No recording.
Internal use only.

No photography

No recording

No videography

No posting on social media

cisco

CISCO Connect

« Sécurité, Résilience, Simplicité »
Nouveaux standards de vos Réseaux Campus

Cisco Connect - Track 4 Session 2

Jean-Charles Griviaud
Principal Engineer, jgriviau@cisco.com

Sébastien Fernandez
Solutions Engineer, sebastfe@cisco.com

Agenda

1. Cisco Trustworthy
2. Challenges & Limitations of Traditional LANs Campus
3. Fabric IP & Fabric SDA
4. Conclusion

Cisco Trustworthy

A Trustworthy Solution Is:

"Security embedded throughout the solution lifecycle and across the Cisco product portfolios"

Where and How “Attacker”can attack?

Why there is a need for Trustworthy Systems

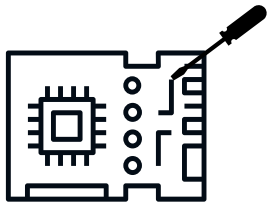
Where

- Supply Chain Attack
- HW Tampering Attack
- BIOS/ ROMMON Attack
- SW Binary Attack
- Runtime Attack
- Asymetric cryptography

How

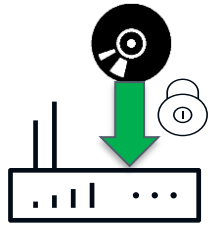
- **Exploited Vulnerability**
  - Compromised Credentials
  - Physical access to device/images
- **Infection Method**
  - In-Memory Modifications
  - Modified OS Binaries
  - ROMMON changes
- **Result**
  - Malware Installed
  - Boot loader corrupted
  - Confidentiality broken
- **Quantum Computer**

Cisco’s Top Security Design Considerations

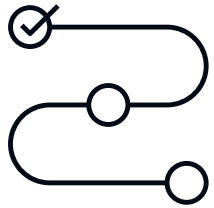


Hardware Tampering Detection

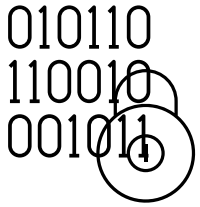
Counterfeit Hardware Detection



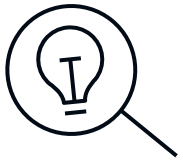
Secure Boot



Operational Security



Data Protection



Product Integrity Visibility

Legal / Certification Requirements

Internal Threats

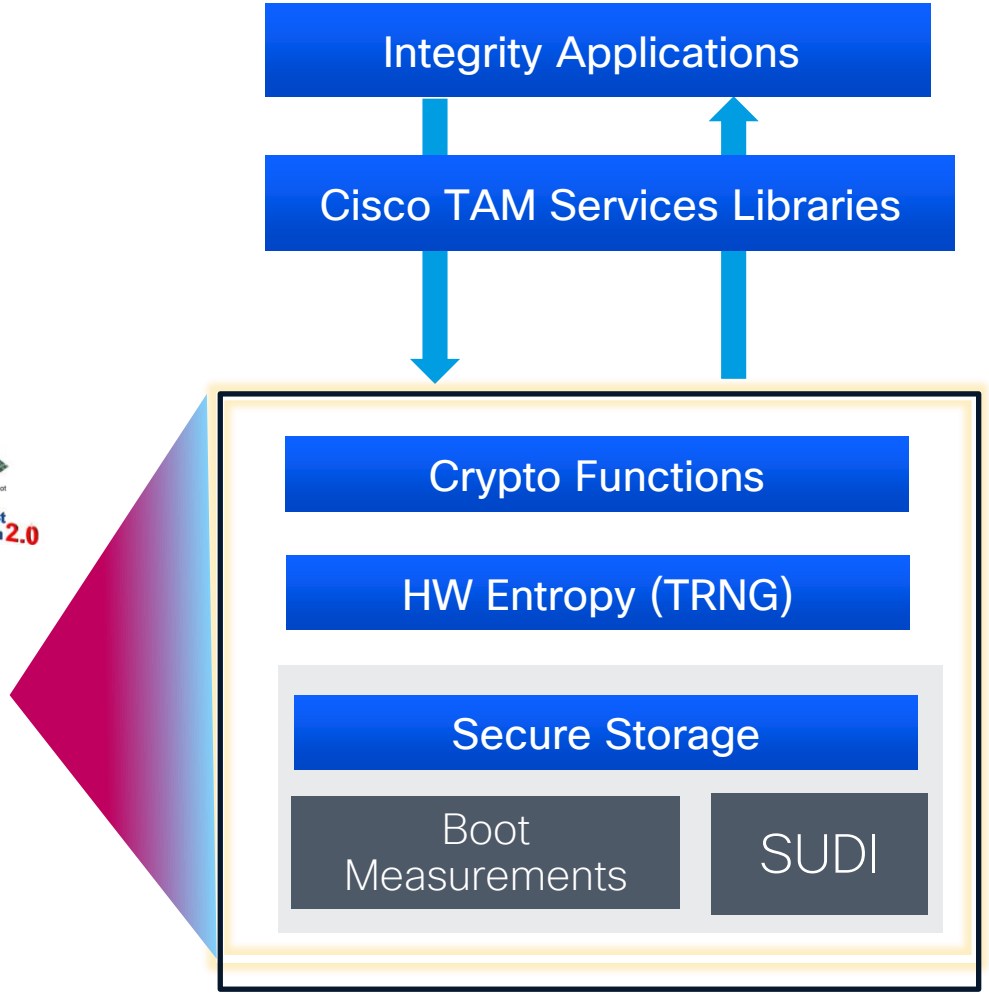
Quantum Safe

Transparency

Tamper Resistant Chip
Hardware Root of Trust

Chip Functionality

- Tamper-proof Chip for Cryptography
- Secure Storage
- Built-in Crypto Functions
- HW Entropy Source
- Hardware Authenticity Check (w/SUDI)
- Secure PnP/ZTP (w/SUDI)
- Integrity Verification

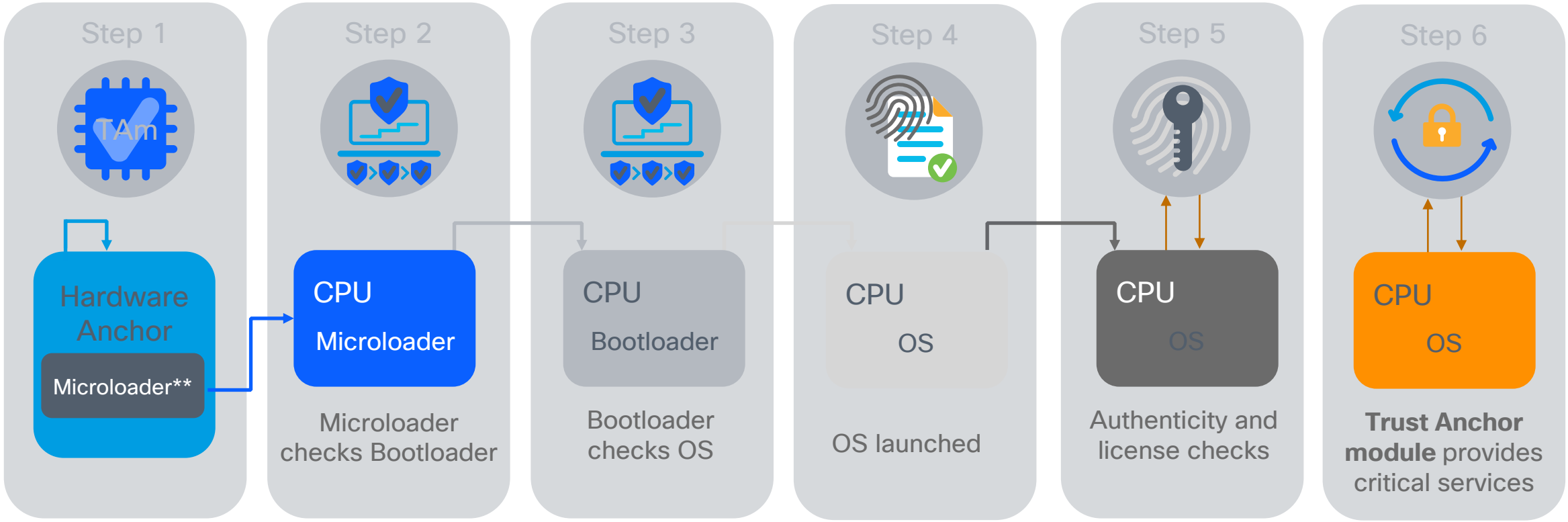


Aikido is a Cisco Trust Anchor Module (TAM)

- Secure Boot + Trust Anchor module (TAm) + Secure JTAG solution
- all integrated in one Microsemi SmartFusion2 FPGA chip
- with support to many other Trustworthy Technologies.

