

Cisco Campus Update

Jesse Schmidt
Systems Engineer

Date placeholder



Agenda

1 Switching

- Recap & New Hardware
- Software updates & High Availability
- Secure Networking

2 Fabric Updates

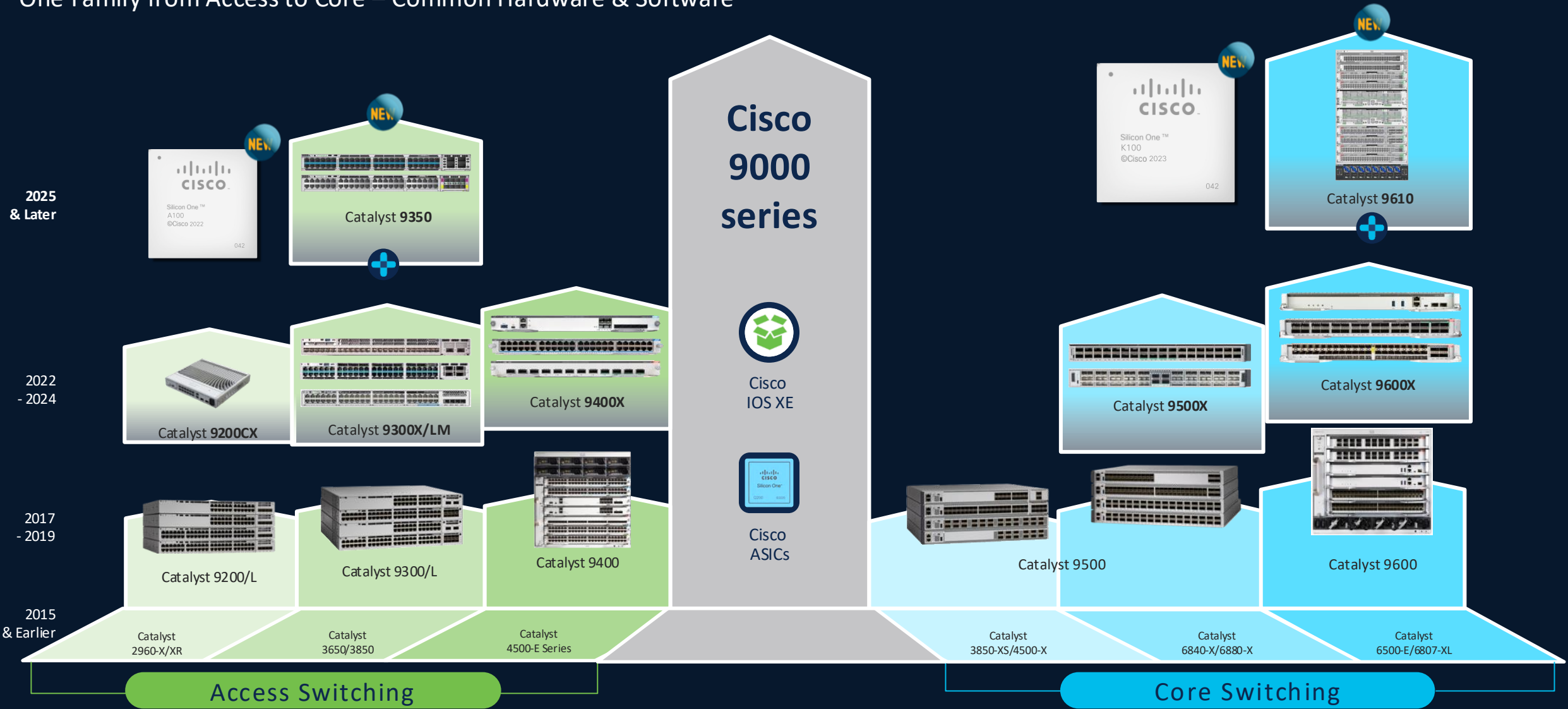
- Campus Fabric Positioning
- SDA (LISP)
- BGP EVPN
- Cloud

Switching

Recap & New Hardware

Cisco Catalyst 9000 Switching Portfolio

One Family from Access to Core – Common Hardware & Software



The Next Generation of Campus Switching

Cisco Silicon One ASICs, Cloud-native IOS-XE, AI-ready Infrastructure

RECAP



Silicon One ASICs

HW Adaptability

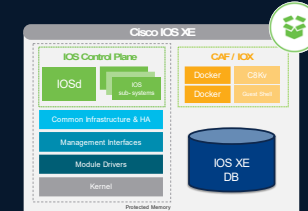
- Massive Campus feature scale (L2/L3, ACL, QoS, NetFlow)
- Innovative Algorithmic TCAM (HCAM) for scaled ACL & FNF
- Permits multiple use cases in a converged solution



Multi-Core X86

AI readiness

- Control-Plane for Agentic Ops and AI agents at scale.
- Enhances Software-assisted Services (AVC/XDR)
- Advanced App-Hosting with AI-Hosting (Edge Compute)



Cloud-native IOS XE

Ops & Security

- Built for Programmability, Telemetry, Virtualization & Unified Management
- Protected Linux system memory to securely host Containers
- Native PQC and Compensating Controls with eBPF Live Protect

Cisco 9350 Series

Portfolio

MultiGigabit SKUs



C9350-48HX
48x 10G mGig
90W UPOE+



C9350-48TX
24/48x 10G mGig
Data only



C9350-24T/48T
24/48x 1G/100M/10M copper
Data only



C9350-24P/48P
24/48x 1G/100M/10M copper
30W PoE+



C9350-24U/48U
24/48x 1G/100M/10M copper
60W UPoE

Gigabit SKUs



C9350-NM-4C
4x40/100G



C9350-NM-2C
2x40/100G



C9350-NM-8Y
8x10/25G or 4x50G

Modular Uplink
100G & 50G at
access

Note: Uplinks/PSU's/Stack Cables are not backward compatible with C9300(X) series

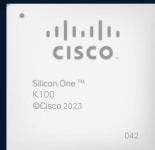
Cisco C9610

Modular core – for high scale/port density

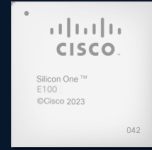
Supervisors



C9610-SUP3XL/3



Enterprise Focus
K100/E100



2M IPv4 / 1M IPv6

3.2 Tbps per slot

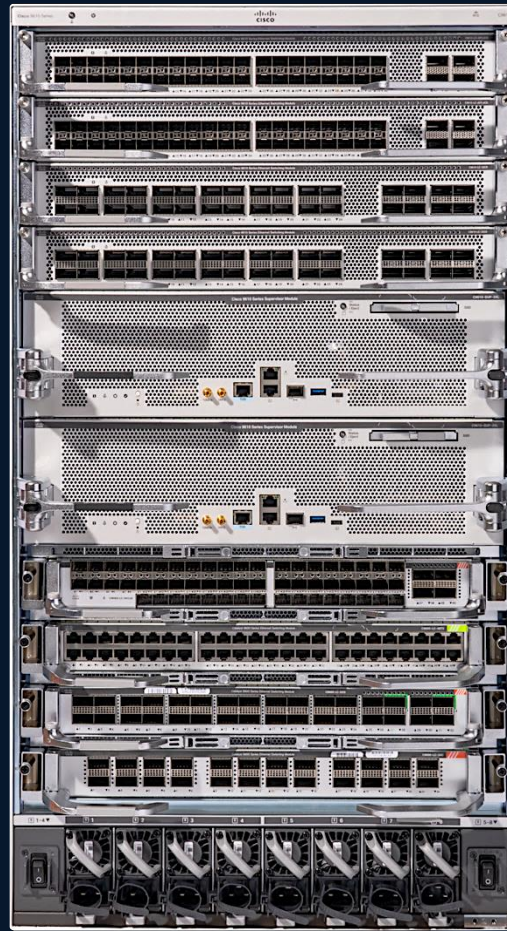
512K hosts or clients*

32G DDR4 memory

256K ACL entries*

8 core X86 CPU
@2.0 Ghz

*Hardware Capable



C9610R

Chassis

51.2 Tbps
System Bandwidth

8-line card slots
(1.25 RU)

2 supervisor slots
(2.5 RU)

4 serviceable
fan trays in rear side

Blue Beacons
(system/fan tray, sup, line
cards)

8 Modular power supplies

Line cards



C9610-LC-40YL4CD



C9610-LC-32CD



4x FAN Trays with
Front to Back Airflow

INTRODUCING

Cisco C9350

Fiber SKUs



Fiber to the Desktop

Stackable with the 9350 Family

Collapsed Designs

Take Cisco C9350 to Fiber Distances



SyncE Timing Port



Integrated GPU



Deep Buffer

Private 5G*

Future AVID Certification

Small Language Model

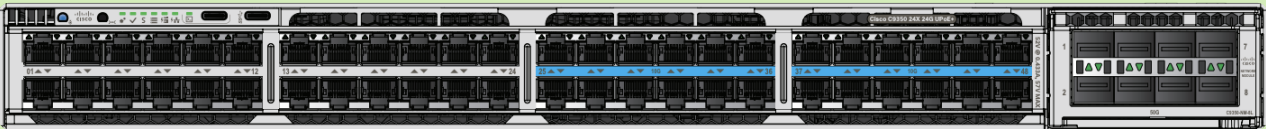
Accelerated App Hosting

Intelligent Buffer
Management

Cisco C9350-48HXG – High End C9350

Cisco C9350 Series

Phase 2 mGig SKU



Cisco C9350-48HXG*
24x 10G-mGig & 24x 1G w/ 90W UPoE+



IOS-XE 26.2.1

8GB DDR	For deep buffering
8-core CPU	Integrated GPU for AI powered workloads
5G ready	PTP and SychE capable



Cisco C9350-48HXN
12x 10G-mGig & 36x 5G-mGig w/ 90W UPoE+



IOS-XE 26.1.1



Cisco C9350-24HX
24x 10G-mGig w/ 90W UPoE+



IOS-XE 26.1.1



Cisco C9350-48HM
48x 2.5G w/ 90W UPoE+



IOS-XE 26.2.1

Quantum Resistant

Hitless Upgrades

Live protect

Smart Stacking



Cisco C9350-NM-8L*
8 port 50/25G/10G/1G Uplink



Cisco C9350-NM-8M
8 port 10G/mGig Data

Flexible 50G uplinks at access

*C9350-24Y & C9350-48HX/TX only

Cisco C9350 Series

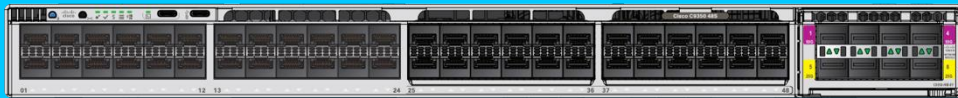
Fiber SKU and flexible stacking



Cisco C9350-24Y
24x 25G/10G/1G SFP28



Cisco C9350-12Y
12x 25G/10G/1G SFP28

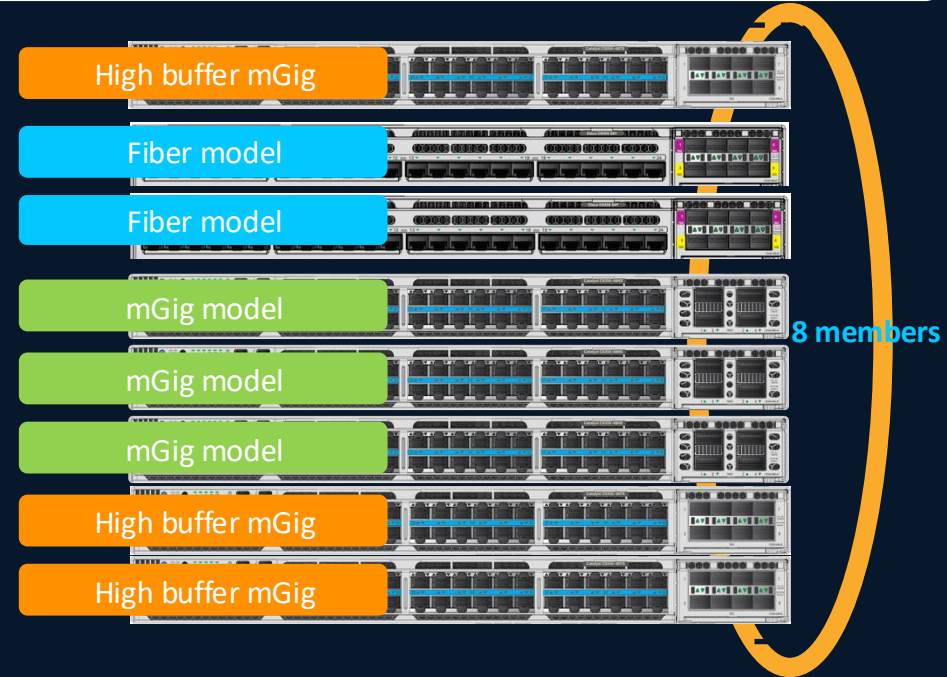


Cisco C9350-48S
48x 1G SFP



Cisco C9350-24S
24x 1G SFP

No restrictions to stacking – Mix and match as per your requirements



1.6T Guaranteed Stacking bandwidth

User friendly Stacking design

Isolated bandwidth loss in event of failure

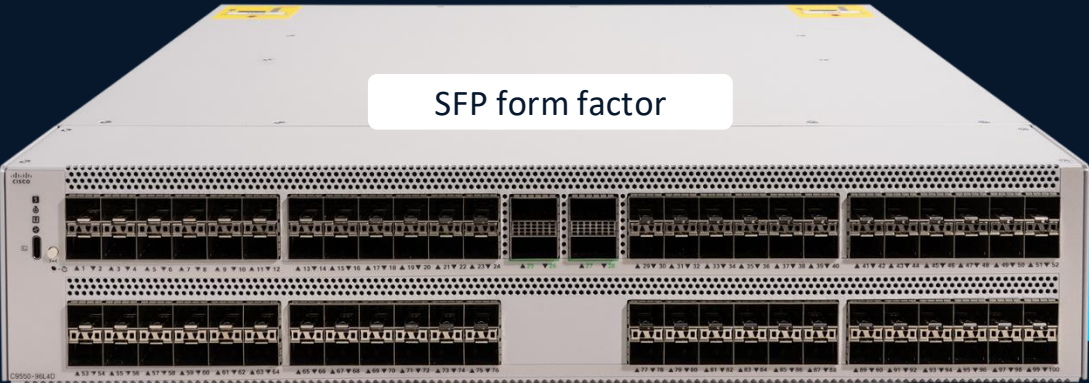
Enhanced Stackpower
More power draw per cable

