Campus update

NtwrkPeople DET

Jesse Schmidt
Solutions Engineer

21-05-2026

Agenda

01 Catalyst Center

02 Fabric (LISP & EVPN)

03 C9k Smart Switches

Catalyst Center 3.1.X Release

3.X Releases Numbering Scheme

A | Major

Significant market value

Required when there is a break in backward compatibility of published API; significant regressions or changes in semantics or workflow

B | Minor

New market value; anchor point for long-lived release

Required when: Extended update times, or significant jump points in platform which requires application updates (i.e., platform revisions)

Permitted only with seamless upgrade, preserve backward compatibility, no regression in functionality, no regression in telemetry, etc.

C | Patch

Value: Bug-fixes and new device support

Permitted for the correction of errors or omissions only, seamless installation with full roll-back, no new functionality or changes in semantics or workflows

New features and key enhancements – 3.1.x

Platform

- Catalyst Center on Azure
- Site Based RBAC
- Contextual RCA for Support bundle
- CCGM Updates

NetOps

- Brownfield device onboarding workflow
- New SWIM Dashboard
- Rule-Based Compliance
- Campus Network Automation
- AP priming for C9K WLC
- Campus Automation – Industrial Configuration
- App Hosting for IE
- REP topology view for fabric and non-fabric
- Per Device Config – AP configuration
- Cloning profiles across multiple WLC
- PRP configuration support

AIOps

- Energy management dashboard
- Install TE agent workflow
- Enhanced visibility into Cisco ISE authentication failures
- Event Analytics AI Outlier
- Service Now Bidirectional Integration

SecOps

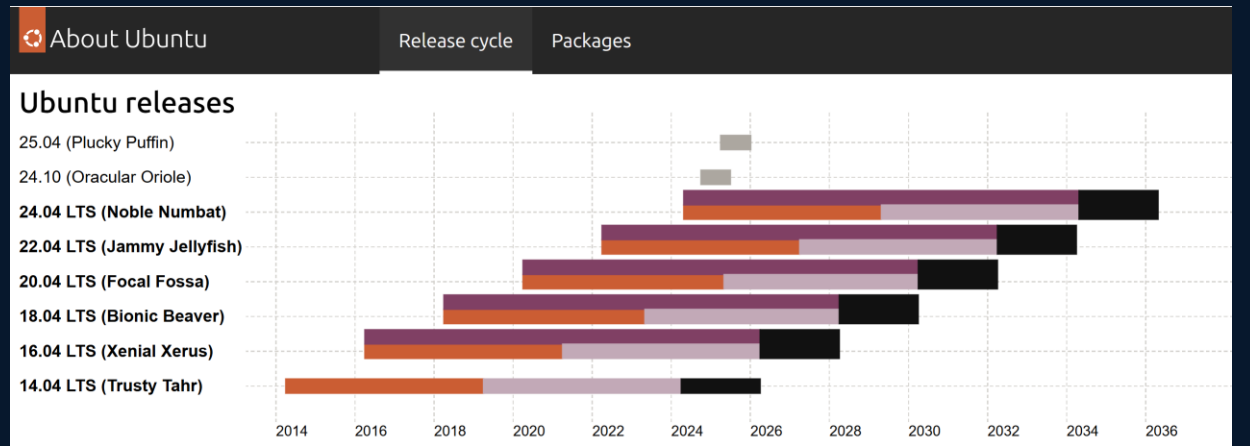
- Security Service Insertion
- Pub-Sub for brownfield deployments and migration-Beta
- Allowed VLAN, add a native VLAN on a TRUNK link
- Voice VLAN template for user ports
- SDA Fabric can experience outages caused by SSDP
- Overlapping IP Pools

DevOps

- New APIs
- API enhancements
- New reports

What's new under the hood of 3.X release

- New Linux
- New File System
- NFS Backup Support
- Parallel Install
- 2.3.x = Ubuntu 18.04.6 LTS
  - Kernel: 5.4.0-139-generic
  - Kubernetes: 1.18.15-cisco
  - File System
    - ext4
- 3.1.x = Ubuntu 22.04.5 LTS
  - Kernel: 5.15.0-72-generic
  - Kubernetes: 1.29.10-cisco
  - File Systems
    - xfs



	RELEASED	END OF STANDARD SUPPORT	END OF UBUNTU PRO SUPPORT	END OF LEGACY SUPPORT
25.04 (Plucky Puffin)	Apr 2025	Jan 2026		
24.10 (Oracular Oriole)	Oct 2024	Jul 2025		
24.04 LTS (Noble Numbat)	Apr 2024	Apr 2029	Apr 2034	Apr 2036
22.04 LTS (Jammy Jellyfish)	Apr 2022	Apr 2027	Apr 2032	Apr 2034
20.04 LTS (Focal Fossa)	Apr 2020	May 2025	Apr 2030	Apr 2032
18.04 LTS (Bionic Beaver)	Apr 2018	May 2023	Apr 2028	Apr 2030

Upgrade Methods

Same appliance (DN2 and DN3) in place update using network upgrade package

From Appliance A (2.3.7) to Appliance B (3.1.X) – Appliance B on 3.1X will connect to Appliance A 2.3.7 and grab the backup, convert it and restore (IP change)

From Medium Appliance to Virtual Appliance (AWS/ESXi/Azure)

- Backup
- Run conversion script
- Restore

Virtual Appliance to Virtual Appliance

- Backup
- Restore

Easier B’n’R

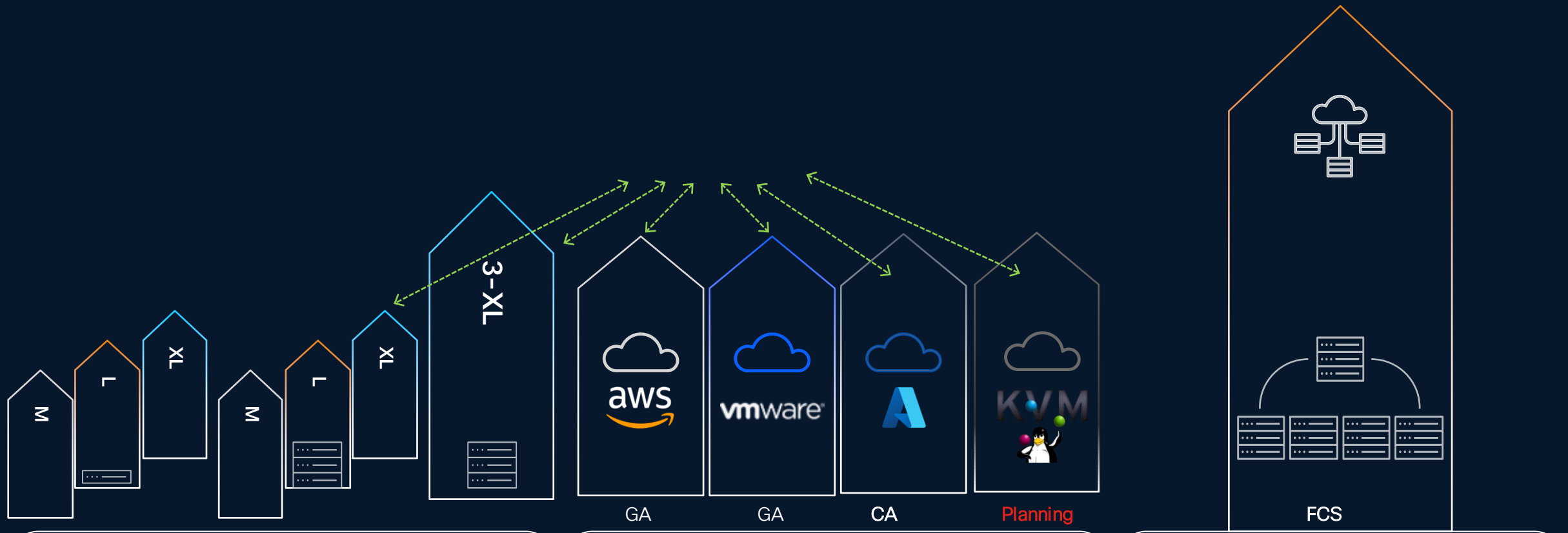
In 2.X release B’N’R Had to be to identical versions

With 3.x with can convert N-2 backups into 3.X format on the fly

ROADMAPS AND TIMELINES SUBJECT TO CHANGE
ALL FUTURE DATES ARE FCS RELEASES AND SUBJECT TO CHANGE

Catalyst Center operational evolution

Vertical and Horizontal scaling for simplified architecture



Single appliance

HA cluster

3x scale with XL appliances

VA scale parity with DNx-HW-APL(medium appliance)

