

GO BEYOND

Campus Zero-Trust:

Transformez votre réseau pour le rendre plus programmable, sécurisé et modulaire (CI)

Thomas Matzeu,

tmatzeu@cisco.com

Sébastien Fernandez,

sebastfe@cisco.com

Technical Solutions Architect

Technical Solutions Architect

Track 3 - Session 2



Agenda

- Challenges & Limitations of Traditional LANs Campus
- Fabric IP & Fabric SDA
- Native Zero-Trust
- Conclusion

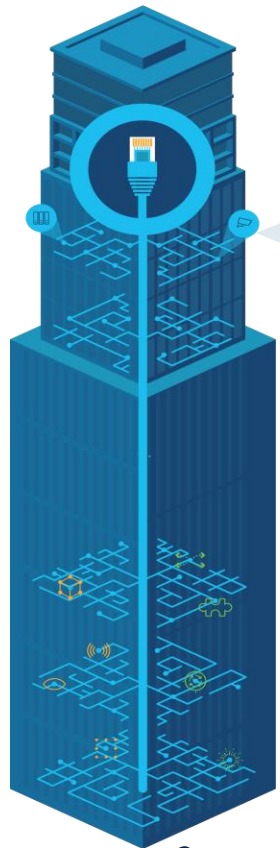


Agenda

- Challenges & Limitations of Traditional LANs Campus
- Fabric IP & Fabric SDA
- Native Zero-Trust
- Conclusion

Challenges & Limitations of Traditional LANs Campus

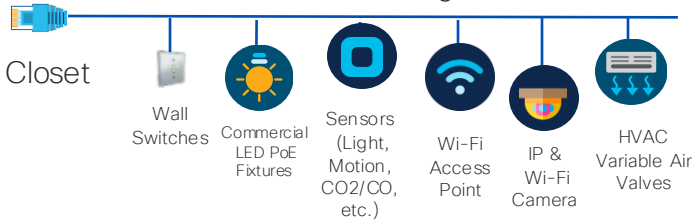
90W UPOE+ Standard driving new IT/OT Use Cases



Cisco/ Partner Cloud Services



Smart Building Devices



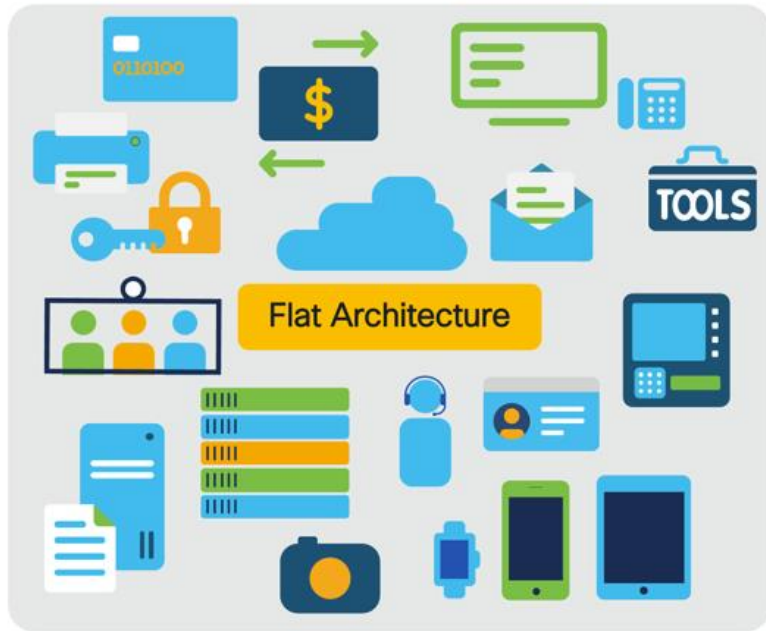
<p>POE Displays</p> <p>UHD IP Cameras</p> <p>HVAC VAV's</p>			<p>USB-C Power + Data</p>
<p>High Power PoE End-points</p>	<p>Daisy-chaining (Cost saving with 90W)</p>	<p>UPOE Pass-through (for extended reach 60W)</p>	<p>USB-C power (laptop charging + data)</p>



Challenges & Limitations of Traditional LANs Campus

Transition from Flat Network to Zero Trust Segmentation

Current State



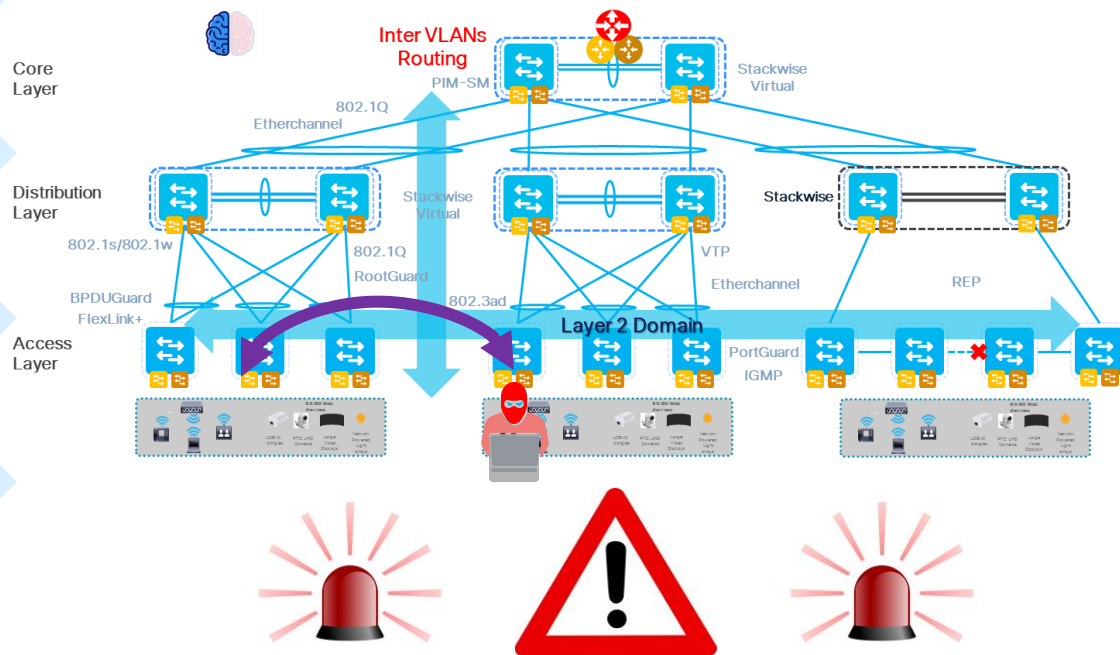
Challenges & Limitations of Traditional LANs Campus

Urbanization & Mobility

High Availability & Reliability

Programmability & Agility

Security & Zero-Trust



Challenges & Limitations of Traditional LANs Campus

Urbanization & Mobility

High Availability & Reliability

Programmability & Automation

Security & Zero-Trust

Needs for Level 2 Services
without the constraints and
difficulties induced by Level 2
Architectures