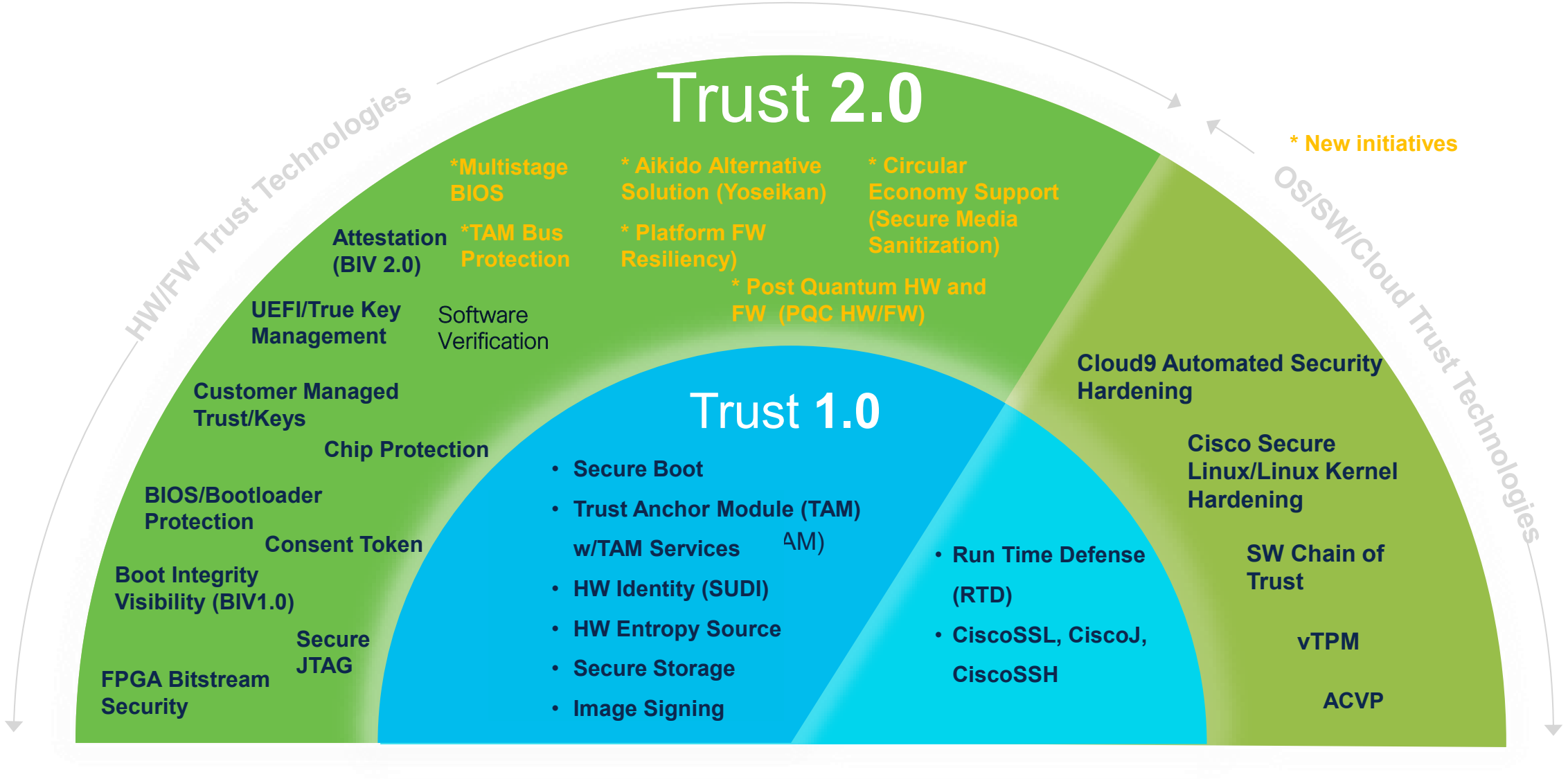
cisco

Secure Boot ROT (Root of Trust) Process



Confidentiality | Integrity | Authenticity

Trustworthy Technologies 2.0 Summary



Cisco Infrastructure Resilience initiative

prioritizing modern practices to keep you safe

Reduce the attack surface

Protect sensitive data

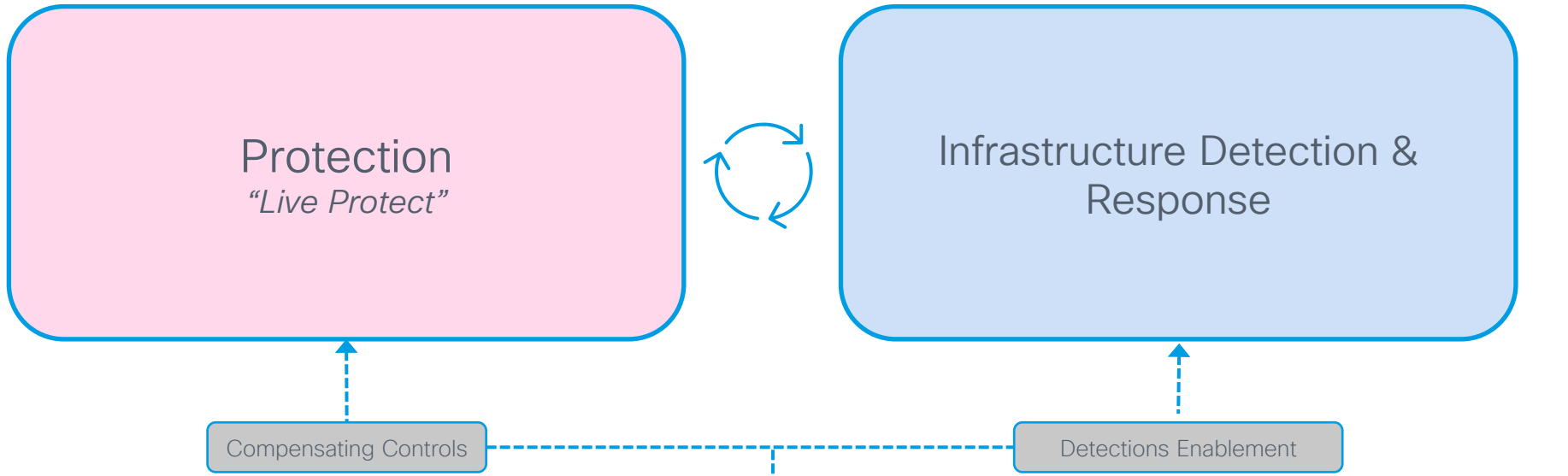
Enable the defender

- https://cisco.com/go/ri

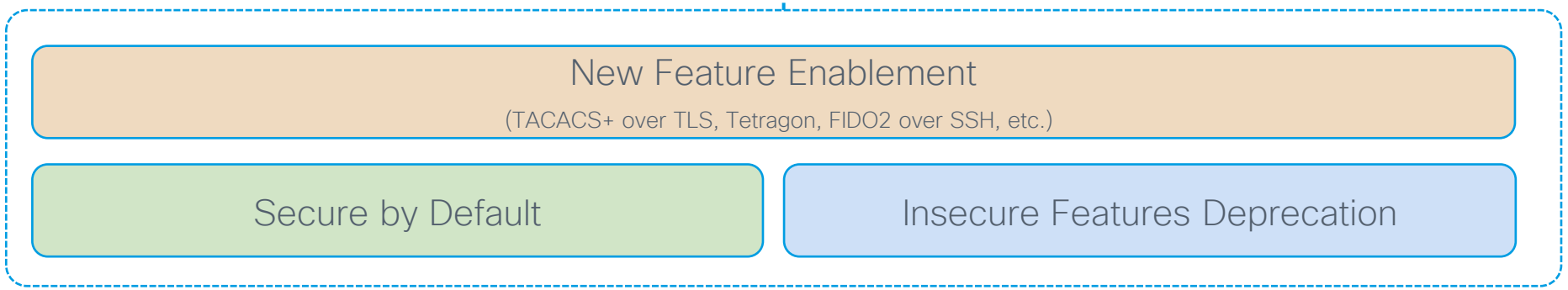
Cisco Infrastructure Resilient Initiative

A compelling vision of security and resilience

Enhanced Detections & Protections



Baseline Security Posture



cisco

Cisco Infrastructure Resilient Initiative

Secure By Default

- Always encrypt or use strong hashes for storing credentials in configuration files
- Default SSH keys to strong key lengths
- Disable services by default (HTTP/HTTPS (Web) Server + Guest Shell + SNMP Server)
- Require explicit configuration of management protocols
- Require access lists to permit management traffic from specific networks
- Default logging timestamps to msec precision date and time instead of uptime

Cisco Infrastructure Resilient Initiative

Feature Deprecations

Warn → Restrict → Remove

- SSHv1
- Smart Install
- SNMPv1/v2c (phased deprecation)
- IP Source Routing
- TLS1.0 / 1.1
- Weak ciphers (e.g. SHA1, MD5)
- Telnet
- FTP
- TFTP
- HTTP
- On Demand Routing (ODR)
- BootP Server
- IP Finger
- TCP / UDP Small Servers
- SNMPv3 without authPriv
- Ability to decrypt type 6 credentials
- TACACS+ with MD5
- RADIUS without RadSec

Cisco Infrastructure Resilient Initiative

Features Deprecations / Removal

- Releases where each deprecation phase will start (subject to change)
- Some features will be warned / restricted in later releases

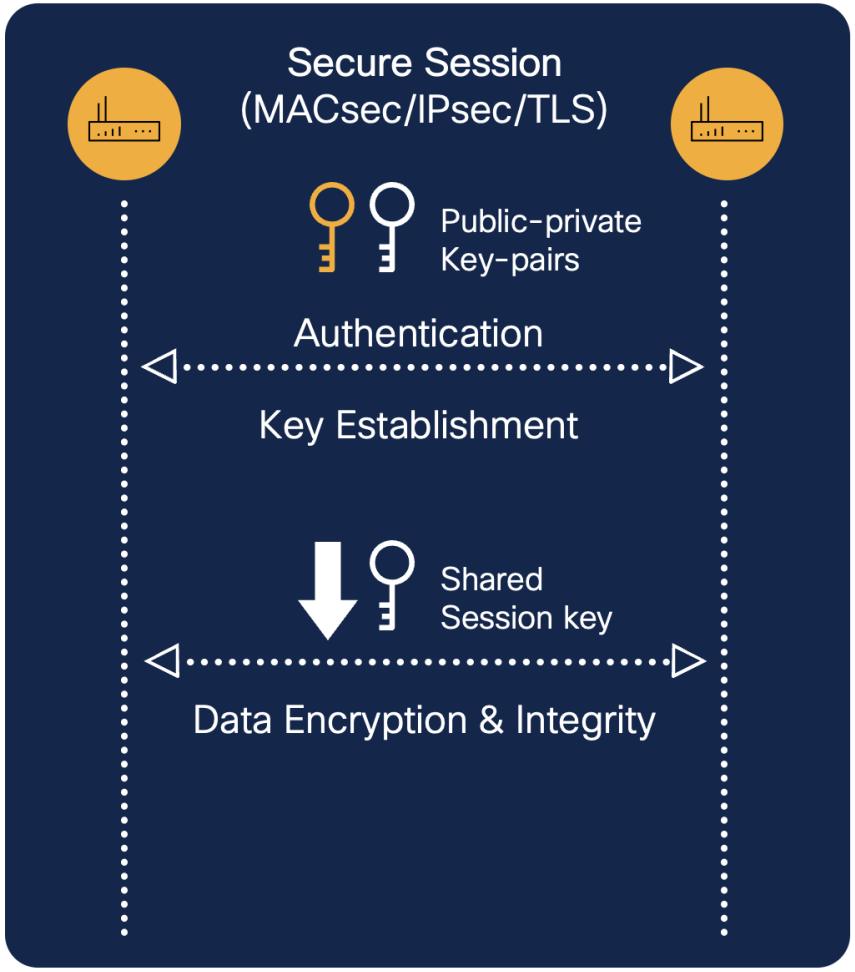
	IOS XE	IOS XR	NX OS	ISE	ASA/FTD
Warnings	17.18.2	25.4.1	10.7.1	3.6	10.5/9.25
Restrictions	26.1.1	26.3.1	10.7.2	3.6	11.0
Restriction Mechanism	'insecure mode'	Optional RPMs	'insecure mode'	GUI Confirm	'insecure mode'
Removals*	27.1.1+	26.3.1+	10.8.1+	3.8+	11.0+

- Latest information will be published on public Resilient Infrastructure site at cisco.com/go/ri

Cisco Infrastructure Resilient Initiative
New Features and Enhanced Capabilities

- TACACS+ over TLS 1.3
- FIDO2 support for SSH
- SSH authorized host key scalability via TACACS+
- Secure credential types (recoverable type 6, non-recoverable 8/9/10)
- Syslogs for security-relevant events (root shell, packet captures, AAA configuration changes)
- Periodic reminder logs for insecure config

Quantum computing impact on transport protocols



Quantum-resistant?