Catalyst Center Global Manager use cases

Global Search

Global search via

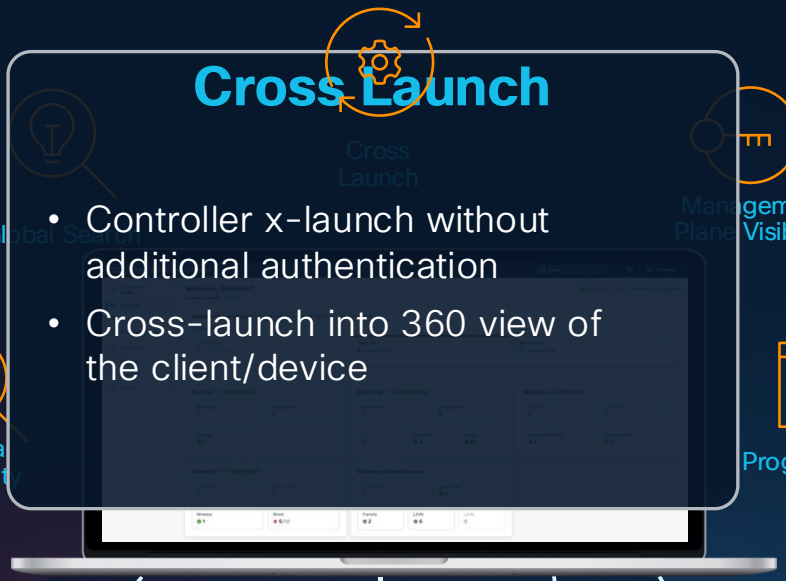
- IP Address
- Hostname
- MAC address
- other metadata

Cross Launch

- Controller x-launch without additional authentication
- Cross-launch into 360 view of the client/device

Mgmt Plane Visibility

- Enhanced Administrative Efficiency
- System Health / Monitoring
- Appliance Health / Monitoring



Global Visibility

- Monitoring of networks, sites, clients, devices
- Aggregated inventory reporting
- P1/P2/P3 issues drill-down from any Catalyst Center

Programmability

- Open APIs for 3rd party solutions integration
- APIs for monitoring mgmt plane health
- APIs to query global networks/devices/ inventory details

Catalyst Center Physical Single Node M/L/XL

Catalyst Center Physical Three Node Cluster

Catalyst Center VA ESXi

Catalyst Center VA AWS

Catalyst Center VA Azure (Future*)

Site-Based Role Based Access Control

Site-Based Role Based Access Control

A new feature in Catalyst Center 3.x that grants user access to network devices based on their location within Catalyst Center's hierarchy. Custom Roles can now be applied at the Site level with the introduction of a new feature called an Access Group. This allows Catalyst Center to grant or deny access to network resources, based on location.

Site

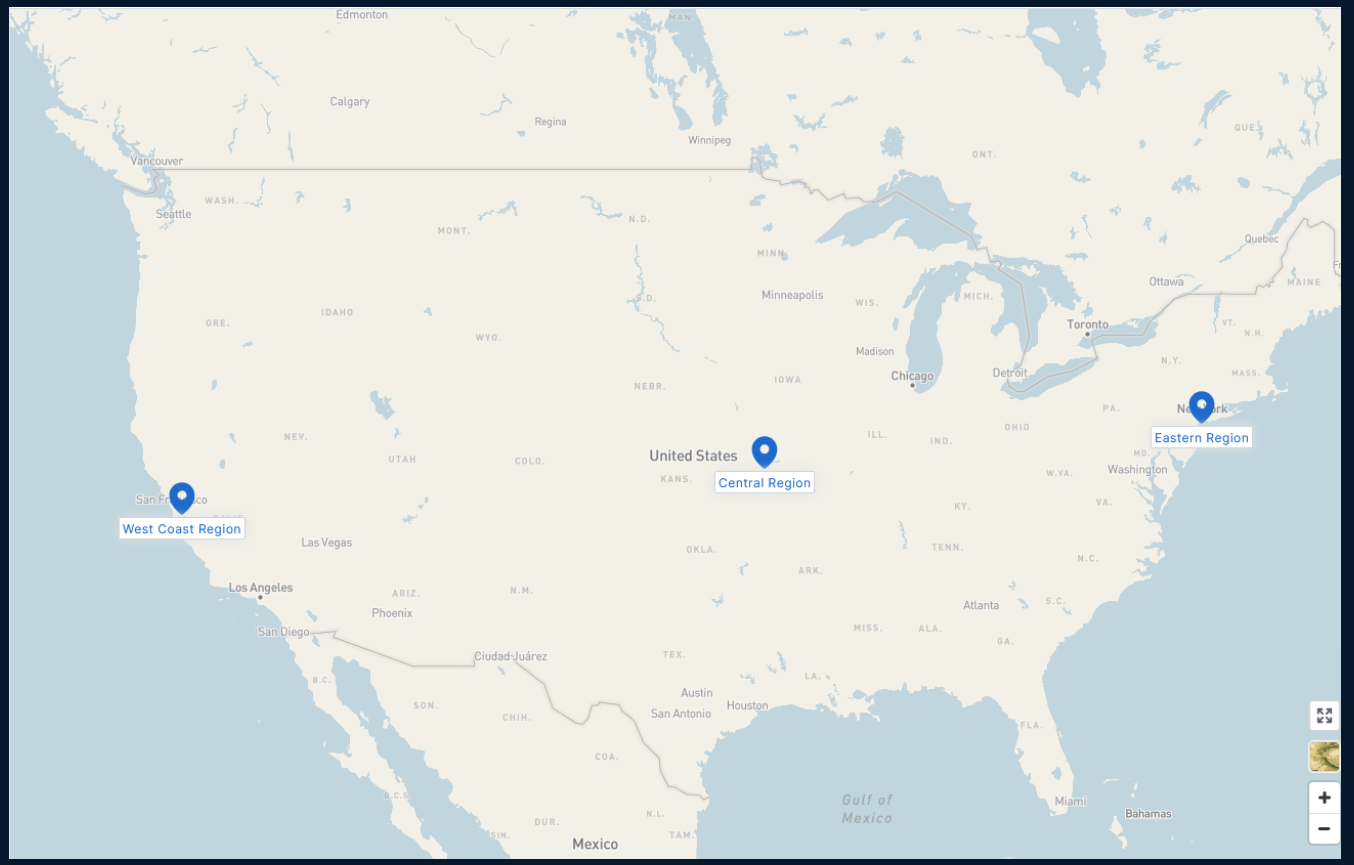
An Area, Building or Floor within Catalyst Center hierarchy.

Custom Role

A user-defined set of access privileges used to permit and/or deny access to network devices within Catalyst Center.

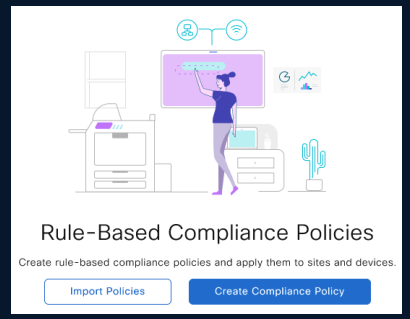
Access Group

An object that applies the settings of a custom role to a particular site, providing Site-Based Role Based Access Control.