Introducing C9550 Series

New 2RU units



IOS-XE 26.2.1
Day-0 Unified Management



SFP form factor

Quantum Resistant

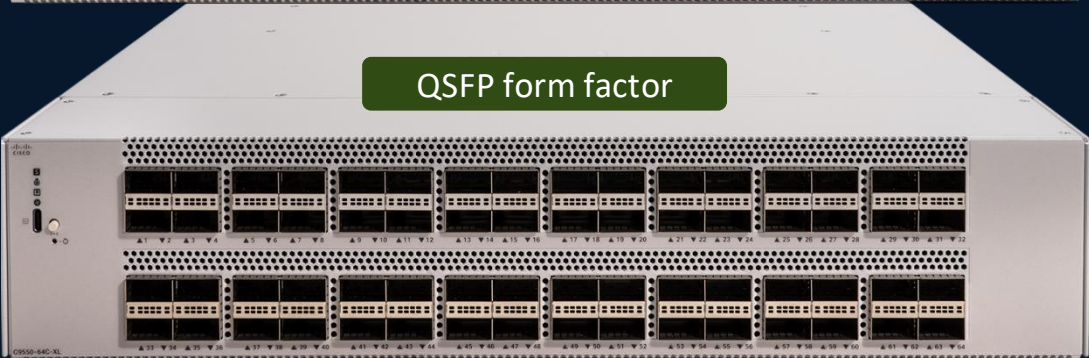
Live protect

Enhanced
Stack Wise Virtual

C9550-96L4D
96 x 10/25/50G
4 x 40/100G/400G

2x – 25G port-density compared to C9500-48Y4C

1.6x – 25/50G port-density compared to C9500X-60L4D



QSFP form factor

C9550-64C-XL
64 x 40/100G
With 8 GB HBM

2x – 100G port-density compared to C9500-32C

1.8x – 100G port-density compared to C9500X-28C8D*



C9550-FAN-2U
Same PID for 2RU units

3 x fan tray units
2 + 1 redundant

Reversible airflow fantrays*



C9K-PWR-1100WAC
1 + 1 redundancy

Titanium power supplies

8x – IPv4 route scale compared to C9500H series

1x – IPv4 route scale compared to C9500X series

9x – ACL scale compared to C9500X series

1.3x – ACL scale compared to C9500H series

Introducing C9550 Series

Refreshing current portfolio



IOS-XE 26.2.1
Day-0 Unified Management

Quantum Resistant

Enhanced StackWise Virtual

Live protect

SFP form factor



C9550-24L4CD
24x 1/10/25/50G
4x 40/100G/ 2x 400G



C9550-48L4CD
48x 1/10/25/50G
4x 40/100G/ 2x 400G

Reversible airflow fantrays*



C9550-FAN-1U
Same PID for 1RU units

5 x fan trays
4 + 1 redundancy

QSFP form factor



C9550-32C
32x 40/100G

Titanium power supplies



C9K-PWR-750WAC
Same PID for 1RU units

2 x PSU
1 + 1 redundancy

2x IPv4 route scale
Compared to C9500H series

Cisco C9550 Smart Fixed-core

Full Portfolio

SFP form factor



C9550-48L4CD

48x 1/10/25/50G
4x 40/100G/ 2x 400G

Now Orderable!



C9550-24L4CD

24x 1/10/25/50G
4x 40/100G/ 2x 400G

QSFP form factor



C9550-32C

32x 40/100G

Orderable Sept 2026



Powered by
Silicon One E104

SFP form factor



Powered by
Silicon One E100

Now Orderable!

2 RU box



C9550-96L4D

96x 10/25/50G
4x 40/100/400G

QSFP form factor

Orderable Sept 2026



2 RU box

C9550-64C-XL

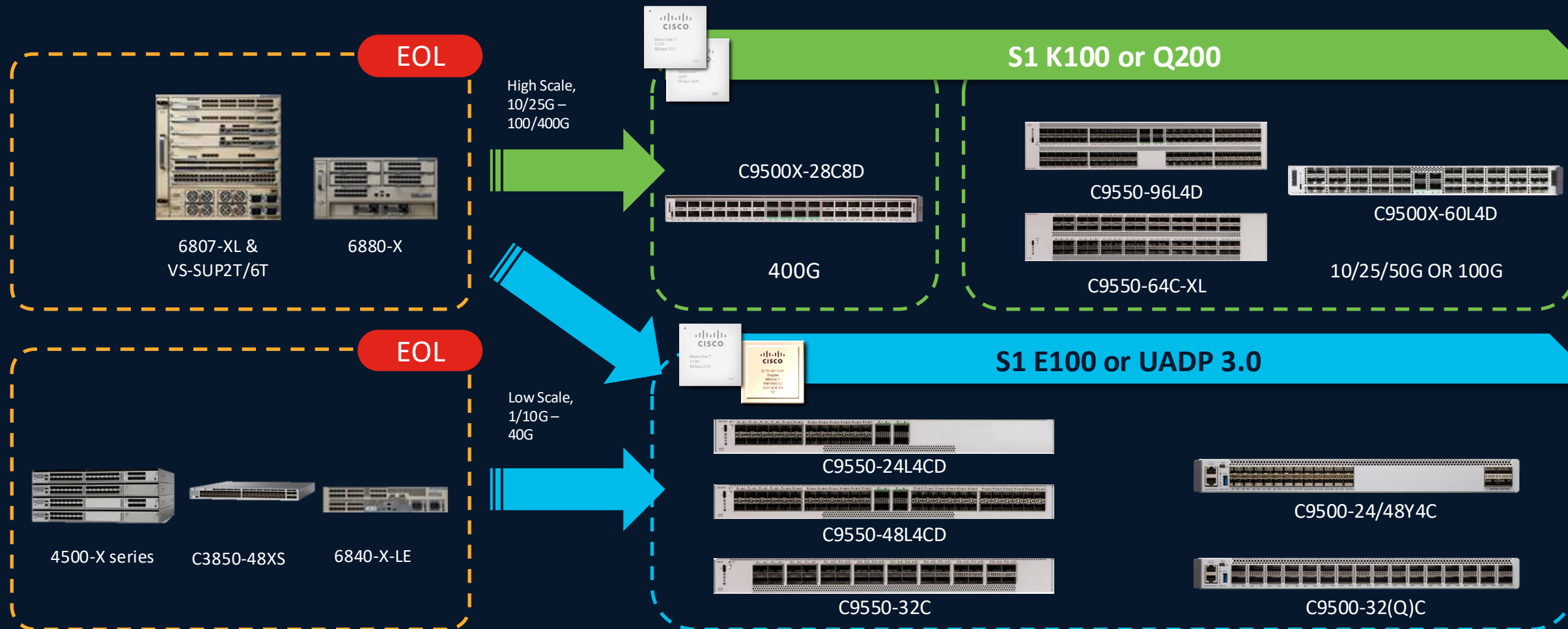
64x 40/100G

With 8 GB HBM



Powered by
Silicon One K100

Cisco 9500 Series 'Statement of Direction'



No plans to EoS/EoL the above Catalyst 9000 series of switches

Don't hesitate to position the above Catalyst 9000 series core switches

Switching

Software updates & High Availability



OnPrem



Cloud

Enterprise Campus HA Framework

System | Network | Operational



IT



Multitenant



Security



AV Networks



Space

OT



BMS



Scada



Sustainability



Industrial

Resilient Converged Enterprise Campus Network Infrastructure

System

General

Fixed | Modular

PSU Redundancy
Fan Redundancy
Online Insertion (OIR)

StackWise

Fixed

StackWise (N+1, 1:1)
StackPower
Hosted App Redundancy
Redundant Stack (SSO)
Redundant Storage
Fast POE
Perpetual POE

StackWise Virtual

Fixed | Modular

StackWise Virtual
Dual Active Detection
Redundant Sup (SSO)
Quad-Sup RPR-WARM

Network

Interface

Carrier Delay
Fast Link Notification (FLN)

Layer 2

Enhanced PAgP (ePAgP+)
UDLD
Layer 2 MEC
Flexlink+
Resilient Ethernet Protocol (REP)
Layer 2 LoopDetect

Layer 3

NSF | NSR
Layer 3 MEC
Fast IGP – OSPF | IS-IS
GIR Maintenance - IGP, BGP
BFD – Single | Multi Hop
HSRPv2 – Fast-Hello, BFD
Enhanced Object Tracking
LFA IPFRR – OSPF | EIGRP

Operational

Software Mgmt

Inservice SW Upgrade (ISSU)
Ext. Fast SW Upgrade (xFSU)
SMU - Hitless | Cold

HA Automation

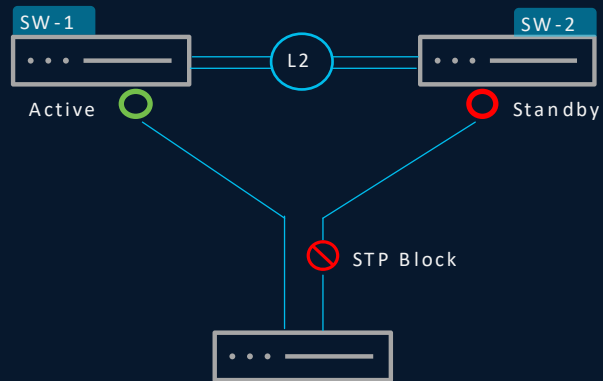
Machine Reasoning Engine (MRE)
Integrated GOLD Test
Link TDLR Test
EEM – Event Driven Automation



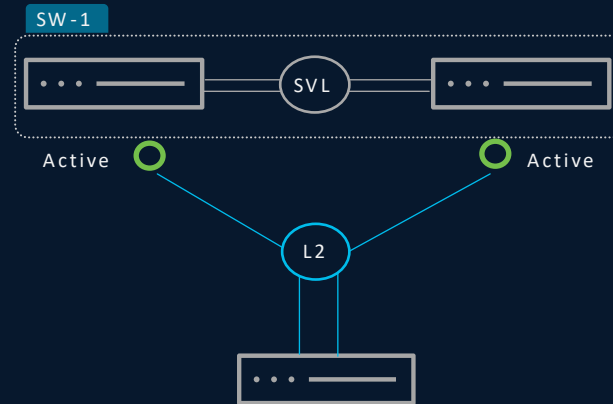
Power of **Cisco IOS-XE™** – Industry's most Versatile, Open and Resilient Network OS

FHRP

HSRP | VRRP | GLBP

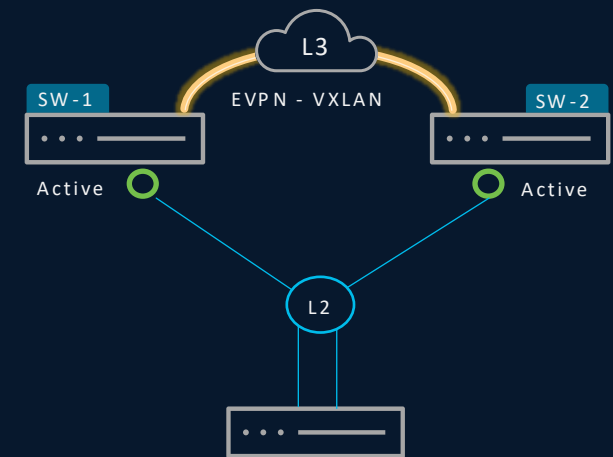


StackWise Virtual

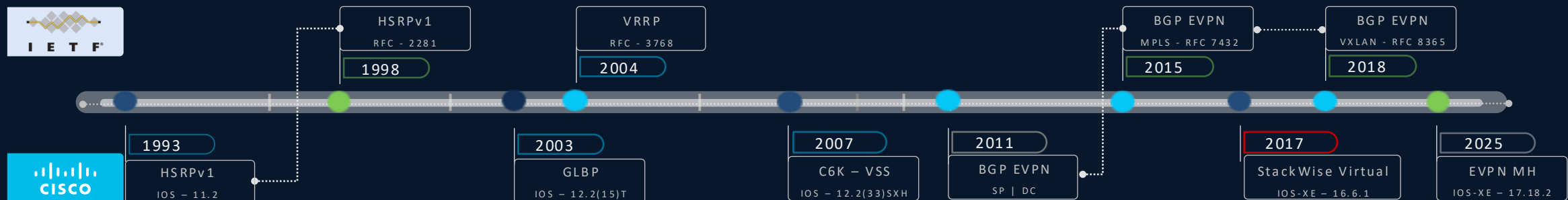


EVPN Multihoming

RFC 8365



○ Active VLAN
○ Standby VLAN





Catalyst Center

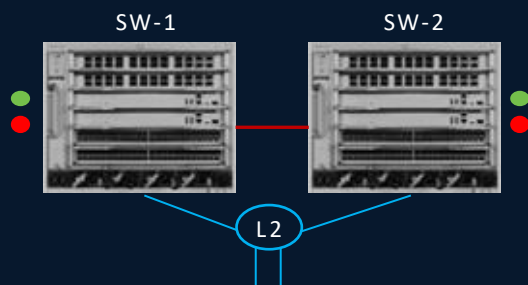


Dashboard

Device Mgmt | 360° | Topology | Base Automation | Network Profile | SWIM | ISSU/SMU Upgrade

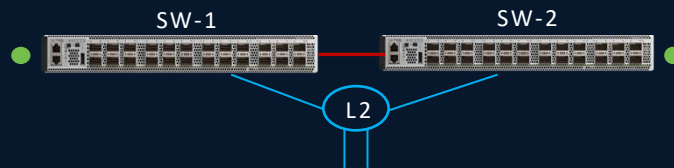
Catalyst 9600 9400

Modular - HA | Non-HA



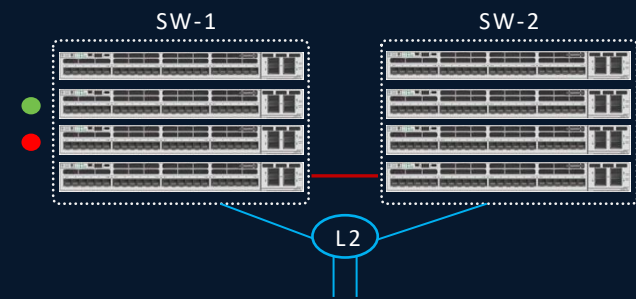
Catalyst 9500 9300

Fixed - Non-Stacking



Catalyst 9300

Fixed - StackWise



Switch



Wireless



Firewall



Host

● Active
● Hot-Standby



Standard-Based

Standard-based L2 Multipath
Follows RFC 7432 | 8365
Proven BGP control-plane



Flexible

Non-Fabric | Fabric Network
Least-disruptive integration
Elastic network placement



Distributed

Fully Distributed Planes
Advanced synchronization
Independent Upgrades



Performance

Non-blocking architecture
All-Active Ports | VLANs
Increase 2X Performance



Resilient

Near Hitless Upgrades
Non-Stop communication
Deterministic Availability

EVPN Multihoming – Product Support Matrix

Catalyst 9K
Modular Switch

Catalyst 9600 Series – Sup-1
Catalyst 9600 Modules – Any

Catalyst 9400 Series – Sup-1
Catalyst 9400X Series – Sup-2
Catalyst 9400 Modules – Any

