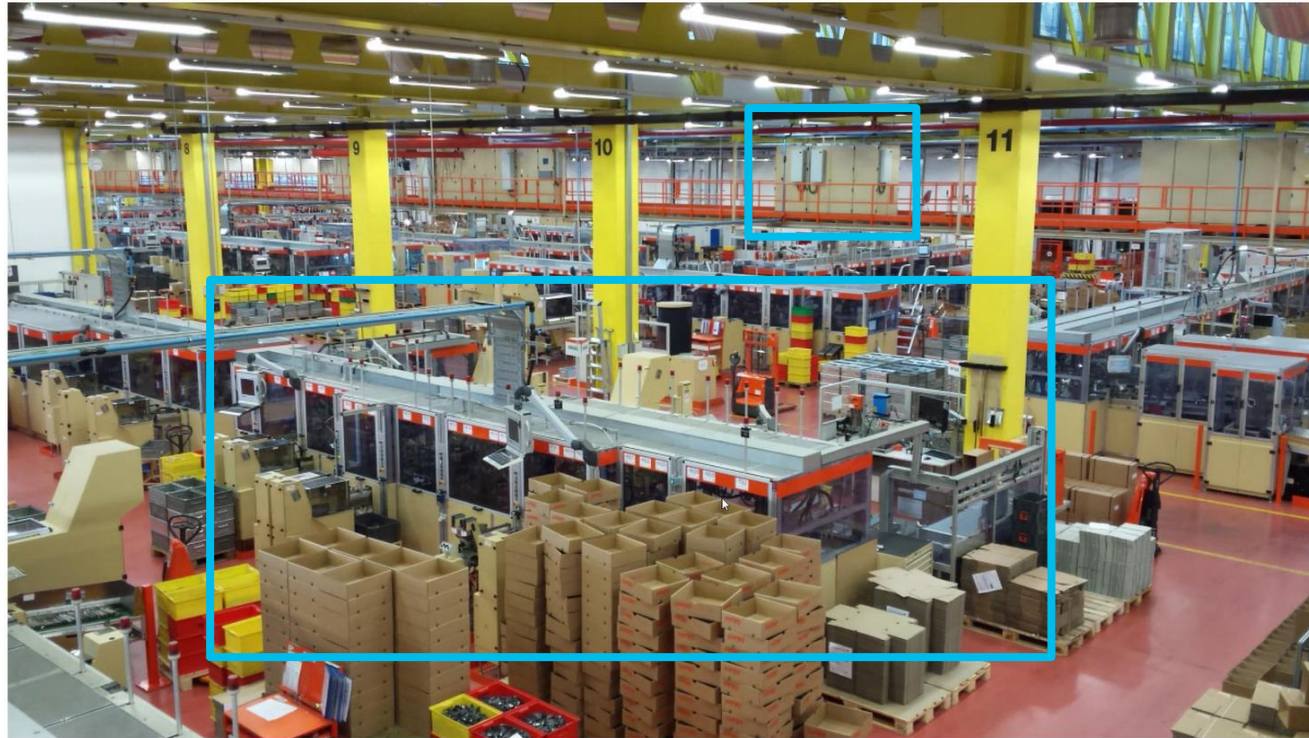
80 Machine
Movements per
Year

MAB/dot1x

11 Firewall
Clusters

850 Networks

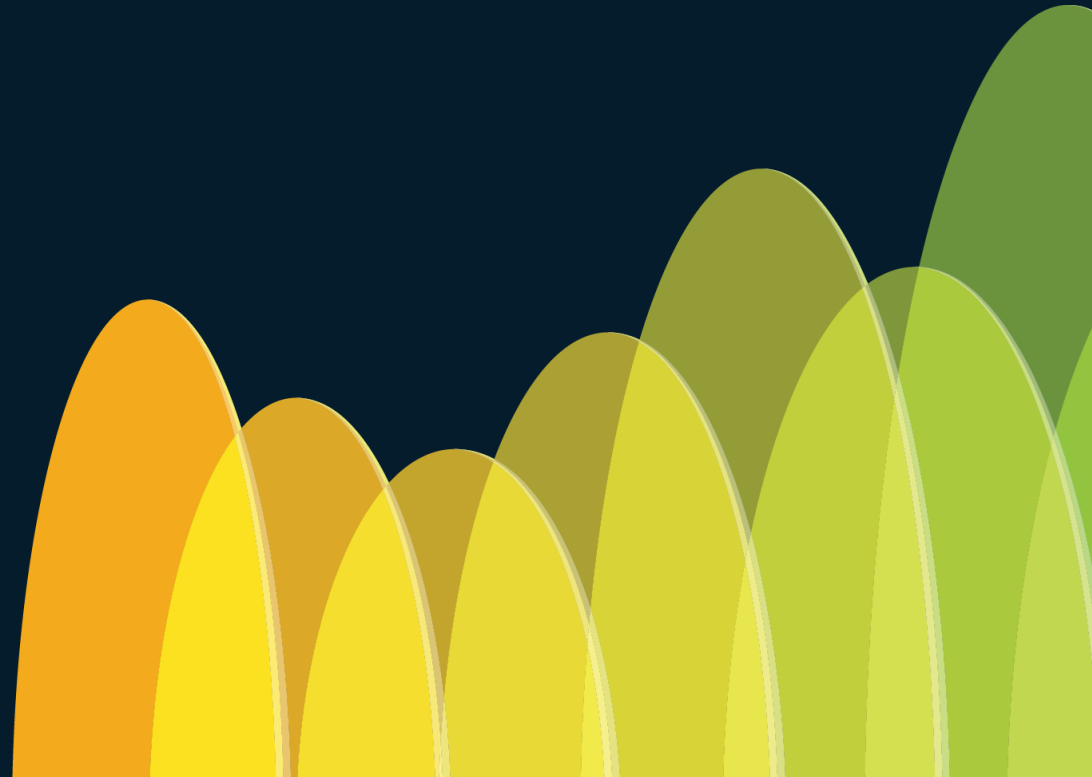
Clients in the Network – Machines



Clients in the Network – Machines



SD-Access Project Overview



Review: 802.1x/MAB Project

Enabled ~ 25000 Ports with Open Authentication

2 Months of collecting data from:

- ISE Endpoints (Profiler enabled)
- Nedi (Open Source Network Inventory)
- Catalyst Center
- Hard and Software Management