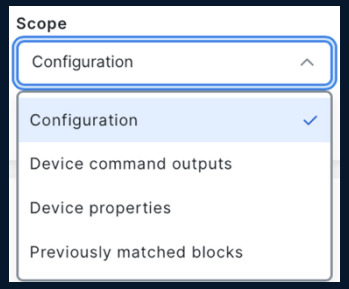


Rule-Based Compliance

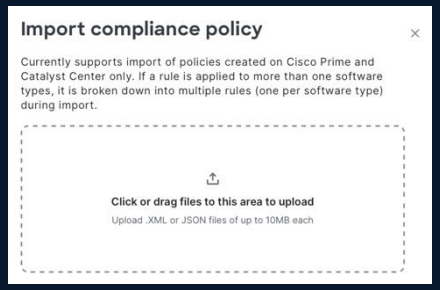
Custom network compliance policies



Validate the presence or absence with powerful Scope options – audit ready



Prime parity and import support

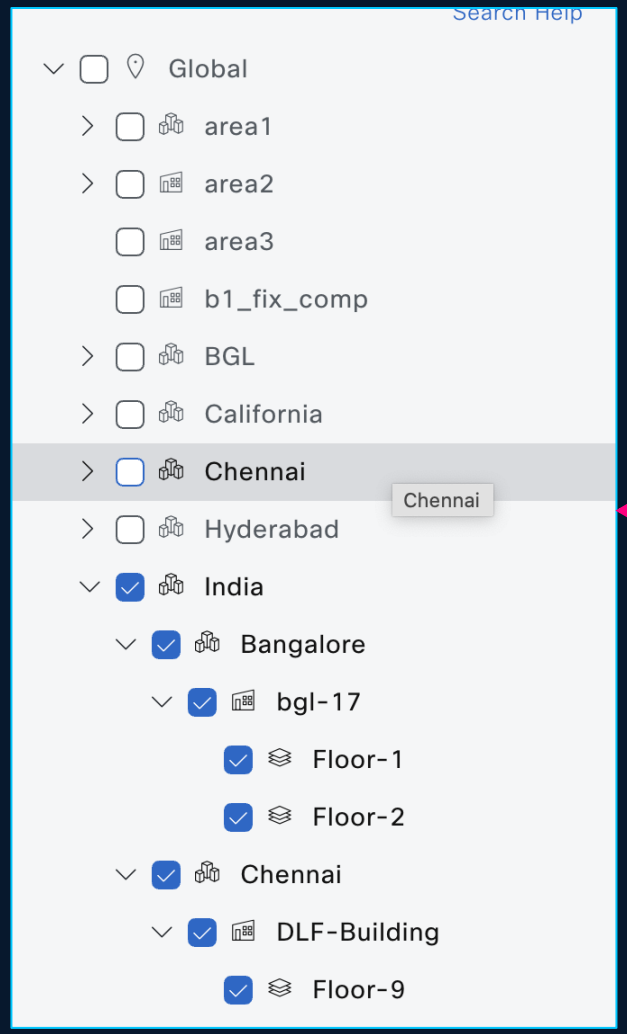


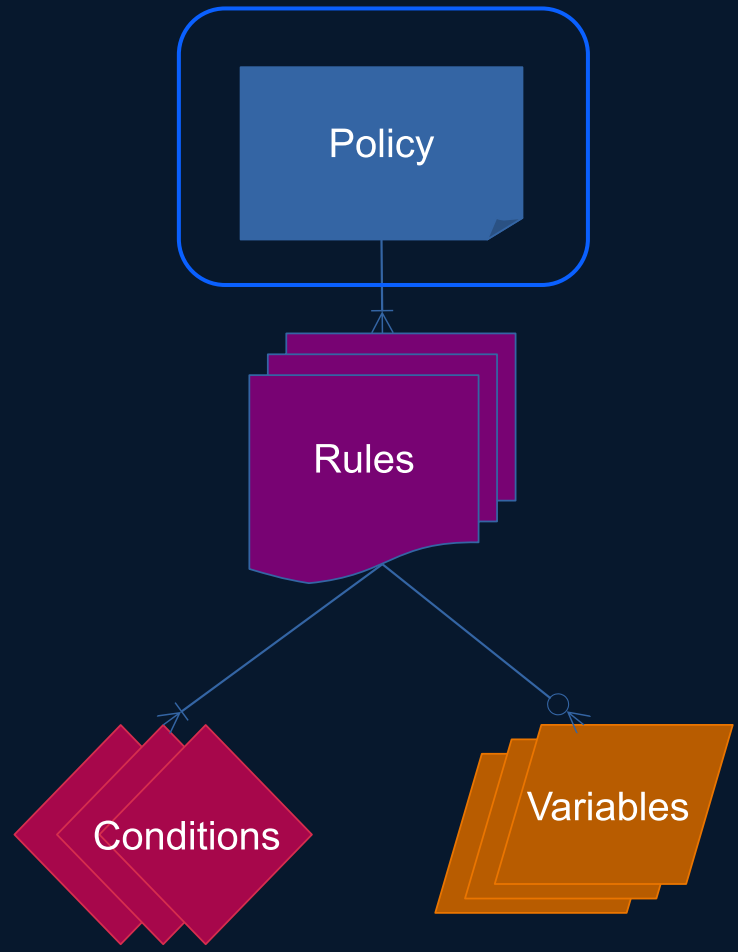
Precursor for future innovation and

Policies to simplify Regulatory Compliance
NIST types, PCI, HIPPA, STIG, and others

Secure Posture Protection
Validate best practices in place

Rule-Based Compliance





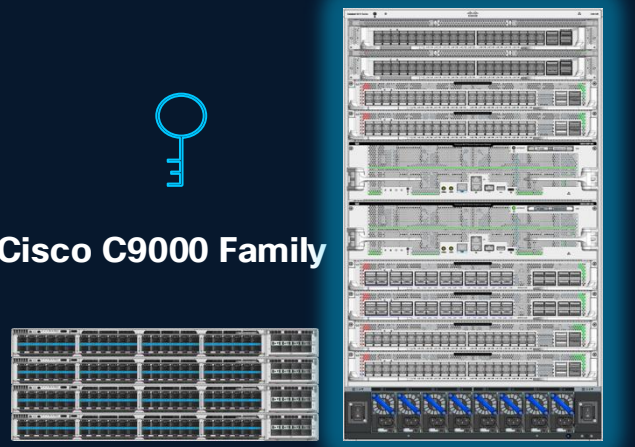
Campus Fabric Update

Campus Fabric Positioning Guidance

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

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

SDA LISP: Advancing Automation Capabilities

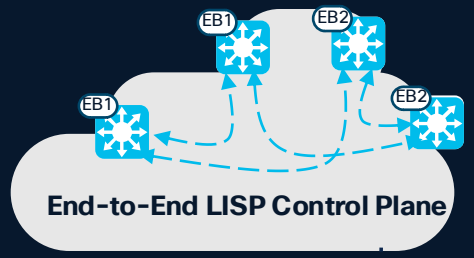


Silicon One Hardware Support

C9350 with IOS-XE 17.18.2, Dec'25
Catalyst Center 2.3.7.11 & 3.1.6

C9610 with IOS-XE 26.1.1
Catalyst Center 3.2.1 Mar'26

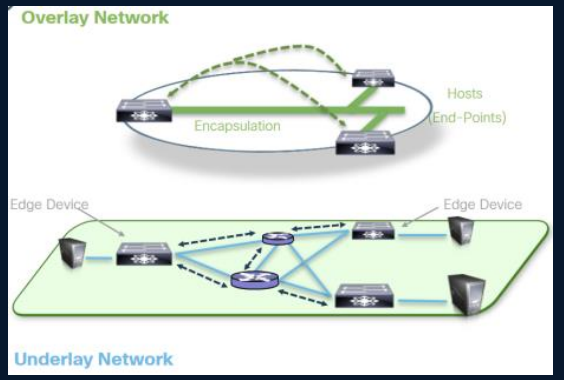
EFT



PubSub Architecture & Migration

Simplified border design with faster convergence with the new PubSub architecture.

Streamlined migration path from BGP/LISP to enhanced PubSub-based fabrics (IP/SDA Transits)



Automated IPv6 Underlay

Ipv6 Only Underlay – 3.2.1
Dual Stack Underlay - 3.2.3

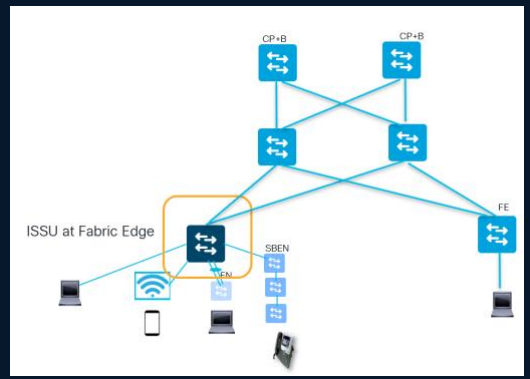
SDA LISP: Advancing Automation Capabilities

IOS XE 26.2.1
Catalyst Center 3.2.3

Silent Host Discovery in SDA LISP

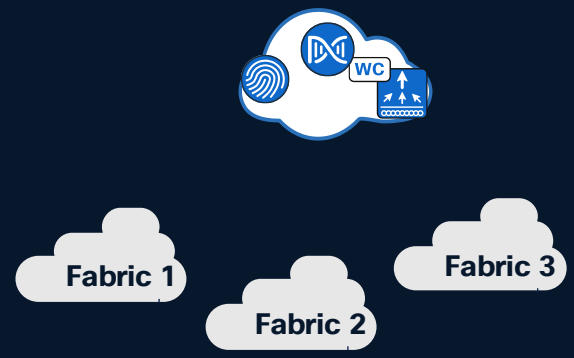
Discover silent/sleeping endpoints without L2 flooding using an on-demand, control-plane approach. Scales seamlessly across fabrics

➡ New CLI: *silent-host-detection* under router LISP.