Catalyst 9K
Fixed Switch

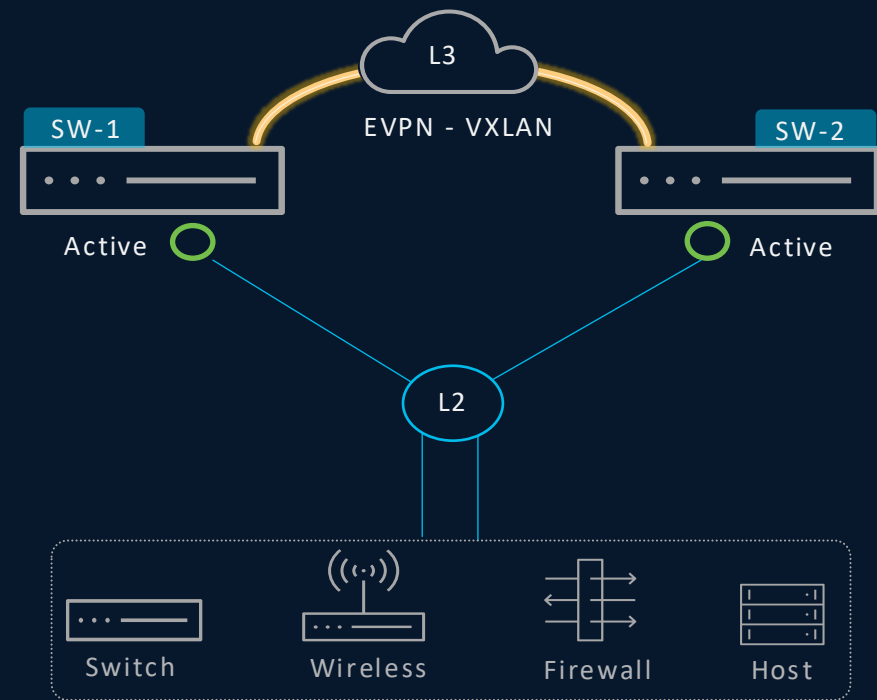
Catalyst 9500-H Series

Catalyst 9300X Series

Catalyst 9300 Series

Software License

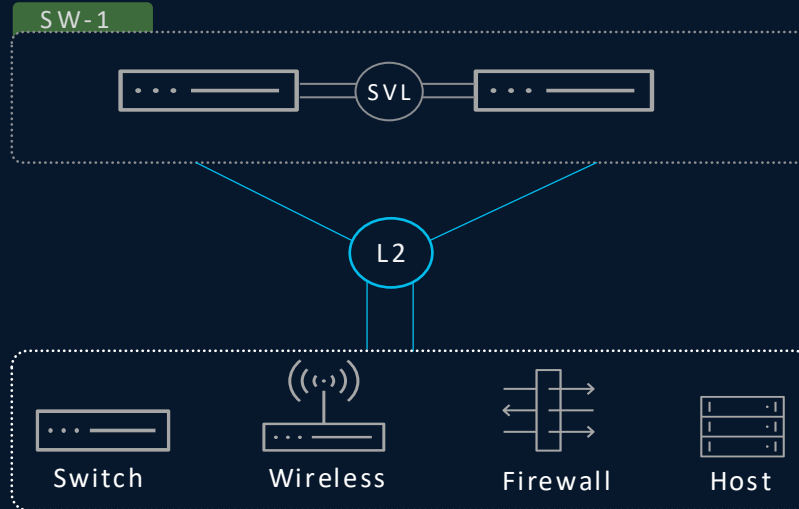
Network Advantage





StackWise Virtual

Recommended



Switch Support : Catalyst 9500, 9500-X

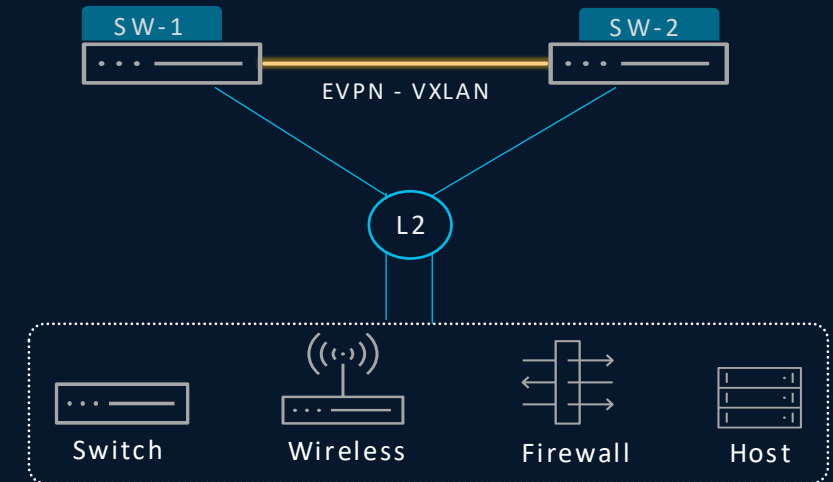
Benefits : Simple, L3 MEC, Resilient, Inter-Switch ISSU, Proven

Competitive : Differentiator since 17+ years

Limitation : Extended ISSU Compatibility Matrix impacting downtime



EVPN Multihoming



Switch Support : Catalyst 9500, 9300, 9300-X

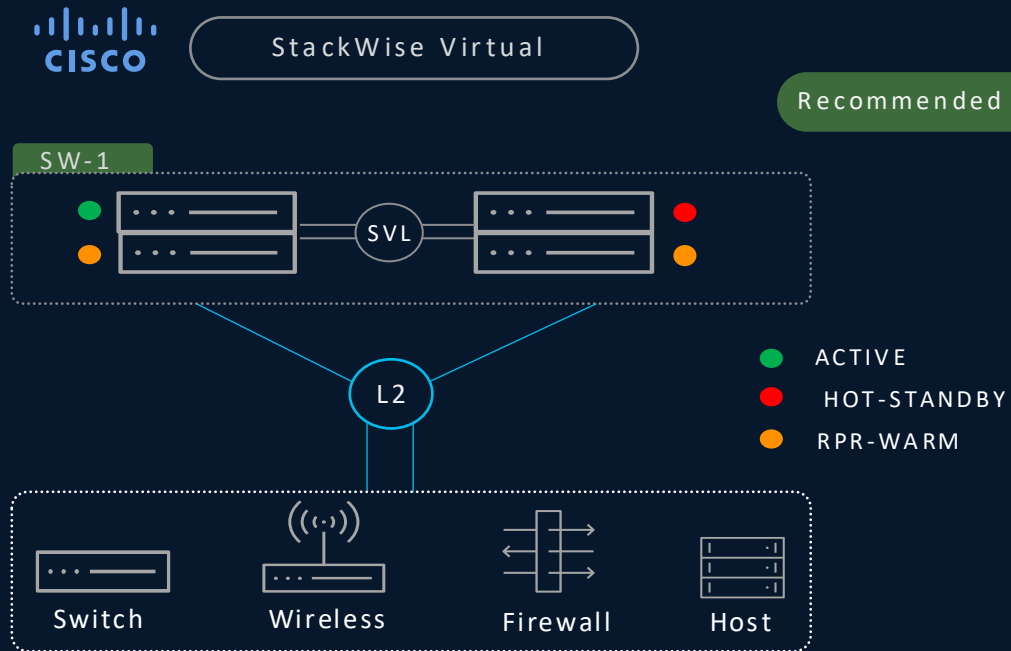
Benefits : Distributed Planes, ISSU independent, Resilient

Competitive : Multi-vendor compatible

Limitation : Advanced technology, Scale, L3 MEC

Fallback :

Network Availability during software upgrade is must



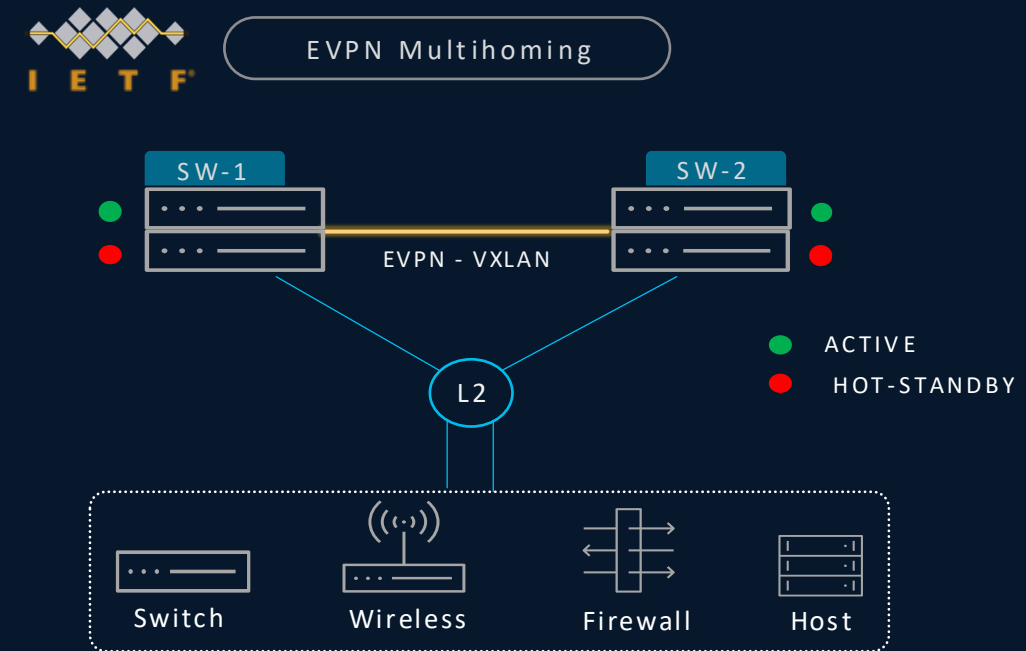
Switch Support : Catalyst 9400, 9400X, 9600 (Sup-1 | Sup-2)

Benefits : Simple, L3 MEC, Resilient, Inter-Switch ISSU, Proven

Competitive : Differentiator since 17+ years

Limitation :

- Extended ISSU Compatibility Matrix impacting downtime
- Quad-Sup NSF | SSO



Switch Support : Catalyst 9400, 9400X, 9600 (Sup-1)

Benefits : Distributed Planes, Quad-Sup NSF/SSO, ISSU, Resilient

Competitive : Multi-vendor compatible

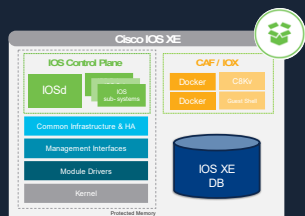
Limitation : Advanced technology, Scale, L3 MEC

Fallback :

Network Availability during software upgrade is must
Quad-Sup NSF/SSO is must



Unified Management



Common Operating System & Image

Cloud-native IOS XE



Common ASIC Architecture

Silicon One



Live Protect
Ready

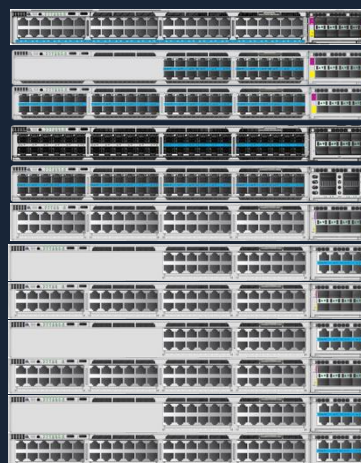


PQC
Compliant

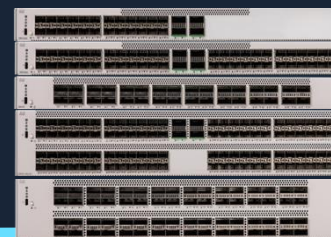


Intelligent
Power Optimization

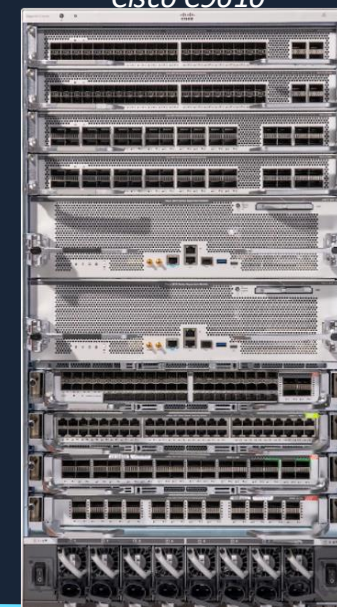
Cisco C9350



Cisco C9550



Cisco C9610



Cisco C9000 Smart Switch Family

Common Hardware, Software and Management

Available Now

It starts with a streamlined onboarding process

Users can quickly onboard new devices to the network, choose the configuration source, and begin cloud management without any additional applications.

Add devices to network



Select network

2

Configure IOS-XE
devices

3

Summary

Device management and configuration source

C9500

Device

C9500H refers to C9500-48Y4C, C9500-24Y4C, C9500-32C, C9500-32QC

C9200/C9300/C9500H ⓘ devices



Cloud configuration ⓘ

Configuration is sourced from the Meraki Dashboard.



Device configuration ⓘ

Configuration remains local to the device.

Device configuration credentials

Please provide the [level 15 configuration access credentials](#) ⓘ so the Meraki dashboard can make necessary configuration changes to these devices.

Username

Password

Maintain operational flexibility with cloud management

Configuration Source: Cloud



UNLOCK FULL CLOUD SIMPLICITY

Configurations are performed in the cloud and managed using the dashboard UI

Configuration Source: Device



RETAIN ADVANCED CONTROL

Configurations are managed via traditional methods and performed local to the device

FLEXIBLE OPTIONS FOR MANAGING YOUR DEVICES FROM THE CLOUD

Configuration Source: Cloud

The full cloud experience with management and configurations performed in the cloud

- Cloud CLI Support for read-only 'show' commands for advanced troubleshooting
- Leverage the intuitive user interface to build configurations that are performed directly from the Meraki cloud at scale.

The screenshot shows a three-step process for adding devices to a network. Step 1, 'Select network', is completed. Step 2, 'Configure IOS-XE devices', is the current step. It features a section for 'Device management and configuration source' with two radio button options: 'Cloud configuration' (selected) and 'Device configuration' (marked as Beta). The 'Cloud configuration' option includes a description: 'Configuration is sourced from the Meraki Dashboard.' At the bottom of the form are 'Cancel', 'Back', and 'Next' buttons.

Add devices to network

1 Select network 2 Configure IOS-XE devices 3 Summary

Device management and configuration source

C9200/C9300 devices

☒ Cloud configuration
Configuration is sourced from the Meraki Dashboard.

☐ Device configuration **Beta**
Configuration remains local to the device.

Cancel Back Next

[Full List of Supported Models Here](#)

Configuration Source: Device

Cloud scale visibility with localized configurations and the full IOS XE feature set

- Non-destructive onboarding preserves configurations, which are managed and performed local to the device via traditional methods.
- Cloud CLI support for show and config commands in dashboard
- Configuration back up in the cloud.

Add devices to network

1

Select network

2

Configure IOS-XE devices

3

Summary

Device management and configuration source

C9200/C9300 devices

☐

Cloud configuration
Configuration is sourced from the Meraki Dashboard.

☒

Device configuration Beta
Configuration remains local to the device.

[Cancel](#)[Back](#)[Next](#)

[Full List of Supported Models Here](#)

Release strategy

New release structure for a new product family



1 x **EM release** per year
2 x **SM releases** per year

EMR supported for 48 months from FCS
SMR supported for 12 months from FCS

Changing to

Why should you care?