Review: 802.1x/MAB Project

1 Excel with all the Data

Grouped Clients

Find a Responsible Person for the Group of Devices

Details in an easy-to-use GUI that uses API of ISE

Recreate Excel

If all clients are managed or no information is found change to closed mode

Why SD-Access

Simplify Operation

- Mobility of Machines
- Simple onboarding
- Safe stretching of Prefixes across all plants

Automation

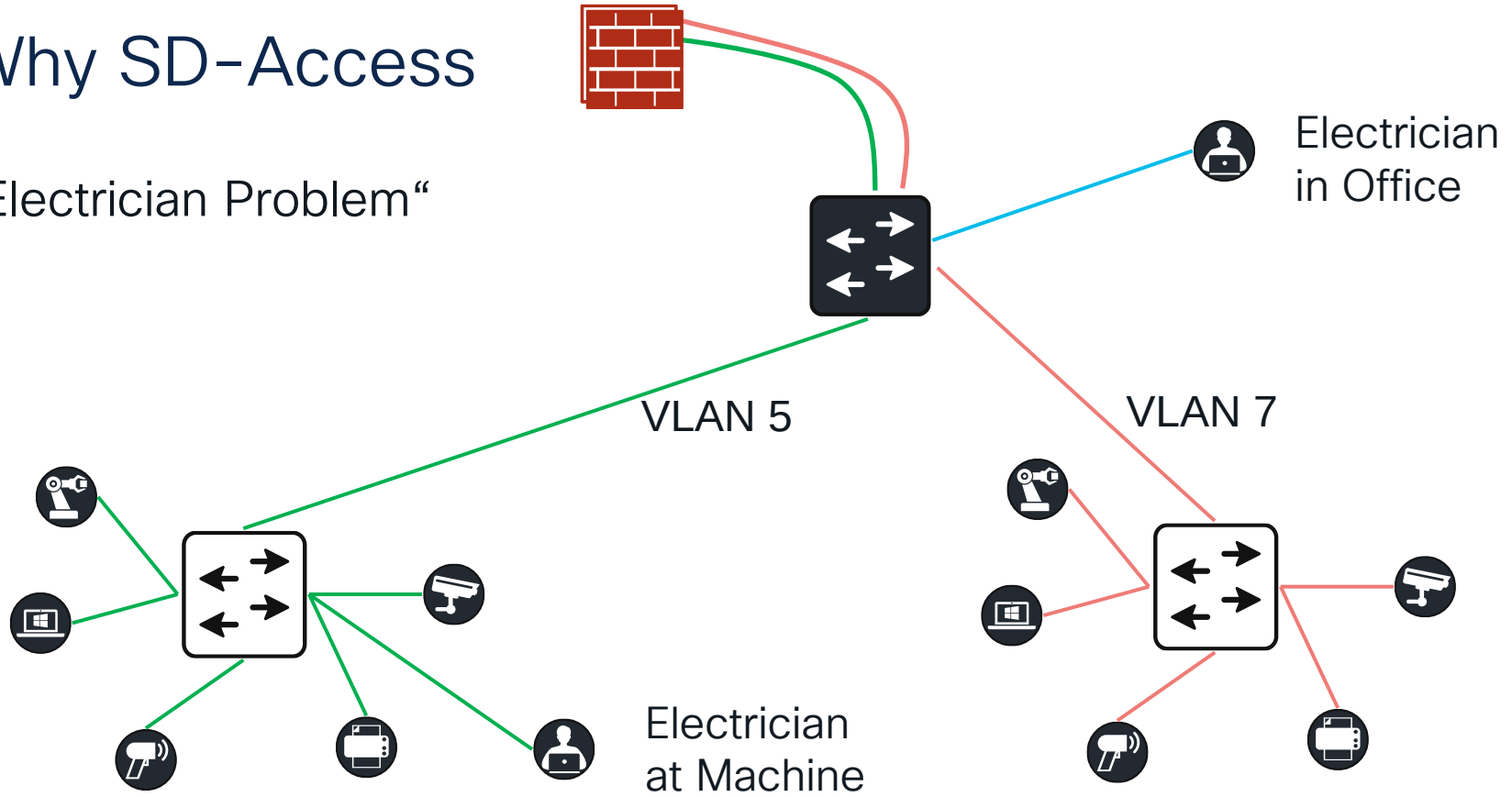
- Automating VLAN's is very hard
- With SD-Access full automation via IPAM/DCIM

Segmentation

- Easy Introduction of VRF's
- Platform for Microsegmentation
- Solve the „Electrician Problem“