Asymmetric cryptography

- Based on **mathematically related** public-private key-pairs
- Used for control plane operations
  - Authentication, key establishment
- Examples: RSA, DH, ECC

Large, reliable quantum computers can break RSA, DH, ECC

Symmetric cryptography

- Based on shared key
- Used for bulk data encryption and integrity
- Protection level based on key strength
  - Key size and entropy
- Example: AES-GCM

Symmetric crypto with large and high-entropy keys is resistant to quantum computer attacks

Path to Post Quantum Cryptography

PQC Algorithms & Standards

LMS – RFC8554 – approved

XMSS – RFC8391 – approved

NIST SP.800-208 – approved
(implementation requirements for LMS & XMSS)

FIPS-203 ML-KEM
- Module-Lattice-Based Key-Encapsulation Mechanism Standard

FIPS-204 ML-DSA
- Module-Lattice-Based Digital Signature Standard

FIPS-205 SLH-DSA
- Stateless Hash-Based Digital Signature Standard

Protocol standards (the most urgent set)

IKEv2:

RFC 9370 – Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2) – approved

RFC 9242 – Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2) – approved

Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2) – draft

TLS:

Hybrid key exchange in TLS 1.3 – draft

SSH:

Post-quantum Hybrid Key Exchange in SSH – draft

Crypto Services:

Composite Signatures For Use In Internet PKI – draft

Internet X.509 Public Key Infrastructure: Algorithm Identifiers for ML-DSA – draft

Internet X.509 Public Key Infrastructure - Algorithm Identifiers for Kyber – draft

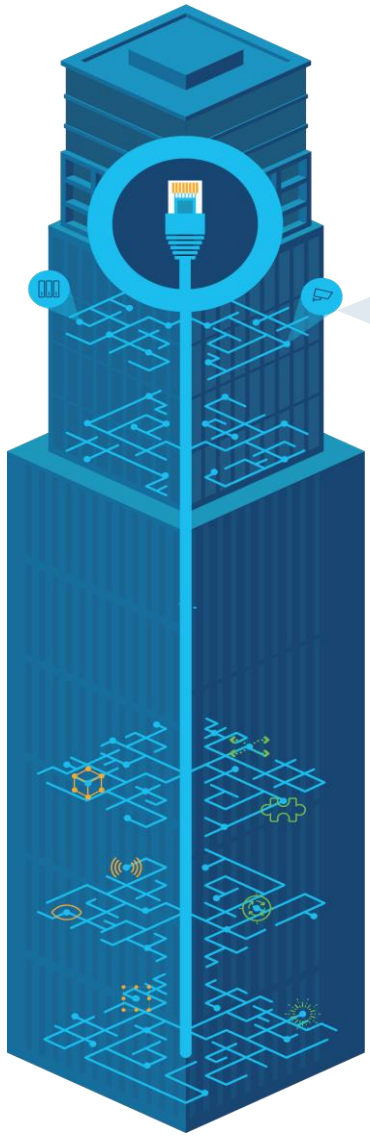
PQC Roadmap on C9000 Switches

PQC Algorithm	C9350	C9610
LMS signing and verification capability on bootloader/ROMMON	17.18.2	26.1.1
ML-DSA-87 image signing to enable verification of IOS-XE	26.2.1	26.2.1
PQC-signed SUDI certs with ML-DSA-87	26.2.1	26.2.1
MACsec Certificate Based Authentication with ML-KEM	26.1.1	26.1.1
IPsec key exchange IKEv2 with ML-KEM	26.2.1	26.2.1

Challenges & Limitations of Traditional LANs Campus

Challenges & Limitations of Traditional LANs Campus

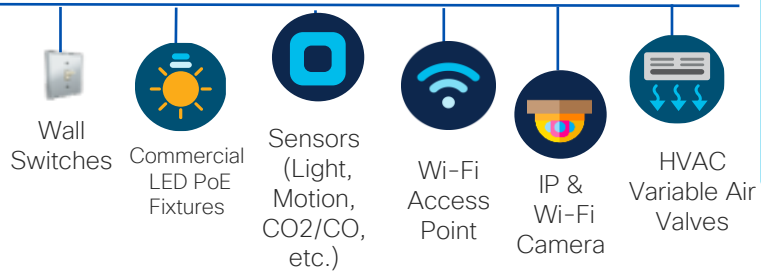
mGig & 90W UPOE+ ➔ Standard driving new IT/OT Use Cases



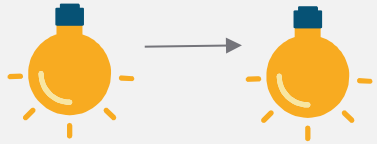
Closet

Cisco/ Partner Cloud Services

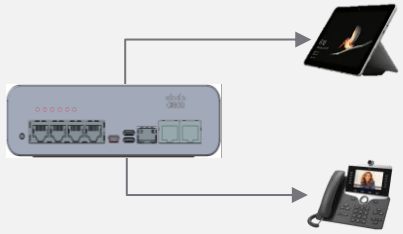
Smart Building Devices



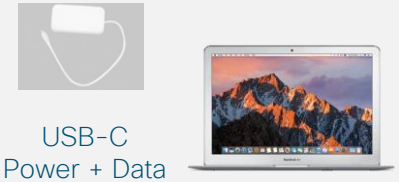
High Power PoE End-points



Daisy-chaining
(Cost saving with 90W)



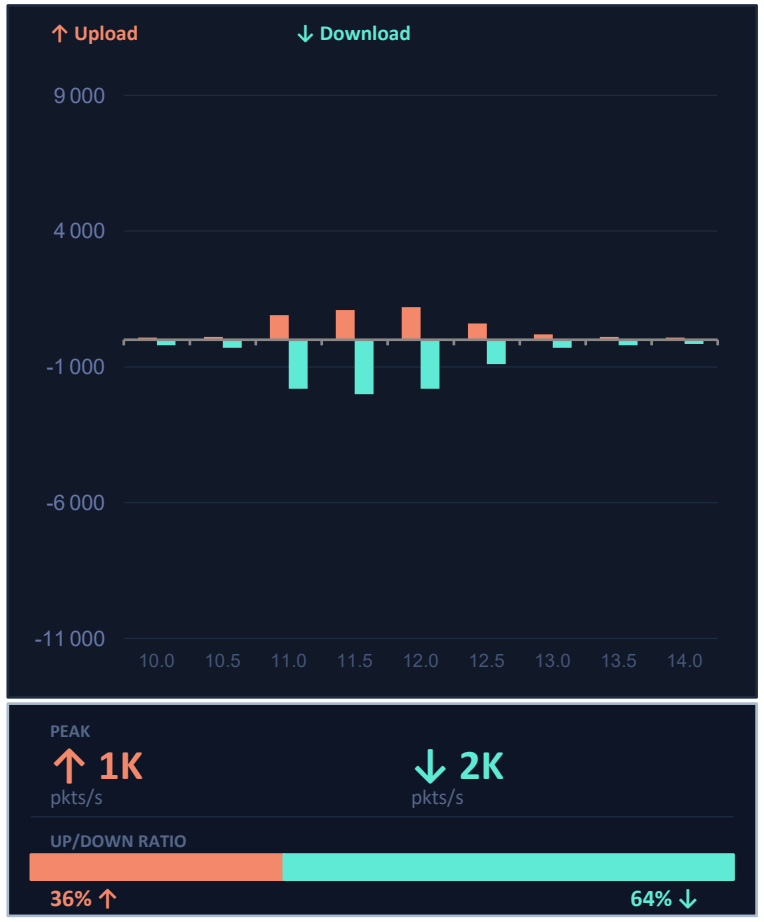
UPOE Pass-through
(for extended reach 60W)



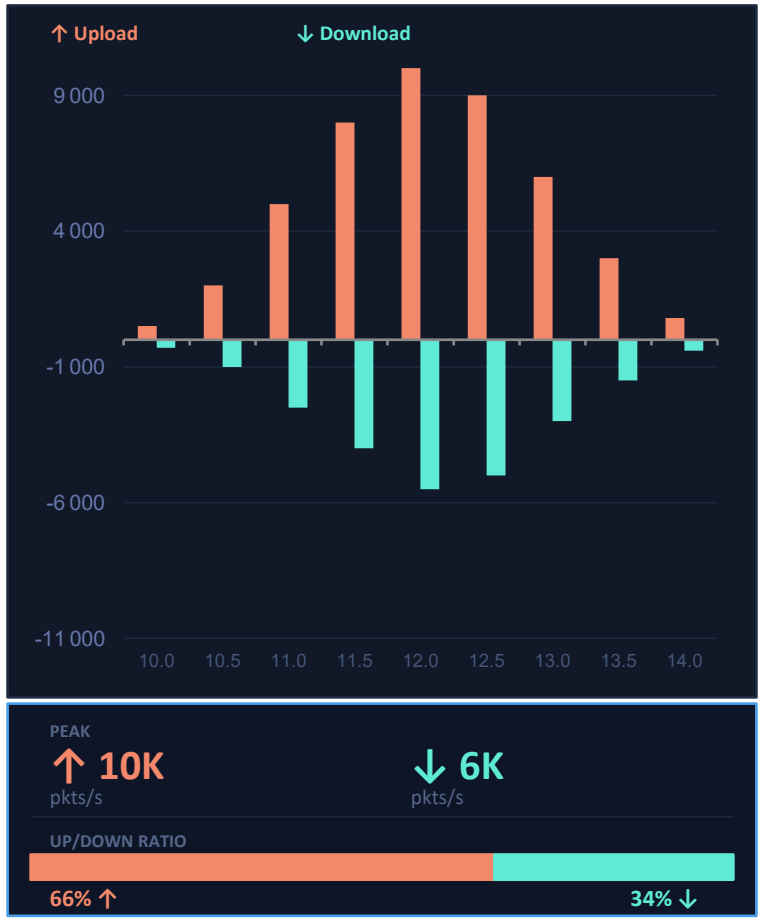
USB-C power
(laptop charging + data)