Resilient Architecture

- XFSU Support- Cat9300 Fabric Edge
- ISSU Support for 9500/9600 Edge/Border/Control Plane, 9400 Border/CP

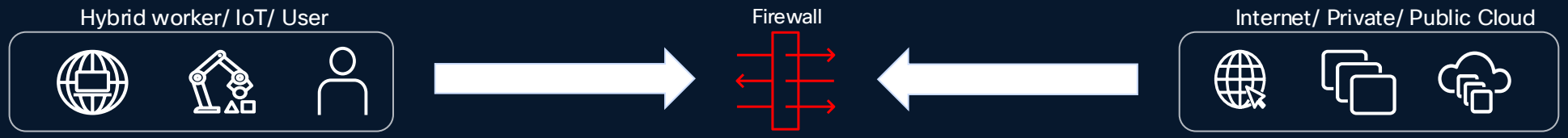


Shared WLC across Fabrics

Single Wireless Controller across multiple Fabric sites for ease of use and flexibility in wireless SDA deployments

SSI Fabric: Stateful Security On-Demand

Intelligent Protection for Your SD-A Fabric Network



Key Concept

SSI Fabric empowers NetOps and SecOps to **divert *only the required traffic*** on the fly 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

Campus Fabric Update (Cloud)

We have been accelerating feature development...

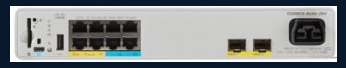
Platform Enablement

C9500

C9350

C9300/X/L/LM

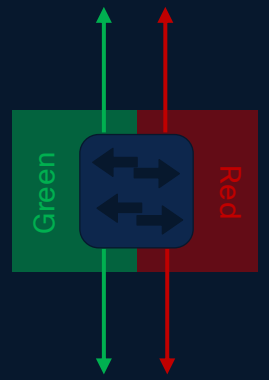
C9200/L/CX



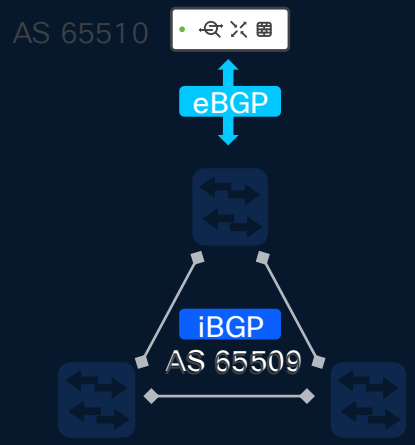
More Coming...

Enterprise Feature Development

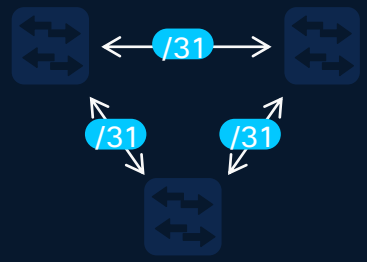
VRF



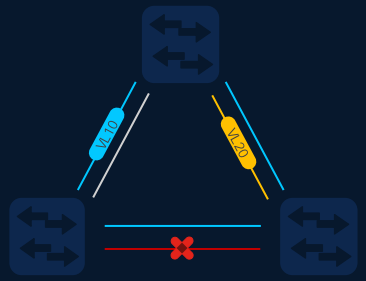
BGP



Routed Interfaces

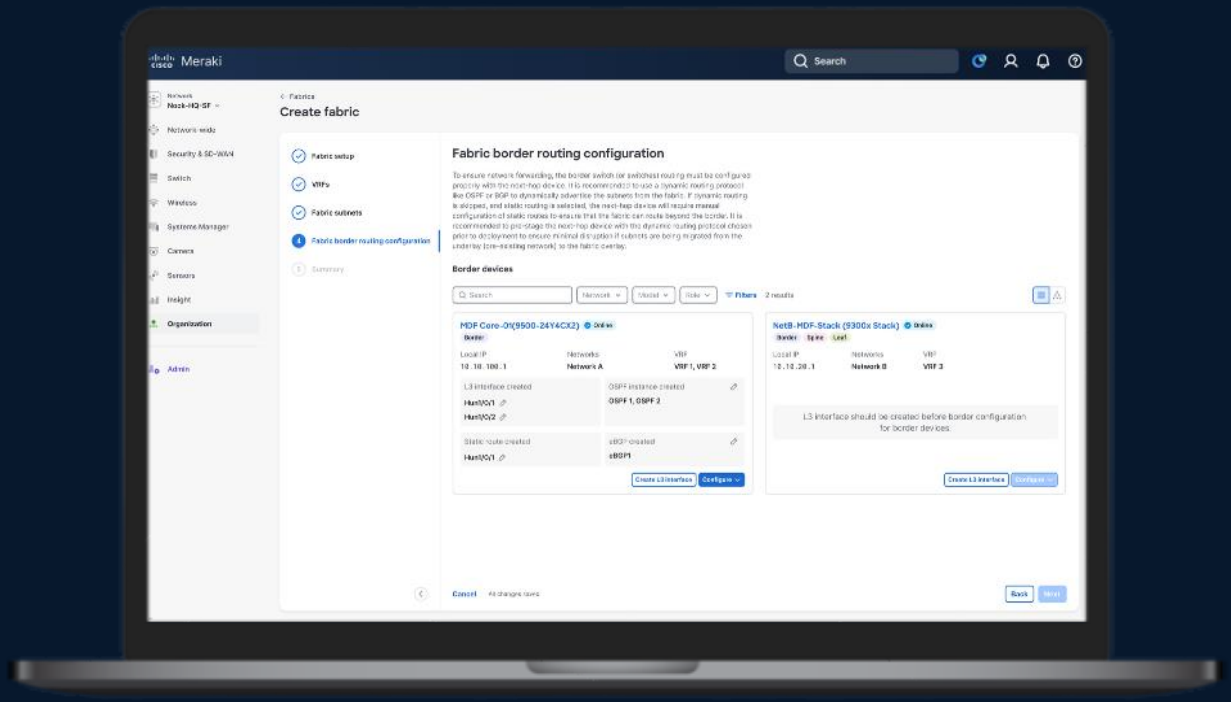


R-PVST



Introducing Cloud-Managed Fabric

EVPN Fabric Orchestration from Meraki Dashboard



Benefit from Cloud Simplicity

Build and manage large sites from an intuitive cloud networking platform

Leverage Existing Investments

Modernize the network while utilizing existing C9K infrastructure

Migrate at Your Own Pace

Incrementally migrate devices and subnets to the cloud over time

Alot more to come....

Cloud Fabric Limited Availability

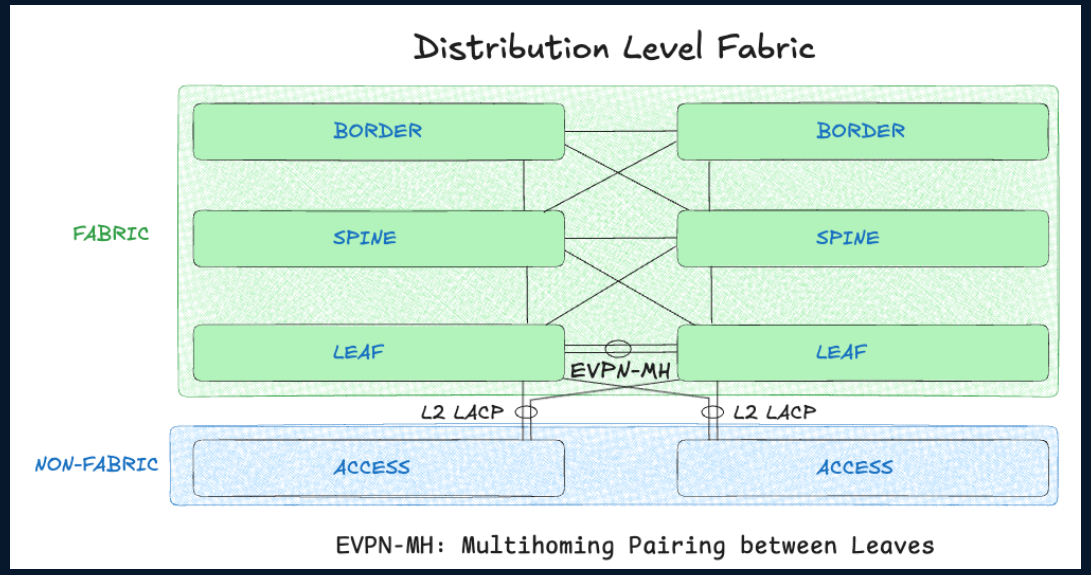
- Distribution Level Fabric
  - Fabric begins at the Distribution/Core
  - Multicast/Broadcast limited to Leaf
- Scale (1k Aps, 10k clients, 4 Leafs, 384 Switches, 300 Subnets)