Why SD-Access

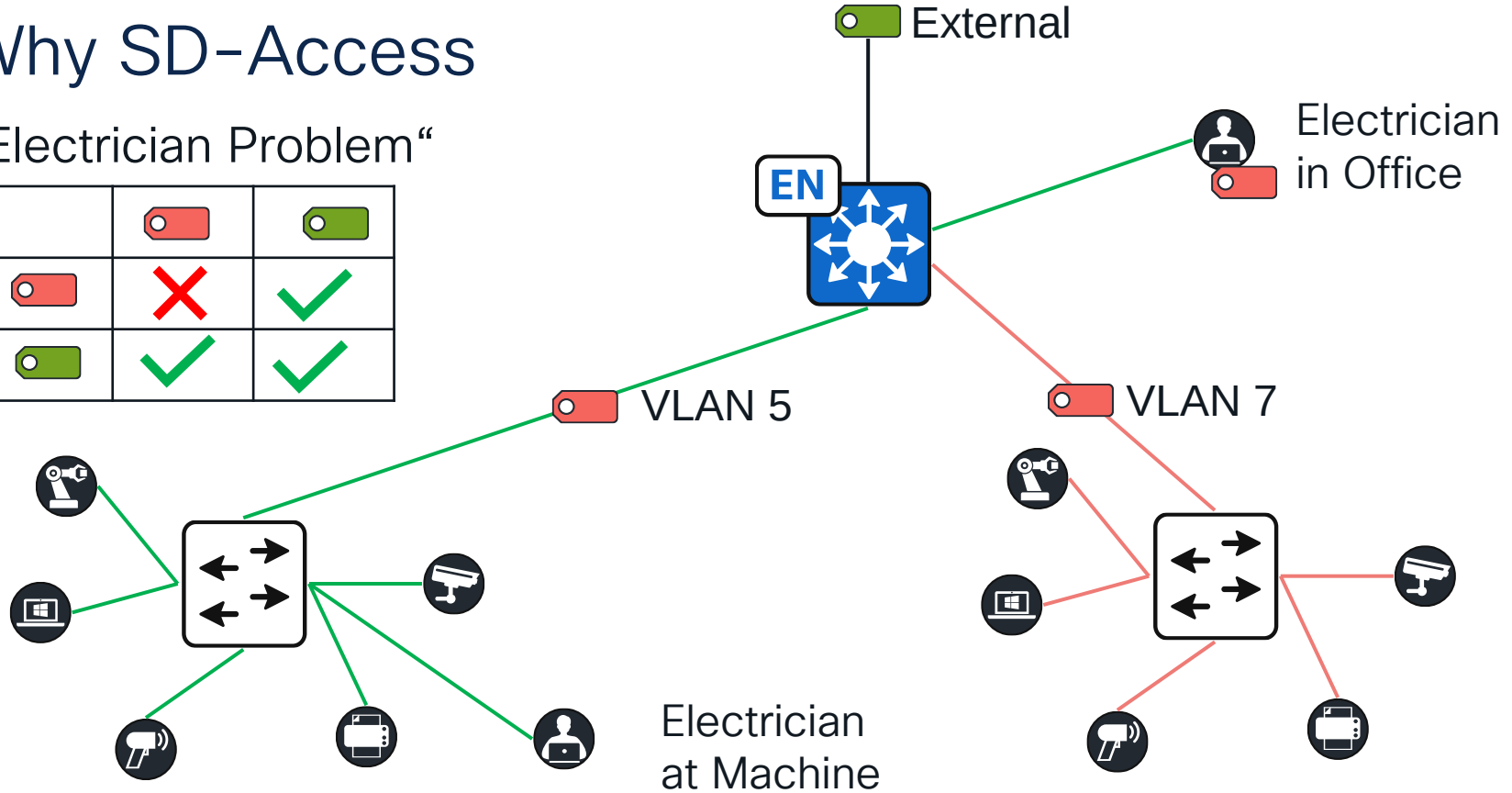
„Electrician Problem“



Why SD-Access

- „Electrician Problem“

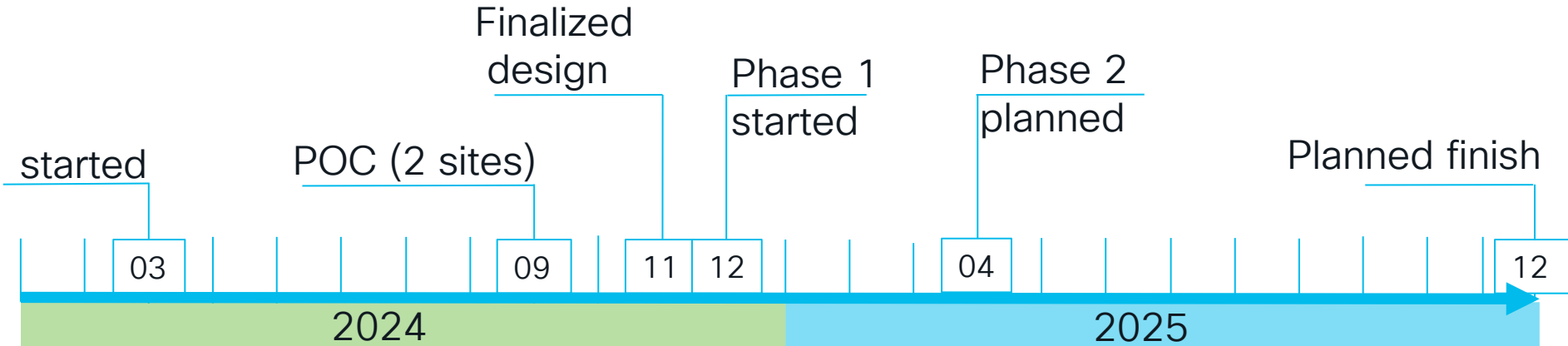
		
		
		



SD-Access Project

This is my Second SD-Access Project

Idea started when I moved to Blum



SD-Access Project

Discussions and Design together with Peter Fuchs (Cisco) and Evelyn Riha (NTS, Cisco Partner)

5 Days Workshop onsite

Status Update calls Every 2 Weeks

Active Webex space between all parties for quick questions

Implementation done by Blum Network Team

SD-Access Project

- 7 Plants in SD-Access 3 Sites in SD-Access
- 160 Anycast Gateways
- 553 L2VN's
- 23 Fabric Devices