6 months between recommended
releases (compared to 12 months today)

2 x **EM releases** per year
One in **Feb** and second in **August**

EM releases are supported for 48
months from FCS date (same as before)

IOS-XE release naming
Year.Release.Build

Next Upcoming releases will be **IOS-XE 26.1.x and 26.2.x**

xFSU Evolution on Catalyst 9300 Series

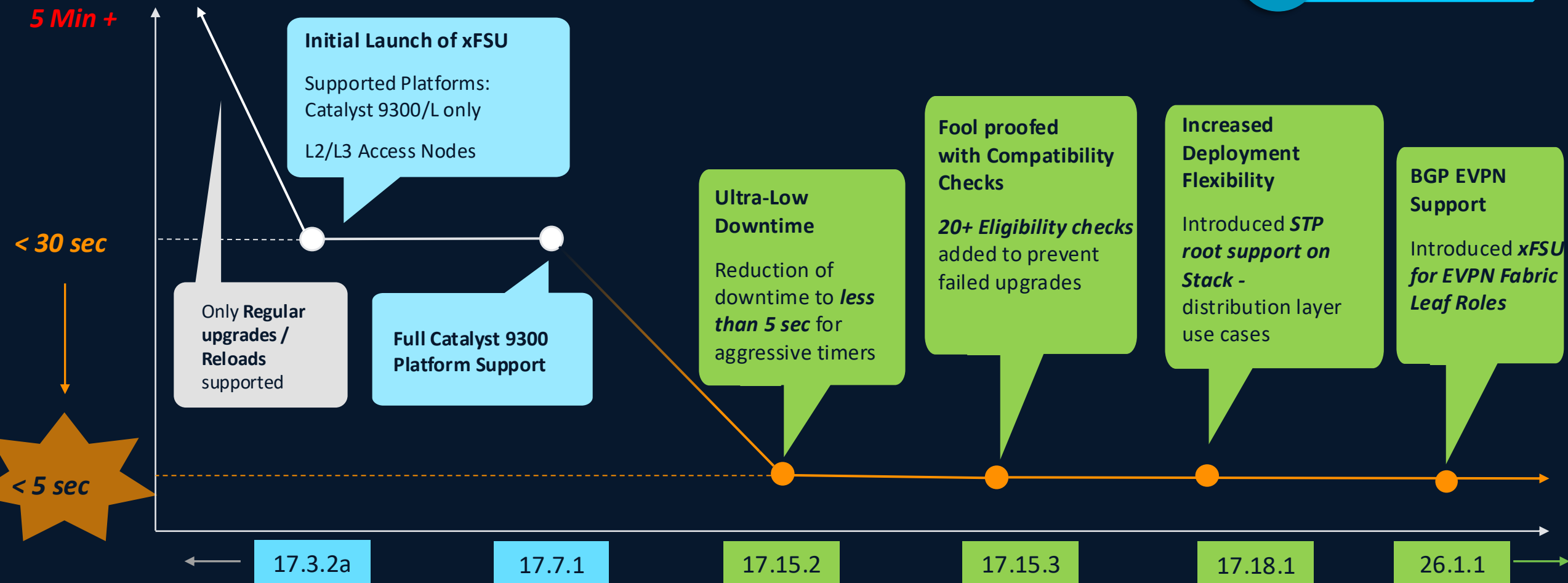
From **Downtime Reduction** to more **Flexibility**



IOS-XE 26.2.1
SDA Support



Catalyst Center 3.2.1
xFSU Workflow



The Next Gen xFSU on C9350 Smart Switches

Achieving **Sub-sec downtime** for upgrades and reloads

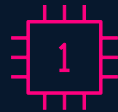


IOS-XE 26.1.1
Standalone switches
Stack switches Roadmap



Control Plane Reload Now 3x Faster

C9350 uses **kexec-based reload** instead of ROMMON.
This reduces bring-up time from **3 min to just 1 min.**



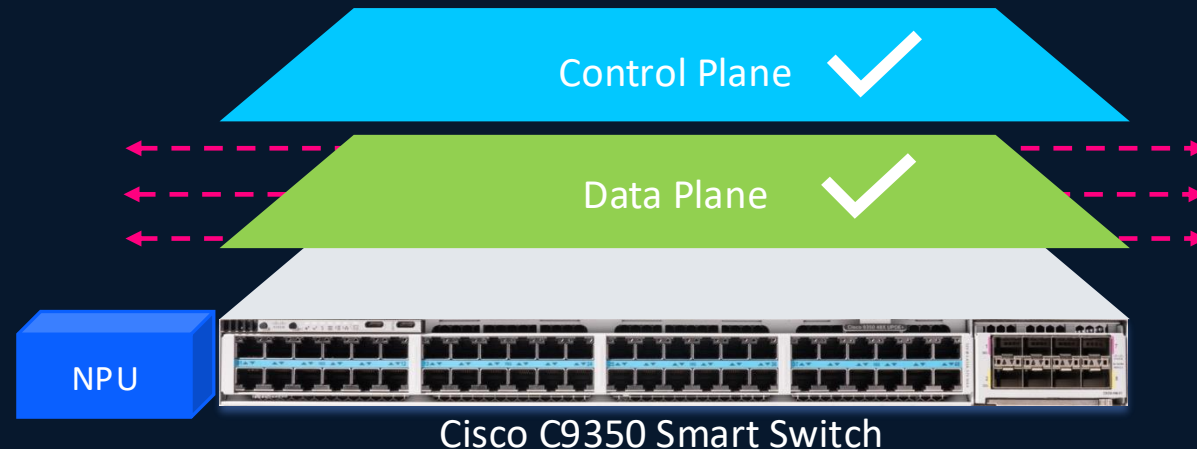
S1 ASIC Preservation Minimized Downtime

Unlike UADP, S1 ASIC isn't fully reprogrammed.
Traffic impact limited to **select registers** based on operational features



Layer 2 Resiliency with STP Offload

STP offload to NPU Host ensures **uninterrupted BPDU** transmission.
This allows xFSU support on Layer 2 roots.



Performance
Breakthrough

<1 sec
Downtime*

Flexible xFSU Implementation (C9350 Standalone)