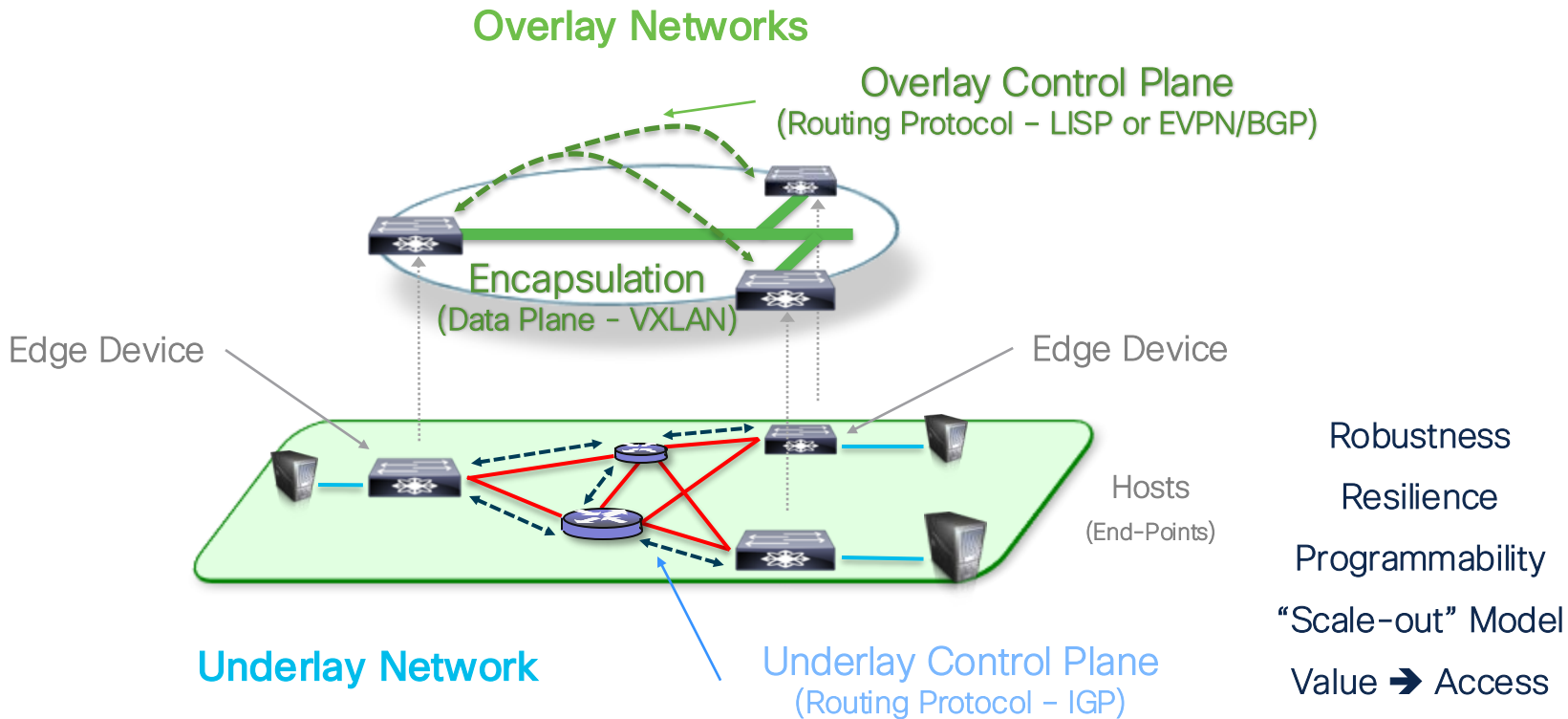


Agenda

- Challenges & Limitations of Traditional LANs Campus
- **Fabric IP & Fabric SDA**
- Native Zero-Trust
- Conclusion

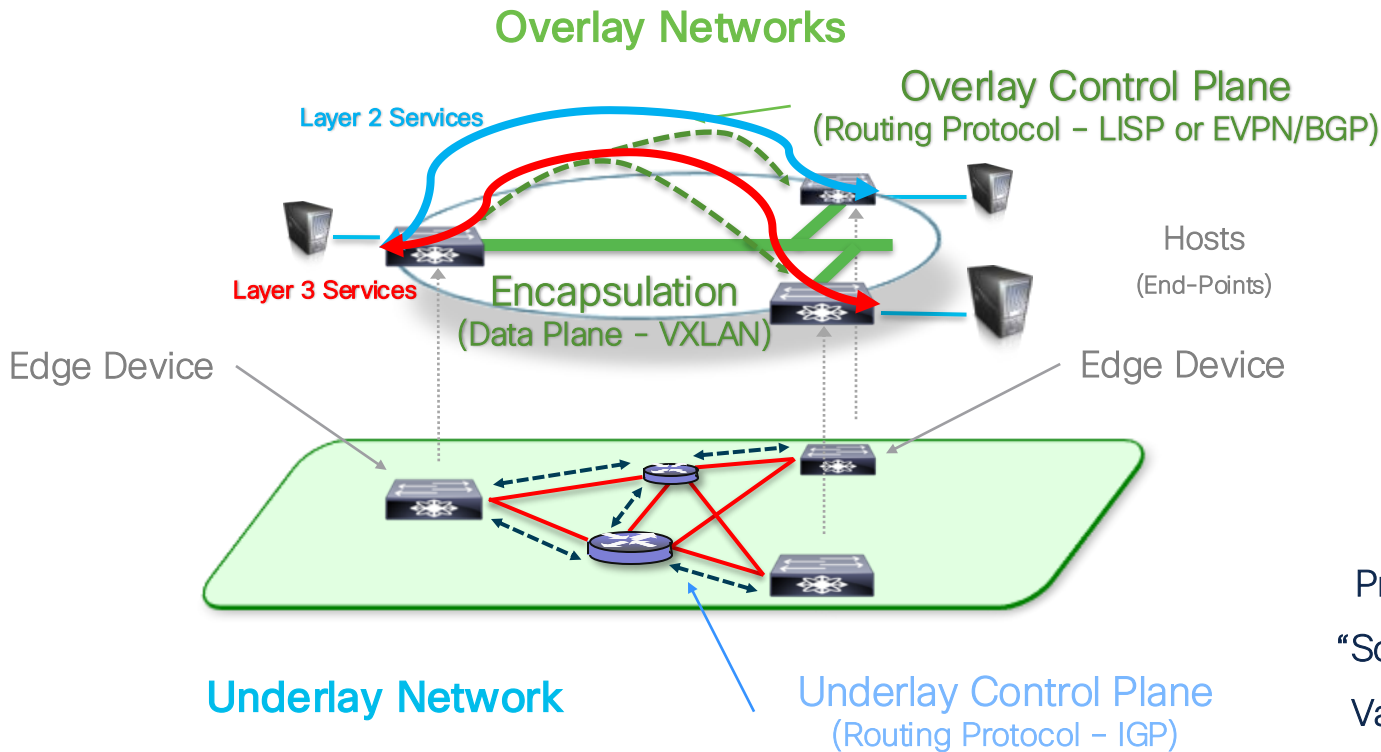
Fabric IP – The Fundamentals

Level 3 Architecture: Robustness, Resilience, Programmability, “Scale-out” Model...