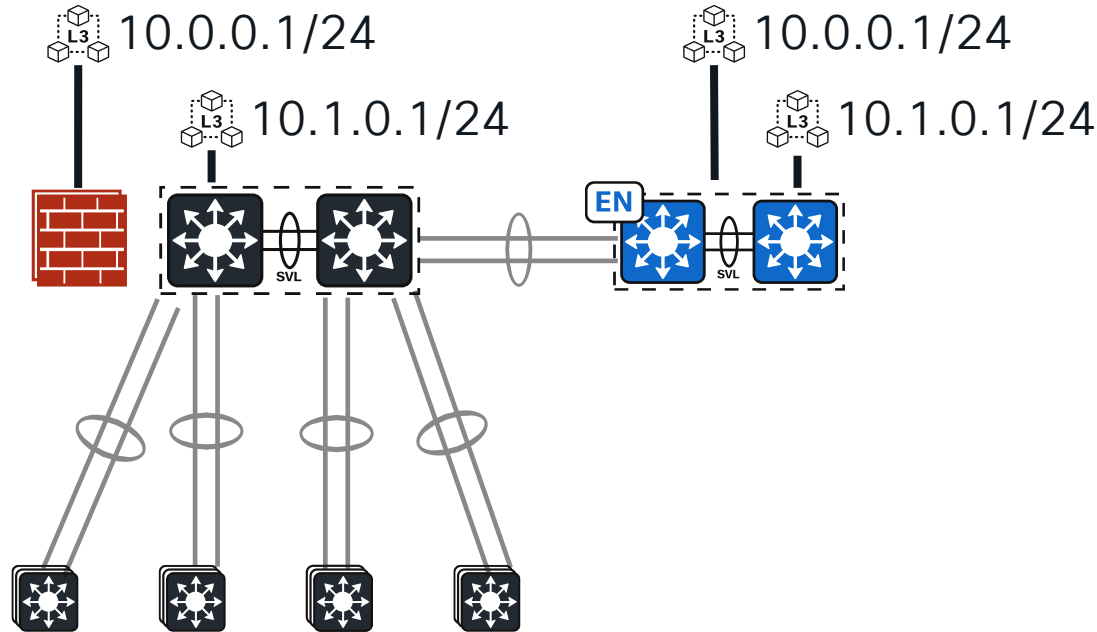
80 % Finished of Phase 1

Migrating to SD-Access

SD-Access Project

Phase 1

```
%IP-4-DUPADDR: Duplicate address 10.6.250.1 on Vlan1699, sourced by 0000.0c9f.f253
```



Downtime 4-6 Seconds,
depends on client (ARP
cache)

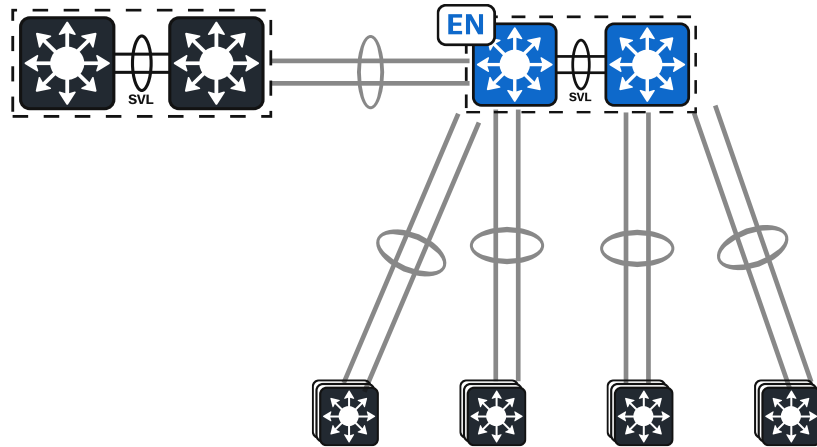
Faster is Possible

Done without
Maintenance Window for
95%

Automated Warehouses
With Maintenance
Window

SD-Access Project

Phase 1



Relocate Portchannels to Edge Node

Reconnect half of the Ports

Shutdown second half

Reconnect interface will come up ~ 1 sec.