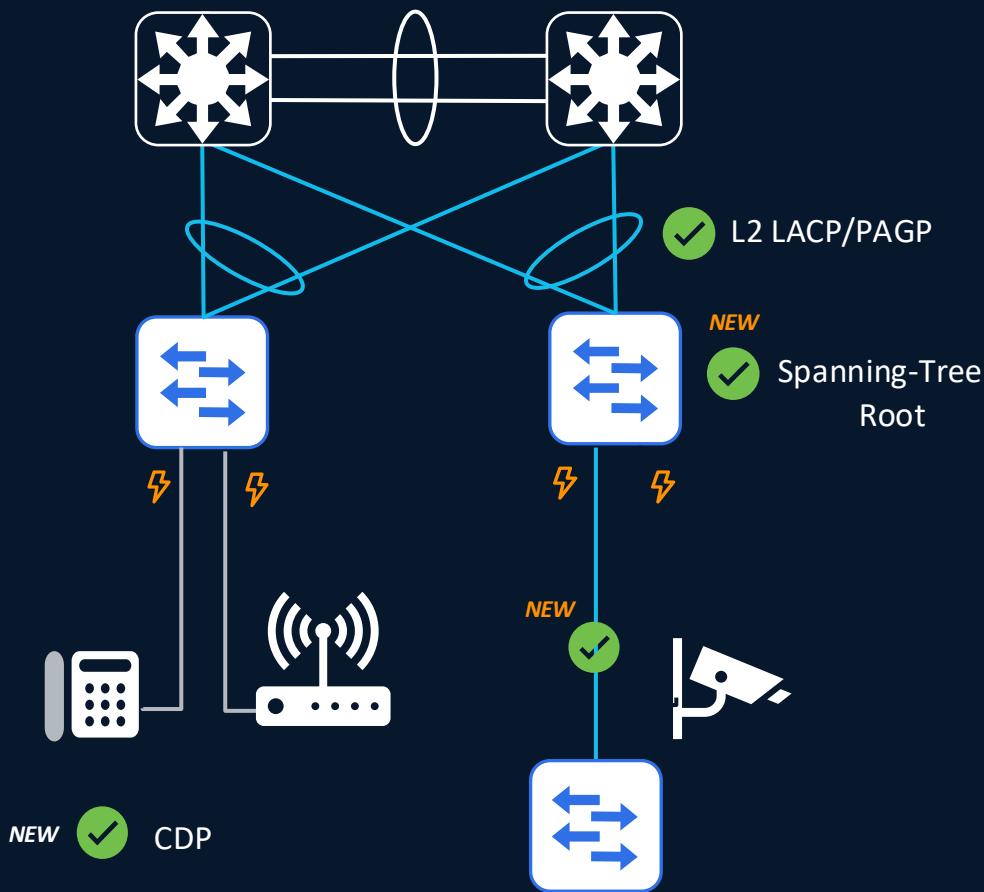
No Topology Modification Needed



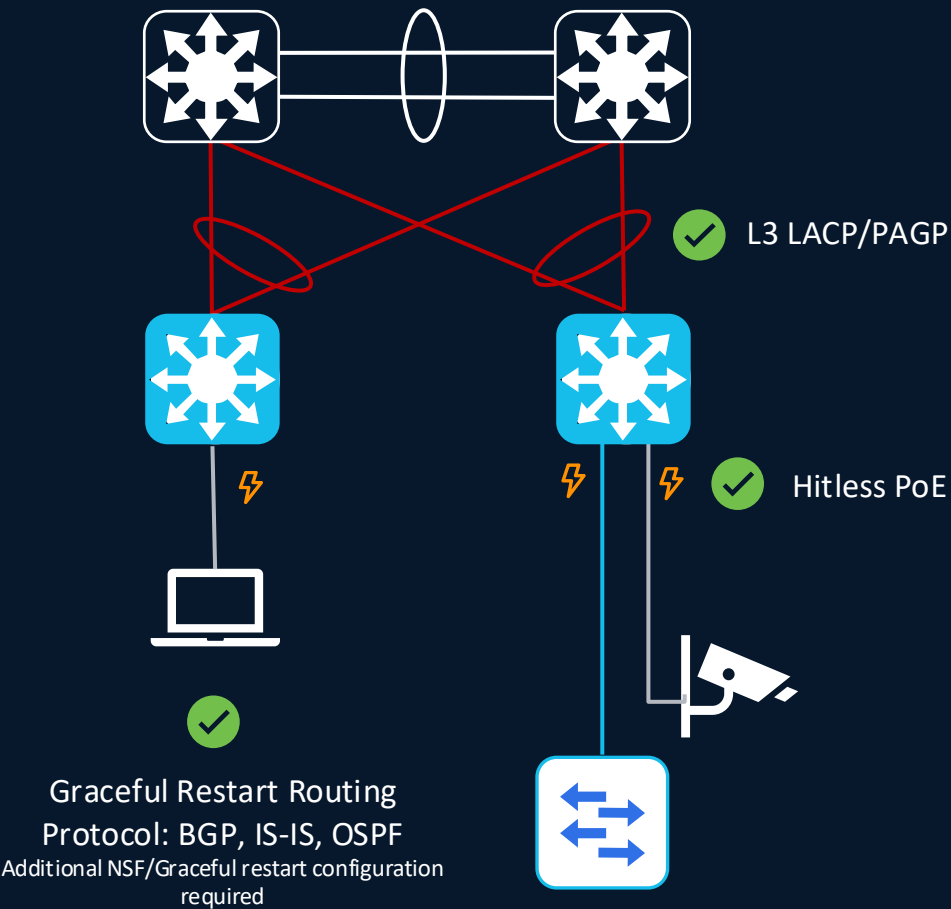
IOS-XE 26.1.1

Standalone switches

L2 Access/Distribution Node



L3 Routed Access Node

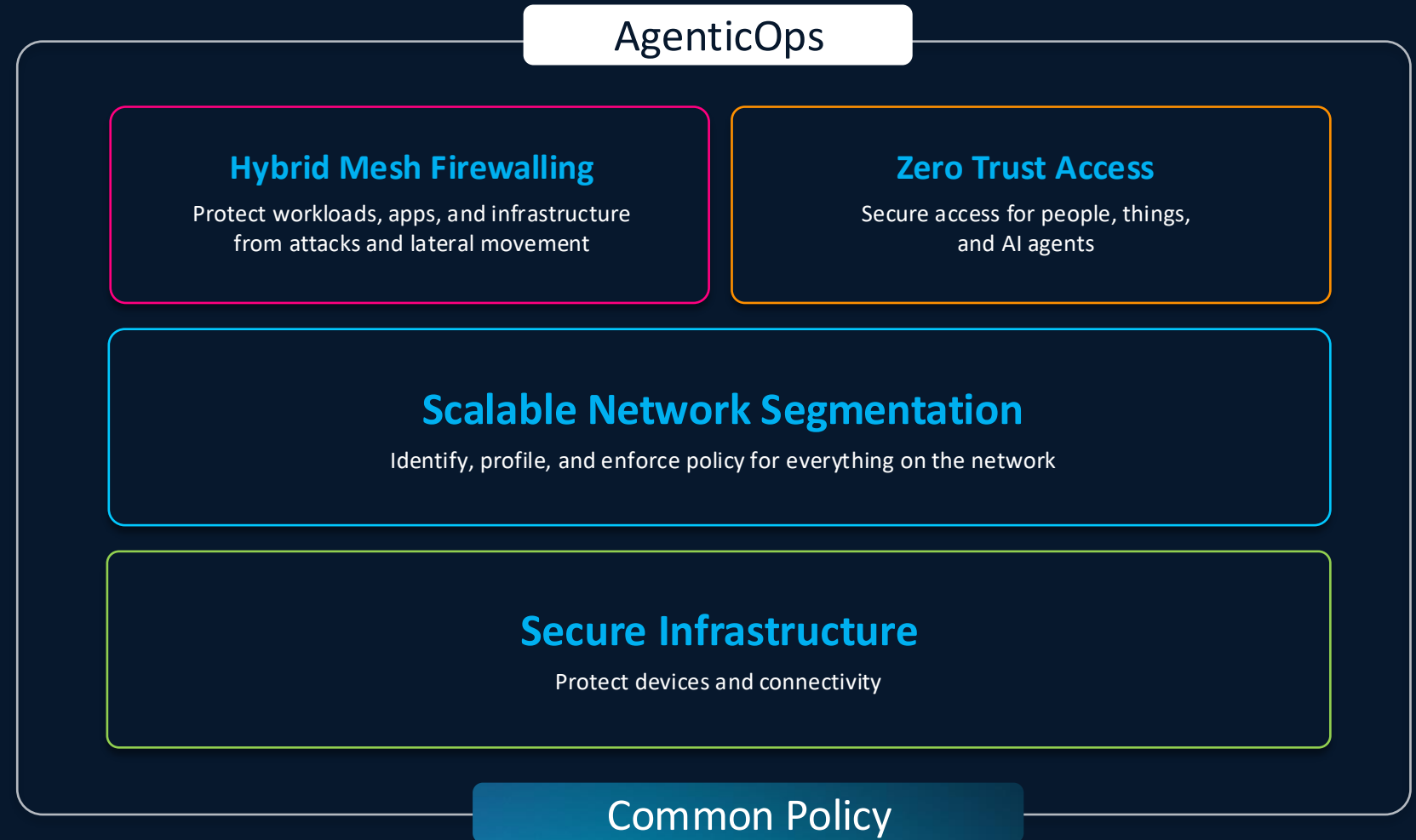


Secure Networking

Introducing Cisco's approach to secure networking

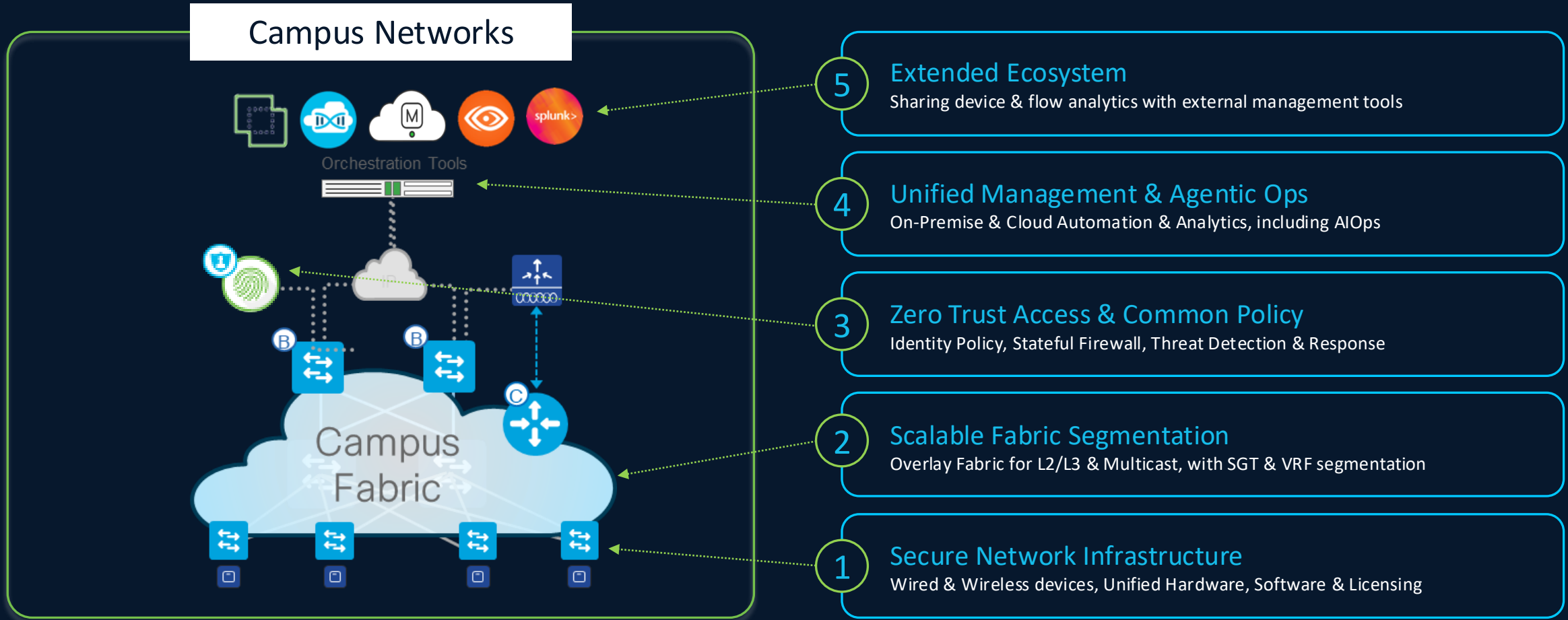
Security infused into everywhere the network extends

- Identity-first
- Continuously verified
- Enterprise-wide policies
- Comprehensive threat intel
- Distributed enforcement
- Streamlined Operations

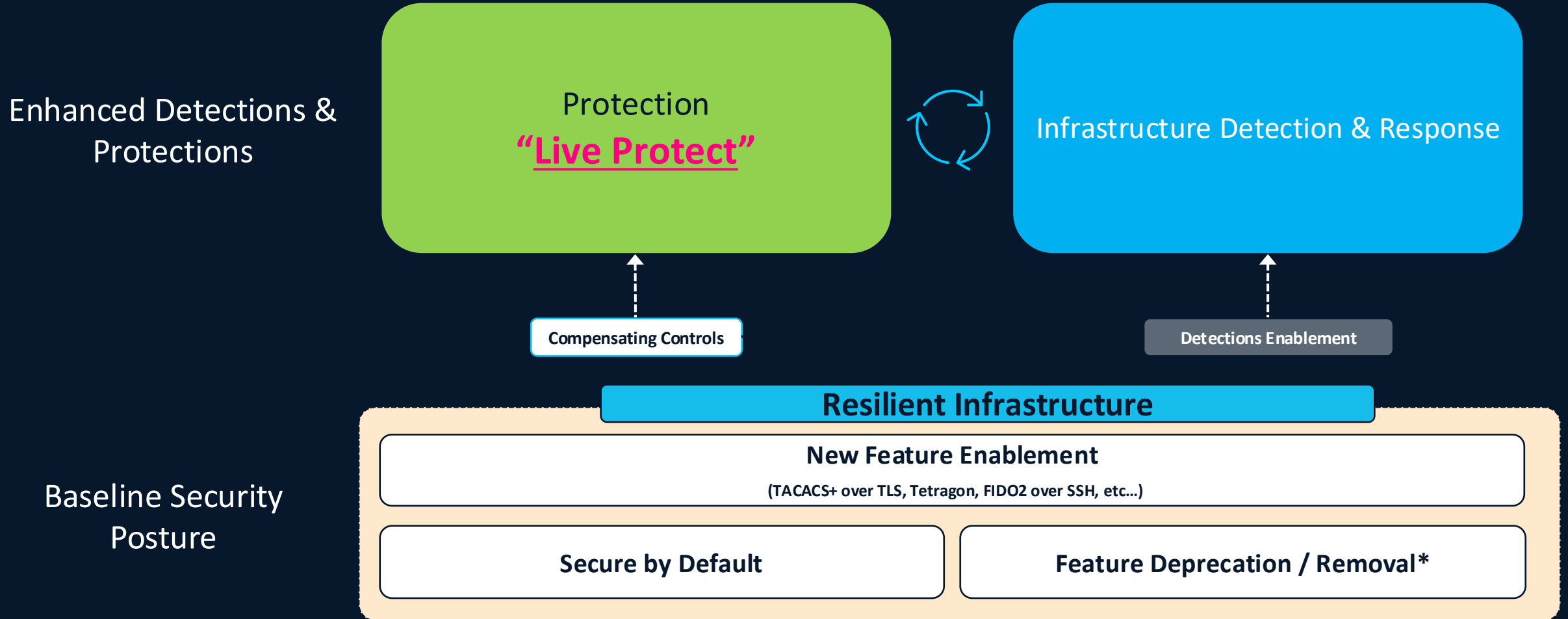


Secure Networks – Solution Components

Full-Stack Multi-Layer Reference Model (like the OSI Model)

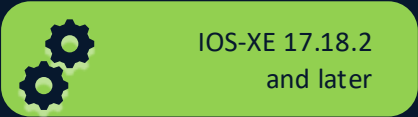


A compelling vision of security and resilience



Resilient Infrastructure

Driving comprehensive improvements to our baseline security posture



What is the issue?

Global threat actors have changed the game and raised the stakes for Cisco and industry

What can we do?

Harden our devices by avoiding configuration of known insecure commands

How are we doing this?



Encourage gradual migration from known insecure commands to secure alternatives

Examples of insecure cli*	Line vty 0-15 transport input telnet	Copy ftp: switch: Copy tftp: switch:	ip http server
---------------------------	---	---	----------------



New CLI

Switch# show system insecure configuration

Display current configured insecure commands and remedial options

Switch (config)# system mode insecure

Enables configuration of insecure features

- Insecure commands without changing system mode to insecure will be rejected.
- Insecure mode automatically gets added to CLI on upgrade to IOS-XE 26.1.1 if insecure cli are detected.

New Syslog

%SYS-4-INSECURE_CONFIG or %SYS-4-INSECURE_DYNAMIC_WARNING.

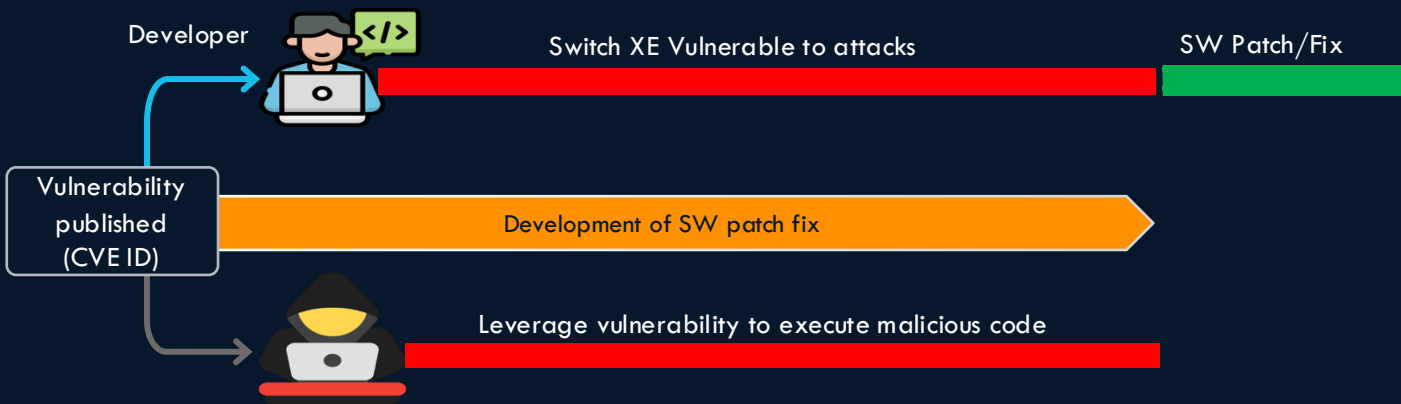


- Logs generated on boot/upgrade when system detects insecure commands in the running-config
- Text after log will show reason for log generation and potential remedial actions

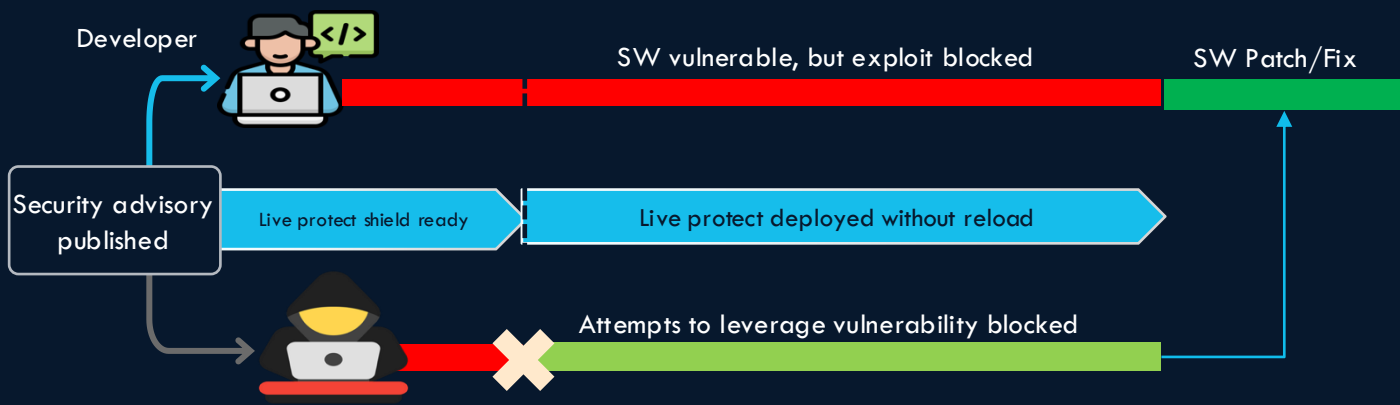
Details of these changes can be found here - [Resilient Infrastructure Playbook](#)

Live Protect for Blocking Attacks Leveraging Security Advisories

Vulnerabilities today



With Live Protect



eBPF

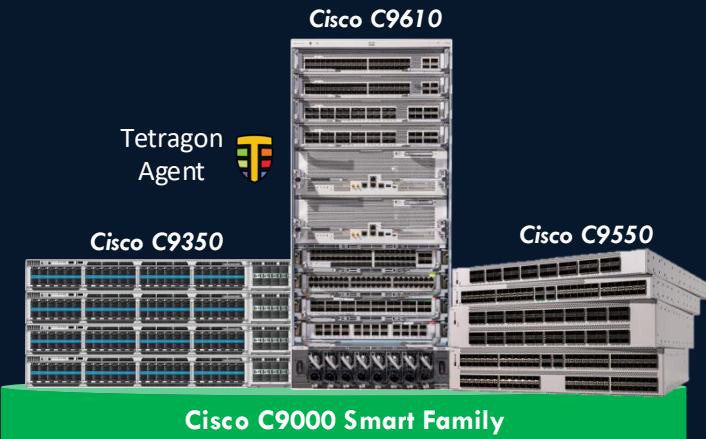
Allows you to extend and modify kernel behavior at runtime without changing kernel code

Isovalent

Maintains and productized an open-source eBPF project called Cilium to deliver security, observability functions for containers.