Fabric IP – The Fundamentals

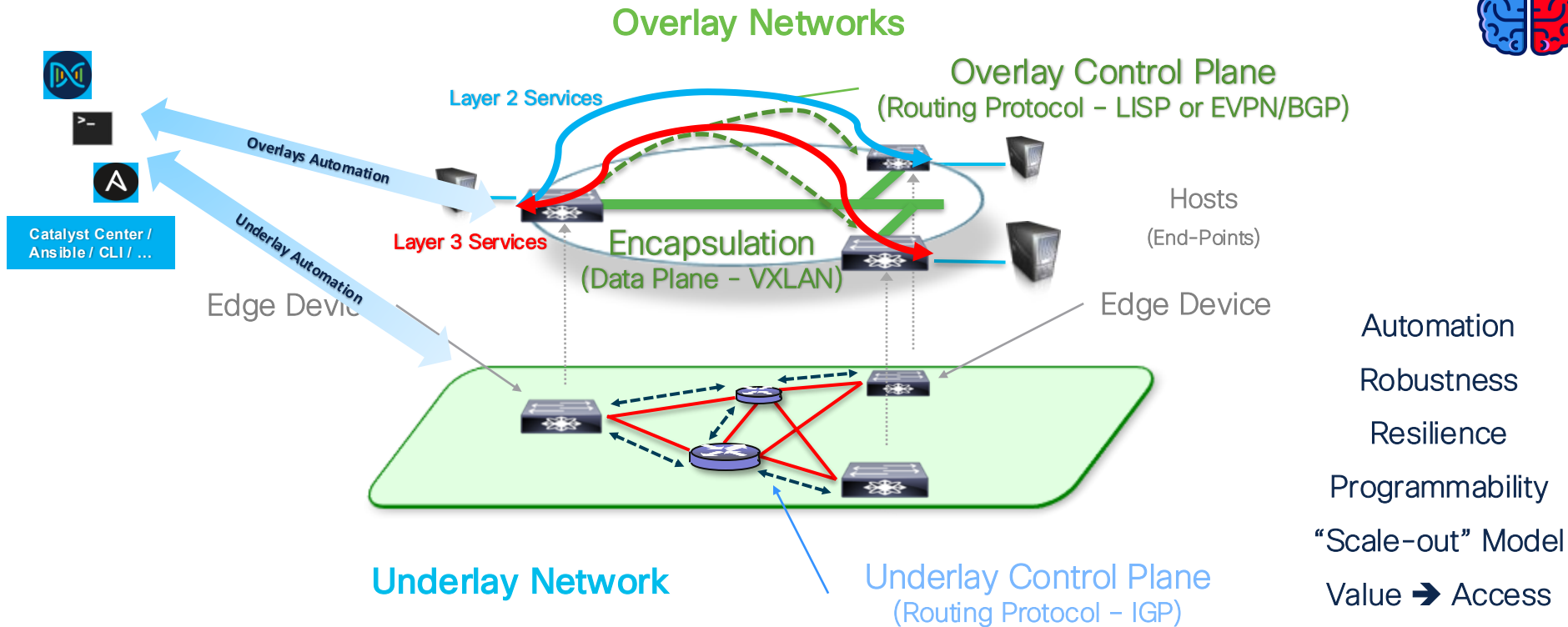
Level 3 Architecture: Robustness, Resilience, Programmability, “Scale-out” Model...



Robustness
Resilience
Programmability
“Scale-out” Model
Value ➔ Access

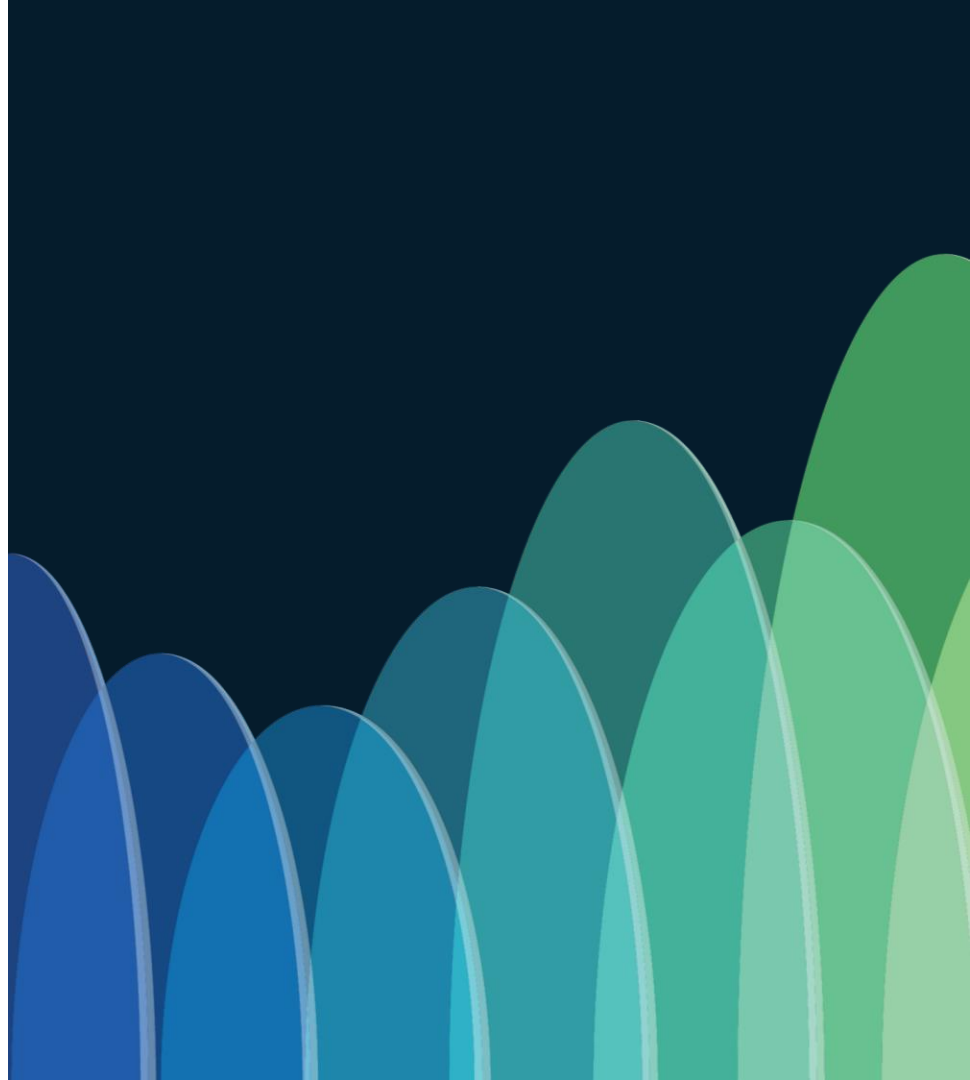
Fabric IP – The Fundamentals

Level 3 Architecture: Robustness, Resilience, Programmability, “Scale-out” Model...



Demo / Video 1

Video showing how to automate
an Edge Node in a Fabric (NetOps) ...



Home - Cisco Catalyst Center

Not Secure https://csv-dnac1.cisco.com/dna/home

Incognito (2)

Catalyst Center

admin

Welcome to Catalyst Center!

Explore

Some of your license compliance requirements have not been met. [Learn more.](#)

Assurance Summary

Health ⓘ

Healthy as of May 16, 2025 4:13 PM

89%

Network Devices

100%

Wireless Clients

72%

Wired Clients

View Details

Critical Issues

Last 24 Hours

2

P1

0

P2

View Details

Trends and Insights

Last 30 Days

0

AP Performance Advisories

0

Trend Deviations

View Details

Network Snapshot

Sites

As of May 16, 2025 4:13 PM

9

DNS Servers : 2

NTP Servers : 2

Add Sites

Network Devices

As of May 16, 2025 4:13 PM

19

Unclaimed: 0

Unprovisioned: 0

Unreachable: 0

Find New Devices

Application QoS Policies

As of May 16, 2025 4:13 PM

2

Successful Deploys: 2

Errored Deploys: 0

Stale Policies: 1

Add New Policy

Network Profiles

AI Endpoint Analytics ⓘ

Images ⓘ

Group Based Policy Simplifies Segmentation

The diagram illustrates a network architecture with the following components and connections:

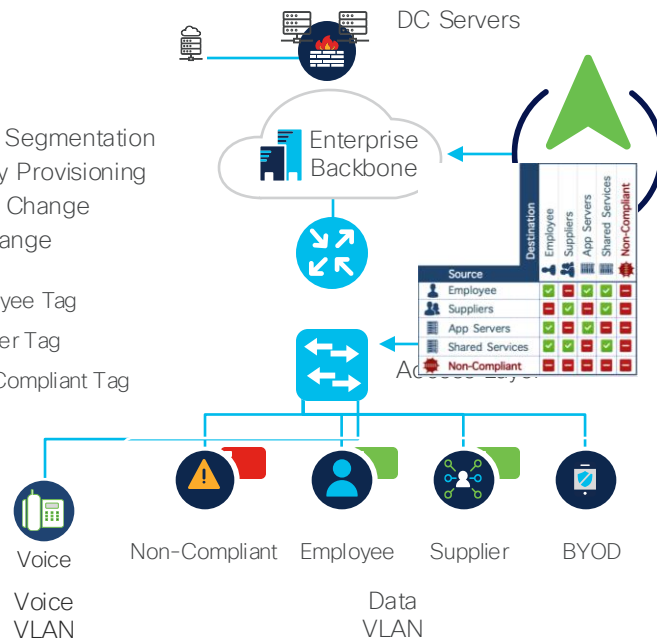
- Enterprise Backbone:** Represented by a cloud icon with a server rack.
- Aggregation:** Represented by a blue circle with two arrows pointing in opposite directions.
- Access Layer:** Represented by a green circle with a large 'A' and a green arrow pointing upwards.
- Static ACL:** A green box containing a list of IP addresses and their associated VLANs.
- Routing Redundancy DHCP Scope Address VLAN:** A green box containing a list of IP addresses and their associated VLANs.
- Access Layer Segments:** Six segments representing different user groups, each with a specific icon and a set of IP addresses:
 - Non-Compliant:** Represented by a yellow warning triangle icon. IP addresses: 10.10.10.10 to 10.10.10.100.
 - Voice:** Represented by a white telephone handset icon. IP addresses: 10.10.10.101 to 10.10.10.110.
 - Employee:** Represented by a white person icon. IP addresses: 10.10.10.111 to 10.10.10.120.
 - Supplier:** Represented by a white person icon with a checkmark. IP addresses: 10.10.10.121 to 10.10.10.130.
 - BYOD:** Represented by a white person icon with a laptop. IP addresses: 10.10.10.131 to 10.10.10.140.

Security Policy based on Topology
High cost and complex maintenance



Micro/Macro Segmentation
Central Policy Provisioning
No Topology Change
No VLAN Change

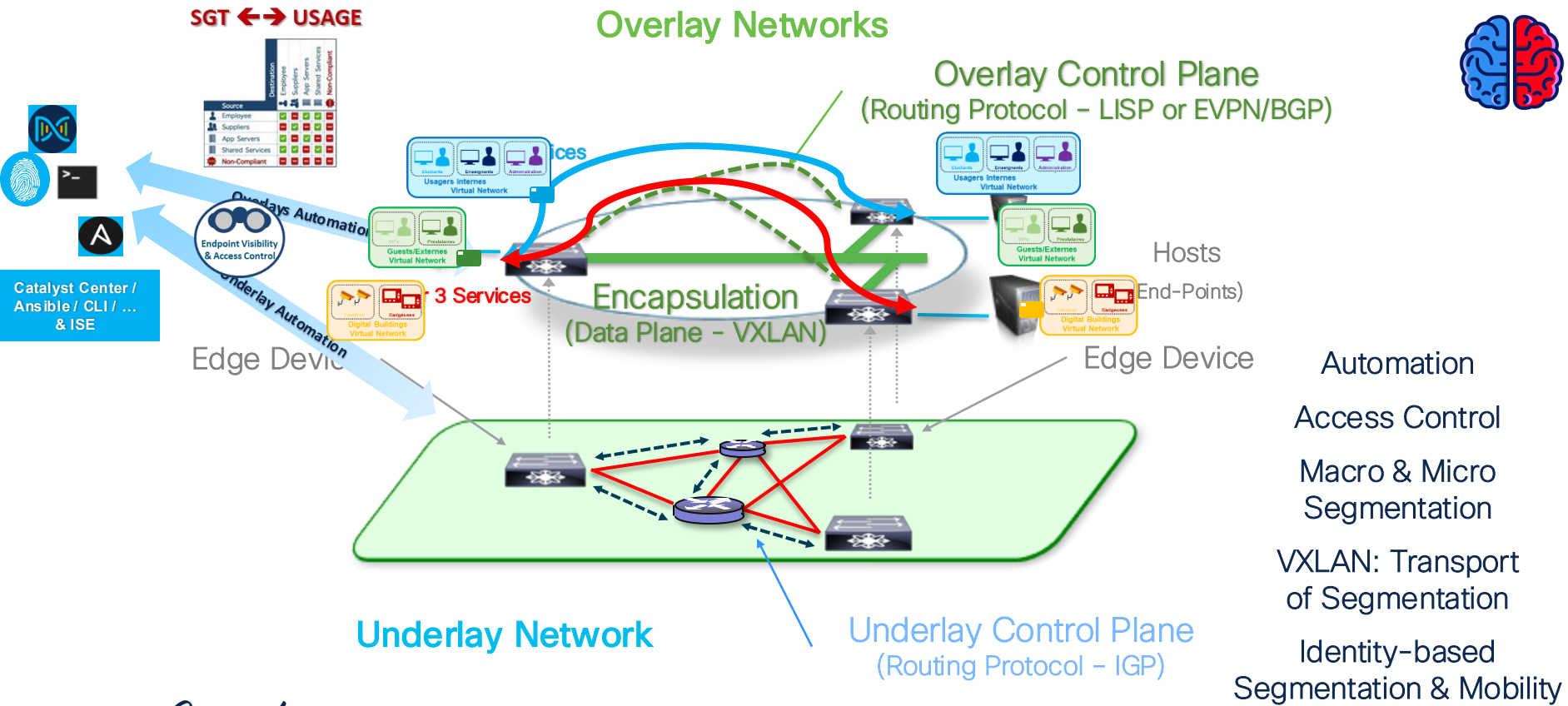
- Employee Tag
- Supplier Tag
- Non-Compliant Tag



Use existing topology and automate security policy to reduce OpEx

SD-Access: IP Fabric + Automated Security Services

“Security Plane”: Access Control + Macro & Micro Segmentation...



SD-Access: 2 technological offers

Flexibility in Fabric options according to Customer needs

CUSTOMER PROFILE:

“Network Centric”

Go with **Fabric IP with BGP EVPN**

One Fabric Technology (Campus & DC)

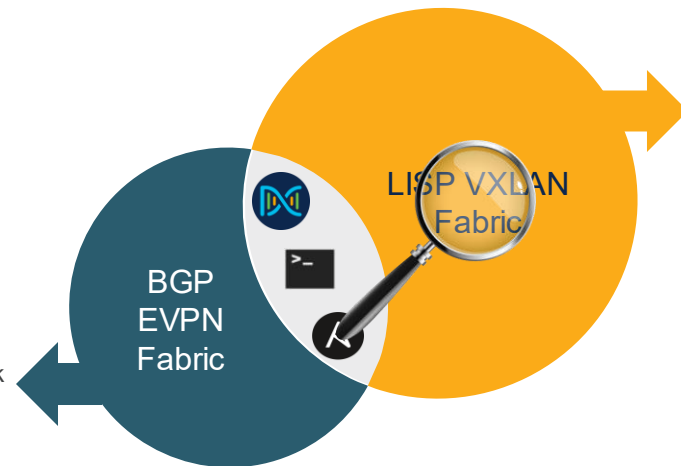
Operational ease with a single familiar protocol

Multi-vendor interoperability

Vendor-agnostic solution with unique Cisco differentiators

Segmentation

Zero-Trust Architecture with Micro and Macro Segmentation with customizable Overlay Network Types and Topologies.