SD-Access Project

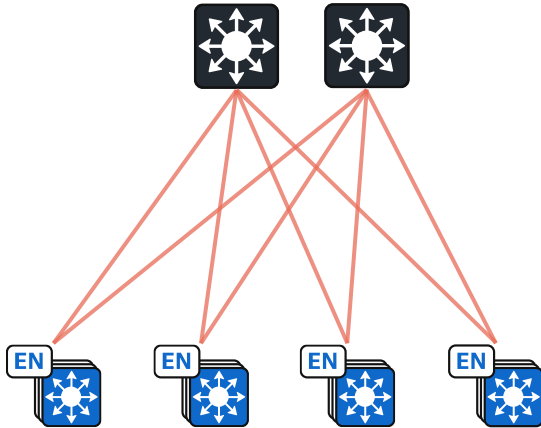
Phase 2 - Future

Factory Default Accessswitches

LAN Automate and onboard as Edge Node

Remove Edge Node Role from Distribution Layer

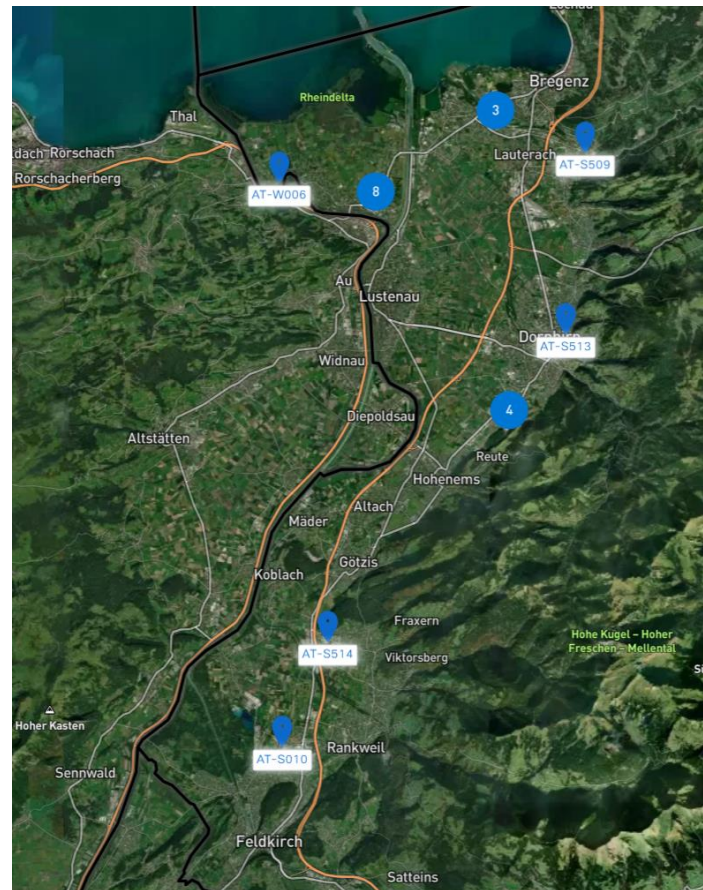
Split Stackwise Virtual



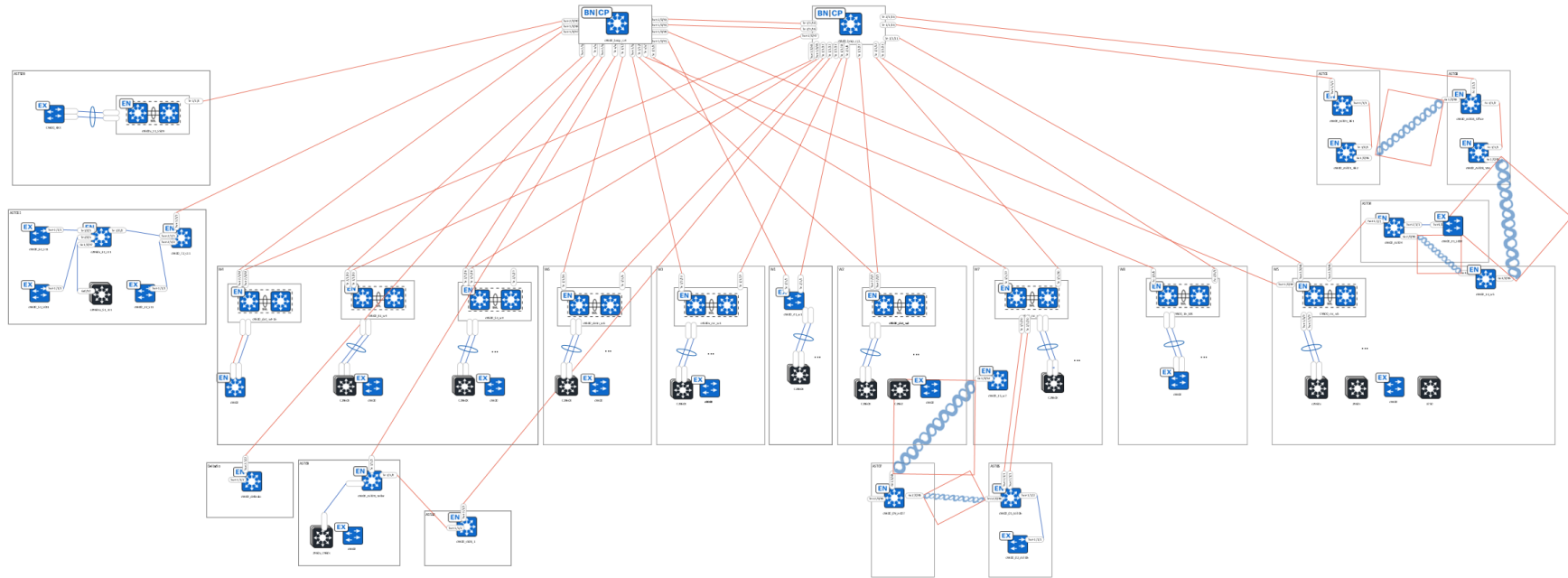
1 Site to rule them all

Multiple Physical Locations in Single SD-Access Site

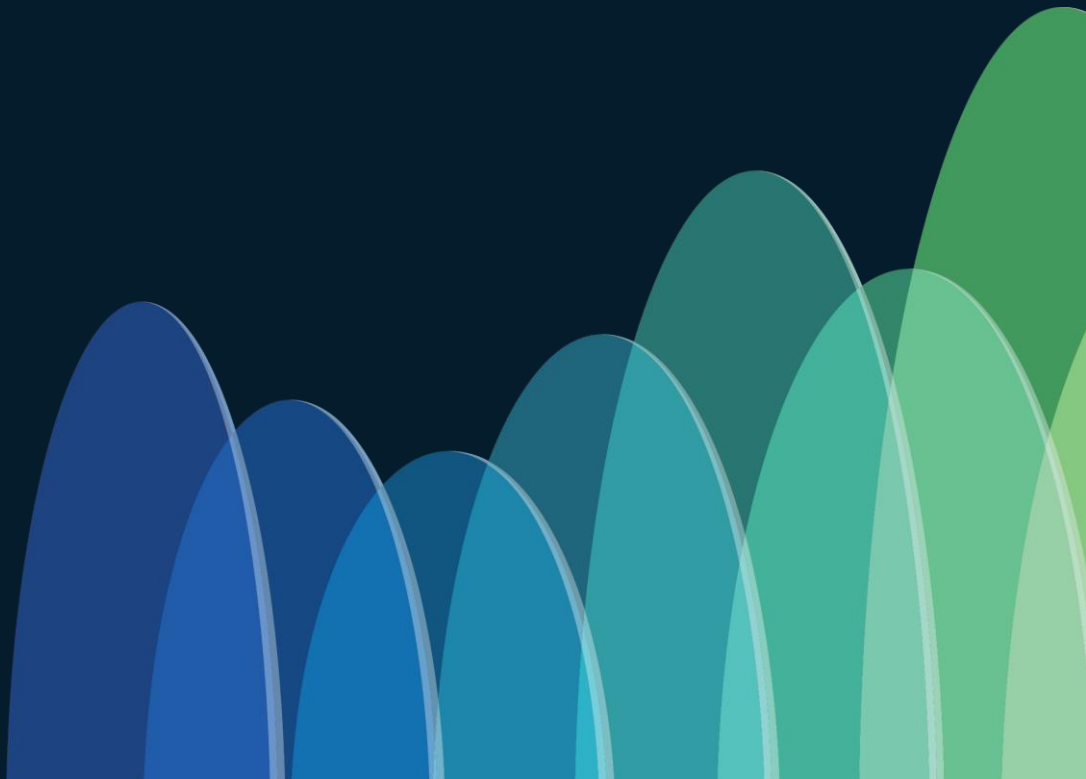
- 10 Bigger Production Plants
- 10 Smaller Sites
- All redundant connected via Darkfiber+DWDM and directional Radio
- Distances of 25km inside of the Fabric



Multiple Physical Locations in Single SD-Access Site



Automation



Our Base

Netbox is used as documentation

Started to use its webhooks for automation via Microsoft System Center Orchestrator

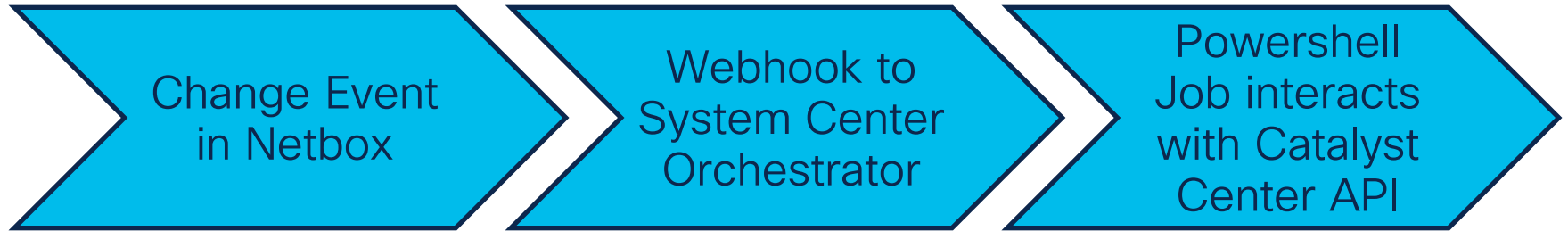
Using custom Powershell scripts and modules

Automation: past, presence, ...