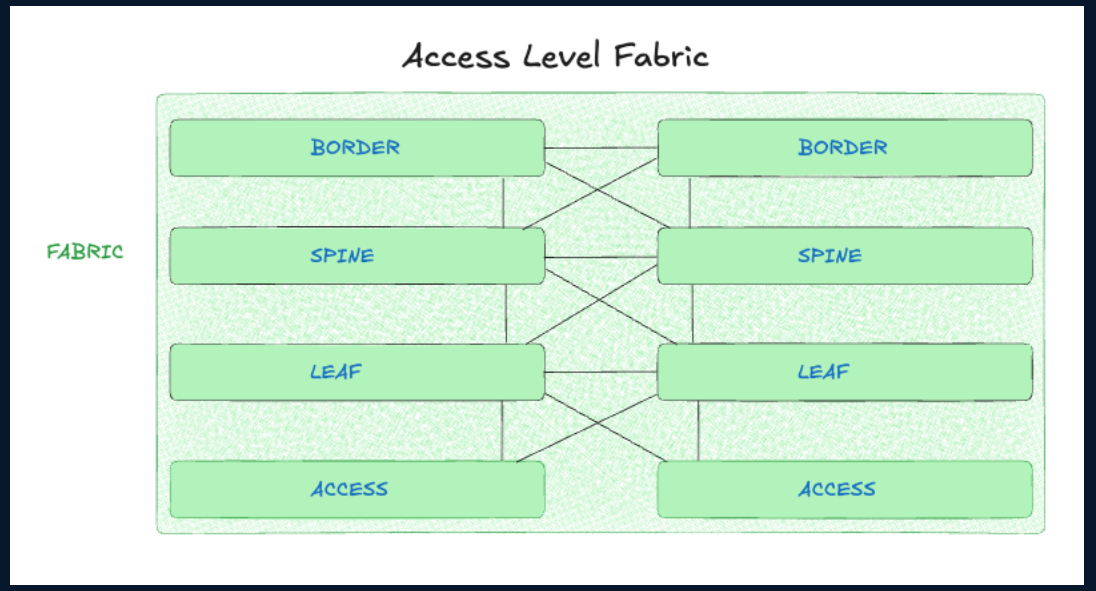
Cloud Fabric – Phase 1 (Spring ‘26)

- EVPN-MH Multihoming
- Brownfield subnet migration

Cloud Fabric - Phase 2 (Sept ‘26)

- Access Level Fabric
  - Pure-Layer 3 underlay
  - Fully Flood-free Routed Access
- Tenant Routed Multicast and MSDP
- Multi-Cluster support for scale
- Topology-based Fabric Automation and Assurance
- Increased scale -> 100K clients
- AI-driven day2 operations