cisco

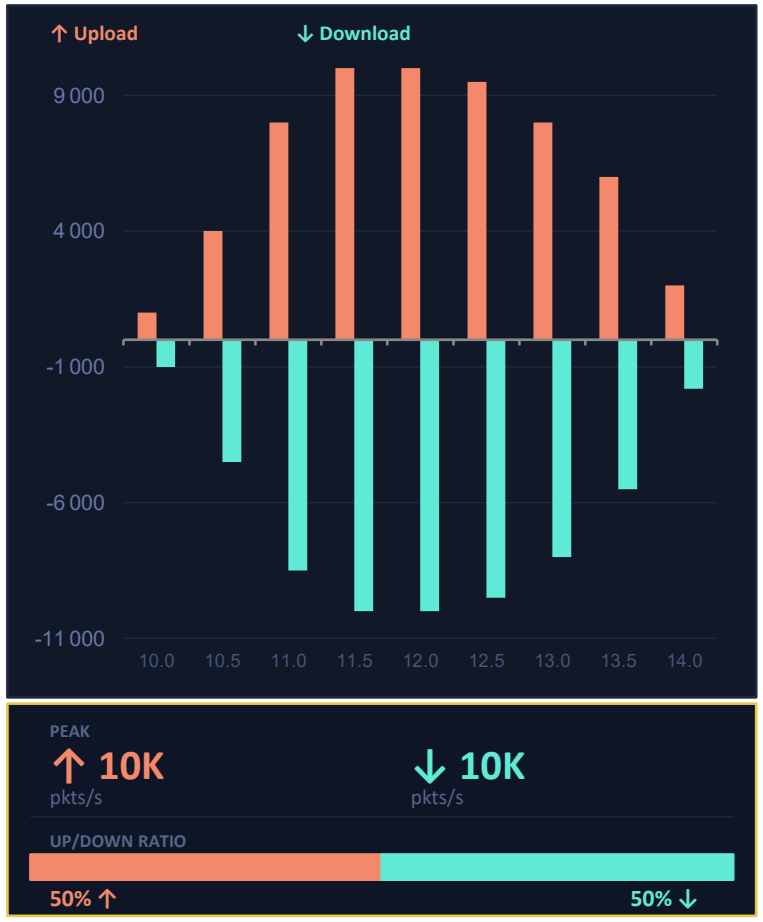
Non-AI Traffic



ChatGPT (Chatbot)



GeminiCLI (AI Agent)



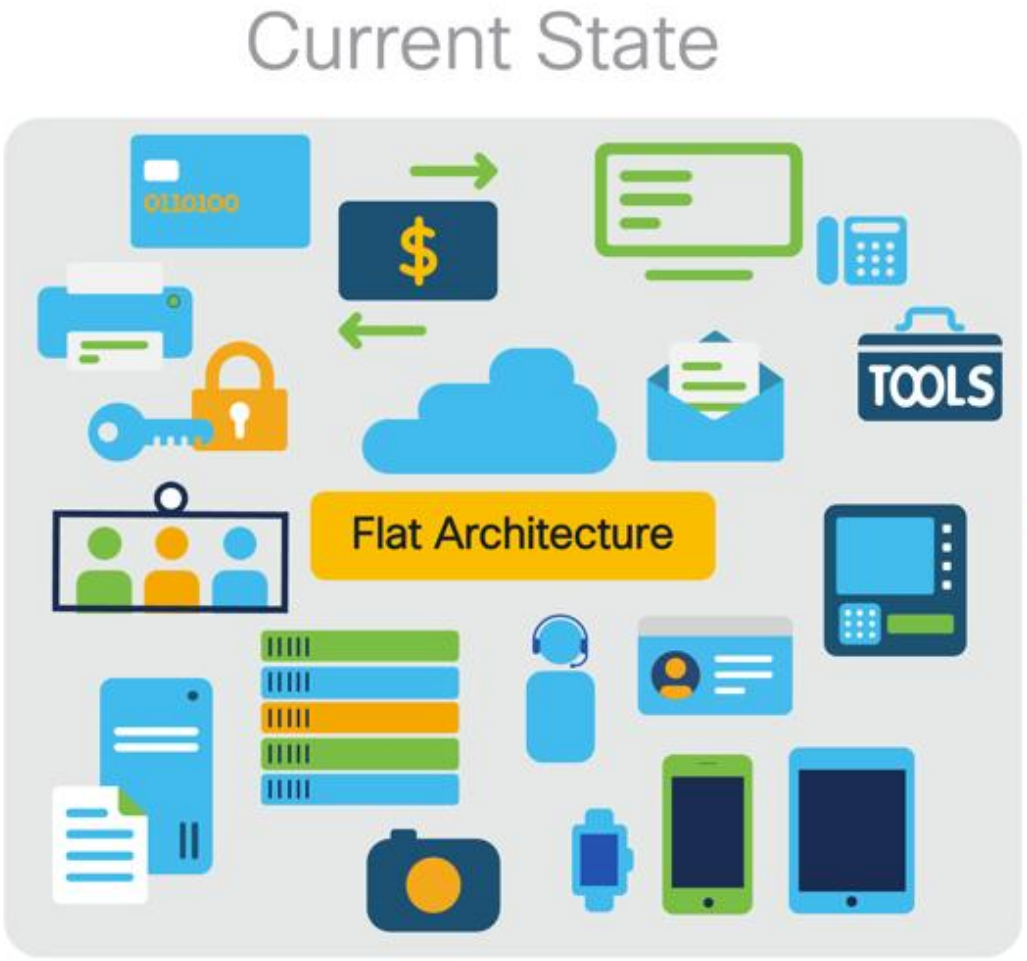
TME Lab Experiments: Upload = positive ↑ | Download = negative ↓ | Pkts/Sec | Same 4-second window (10s – 14s)

AI Applications are changing the Traffic Patterns

cisco

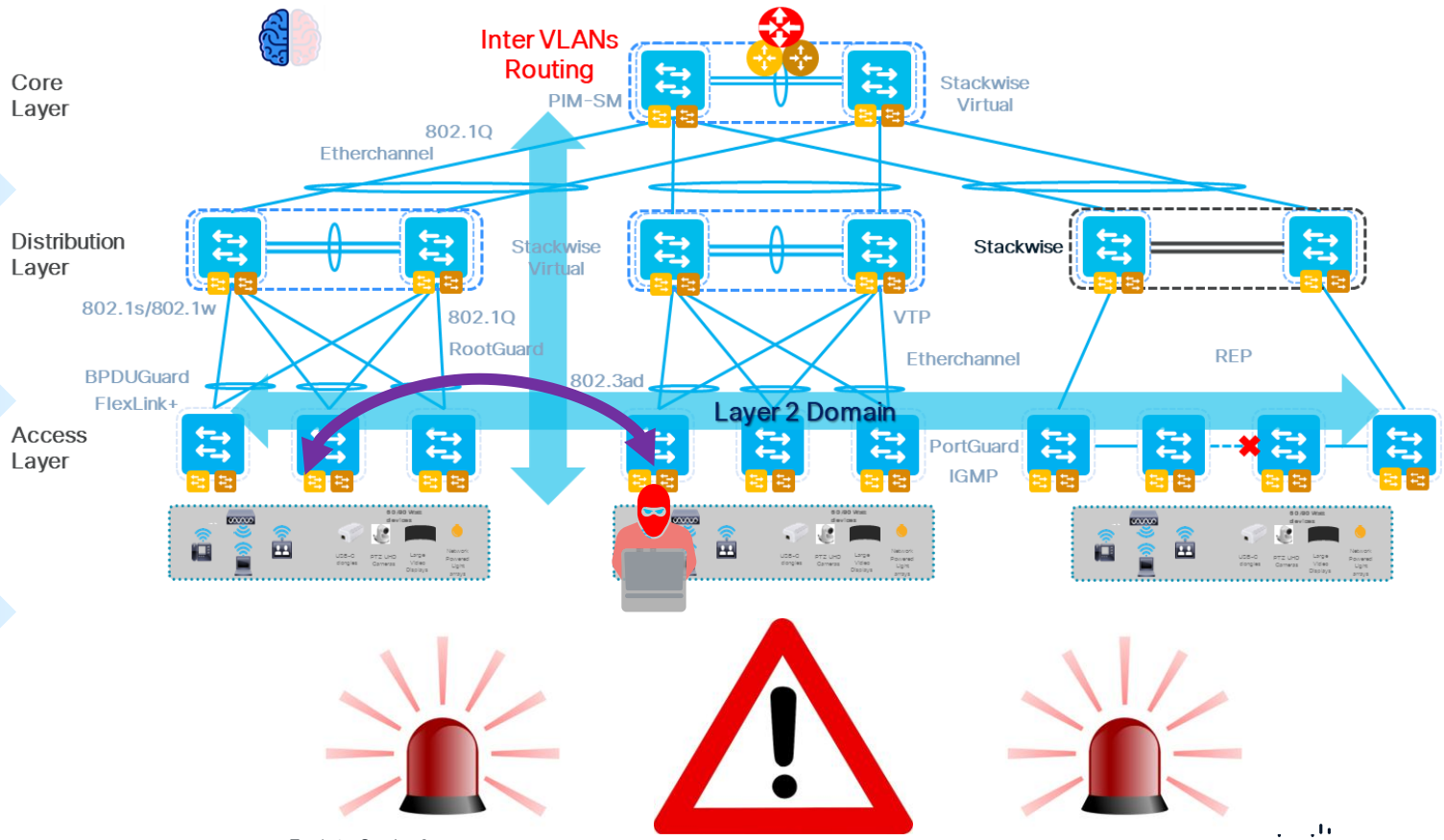
Challenges & Limitations of Traditional LANs Campus