- DHCP Reservations
- Static DNS
- DHCP Scopes (Firewall and Windows Server)
- Firewall Objects, Interfaces, Groups
- Switch SVI Config
- Switch OSPF announcements
- Switch Access Interface
- Handover including Fusion Devices
- Underlay
- SD-Access Anycast Gateway
- SD-Access L2VN
- Portchannel towards Access Switches

Automation

Example of IP Address



Powershell Snippet

```
BlumCatalystCenter.ps1 > > BlumCatalystCenter.ps1 > > function Invoke-BlumCatalystCenterIPPool {
68 function Invoke-BlumCatalystCenterIPPool {
69     param (
70         [Parameter(Mandatory = $true)] $snapshot,
71         [Parameter(Mandatory = $true)] $data,
72         [Parameter(Mandatory = $true)] $cc_address,
73         [Parameter(Mandatory = $true)] $cc_user,
74         [Parameter(Mandatory = $true)] $cc_pw,
75         [Parameter(Mandatory = $true)] $netbox_token,
76         [Parameter(Mandatory = $true)] $netbox_address
77     )
78     if ($null -eq $snapshot.prechange.assigned_object_id -and $null -eq $snapshot.postchange.assigned_object_id) { return }
79     Import-Module CatalystCenter -Force
80     $catalystCenterConnection = Open-CatalystCenterConnection -Username $cc_user -Password $cc_pw -Address $cc_address
81     $netboxConnection = Open-NetboxConnection -Token $netbox_token -Address $netbox_address
82     if ($snapshot.prechange.assigned_object_id -ne $snapshot.postchange.assigned_object_id -and $null -ne $snapshot.prechange.assigned_object_id -and $null -ne $snapshot.postchange.assigned_object_id) {
83         $addit = $true
84         $delete = $true
85     }
86     elseif ($null -ne $snapshot.postchange.assigned_object_id) {
87         $addit = $true
88     }
89     elseif ($null -ne $snapshot.prechange.assigned_object_id -and $null -eq $snapshot.postchange.assigned_object_id) {
90         $delete = $true
91     }
92     else {
93         $addit = $true
94     }
95     if ($addit) {
96         if ($data.assigned_object.device.name -eq "AT-SDA-Fabric") {
97             $device = Get-NetboxDevice -NetboxConnection $netboxConnection -DeviceID $data.assigned_object.device_id
98             $prefix = (Get-NetboxPrefixByAddress -NetboxConnection $netboxConnection -Address $data).results
99             $site = (Get-CatalystCenterSites -CatalystCenterConnection $catalystCenterConnection).response | Where-Object name -Match "BAU Darkfiber Connected"
100             $siteName = Get-BlumAutomationPrefixByPrefix -Prefix $prefix -CatalystCenterConnection $catalystCenterConnection -netboxConnection $netboxConnection
101             $ipPoolName = ($prefix.site.name + "-" + $prefix.description.Replace(" ", "_"))
102             $vlanName = $prefix.vlan.name.replace(" ", "_").Replace("/", "-")
103             $scalableGroupName = $null
104             $multipleIPtoAC = $false
105             if ($null -ne $prefix.tags | Where-Object name -Match "CTS:") { ($scalableGroupName = ($prefix.tags | Where-Object name -Match "CTS:").name.replace("CTS:ADMIN:", "")) }
106             if ($null -ne ($prefix.tags | Where-Object slug -Match "sdamultipletomac")) { $multipleIPtoAC = $true }
107             $existingPool = Get-CatalystCenterSdaAnycastGateway -CatalystCenterConnection $catalystCenterConnection -VlanID $prefix.vlan.id
108             if ($null -eq $existingPool) {
109                 Add-CatalystCenterIPSubpool -CatalystCenterConnection $catalystCenterConnection -Name $ipPoolName -Prefixlength ($prefix.prefix -split "/")[1] -Subnet ($prefix.prefix -split "/")[0] -Gateway ($data.address -split "/")[0] -SiteID $site
110             }
111             else {
112                 Set-CatalystCenterSdaAnycastGateway -CatalystCenterConnection $catalystCenterConnection -ID $existingPool.id -Fabricid $existingPool.fabricid -virtualNetworkName $prefix.vrf.name -IPPoolName $ipPoolName -VlanID $prefix.vlan.id -VlanName
113             }
114         }
115     }
116 }
117 if ($delete) {
118     $oldif = Get-NetboxDcInInterface -NetboxConnection $netboxConnection -InterfaceID $snapshot.prechange.assigned_object_id
119 }
120 if ($oldif.device.name -eq "AT-SDA-Fabric") {
121     $device = Get-NetboxDevice -NetboxConnection $netboxConnection -DeviceID $oldif.device_id
122     $prefix = (Get-NetboxPrefixByAddress -NetboxConnection $netboxConnection -Address $data).results
123     $site = (Get-CatalystCenterSites -CatalystCenterConnection $catalystCenterConnection).response | Where-Object name -Match "BAU Darkfiber Connected"
124     $ipPoolName = ($prefix.site.name + "-" + $prefix.description.Replace(" ", "_"))
125     $subpool = (Get-CatalystCenterIPSubpool -CatalystCenterConnection $catalystCenterConnection -SiteID $site.ID).response | Where-Object groupname -eq $ipPoolName
126     Remove-CatalystCenterSdaPool -CatalystCenterConnection $catalystCenterConnection -SiteNameHierarchy $device.description -virtualNetworkName $prefix.vrf.name -ipPoolName $ipPoolName
127     Remove-CatalystCenterIPSubpool -CatalystCenterConnection $catalystCenterConnection -SubPoolID $subpool.id
128 }
129 }
130 }
```

Automation

Servers Device Credentials **IP Address Pools** Wireless Telemetry Security and Trust

Catalyst Center supports IPv4 and IPv6 dual-stack IP address pools.