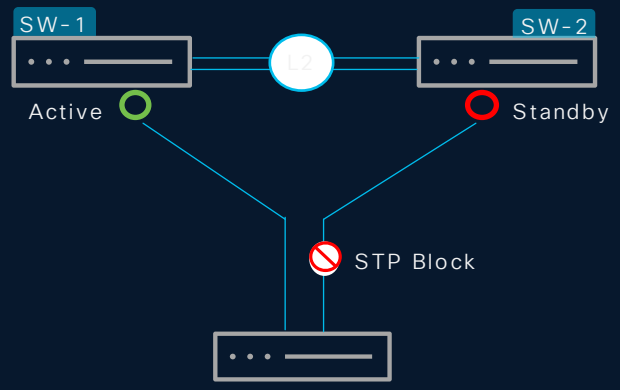




EVPN Multihoming

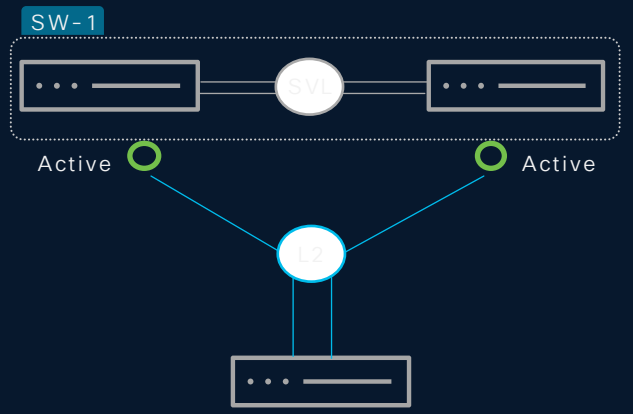
FHRP

HSRP | VRRP | GLBP



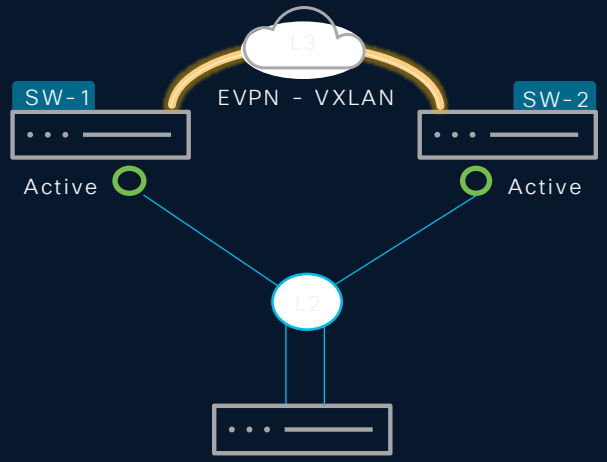
StackWise Virtual

Recommended



EVPN Multihoming

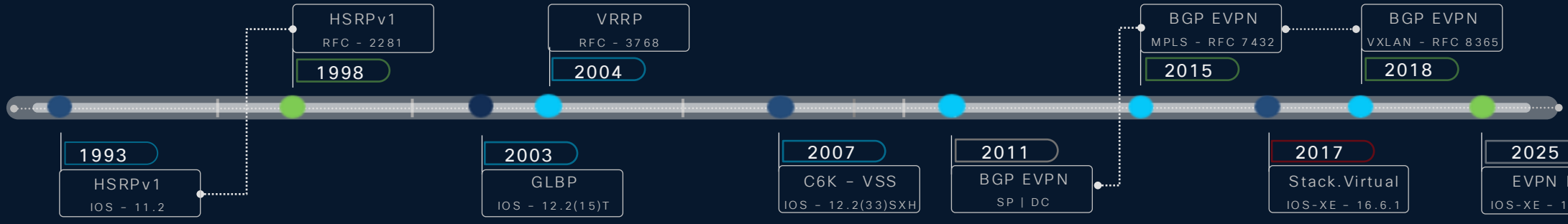
RFC 8365



Active VLAN

Standby VLAN

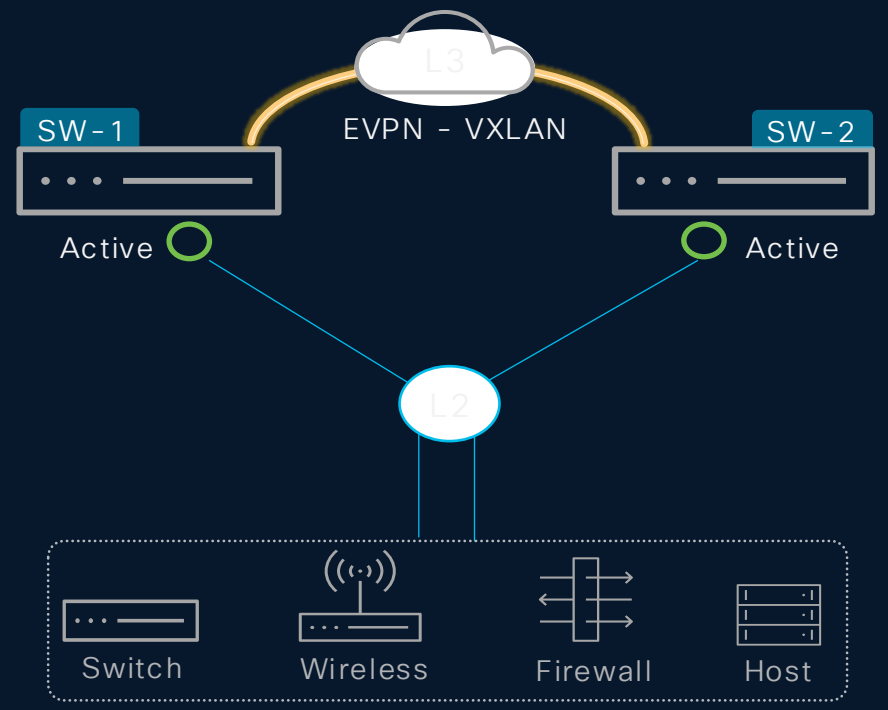
IETF

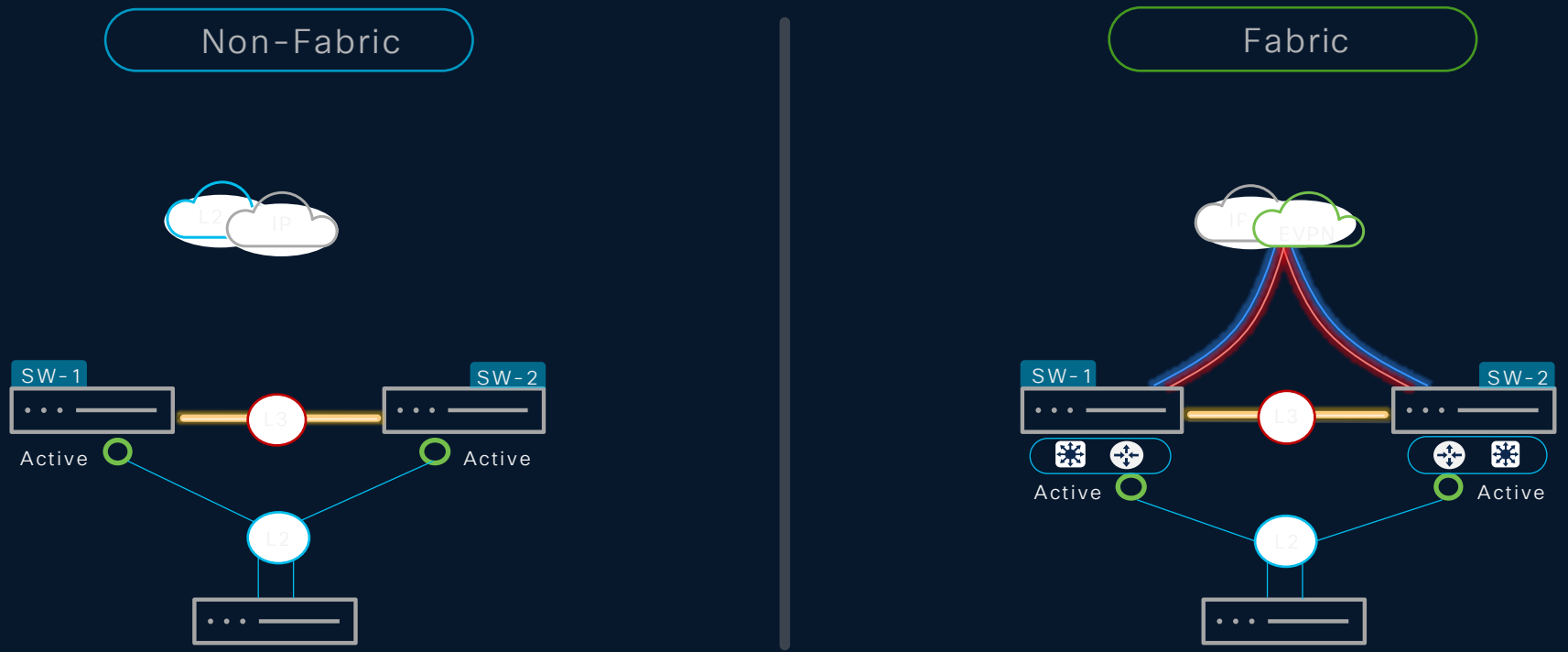


EVPN Multihoming – Product Support Matrix

GA: 17.18.2 – Dec'25

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 Series
	Catalyst 9500-H Series
	Catalyst 9300X Series
	Catalyst 9300 Series
Software License	Network Advantage



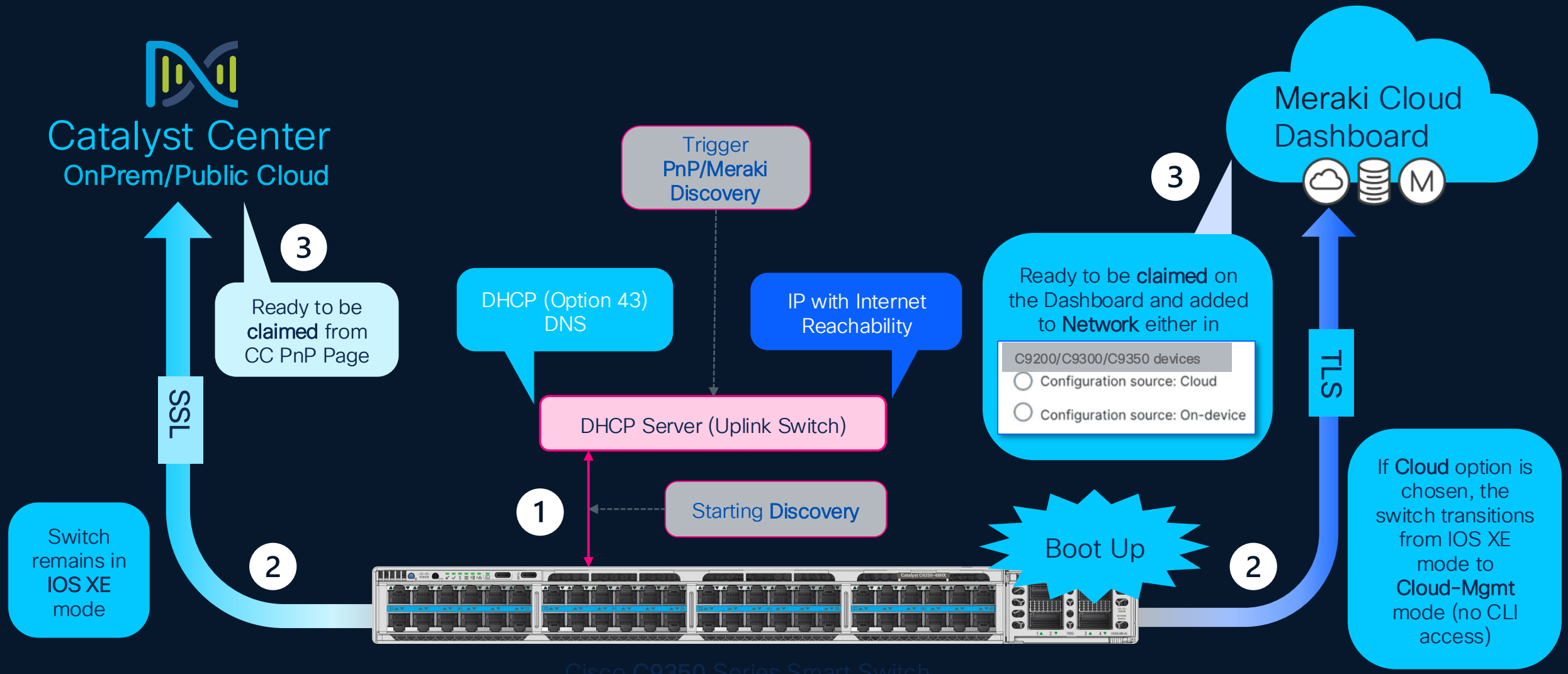


17.18.2 – Dec'25 – General Availability

- Transparent L2 Multipath solution for traditional IP / non-fabric networks
- Seamless transition path from FHRP to EVPN Multihoming – 2X performance, redundancy and scale.
- Extensible technology supporting Layer 3 segmentation and Layer 2 extension with EVPN fabric
- Hybrid L2 network support for hybrid Non-Fabric and Fabric networks