Transition from Flat Network to Zero Trust Segmentation



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

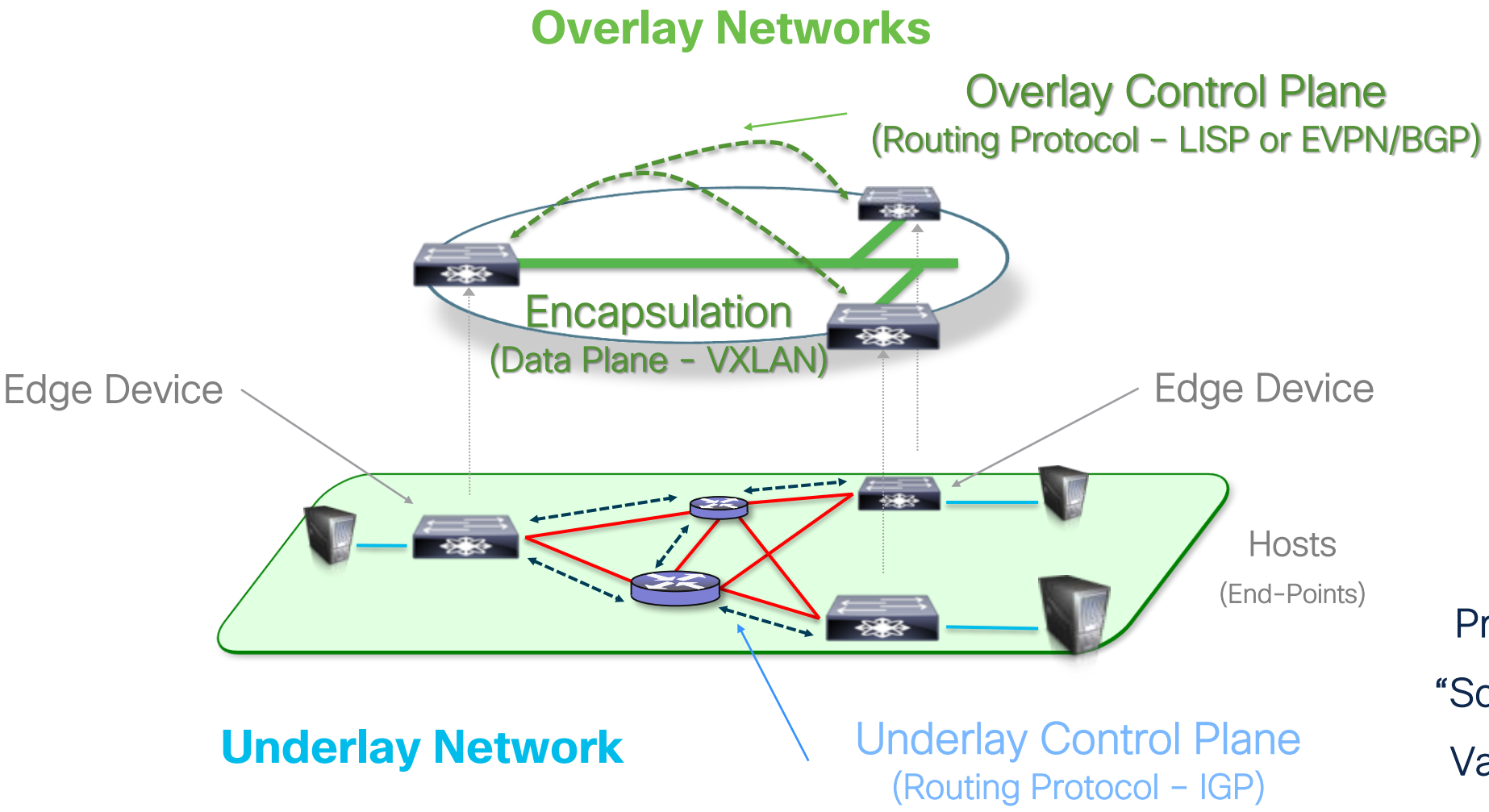
Needs for Level 2 Services without the constraints and difficulties induced by Level 2 Architectures