Subnet Type **All** IPv4 Dual-Stack

IP Address Pools (0)

[Take a Tour](#)



0 Selected [Reserve IP Pool](#) [More Actions](#) ▾

As of: Feb 12, 2025, 11:24



☐	Name ▲	Type	IPv4 Subnet	IPv4 Used ⓘ	IPv6 Subnet	IPv6 Used ⓘ	Inherited from ⓘ	Actions
			10.1.10					

No data to display

Conclusion

Challenges

- Identify if SD-Access is a suitable Solution
- Adapt Machine Network Design to SD-Access
- Migration without Maintenance Windows

Success Factors

- Collaboration between NTS (Cisco Partner), Cisco and Blum
- Collaboration between Blum IT and Industrial IT

SD-Access network design challenges

Not all Machines are in a /24 -> ongoing Project

SD-Access supports only 1000 IP Pools

~1500 Machines statically configured

Mobility to China, Poland and US without changing IP's is still required

One /13 for all machines will be created in parallel

Cisco extends IP-Pool amount to 1500 in a future release

Clients will be migrated to DHCP

When moving to different country a /24 mask will be provided



Journey with Cisco SD-Access

Ricardo Pinheiro, Infrastructure Manager

IKEA Industry



To create a better everyday life for the many people

As an IKEA in-house manufacturing business, we create competitive advantages that move and challenge the total IKEA value chain.



Sawmills, boards, furniture components and furniture production



~15,000 co-workers
30 production units,
in 7 countries



>100 M pcs. produced/year

Business oriented

Security



Scalability



Reduced OPEX



Reduced time to production



CISCO *Live!*

Support tickets
decrease by
50%

VLANs
decrease by
60%

Micro segmentation

With SD-Access we were able to fulfill the security requirement of hundreds of production segments per unit.

No subnetting needed

It can become very hard to manage/predict subnet sizes. With Security Group Tags this issue is solved.

Self service

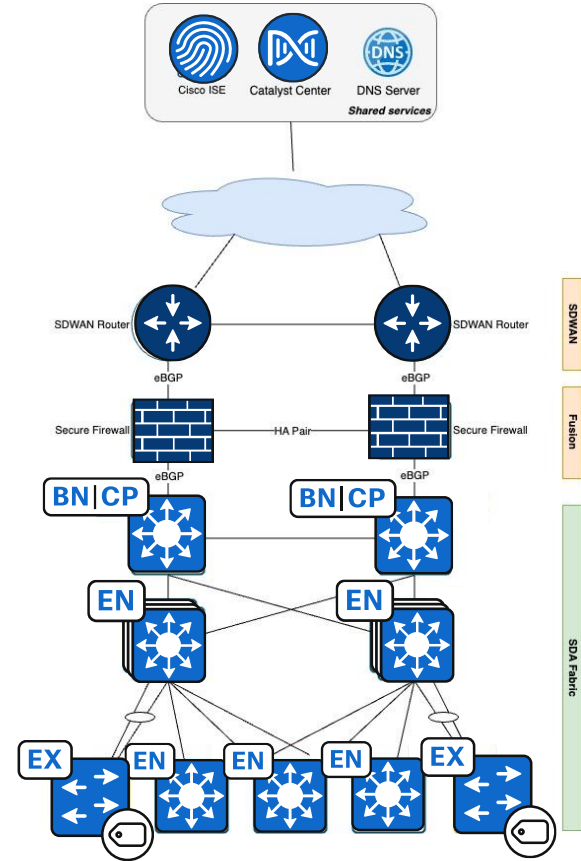
SGTs allow the easy automation and makes network management widely available in the organization, eg. Maintenance Technician.

Simplified connection

Maintenance technician is fully sufficient to commission any new devices and/or production lines. No need to involve any network personal.

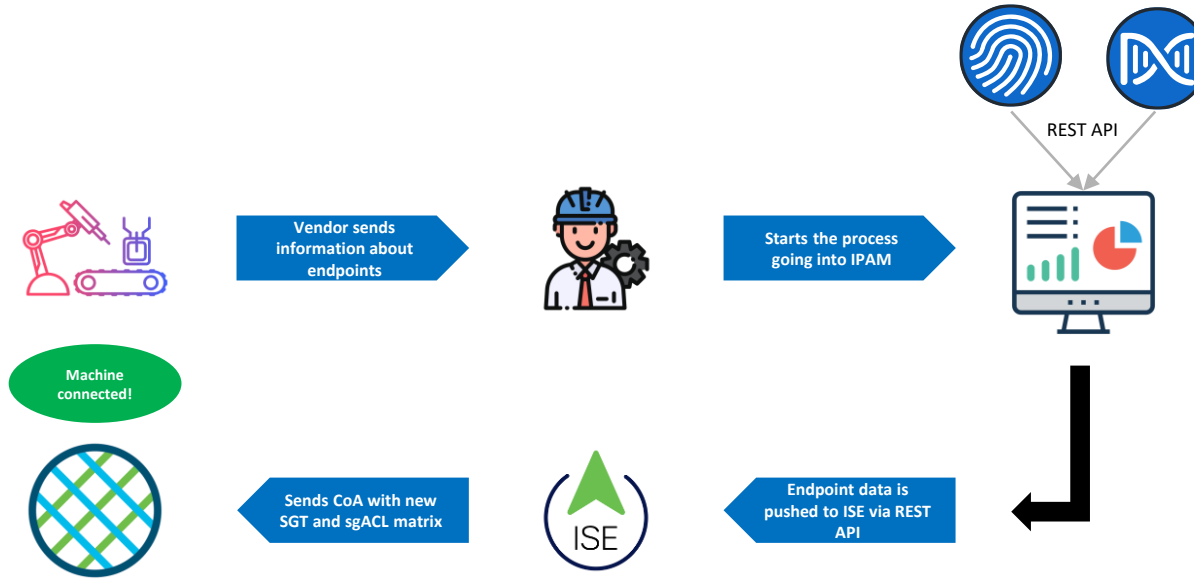
High level design

- Traditional SD-Access Fabric with Catalyst 9K hardware:
 - 9500 as Border and Control Plane
 - 9300 as Edge
 - IE3400 as Policy Extended Nodes
- eBGP towards different vendor SDWAN solution
- Cisco Secure Firewall HA pair as fusion router
- Intermediate nodes (distribution) with Edge role
- Cisco IE 3400 for the OT Cells as Policy Extended Nodes
- Local workloads running also with eBGP for low latency access for OT systems



Real use case

OT engineer receives task to connect new production line in shopfloor:



No network technician involvement!