C9k Smart Switches

Unified Onboarding Experience



© 2026 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Smart Switching

C9350 and C9610 series

RECAP

1.6 Tbps
Stacking bandwidth

4x100G
Uplink Modules

PQC
Post-Quantum Security

4x
Higher MAC & ARP scale

C9350 series

C9610R

25.6 Tbps
System bandwidth

256x100G
Modular Line-Cards

PQC
Post-Quantum Security

10-Slot
To power Core density

INTRODUCING

The Next Generation of Campus Switching

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

RECAP

Silicon One ASICs

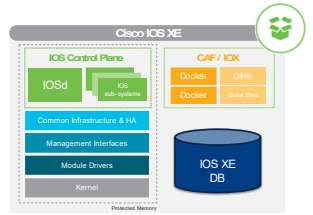
HW Adaptability

- 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

Sustainable

Smart Power | PoE Assurance | Energy Dashboard

Cisco Smart Switching

C9350 and C9610 series

RECAP

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

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

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

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

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

C9350 series

C9610R

C9610-SUP3XL/3

C9610-LC-40YL4CD

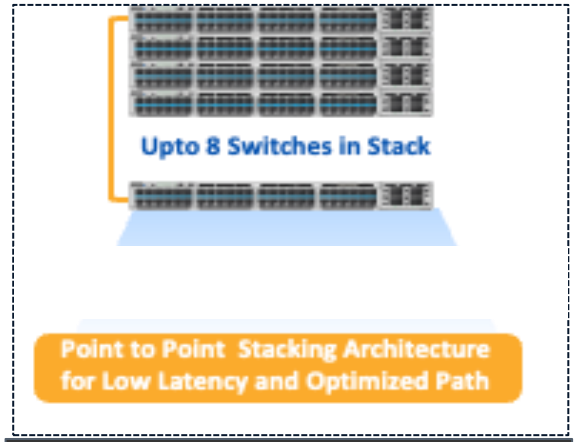
C9610-LC-32CD

Cisco C9350 – Smart Stacking (NG-Stackwise)

New architecture for the new networking demands

1

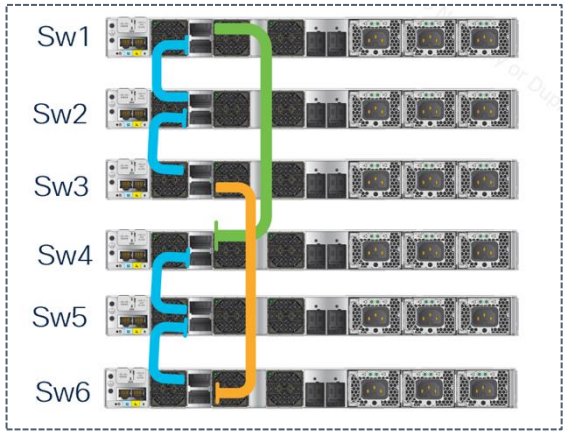
New stacking architecture
Open-standards based



Open shortest path algorithm. Same code base as front-panel stacking.

2

Flexible user-friendly stacking design

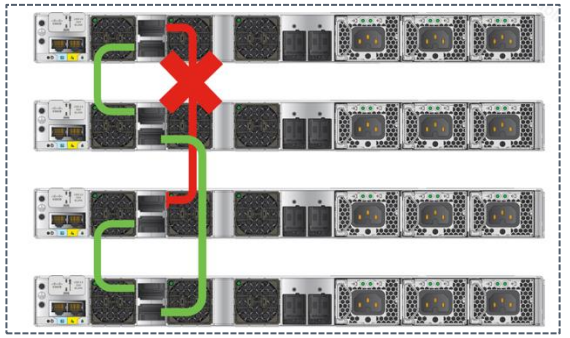


No restrictions on how or where you connect to form a full ring.

Eliminate long cable requirement

3

Isolated bandwidth loss during failure

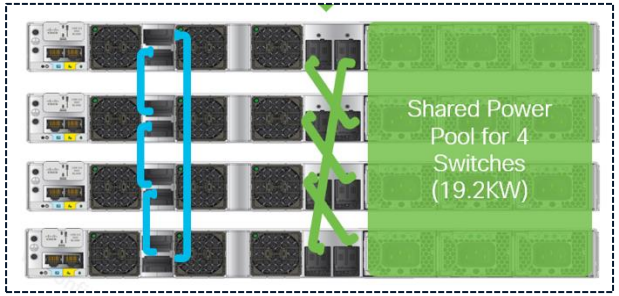


Failure only affects bandwidth for directly connected switches.

Other switches in the stack operate at full bandwidth

4

Enhanced StackPower
Higher power sharing



New cables handle higher current (**55A**)

30% more power sharing via StackPower ports

Unique to the C9350 series. Not applicable for C9300(L)(X) series

C9350 Smart Switch Reload Enhanced

Improving **Boot times** with **Kernal-exec Reload**

CLI	Behavior	What does it do?	When to use?
`reload`	New behavior for existing command. **Replaces the current 'reload' command.**	• Kernel-exec reload • Bypasses ROMMON during boot • ~44 seconds faster boot	• General routine reloads • Memory and CPU related reloads
`reload firmware`	**Same behavior as existing 'reload' command**	• ROMMON based reload • Full hardware (PHY, MCU, FPGA) flush	• Any reload requiring an update to hardware entries • Example – Routing table flush and re-learn.

Tested Boot Time

Platform	Reload (in seconds)	Reload Firmware (in seconds)
C9300X	N/A	197*
C9350-24/48 U/P/T	71	121
C9350 – 24/48 HX/TX	78	157

*C9300X and older will not support Kexec based reload. The behavior of reload command will be equivalent to 'reload firmware' on the C9350 series

Default `reload` : **Catalyst 9300** → ROMMON boot | **Cisco C9350** → Kexec based boot
Use `reload firmware` on **Cisco C9350** for ROMMON boot

The Next Gen xFSU on C9350 Smart Switches

IOS-XE 26.1.1
Standalone switches

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

What's New in C9350 xFSU

Control Plane Reload Now 3x Faster

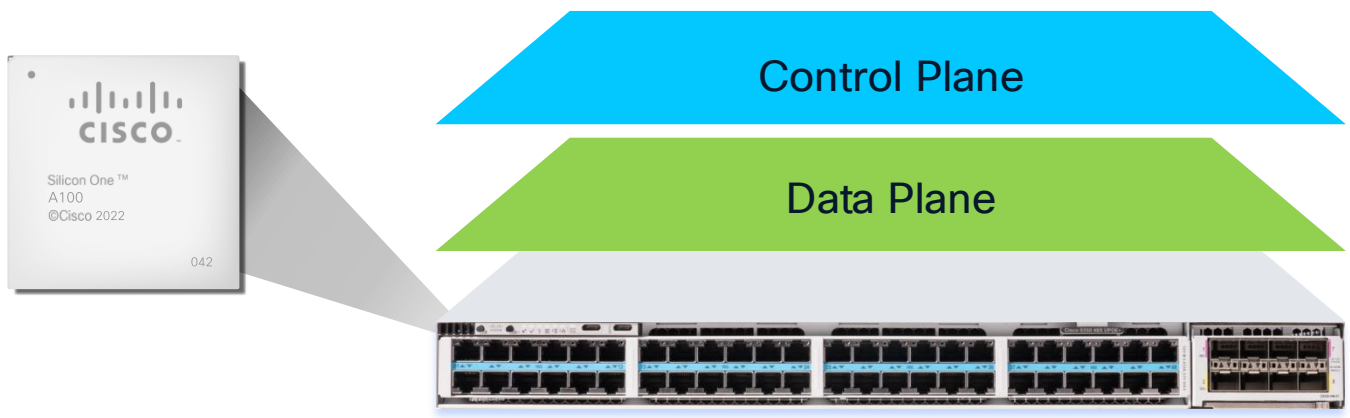
C9350 uses ***kexec-based reload*** instead of ROMMON.
This reduces bring-up time from **3 min to just *1 min*.**

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.