CUSTOMER PROFILE:

“Identity Centric”

Lead with **Fabric IP with LISP**

Network Simplification

Lightweight, extensible, massive scale with rapid convergence. Single overlay for wired/wireless

Mobility First Requirement

Fabric Integrated Wireless, L2 Mobility, Enhanced wireless performance

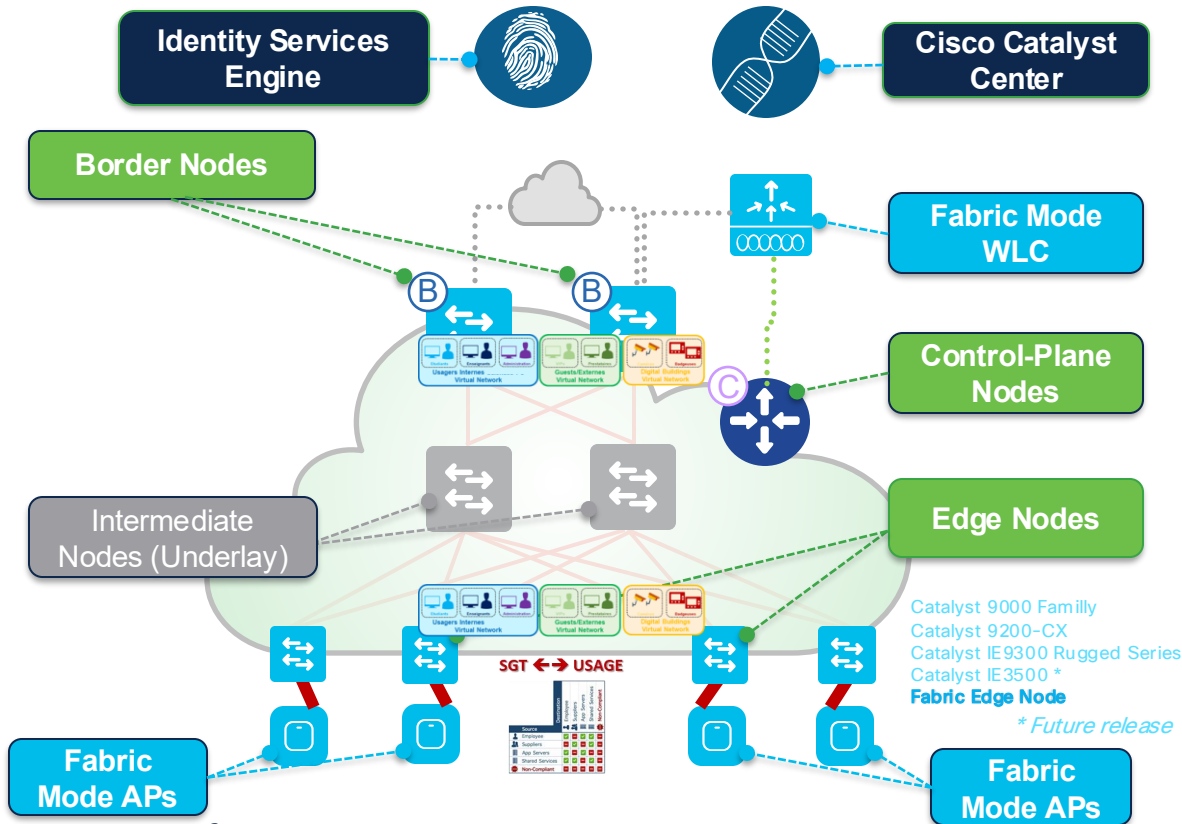
Segmentation

Zero-Trust Architecture with Unified Wired + Wireless Policy

One Infrastructure | Single Data plane | Consistent Zero-Trust Experience

Fabric IP – SDA-LISP

Roles & Terminologies



Fabric SDA-LISP - Compatibility Matrix

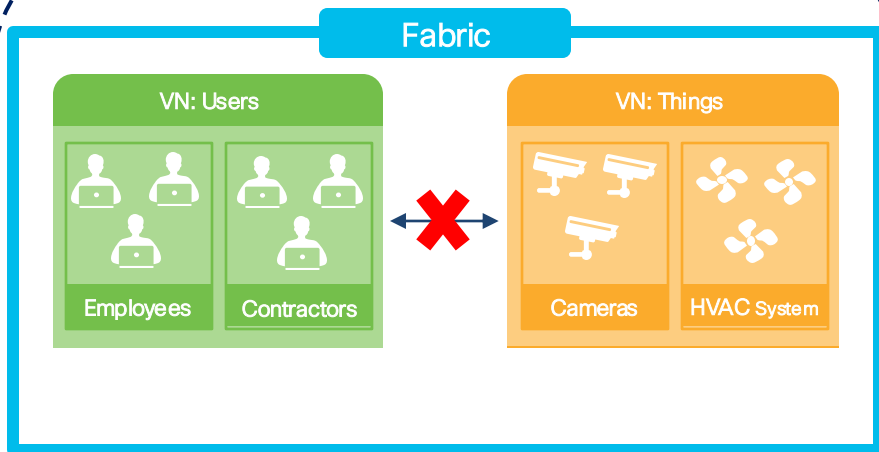
https://www.cisco.com/c/dam/en/us/td/docs/Website/enterprise/catalyst_center_compatibility_matrix/index.html

- **Cisco Catalyst Center** – Automation appliance for fabric automation, policy and assurance
- **ISE – Identity Service Engine** – advanced AAA solution, implements segmentation using trustsec
- **Control-Plane Nodes** – Map System that manages Endpoint ID to Device relationships. Can be collocated with Border Node
- **Border Nodes** – A Fabric device (e.g. Core) that connects External L3 network(s) to the SDA Fabric
- **Edge Nodes** – A Fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SDA Fabric
- **Fabric Wireless Controller** – Wireless Controller (WLC) that is fabric-enabled
- **Fabric Mode APs** – Access Points that are fabric-enabled.

Fabric IP – SDA-LISP

Policy Segmentation Strategy

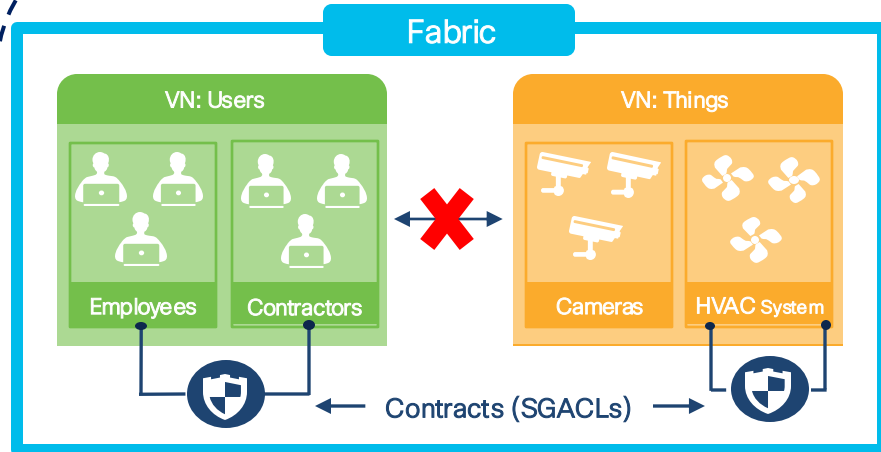
Macro Segmentation



Virtual Network (VN)

- VN = VRF = LISP Instance ID
- Complete Isolation between VN's
- Default Policy: No communication

Micro Segmentation



Security Group Tag (SGT)

- Location Independent Policy
- Simple Permit/Deny/Contracts
- Default Policy: Permit/Deny

Demo / Video 2

Video showing how to apply an Identity Centric Policy Model (SGT) between multiple end users (SecOps) ...