cisco

Fabric IP & Fabric SDA

Fabric IP – The Fundamentals

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



Robustness

Resilience

Programmability

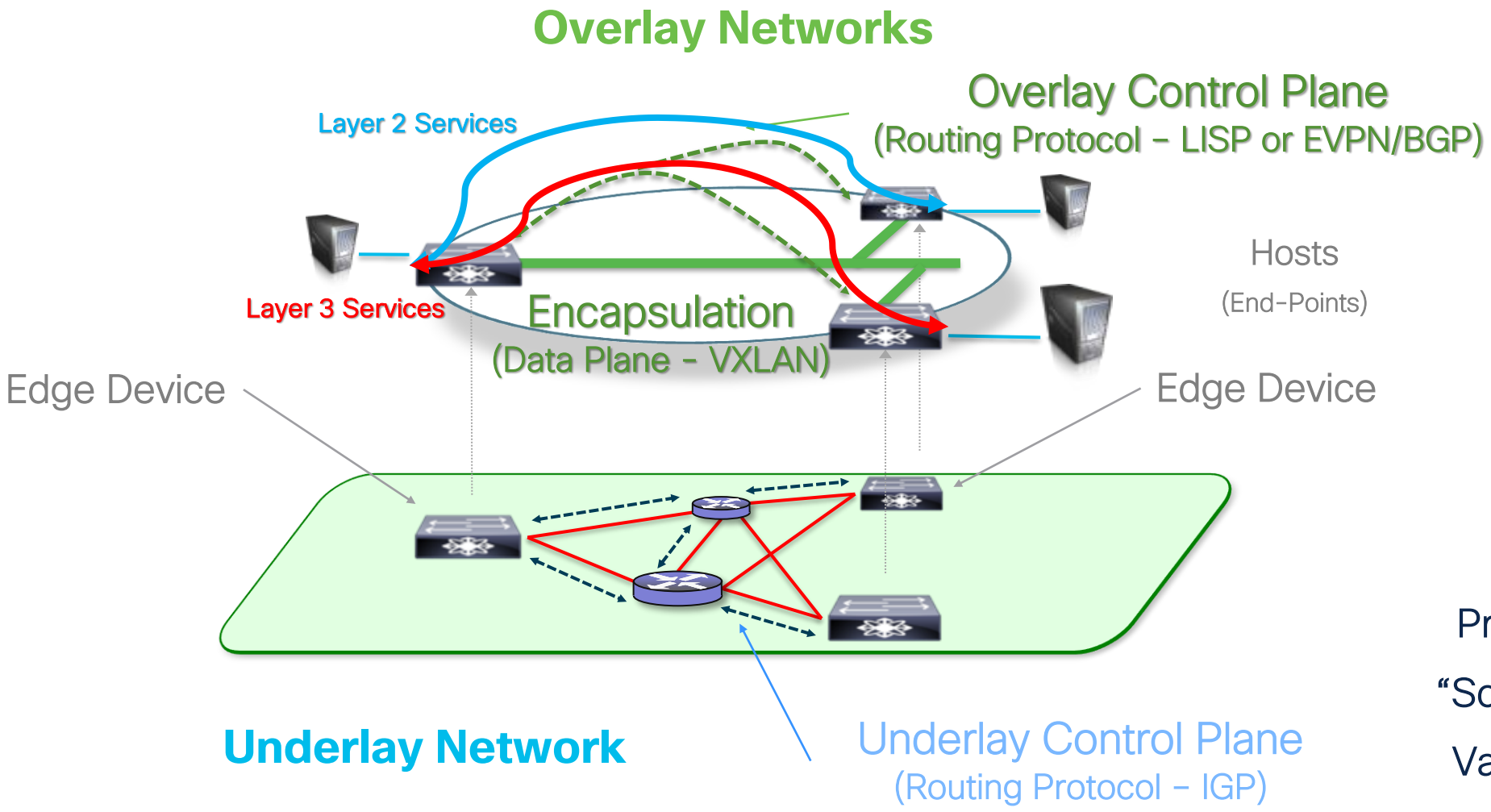
“Scale-out” Model

Value ➔ Access

cisco

Fabric IP – The Fundamentals

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



Robustness

Resilience

Programmability

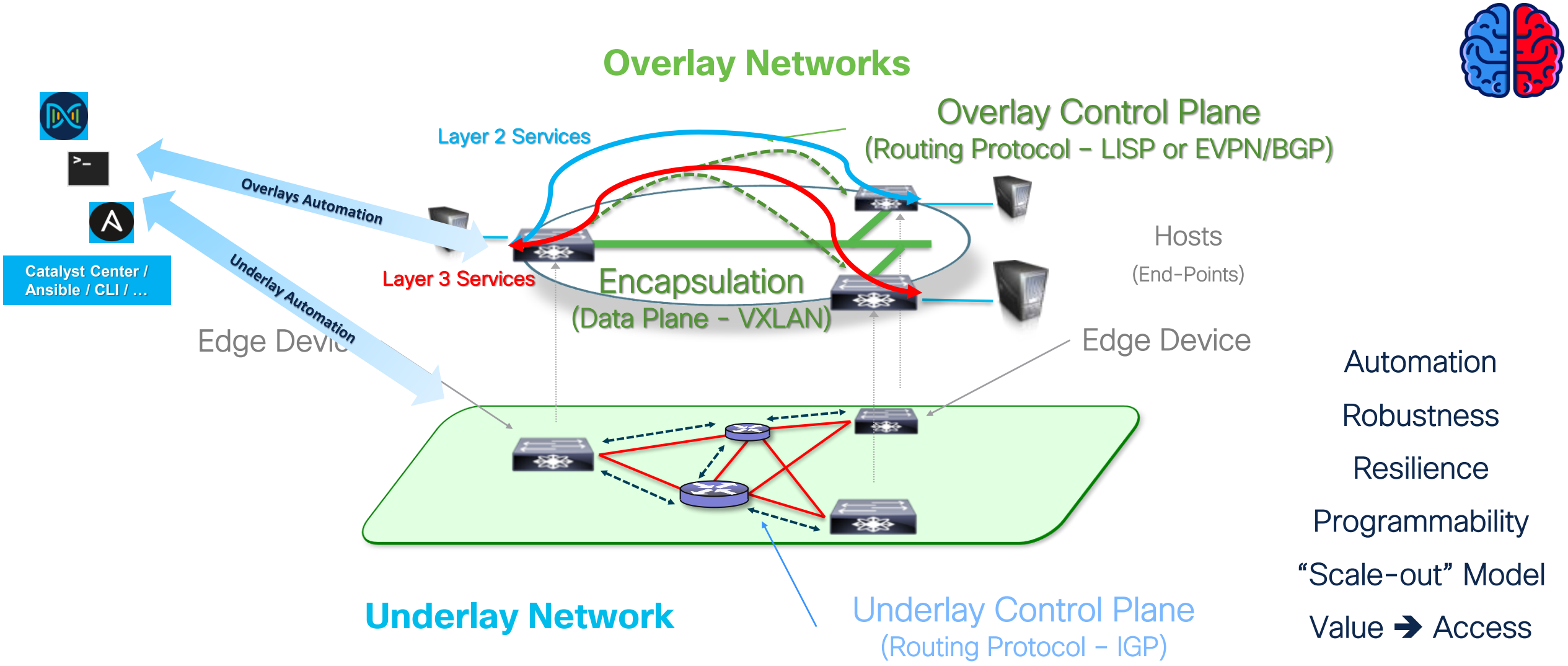
“Scale-out” Model

Value ➔ Access

cisco

Fabric IP – The Fundamentals

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



Automation

Robustness

Resilience

Programmability

“Scale-out” Model

Value ➔ Access

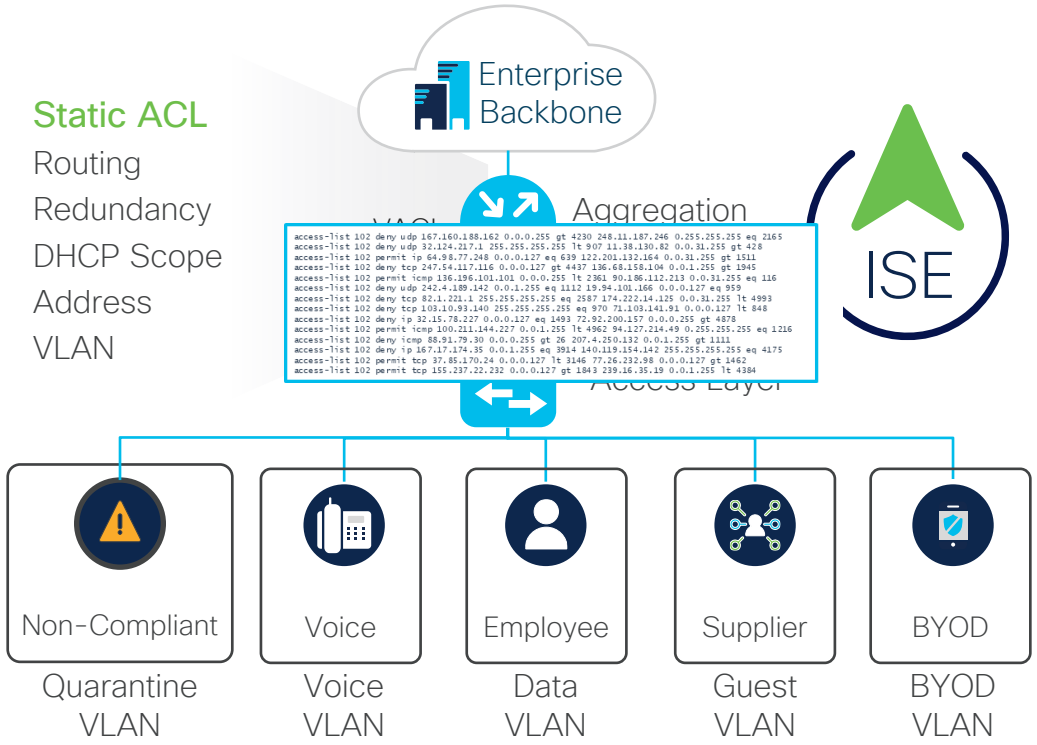
cisco

TrustSec

Group Based Policy Simplifies Segmentation

Traditional Segmentation

Static ACL
Routing
Redundancy
DHCP Scope
Address
VLAN

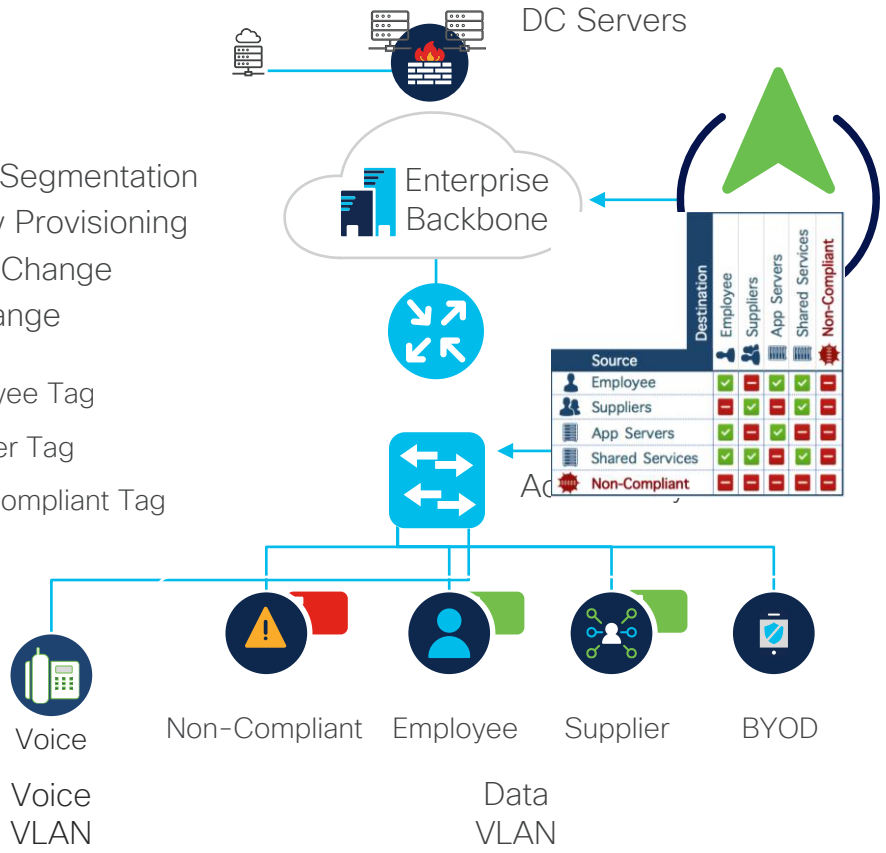


Security Policy based on Topology
High cost and complex maintenance

TrustSec

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

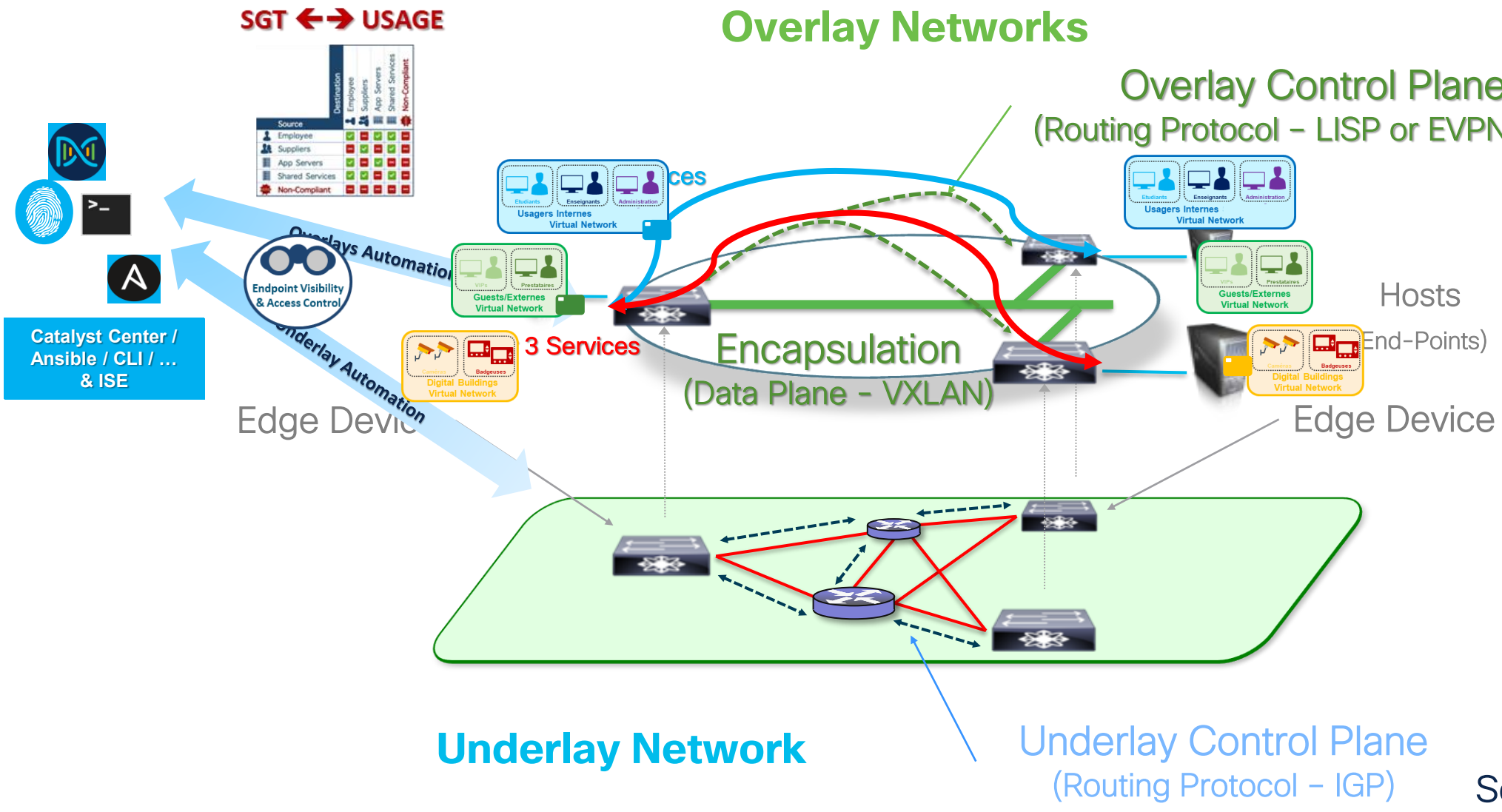
Employee Tag
Supplier Tag
Non-Compliant Tag



Use existing topology and automate
security policy to reduce OpEx

SD-Access: IP Fabric + Automated Security Services

"Security Plane": Access Control + Macro & Micro Segmentation...