The same process is possible on a replacement as well.

Brownfield implementation

• Step 1 – Preparation

- Underlay IP information prepared
- All IP space added in CatC
- All SVIs were migrated from Core to FW
- Confirmation that whole devices are supported SKUs, in our case - 9300, 9500 and IE3400 (PEN)

• Step 2 – Split brain the core

- Core 2 and DIS SVL secondary switch were erased
- All devices added to CatC
- Fabric was built assigning proper roles
- All legacy VLANs were created as L2VNs and added to L2 Handoff

At this moment, the fabric is up and running and all the devices continue to operate since all access layer is still connected to active “legacy” network.

• Step 3 – Flap traffic to fabric side

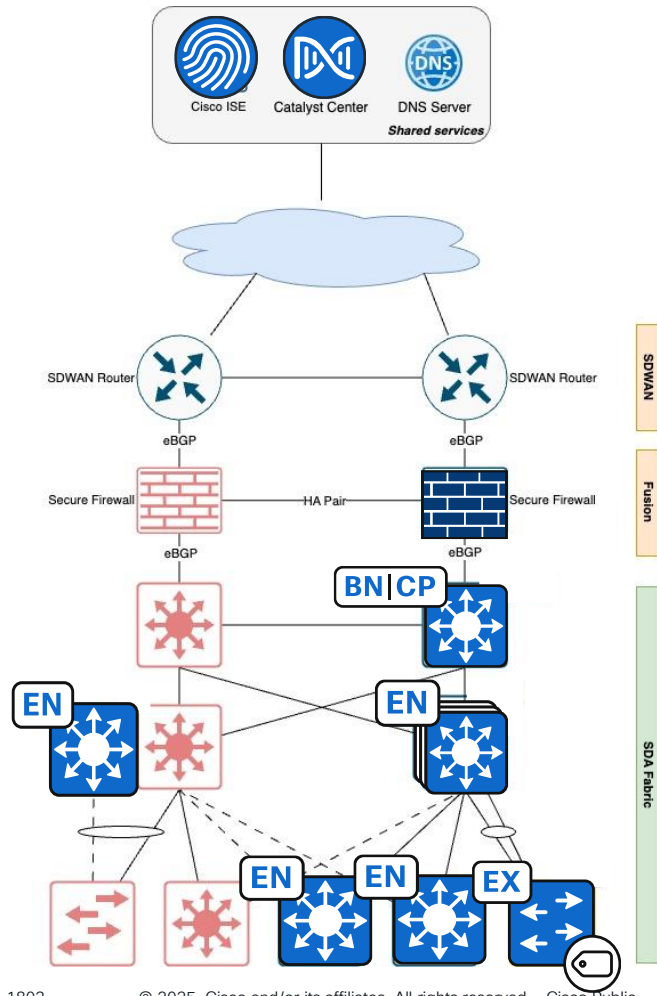
- An empty Edge switch was brought up and connected to the fabric to validate everything is operational
- At this moment we flapped all interfaces between DIS SVL Stack members to move the traffic from non Fabric DIS to Fabric DIS.

• Step 4 – Convert the whole core layer to SD-Access fabric

- Core 1 and other DIS Stack were converted to SD-Access devices with proper roles
- All access layer is now connected over SD-Access fabric as L2 switches with

• Step 5 – Convert Access switches to Edges

- All access switches were converted according to agreed maintenance windows and production lunch breaks
- All these Edges still run a mix of L2VNs from the legacy network, and some endpoints already in Anycast Gateways



Journey and future

Feb 2023	Oct 2023	Jun 2024	2025+	
Cisco CPoC	PoC	First Production site	Rollout	Future
• Business intent presentation • Requirements set • Sales and CX collaboration • Initial design agreed • Customer Proof-of-Concept Lab	• Dedicated hardware order • Discussion with internal OT teams • Replication of CPoC in manufacturing dev. Center in Poland • First SD-Access fabric in IKEA Industry	• Agree with Cisco CX on dates for on site migration • Design/plan all possible migration scenarios • Fully enabled SD-Access (all Edges converted) • First site running SD-Access for 6+ months	• Next two sites with priority due to business need are defined • Migration plans are being created for those two sites • Full IKEA Industry network running on Cisco SD-Access	• <i>Migrate from Wireless OTT to fabric enabled wireless</i> • <i>Common policy across domains (Cisco SSE, Cisco SDWAN)</i> • <i>Leverage the new segment type (SGTs) on many other tools</i>



Q&A

Köszí!

Dziękuję!

Tack!

Thank you!

謝謝!

Obrigado!

Ďakujem!

Děkoju!

Webex App

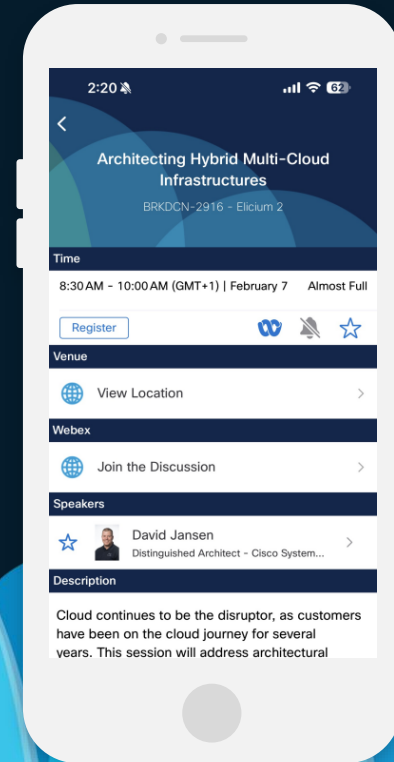
Questions?

Use the Webex app to chat with the speaker after the session

How

- 1 Find this session in the Cisco Events 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 February 28, 2025.



Fill Out Your Session Surveys



Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)



All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the 'Participant Dashboard'



Content Catalog

Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- 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. Sessions from this event will be available from March 3.



Thank you