Home - Cisco Catalyst CenterIdentity Services EngineIdentity Services Enginecsv-esxi - VMware ESXI

Not Securehttps://csv-dnac1.cisco.com/dna/home

Incognito

Catalyst Center

admin

Welcome to Catalyst Center!

Explore

Some of your license compliance requirements have not been met. [Learn more.](#)

Assurance Summary

Health ⓘ

Healthy as of May 21, 2025 5:48 PM

89%100%72%

Network DevicesWireless ClientsWired Clients

[View Details](#)

Critical Issues

Last 24 Hours

20

P1P2

[View Details](#)

Trends and Insights

Last 30 Days

00

AP Performance AdvisoriesTrend Deviations

[View Details](#)

Network Snapshot

Sites

As of May 21, 2025 5:48 PM

9

DNS Servers : 2
NTP Servers : 2

[Add Sites](#)

Network Devices

As of May 21, 2025 5:48 PM

19

Unclaimed: 0
Unprovisioned: 0
Unreachable: 0

[Find New Devices](#)

Application QoS Policies

As of May 21, 2025 5:48 PM

2

Successful Deploys: 2
Errored Deploys: 0
Stale Policies: 1

[Add New Policy](#)

Network Profiles

As of May 21, 2025 5:48 PM

AI Endpoint Analytics ⓘ

As of May 21, 2025 5:48 PM

Images ⓘ

As of May 21, 2025 5:48 PM

Possible Designs: Fabric Edge Node Access



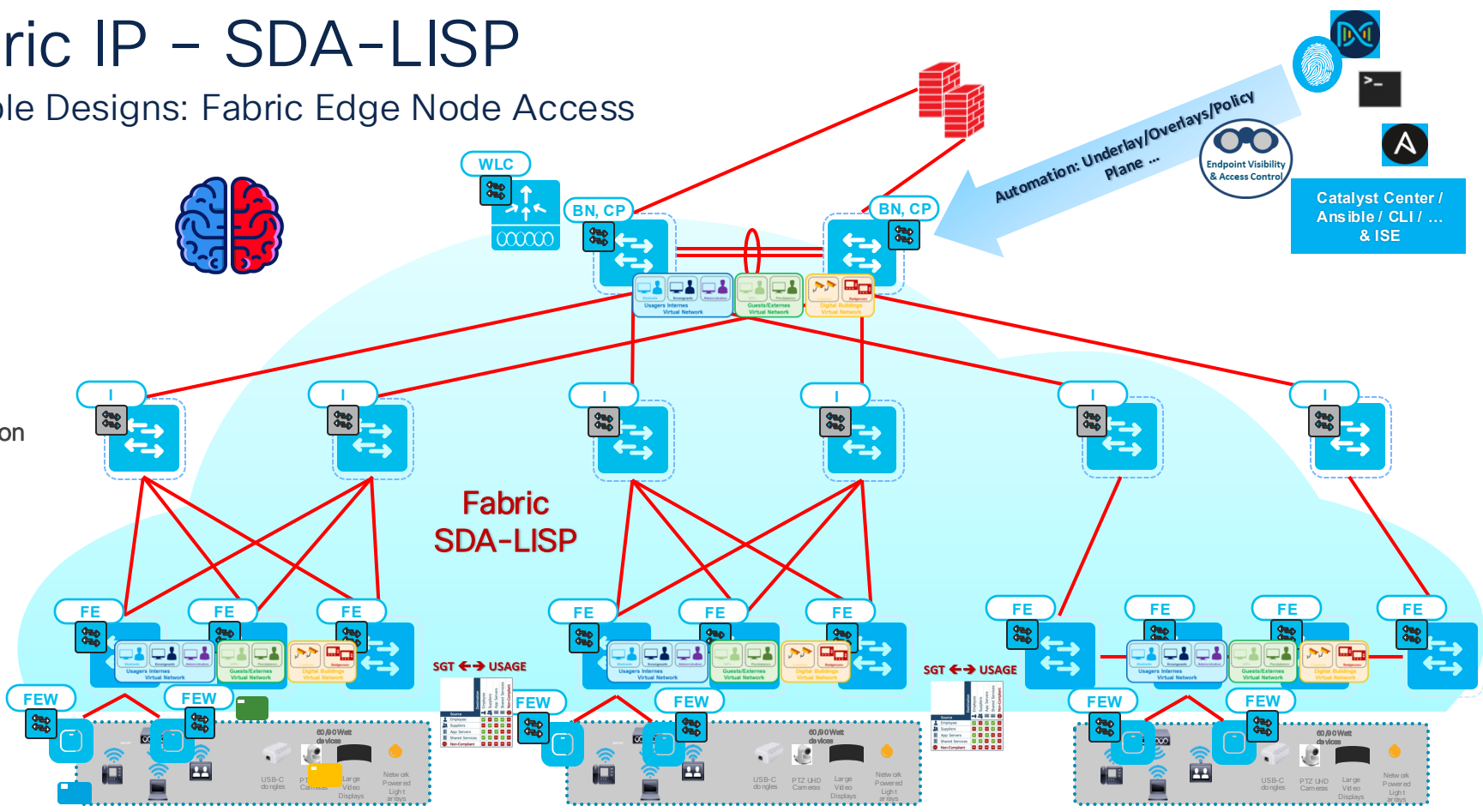
Fabric IP – SDA-LISP

Possible Designs: Fabric Edge Node Access

Core Layer

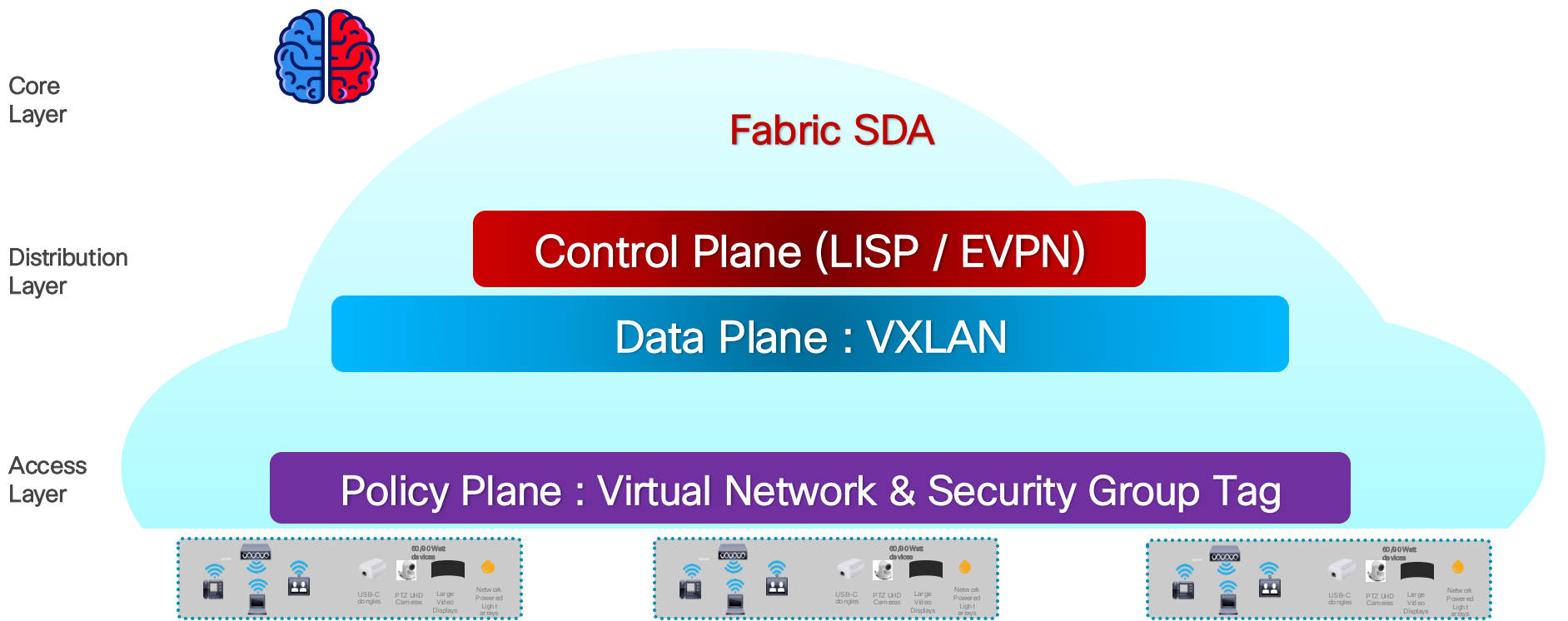
Distribution Layer

Access Layer



Fabric SDA

In summary...



Demo / Video 3

Video showing how Assurance (AIOps)
helps keep a Fabric SDA healthy





Agenda

- Challenges & Limitations of Traditional LANs Campus
- Fabric IP & Fabric SDA
- **Native Zero-Trust**
- Conclusion

Zero-Trust Evolution

LAN Campus → Fabric SD-Access

Three pillars of Workplace Zero Trust Security



Cisco Catalyst Center
& Meraki dashboard



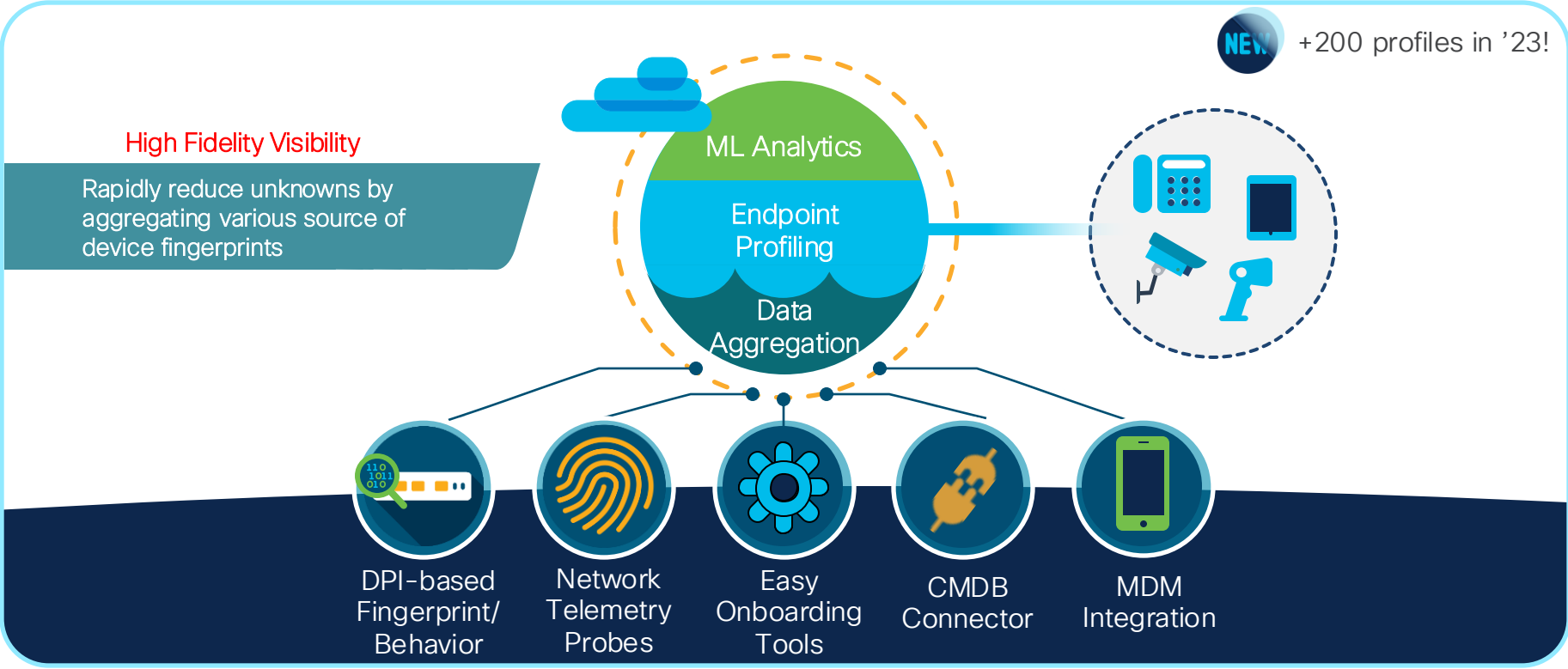
Cisco ISE

Enabled on Cisco Catalyst 9000 Infrastructure (Classical Ethernet or SD-Access)



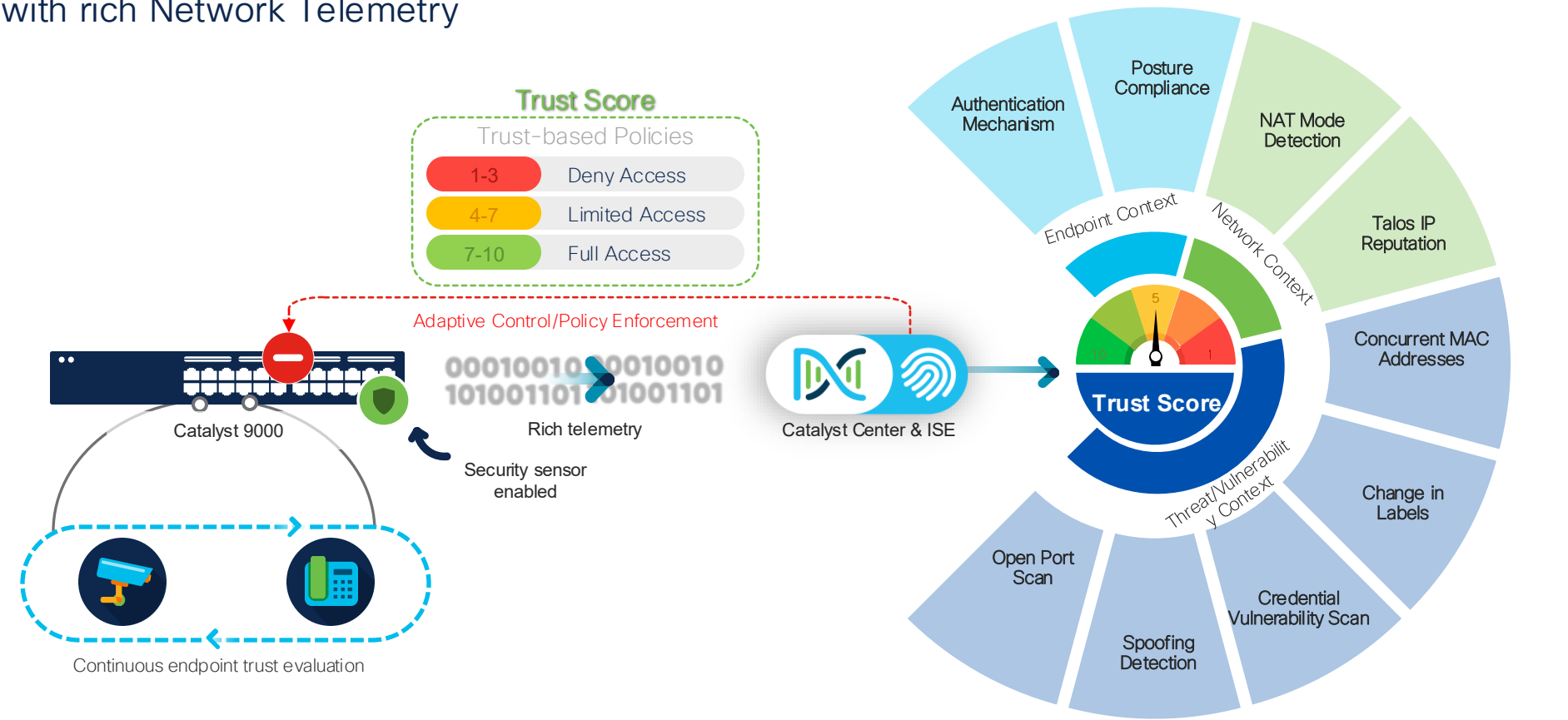
Endpoint Analytics (EA)