Tetragon

Built by Isovalent to provide eBPF- based security policies at the kernel level



Tetragon on Cisco IOS XE

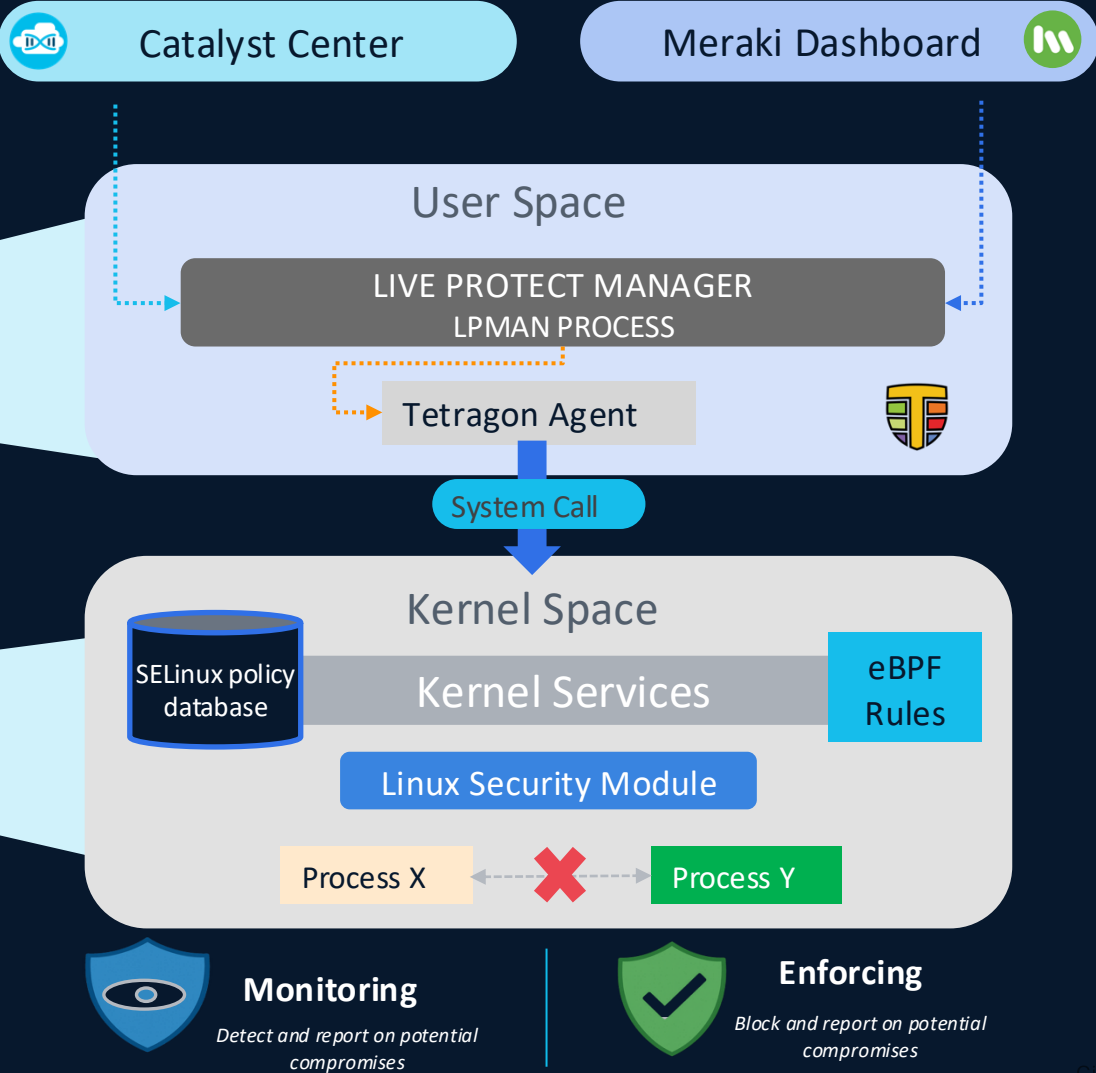
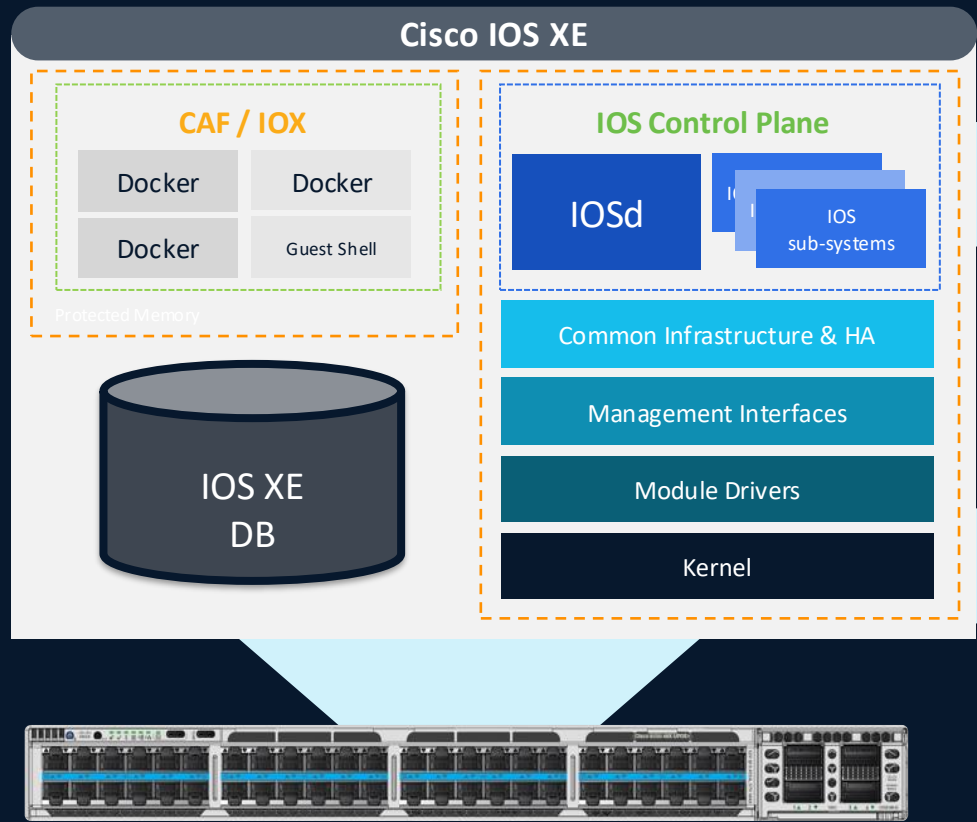
Native eBPF & SELinux

ebpf.io/what-is-ebpf/



IOS-XE 26.2.1

Leverage eBPF based control in Cisco IOS XE Linux Kernel to implement dynamic low-level system protection. Complements SELinux rules.



Post Quantum Cryptography Compliance

Industry-First Innovation on C9000 Smart Switches

Today's Security/Cryptography Provide

Confidentiality

Integrity

Authentication

AES 3DES RSA DH ECDH SHA 256 SHA 3 HMAC-SHA256



- **Quantum computers** solve complex calculations and exponentially faster.
- **Current cryptography** algorithms at **risk of breaking**.



Full Stack
PQC

MACsec

IPsec

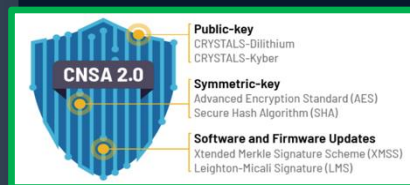
TLS

SSH

NIST-approved algorithms supported via CiscoSSL 8.3+

Software PQC

Cisco C9610



Cisco C9350

Cisco C9550

Cisco C9000 Smart Switches

Hardware PQC

NIST-approved algorithms supported via Programmable FPGA

ROMMON

OS

Datapath
between CPU
and TAM

SUDI*

Attestation*

Impact of Quantum Computers on Cryptography

Symmetric Cryptography

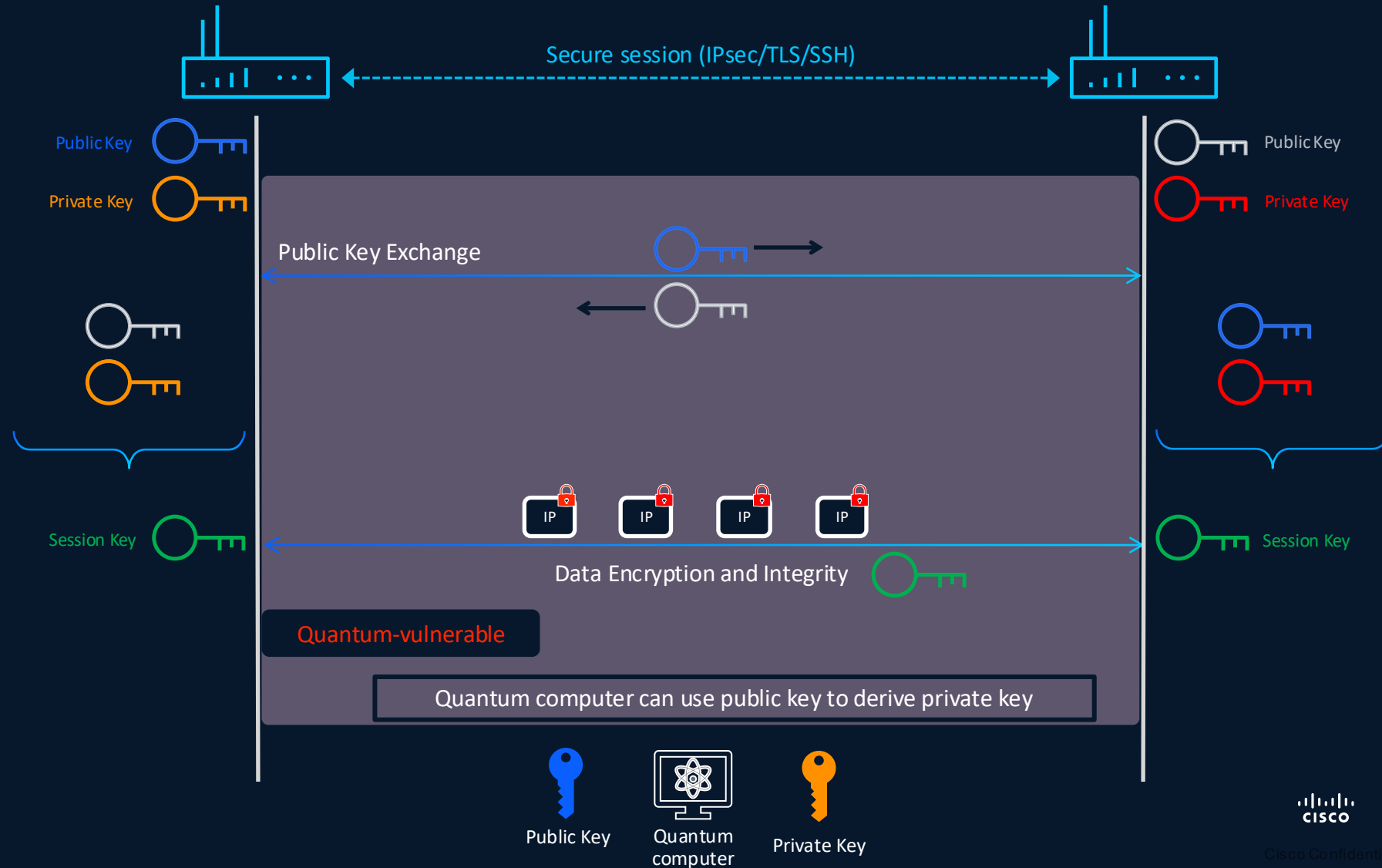
- Based on shared key
- Keys pre provisioned on both ends
- To scale, asymmetric algorithm used to transport keys

Asymmetric Cryptography

- Based on a public key and a private key
- Public key to encrypt
- Private key to decrypt the message

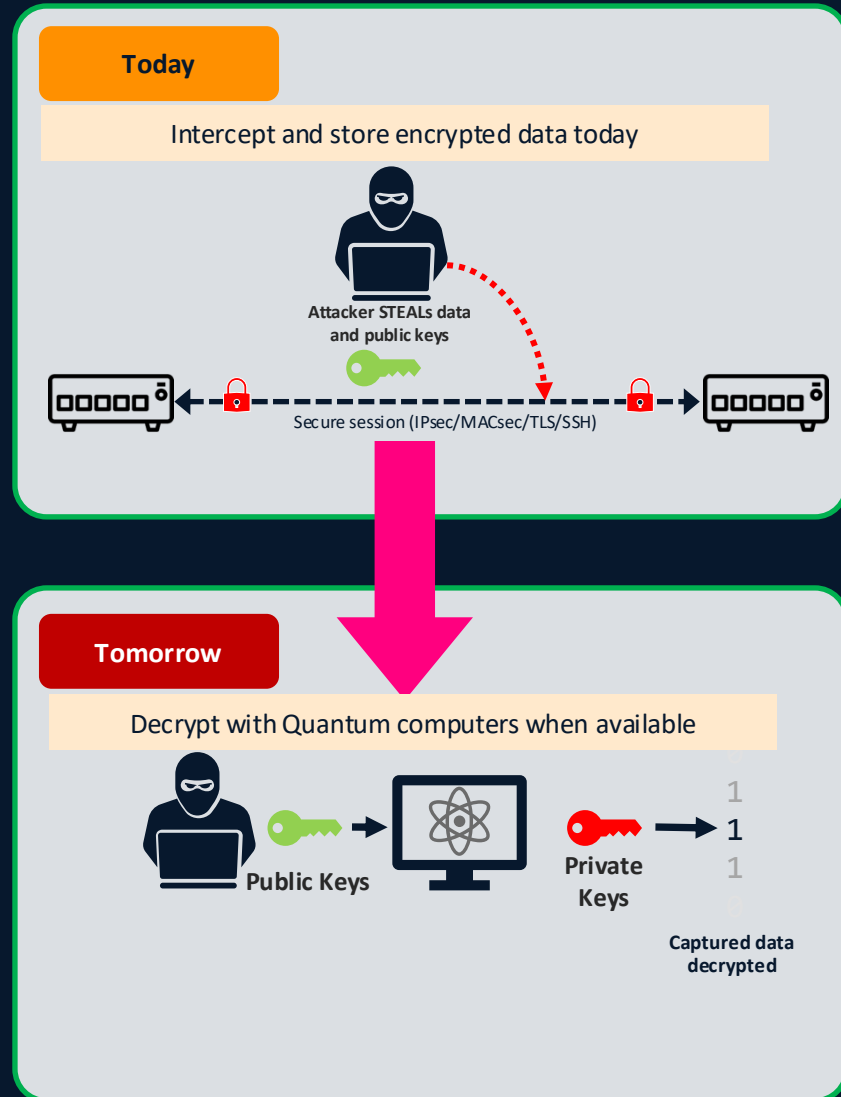
Digital Signature

- A digital signature is based on a private and a public key
- The private key signs the image, and the public key verifies its authenticity.



Importance of PQC today

And how can we protect ourselves



Quantum Key Distribution

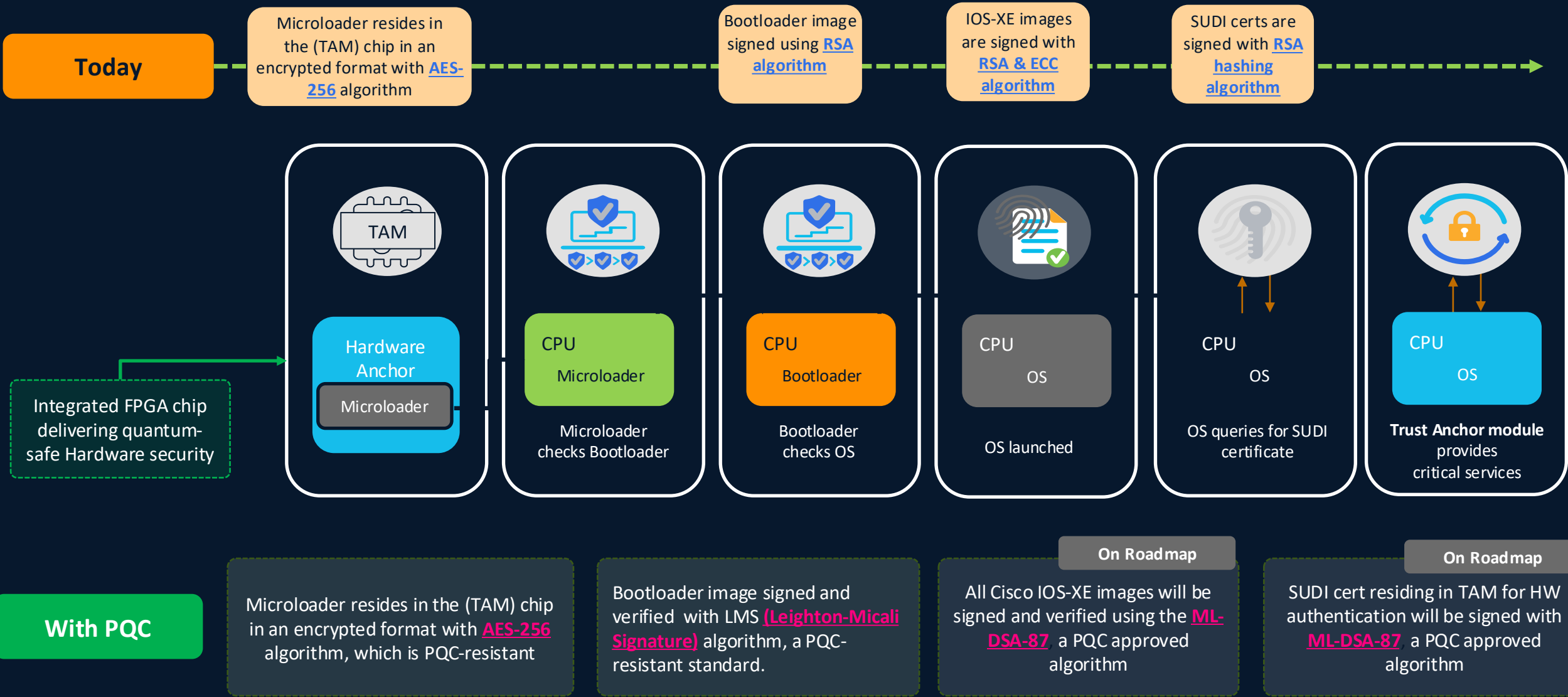
- Use quantum mechanics to protect data
- Technical Limitations