Automation

Access Control

Macro & Micro Segmentation

VXLAN: Transport of Segmentation

Identity-based Segmentation & Mobility

cisco

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

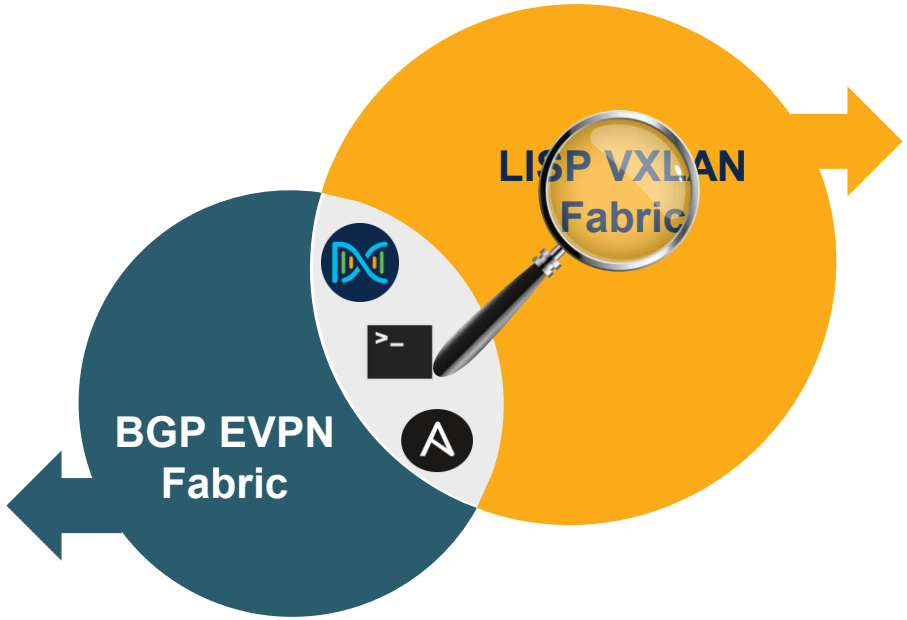
Vendor-agnostic solution with unique Cisco differentiators

Segmentation

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

Operating Mode

Cloud EVPN (**Meraki Dashboard • BGP EVPN-VXLAN**) or Programmable EVPN (**APIs • templates • IaC**)



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

Operating Mode

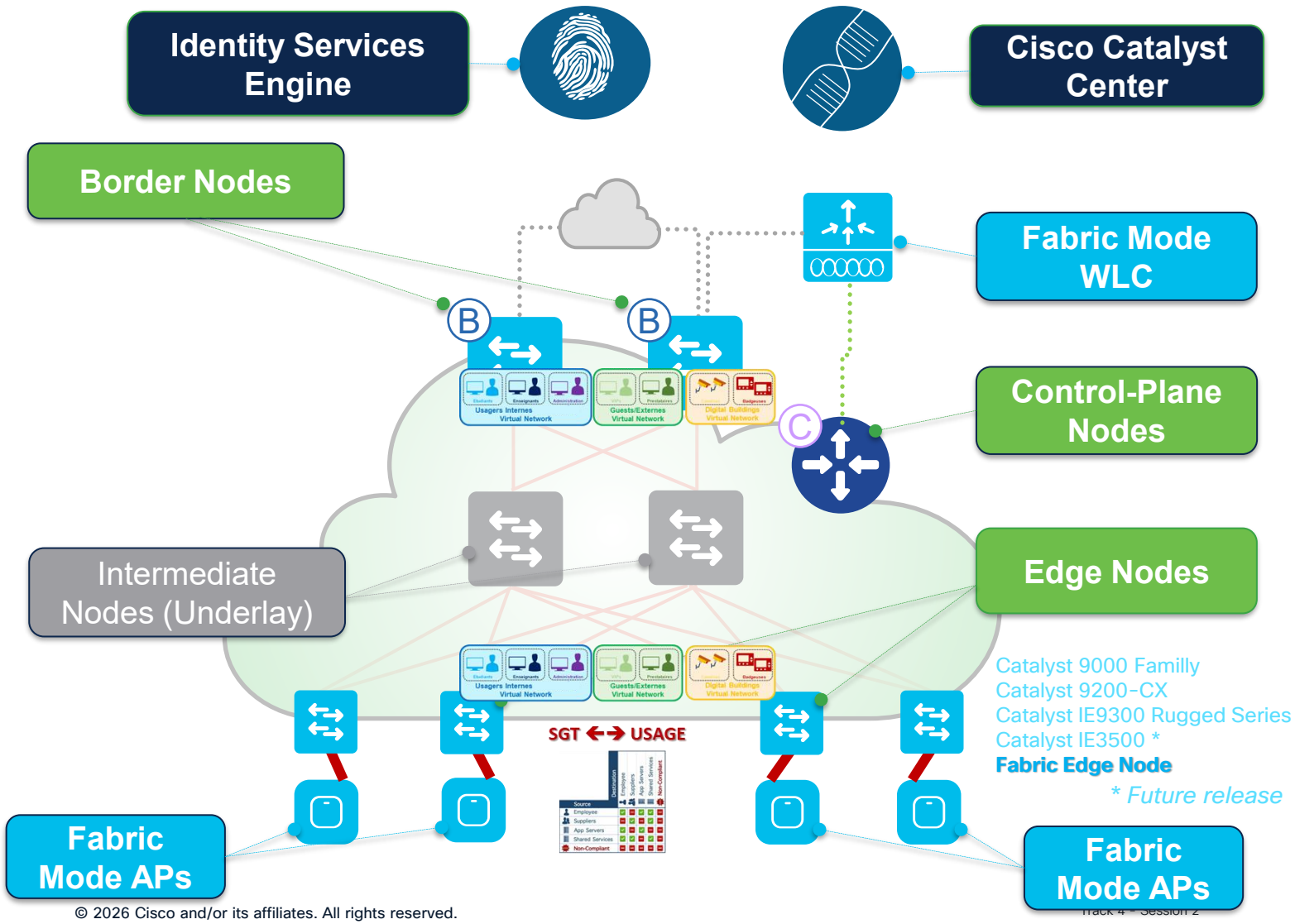
On-Prem SDA (**Catalyst Center • LISP VXLAN**)

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

cisco

Fabric IP – SDA-LISP

Roles & Terminologies



Fabric SDA-LISP - Compatibility Matrix

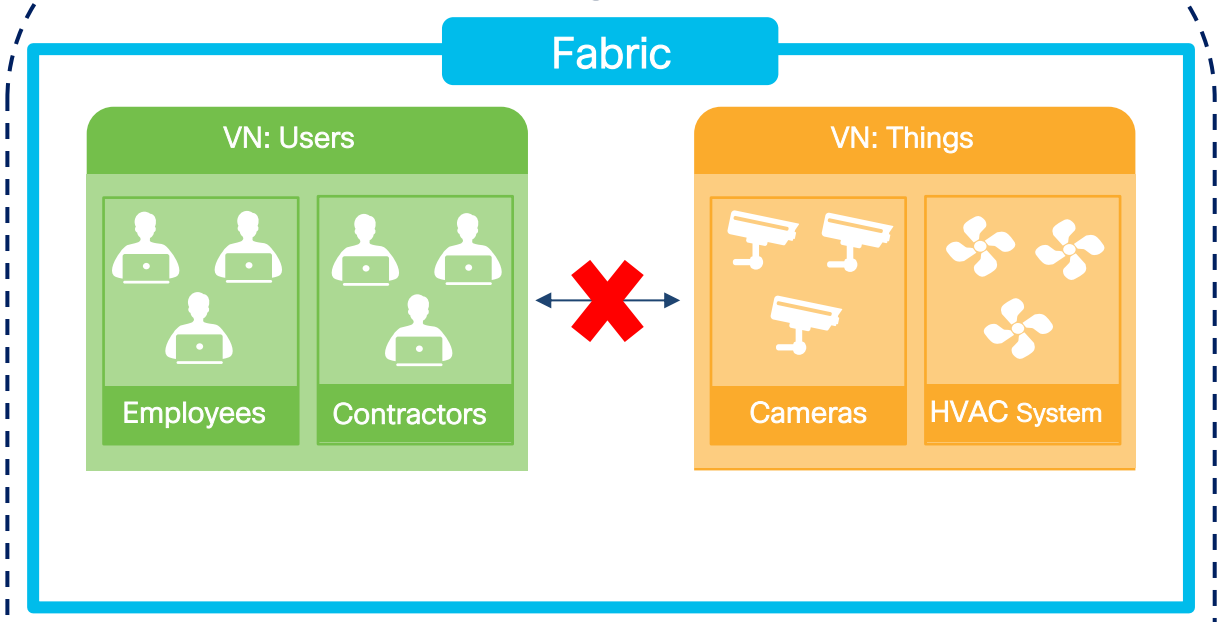
https://www.cisco.com/c/dam/en/us/td/docs/Website/enterprise/catalyst_center_compatibility_matrix/index.html