on Access Infrastructure



Continuously Assess Trust

with rich Network Telemetry



Demo / Video 4


Video showing EndPoint Analytics and
Trust Score (SecOps) ...








Home - Cisco Catalyst Center xIdentity Services Engine xIdentity Services Engine x+

Not Securehttps://csv-dnac1.cisco.com/dna/home


Incognito

Catalyst Center

|  admin

Welcome to Catalyst Center!

Explore

 Some of your license compliance requirements have not been met. [Learn more.](#)

Assurance Summary

Health ⓘ

Healthy as of May 16, 2025 5:01 PM

89%

Network Devices

100%

Wireless Clients

72%

Wired Clients

[View Details](#)

Critical Issues

Last 24 Hours

3

P1

0

P2

[View Details](#)

Trends and Insights

Last 30 Days

0

AP Performance Advisories

0

Trend Deviations

[View Details](#)

Network Snapshot

Sites

As of May 16, 2025 5:01 PM

9

DNS Servers : 2

NTP Servers : 2

[Add Sites](#)

Network Devices

As of May 16, 2025 5:01 PM

19

Unclaimed: 0

Unprovisioned: 0

Unreachable: 0

[Find New Devices](#)

Application QoS Policies

As of May 16, 2025 5:01 PM

2

Successful Deploys: 2

Errored Deploys: 0

Stale Policies: 1

[Add New Policy](#)

Network Profiles

AI Endpoint Analytics ⓘ

Images ⓘ

cisco *Connect*

#CiscoConnect

Track 3 - Session 2

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

35



Agenda

- Challenges & Limitations of Traditional LANs Campus
- Fabric IP & Fabric SDA
- Native Zero-Trust
- **Conclusion**

Key Takeaways

Access Layer → The Key Point of Transformation

mGig, UPoE/UPoE+, diversity of EndPoints (laptops, smartphones, sensors, IoT, ...)

Urbanization, Resilience & Security of the LAN Campus are Major Challenges

“Traditional” Architectures work but have Limitations!!!

Fabric IP / SD-Access

Automation, Robustness, High Availability, Elasticity to adapt to all issues related to urbanization
Single Connectivity Service for Wired & Wireless End-Points
Zero-Trust Native

Fabric IP / SD-Access is part of the Customer's Roadmap

Currently Fabric IP & Fabric SDA are IaaS Solutions
Roadmap to offer a SaaS Solution for Fabric IP & Fabric SDA




Key Takeaways



← ↺

17.06 Création en Direct d'une Fabric SD-Access : Démonstration et Étapes Clés - Cisco Community

🔖 ⚙️ 👤 ⋮ 🌈


 Community

Technologie et Assistance EMEA France Partner Webinaires et événements À propos de

Ce forum

Chercher dans la Événements de technologie en ligne et webinaires - Qu'est ce que vous cherchez?

Nouveau sujet



Cisco Community > Communauté Cisco > Événements de technologie > Événements de technologie en ligne et webinaires > 17.06 Création en Direct d'une Fabric SD-Access : Démonstration et Étapes Clés

S'abonner Options

Publié le 13-02-2025 09:16 PM par cheambot

Mis à jour le 04-03-2025 12:40 AM

🕒 Début : mar., juin 17, 2025 06:00 AM PDT

🕒 Fin : mar., juin 17, 2025 07:30 AM PDT

Mardi 17 juin 2025 à 15h00 (heure de Paris) / 9h00 (heure de Montréal)

Évènement Community Live

Création en Direct d'une Fabric SD-Access : Démonstration et Étapes Clés

Ce webinaire sera présenté par Jérôme Durand.

Vous trouvez SD-Access complexe ? Vous vous demandez par où commencer ? Participez à notre webinaire entièrement dédié aux démonstrations, dans lequel nous vous guiderons à travers chaque étape pour créer une Fabric SD-Access avec l'ensemble de ses services.


Horaires

- 9h00 Montréal, Toronto
- 15h00 Paris, Bruxelles
- 14h00 Tunis, Alger
- 13h00 Conakry, Dakar
- 13h00 Lomé, Abidjan
- 16h00 Antananarivo

Agenda

- (en attente)

* Cet événement est gratuit et ouvert à tous les publics, y compris les partenaires commerciaux, les ingénieurs réseau et télécommunications, les étudiants et les clients de Cisco.



Webinaire en français

Création en Direct d'une Fabric SD-Access : Démonstration et Étapes Clés

Vous trouvez SD-Access complexe ? Vous vous demandez par où commencer ? Participez à notre webinaire entièrement dédié aux démonstrations pour apprendre à créer une Fabric SD-Access.

Mardi 17 juin 2025. Événement en français !

Étiquettes (3)

Community Live

Commutation

Routing

cisco Connect

#CiscoConnect Track 3 - Session 2 © 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public 38

Go Beyond with Cisco CX !

Meet us
@World of Solutions
Booth

CISCO *Connect*

	Premium Support		Solution Attached Services		Lifecycle Services
	Service	Case	Service	Use Case	Example Activities
Secure Campus and Branch Networking Get secure networking with real-time performance data, smart recommendations, and closed-loop automation	Success Tracks Campus Network	Access to digital insights on campus network operations, risks, and devices with quick remediation options (switching, routing, and wireless).	SAS Campus Networking *	Implement and adopt Catalyst (Switching, Wireless, Routing, Cisco Spaces) along with Catalyst Center to ensure consistency of network services through regular device image management and deployment plus software recommendations	Utilize automation capabilities across facets of the network including DNA-C with SVS and Services-as-Code to dynamically adjust network configurations based on real-time demand and usage patterns, and AIA (automated incident and assurance) for automated fault detection.
			SAS Future-Proofed Workplaces Outcomes Program Management	Aligning networking products to business goals via analysis of current IT network capabilities and ongoing single program management for Cisco technology and third-party integrations	
			ThousandEyes Implementation Services	ThousandEyes implementation via onboarding programs with training and advice tailored to specific business outcomes	
	Success Tracks WAN	Insights to improve, optimize, and secure SD-WAN whether the use case is Secure Automated WAN, Secure Direct Internet Access, or WAN Digital Transformation on ramping for customers migrating from a non-controller environment	SAS Meraki	Get assistance with planning and executing a migration from on-premises to cloud through site surveys and migrations deployment planning, execution, and validation. Along with ISE integration into Meraki wireless.	



Thank you

GO BEYOND