Post Quantum Cryptography

- Replace current public key algorithms with new ones
- Protocol upgraded required

C9000 chosen approach

Secure Boot Process on C9000 Smart Switches



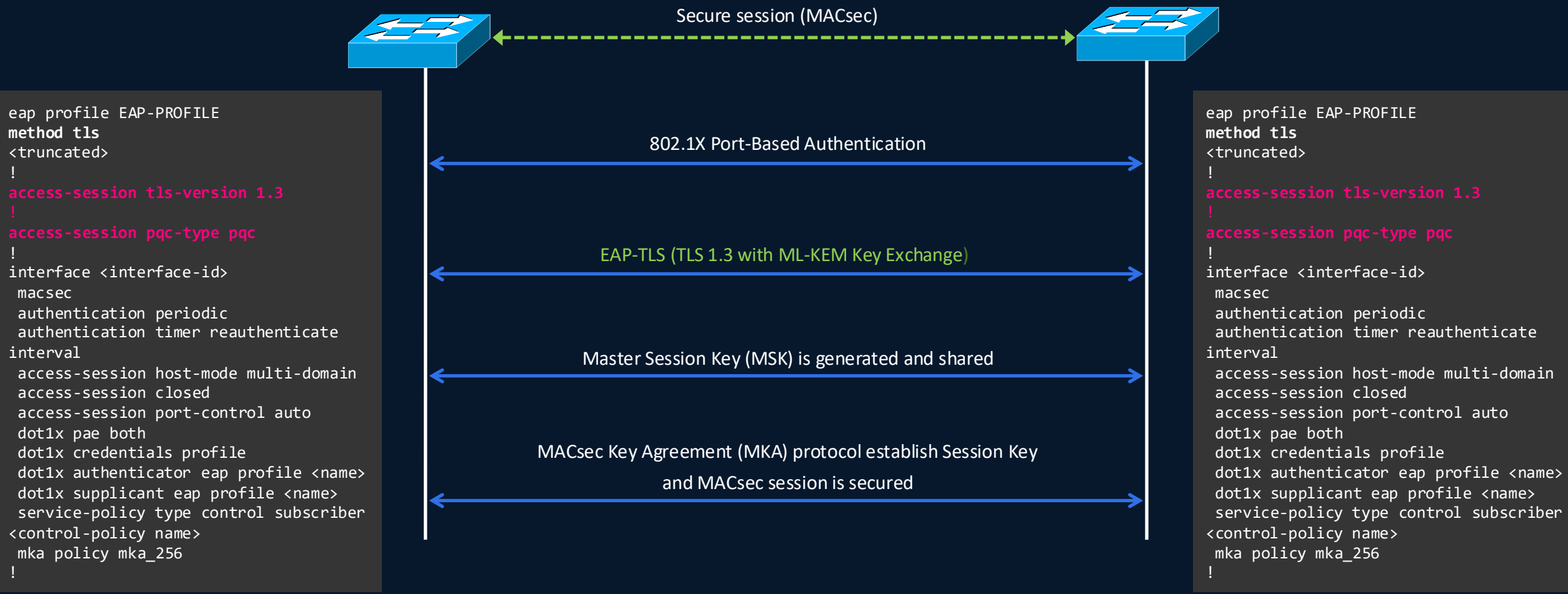
Switch-to-Switch PQC Resistant MACsec

EAP-TLS Certificate Based MACsec



IOS-XE 26.1.1

C9350 Uplink MACSec



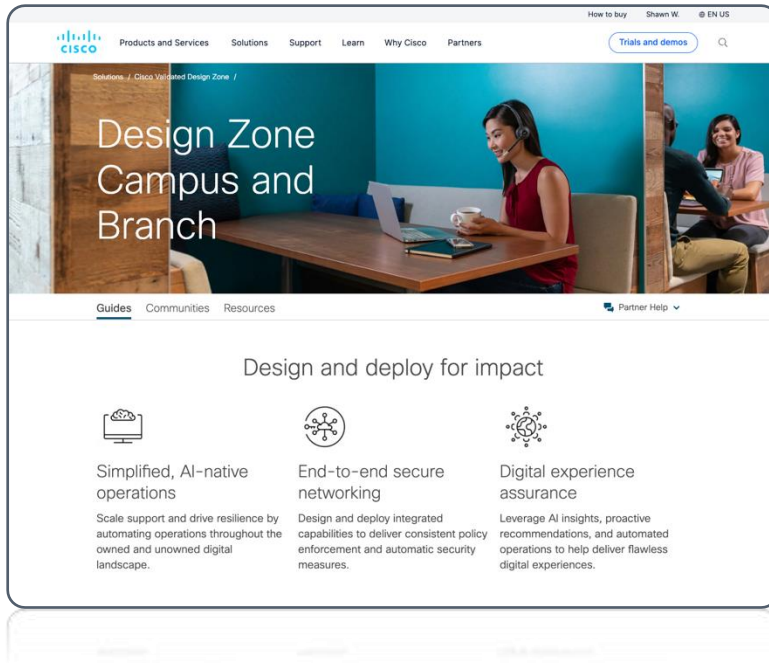
PQC support table

Post Quantum Resilience for algorithm	C9350	C9610	C9550
LMS signing and verification capability on bootloader/ROMMON	26.2.2	26.1.1	26.2.2
ML-DSA-87 image signing to enable verification of IOS-XE	26.2.2	26.2.2	26.2.2
PQC-signed SUDI certs with ML-DSA-87	Roadmap	Roadmap	Roadmap
MACsec Certificate Based Authentication with ML-KEM	26.1.1	26.2.1	26.2.1
TLS 1.3 with ML-KEM	26.2.1	26.2.1	26.2.1
IPsec key exchange IKEv2 with ML-KEM	26.2.1	TBD	TBD
OpenSSH with ML-KEM	26.1.1	26.1.1	26.2.1
Data encryption with AES-256	26.1.1 (MACsec) 26.2.1 (IPsec)	26.2.1 (MACsec)	26.2.1 (MACSec)

Subject to change for releases beyond 26.1.1

Resources – Coming soon...

Cisco Validated Design & Documentation



New SNRA Cisco Validated Designs

- Secure Network Reference Architecture – End-to-End Architecture Guide
- Secure Network Reference Architecture – Cloud-managed Design Guide
- Secure Network Reference Architecture – On-Premises Design Guide
- Secure Network Reference Architecture – Programmable Design Guide

May 2026

June 2026

Existing Cisco Validated Designs

- [Cisco Cloud Fabric Validated Case Study](#)
- [Cisco Common Policy Integration Guide](#)
- [Cisco SD-Access Design Guide](#)
- [Cisco Unified Branch Design Guide](#)

New

New

Updated

Updated

General Fabric / LISP Update

Campus fabrics make secure networking operational.

Customer outcomes that fabrics deliver



Simplify Operations

Automated lifecycle
Unified access operations

Consistent deployment, simpler day-2 operations



Secure by Identity

Identity-based policy
Segmentation across domains

Policy follows users, devices and things



Assurance + AI Insights

Insights, Analytics
AI-Assisted visibility, monitoring

Assurance Powered by AI Intelligence

Operate it your way

On-Prem SDA

Catalyst Center • LISP VXLAN

Cloud EVPN

Meraki Dashboard • BGP EVPN-VXLAN

Programmable EVPN

APIs • templates • IaC

One strategy. Same outcomes. Any fabric, any controller, AI-powered simplicity.

Campus Fabric Positioning Guidance

No two customers are alike; Cisco meets your customer where they are

Outcomes	Business Criteria	Lead with	Profile
- Proven large & multisite scale, deep assurance - Optimized wireless mobility - Common Policy, SSI - Support for CX & IE	- On-Prem operating model (airgap) - Wireless-first user base - Large single site or many sites sharing policy - OT/IoT integration	Catalyst Center & LISP	On-Premises Enterprises
- SaaS simplicity - Cloud-managed, vendor agnostic - Phased deployment (Distro-first) - Adaptive Policy, Access Manager	- Cloud-first operating model - Many geographic distributed sites - Fast rollout needs - Meraki (MS) Access integration	Meraki Dashboard & EVPN-VXLAN	Cloud-First Enterprises
- Deep automation & CI/CD workflows - Vendor interoperability with EVPN - Proven scale with LISP	- Existing NetDevOps pipelines - Multi-vendor environments - Custom control requirements	Programmable (EVPN/LISP)	On-Premise with Strong DevOps

Three Fabric Tracks Driving Towards a Unified North Star

Prioritizing Maturity, Accelerating Innovation, Driving Convergence

- 1 On Prem Fabric
Catalyst Center
- 2 Cloud-managed Fabric
Meraki Dashboard
- 3 Programmable Fabric
infrastructure-as-code



Cisco Cloud Control

2HCY26

Unified Management

- Unified inventory, topology, search , Alerts,
- Consistent automation and Analytics through IaC

Unified Fabric Provisioning

- Cross-domain orchestration (DC+ campus)
- End-to-end Segmentation

Agentic Operations

- AI-Canvas for intelligent troubleshooting
- AI-Assistant for natural language processing

Introducing Unified Cisco Fabric in Cisco Cloud Control

Cisco Cloud Control

• Inventory • Topology • Health • Cross-domain workflows • AI Canvas



Data Center

Nexus switch based EVPN fabrics

Nexus Dashboard



Campus

Catalyst/Cisco based EVPN fabrics

Meraki Dashboard

Design principle: unify the customer experience without changing the deployment model.

Preserve

Existing controller investments and domain-controller depth.

Unify

One operator workflow across campus, data center

Differentiate

Cross-domain workflows + AI-led ops

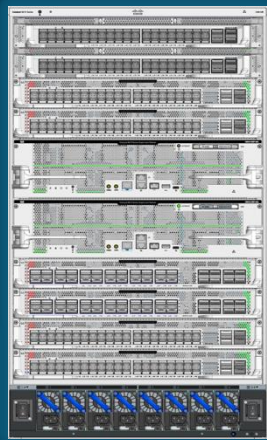
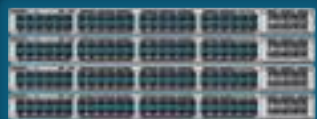
SDA LISP



Faster deployments • Safer changes • Ready for next-gen campus scale



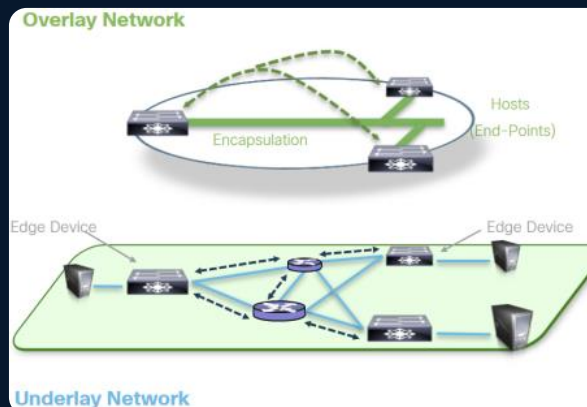
Cisco C9000 Family



Smart Switch Support (C9K)

Modernize hardware without breaking SDA workflows

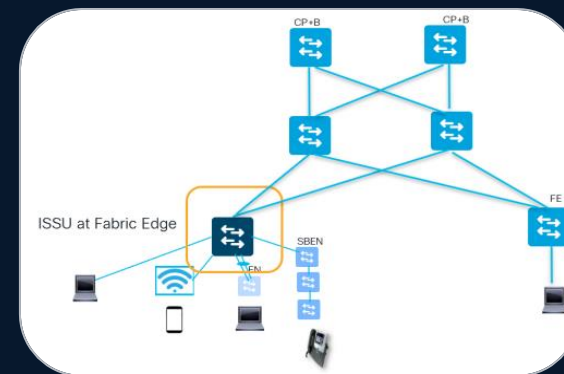
C9350 FE role (2.3.7.11)
C9350 FIAB + eWLC, C9610 (3.2.1)
C9550 (3.2.4, 3.3.1)



Automated IPv6 Underlay

Simplify underlay rollout, future-proof addressing

Catalyst Center 3.2.3



Resilient Upgrades

Reduce Maintenance windows + downtime risk

- Cat9300 FE (XFSU)
- Cat9400/9500/9600 all roles (ISSU)

Catalyst Center 3.3.1

Catalyst Center GA milestones

2.3.7.11
Shipping

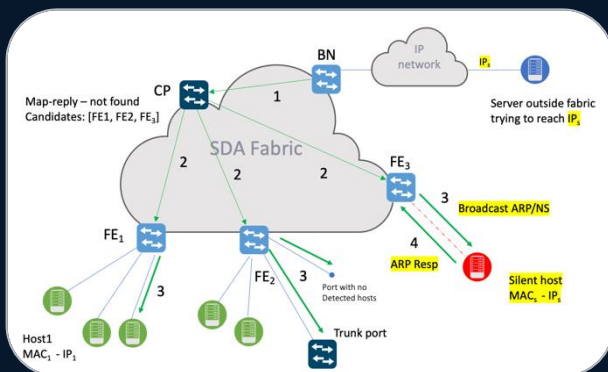
3.2.3
July

3.3.1
August

SDA LISP



Faster upgrades • Lower downtime risk • Simpler multi-site wireless



Silent Host Detection

Eliminate L2 flooding; scalable & fast detection

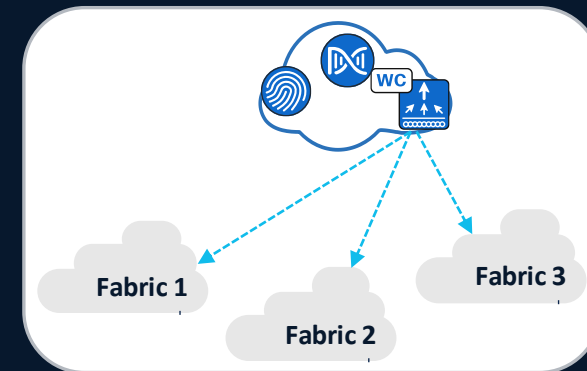
Catalyst Center 3.2.3



Fabric integrated with AI-Assistant

Simplified Fabric Operations

Catalyst Center 2.3.7.11



Shared WLC across 16 Fabrics

Less controller sprawl; simpler wireless ops

**Not committed, Under evaluation*

Catalyst Center GA milestones

2.3.7.11
Shipping

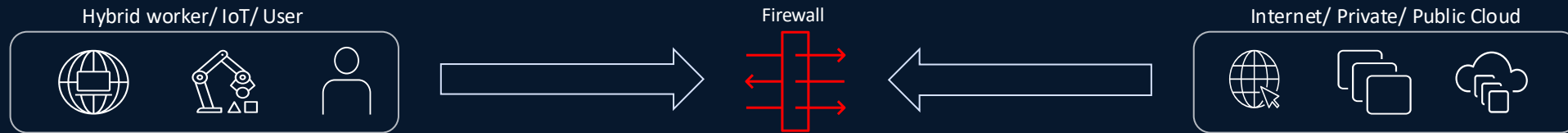
3.2.3
July

3.3.1
August

SSI Fabric: Threat Response On-Demand

Open Beta now, GA 3.3.3

Intelligent Protection for your Network



Key Concept

Allows ***select traffic*** redirection to security appliances.