- **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

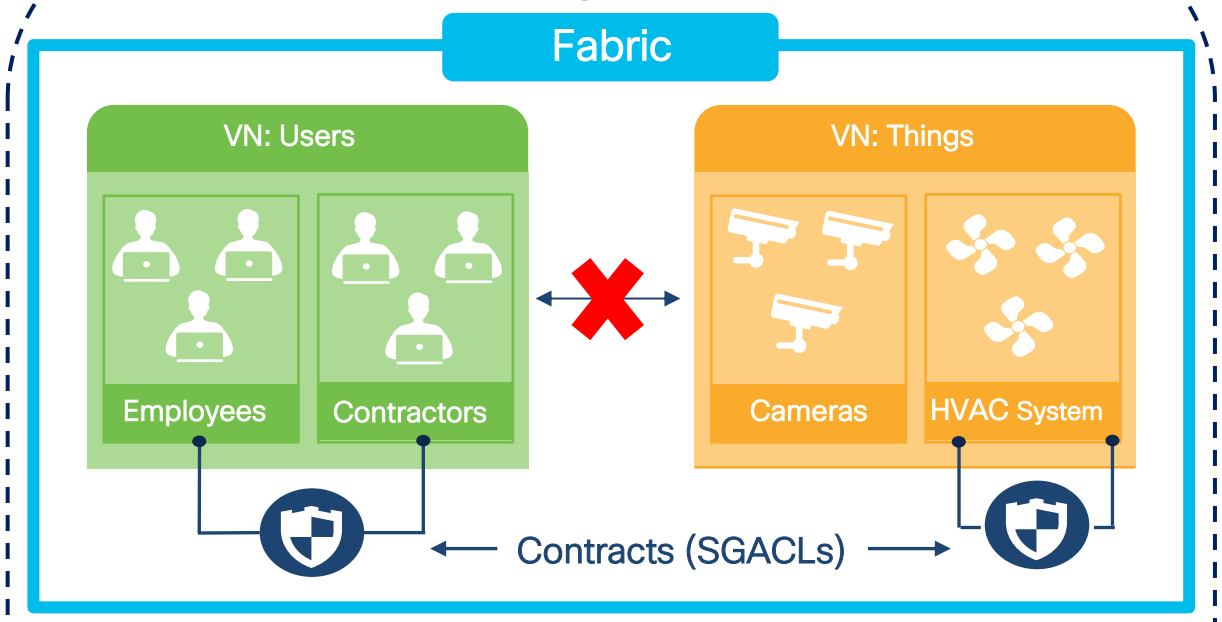
Macro Segmentation



Virtual Network (VN)

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

Micro Segmentation



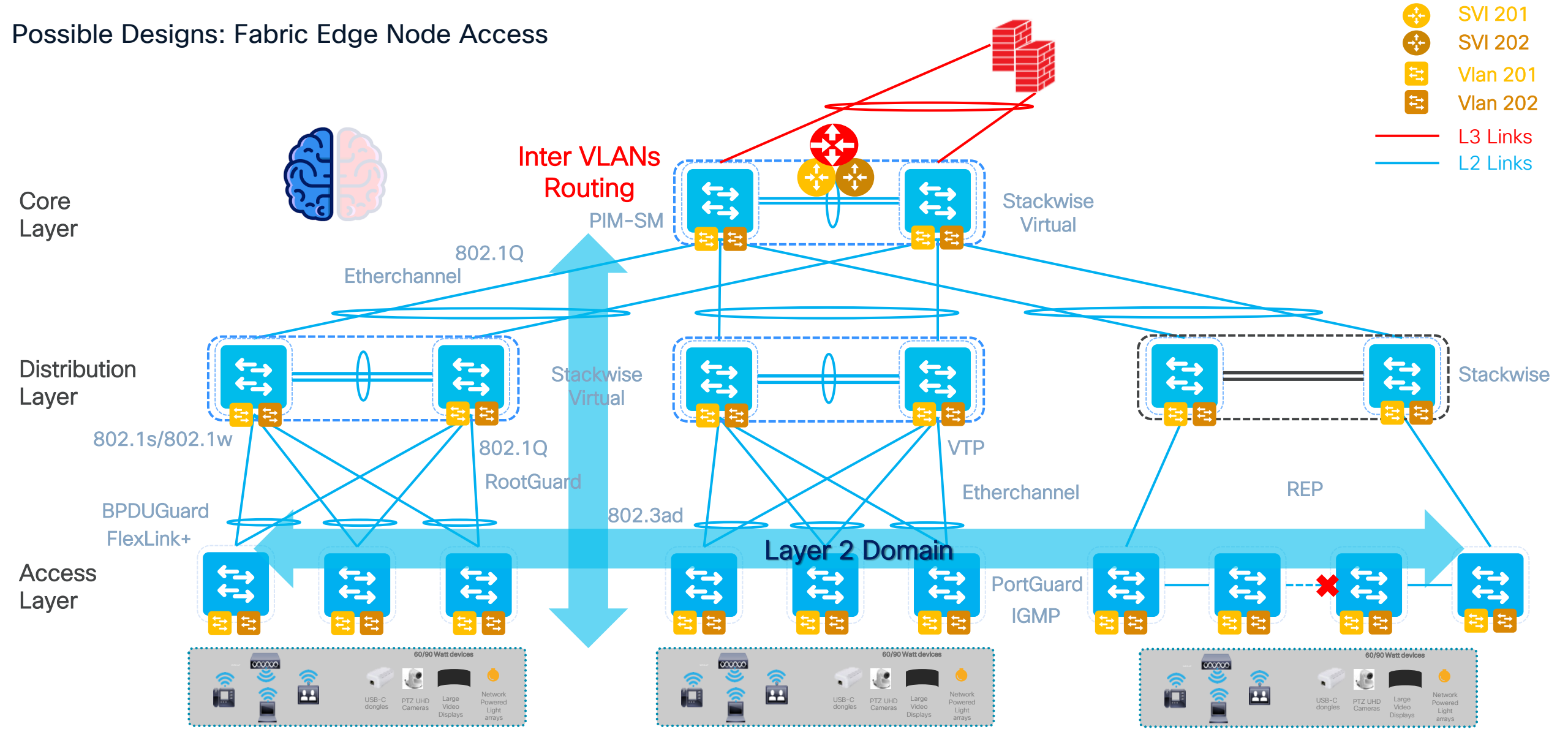
Security Group Tag (SGT)

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

cisco

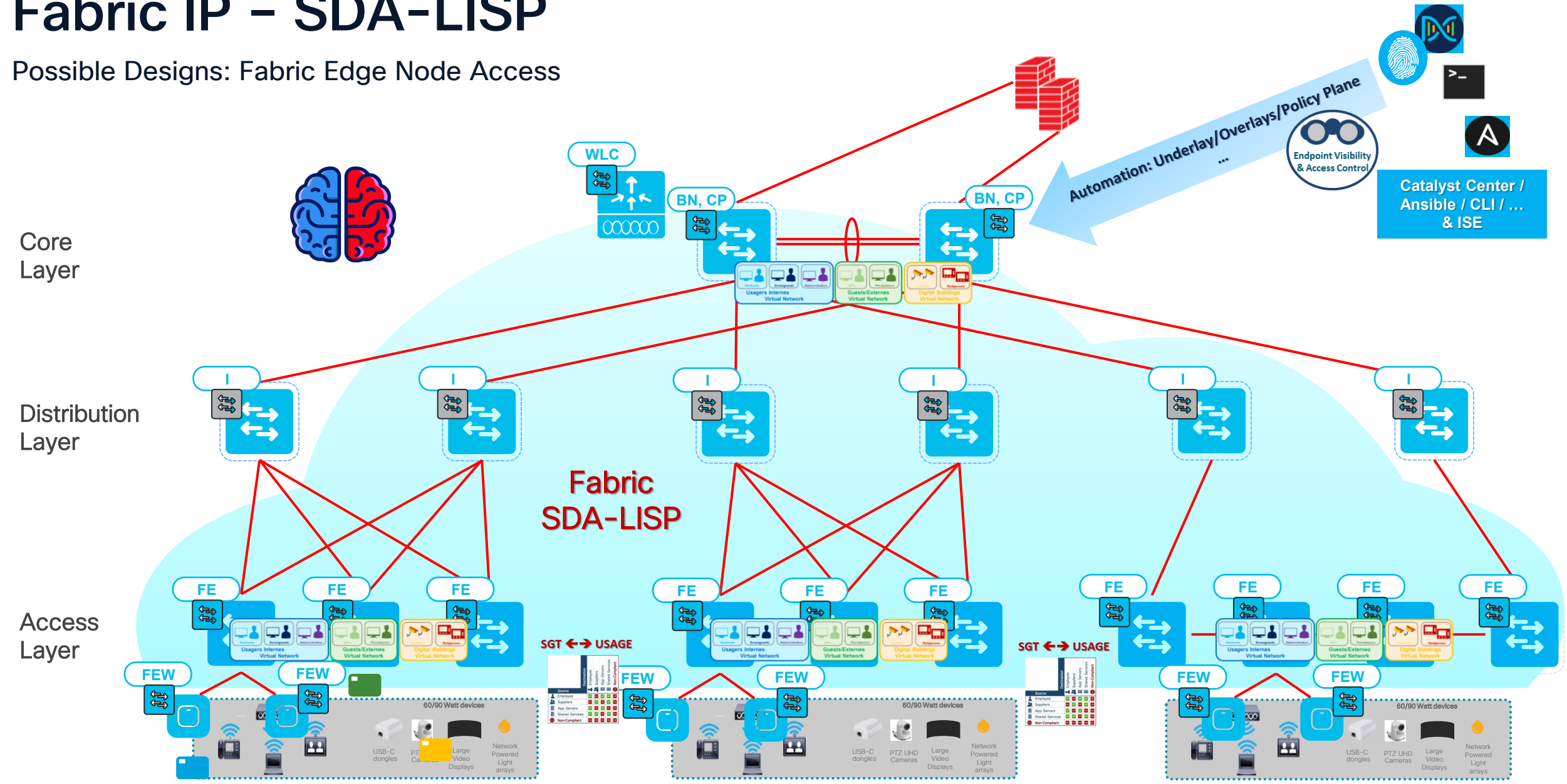
Fabric IP – SDA-LISP

Possible Designs: Fabric Edge Node Access



Fabric IP – SDA-LISP

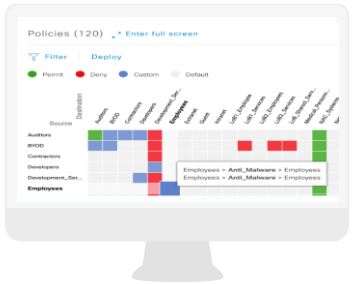
Possible Designs: Fabric Edge Node Access



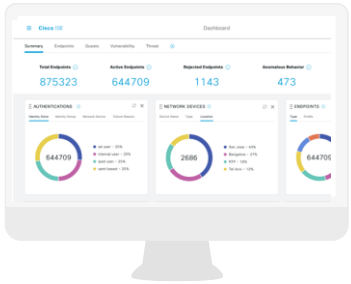
Fabric IP – SDA-LISP

Zero-Trust Evolution

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)

Fabric SDA

In summary...

Core Layer

Distribution Layer

Access Layer

cisco

“Call to action” slides

Key Takeaways

Trustworthy Platform Key foundation for Secure Network

Secure Boot, Security by default, Future proof Capabilities (PQC, Life cycles Management ...)

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

Thank you


CISCO