This means:



Policy-Driven Protection — Seamless Cisco or 3rd-Party Integration



Efficient, Scalable Design — Optimize Firewall Investments



Flexible — topology-agnostic rollout for faster time-to-value

On-Premise: SD-Access LISP 6 Month Roadmap

Updated: May1, 2026

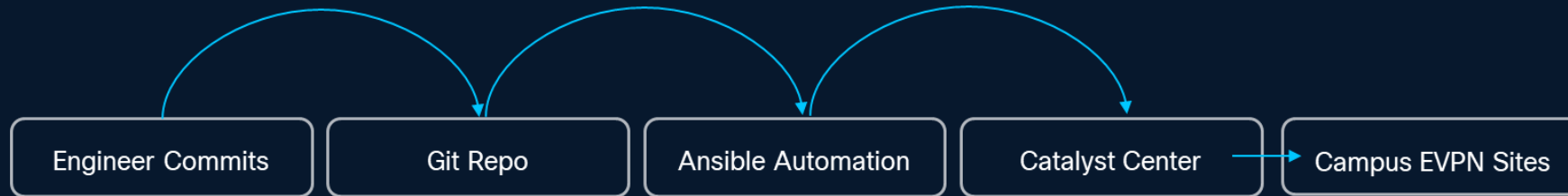


Programmable Fabric (BGP-EVPN)

EVPN VXLAN Campus Fabric Templates

Cisco TAC Supported

Deploy EVPN VXLAN campus fabrics consistently using Catalyst Center templates + Ansible automation



What you get

- 19 production-ready EVPN VXLAN campus fabric templates
- Role-aware config generation (Spine / Leaf / Border)
- Multi-VRF architecture with automatic RT/RD
- TRM Multicast with Anycast RP

Why it matters

Faster rollout: repeatable deployments across sites

Less risk: standardized fabric configs + fewer manual errors

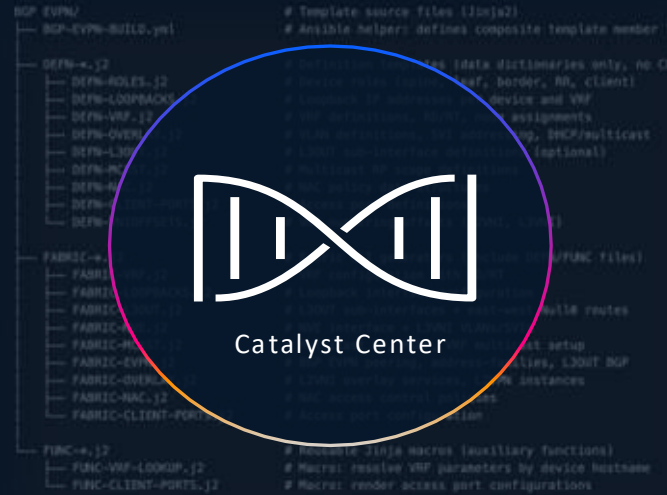
Auditability: every change tracked in Git (PR review-ready)

Cisco- published [Git Repo](#) | Catalyst Center 2.3.7.10 | Cisco IOS-XE 17.15.3 | Redhat Ansible 2.15.0

Simplifying BGP EVPN Fabric Deployment via Catalyst Center

Catalyst Center Template Framework

- Automates BGP EVPN VXLAN fabric deployment on Catalyst 9k switches, enabling Infrastructure-as-Code workflows with full GitOps integration.
- Template-driven automation with role-aware configuration generation
- Ansible Playbook for Git to Catalyst Center template Creation and Updates



Supported Devices | Platforms

- Catalyst 9300 | 9400 | 9500 | 9600 (SUP1)
 - Cisco IOS-XE: 17.15.3 or later
 - Catalyst Center: 2.3.7.10
 - Redhat Ansible 2.15.0 or newer
-
- Distributed Anycast Gateway
 - Tenant Routed Multicast with Anycast RP
 - VRF lite based Border Handoff
 - Single Cluster Fabric Deployments

[Github: Catalyst Center BGP EVPN VXLAN Templates](#)

Simplifying BGP EVPN Fabric Deployment via Catalyst Center

CodeIssuesPull requestsAgentsActionsProjectsSecurity and qualityInsights

On April 24 we'll start using GitHub Copilot interaction data for AI model training unless you opt out. [Review this update](#) and manage your preferences in your [GitHub account settings](#).

CatalystCenter-BGP-EVPN-VXLAN / BGP-EVPN

main

Igor Manassypov fix(merge): resolve conflicts with m

Building P0 x

Name

..

BGP-EVPN-BUILD.yml

DEFN-CLIENT-PORTS.j2

DEFN-L3OUT.j2

DEFN-LOOPBACKS.j2

DEFN-MCAST.j2

DEFN-NAC.j2

DEFN-OVERLAY.j2

DEFN-ROLES.j2

DEFN-VNI-OFFSETS.j2

DEFN-VRF.j2

FABRIC-CLIENT-PORTS.j2

FABRIC-EVPN.j2

FABRIC-L3OUT.j2

FABRIC-LOOPBACKS.j2

FABRIC-MCAST.j2

FABRIC-NAC.j2

FABRIC-NVE.j2

FABRIC-OVERLAY.j2

FABRIC-VRF.j2

FUNC-CLIENT-PORTS.j2

FUNC-VRF-LOOKUP.j2

Catalyst Center

Design / CLI Templates

admin

FILTERED BY

Building P0 x

SUMMARY

Project Name (5)

Building P0

Sample Jinja Templates

Sample Velocity Templates

Cloud DayN Templates

Onboarding Configuration

Type (2)

Template Language (2)

Category (2)

Device Family (2)

Device Series (5)

Commit State (2)

Provision Status (2)

Potential Design Conflicts (2)

Site (1)

TEMPLATES (21)

Search

0 Selected

DEFN-CLIENT-PORTS.j2

DEFN-L3OUT.j2

DEFN-LOOPBACKS.j2

DEFN-MCAST.j2

DEFN-NAC.j2

DEFN-OVERLAY.j2

DEFN-ROLES.j2

DEFN-VNI-OFFSETS.j2

DEFN-VRF.j2

FABRIC-CLIENT-PORTS.j2

FABRIC-EVPN.j2

FABRIC-L3OUT.j2

FABRIC-LOOPBACKS.j2

FABRIC-MCAST.j2

FABRIC-NAC.j2

FABRIC-NVE.j2

FABRIC-OVERLAY.j2

FABRIC-VRF.j2

FUNC-CLIENT-PORTS.j2

FUNC-VRF-LOOKUP.j2

Catalyst Center

Design / CLI Templates

admin

FILTERED BY

Composite x

SUMMARY

Project Name (5)

Type (2)

Regular

Composite

Template Language (2)

Category (2)

Device Family (2)

Device Series (5)

Commit State (2)

Provision Status (2)

Potential Design Conflicts (2)

Site (1)

Simulations (1)

Search Table

0 Selected

Simulation Name

Date

Fab-SJ

05 May 2026

1 Record(s)

Catalyst Center

Design / CLI Templates

admin

CLI Templates / BGP-EVPN-BUILD.j2 (1)

Properties

TemplatesSimulationProvision Conflicts

Update Simulation

Simulation Name* Fab-SJ

Import Template ParametersExport Template Parameters

BIND TO SOURCE

This template has binding or system variables. Select the device and site for simulation.

Device* Leaf-01.dcloud.cisco.com (198.19.1...

Site* Global/PODS/POD 0/Bui...

Change

Search

FABRIC-VRF.j2

TEMPLATES

FABRIC-VRF.j2

FABRIC-LOOPBACKS.j2

FABRIC-L3OUT.j2

FABRIC-NVE.j2

FABRIC-MCAST.j2

FABRIC-EVPN.j2

FABRIC-OVERLAY.j2

FABRIC-CLIENT-PORT...

FABRIC-NAC.j2

CancelSaveRun

GitHub repository

Templates uploaded

Composite templates

Simulate and/or Provision composite templates

BGP EVPN Fabric Solution 6 month Roadmap

IOS XE 17.18.2 - Dec '25

IOS XE 26.1.1 - Mar '26

IOS XE 26.2.1 - Aug '26

Controlled Available

EVPN Multihoming

- Fabric + Non-Fabric support

Catalyst 9300, 9400, 9500-H, 9600-Sup1

- C9350 leaf role enablement
- Silicon One readiness (9500-X / 9600-Sup2 ingress replication)

- Catalyst 9300 EVPN xFSU
- Scalable Fabric overlay with DAG routed proxy

- C9610, C9550 border/spine role enablement
- Scalable IPv4 routing with IPv6 Next-hop (RFC 5549)
- Atomic Config Manager
- EVPN host route leaking to global routing table

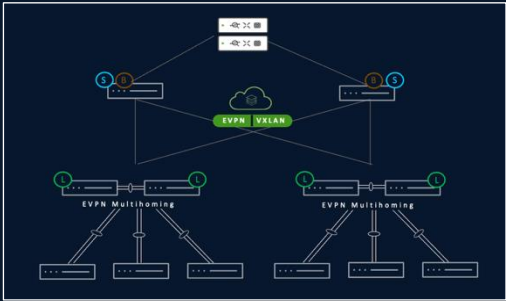
Cisco Feature Navigator (CFN)

<https://cfnng.cisco.com>

Cloud Managed Fabric Updates

Cloud Managed Fabric Updates

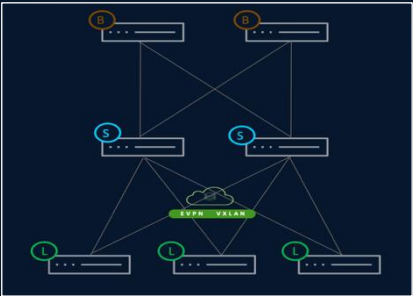
Resilient network • Easy migration • Simpler operations



EVPN Multihoming

Standard based High Availability at Distribution

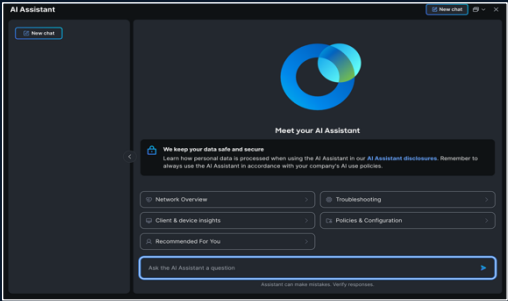
9300X & 9500H in Leaf mode



Fabric with Routed Access

STP Free Underlay with Scalable Overlays

9300 | 9300L | 9300X | 9350 | MS390



AI Assistant

Simplified Fabric Operations: Day-0 to Day-N

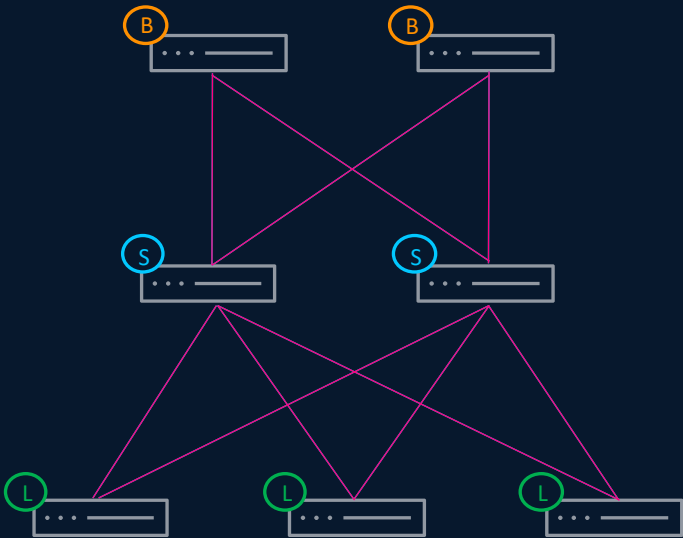
AI Assistant Integrated with Fabric

Underlay Automation with Routed Ports

Cloud Managed Fabric – Simplifying Underlay Automation

Today

- Optional SVI based Underlay Automation as part of Fabric Creation
- Manual Per port Routed port configuration outside fabric workflow



Q4FY26

- Layer 3 Routed port Underlay Automation as part of Fabric Automation
- Neighbors Auto discovered as part of Underlay
- Add/remove links as part of Underlay Automation
- Optional SVI based Underlay Automation

Create fabric

1 Fabric setup

2 Underlay config and port selection

3 VRFs

4 Fabric subnets

5 Fabric border routing configuration

6 Summary



device1 Border 2

Local port	Peer devices	Roles	Peer port	Uplink	Used for underlay	Actions
Port 1	device2	Border	Port 10	Yes	Yes	
Port 9	device5 (stack1)	Border Spine	Port 8	No	Yes	
+ Add port						

Cloud Fabric Solution 6 Month Roadmap

Dec '25

Apr '26

Sep '26

Product Matrix

- Catalyst 9200, 9300, MS and 9500-H

Fabric - Automation

- C9300X Leaf, Spine, Border
- C9500-H, Spine and Border
- Fabric Leaf – Distribution Layer
- Macro and Micro-segmentation
- Scalable Distributed Wireless
- Border connectivity – eBGP
- Overlay IPv4 | IPv6 Networks
- Overlay Multicast – per Agg block

Fabric - Assurance

- BGP Peering
- Virtual Networks, Overlay Routes, more

Fabric - Automation

- EVPN Multihoming – Fabric (Public Beta, GA – July '26)
- C9500H as Leaf (Public Beta – Apr, GA – July '26)

Target July 2026

- L3 Routed ports + LAN Automation
- Leaf at Access (Routed Access)
- AI Assistant for Fabric
- 9300/9300X/9300L/MS390 as Leaf Role

Product Matrix

- C9350 - Leaf

Fabric - Automation

- Topology-driven Automation
- Overlay IPv4 | IPv6 Multicast
- Border connectivity – Static / OSPF
- Centralized Wireless – Campus Gateway
- Border-Leaf support
- Border/Leaf/Spine support

Fabric - Assurance

- AI Assistant Fabric assurance Enhancements
- Overlay Multicast, Per-VNI statistics

Explore Resources

- [Secure Network Reference Architecture Master Class Session - Shawn Wargo](#)
- [SD-Access: Intelligent Traffic Redirection Using Security Service Insertion - Mahesh NagiReddy](#)
- [Cisco SD-Access Design Guide v 2.0](#)
- [Cloud Managed Fabric Click through Demo](#)
- [Cisco Sales connect – Cloud Manged Fabric](#)
- [Cisco Sales connect – SD-Access](#)
- CiscoLive Breakout Sessions