Cisco C9350 Smart Switch

Performance Breakthrough
<1 sec
Downtime*

*Pending full verification from engineering

A compelling vision of security and resilience

Enhanced Detections & Protections

Protection
“Live Protect”

Infrastructure Detection & Response

Compensating Controls

Detections Enablement

Cisco Infrastructure Resilience

New Feature Enablement
(TACACS+ over TLS, Tetragon, FIDO2 over SSH, etc…)

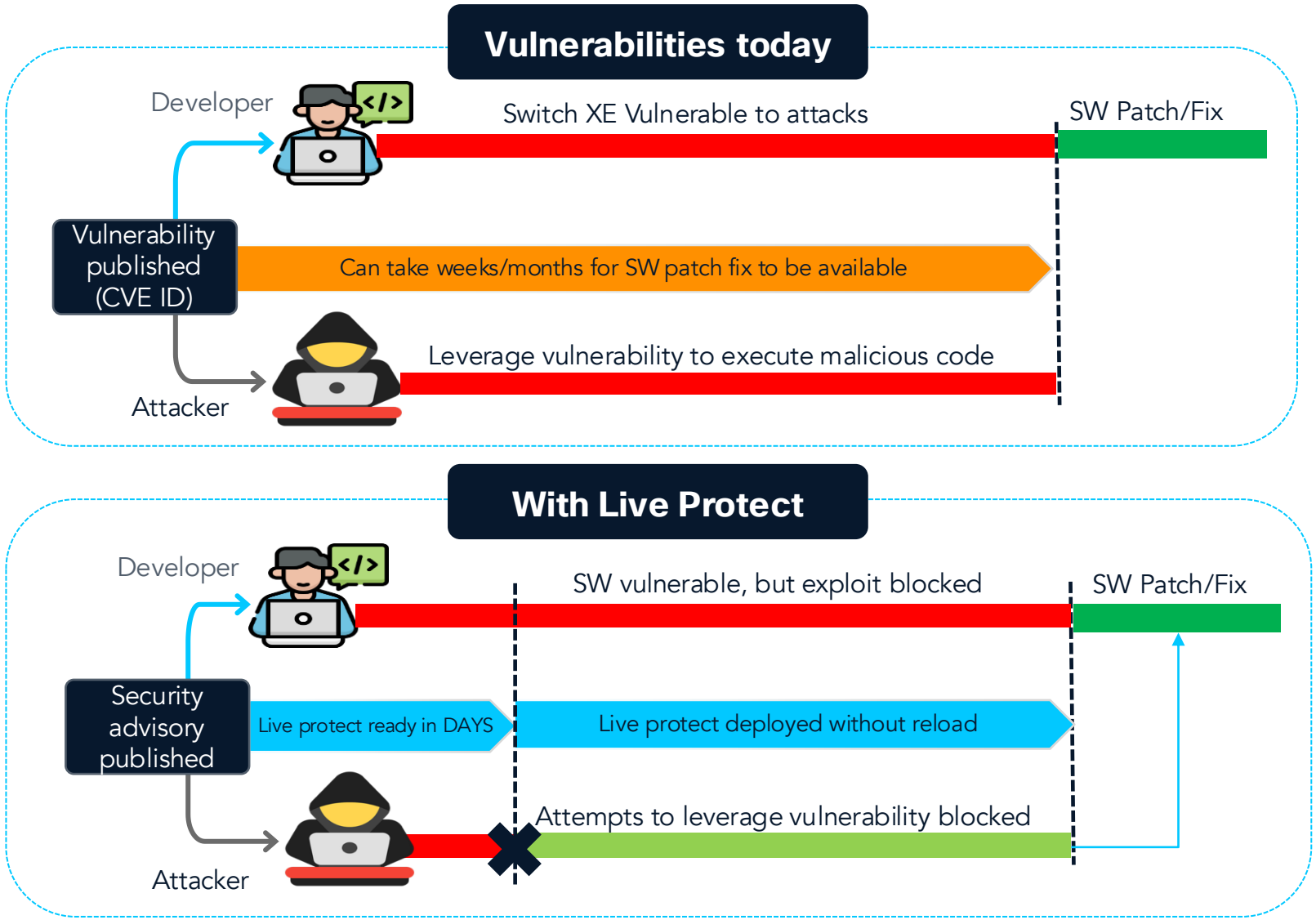
Secure by Default

Feature Deprecation / Removal*

Baseline Security Posture

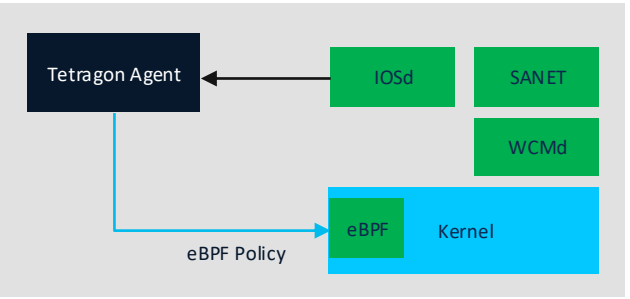
*https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-infrastructure-resilience-feature-removal-and-suggested-alternatives.pdf

Live Protect for Blocking Attacks Leveraging Security Advisories



How does it work?

IOS-XE based network element



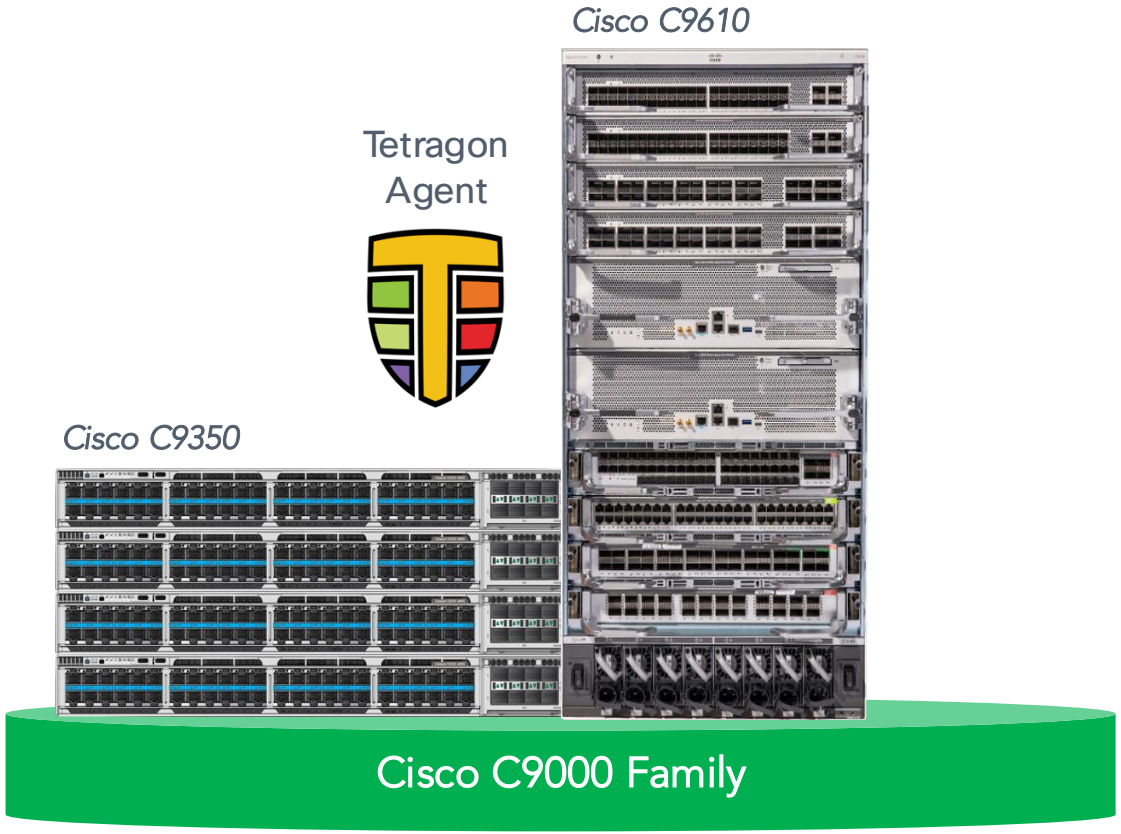
Integrate Tetragon into IOS-XE

Tetragon uses eBPF to monitor/enforce security policies at kernel level for network events

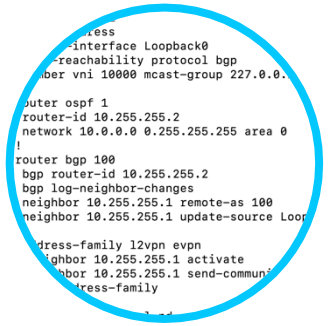
Mitigate threats to network devices without waiting for patches and without downtime.

Live Protect Deployment

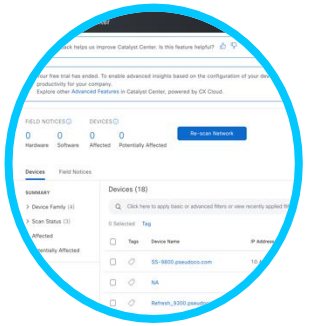
IOS-XE 26.2.1



Mode of Operations



CLI



Catalyst Center

Meraki Dashboard

Mode of Enforcement

Observing

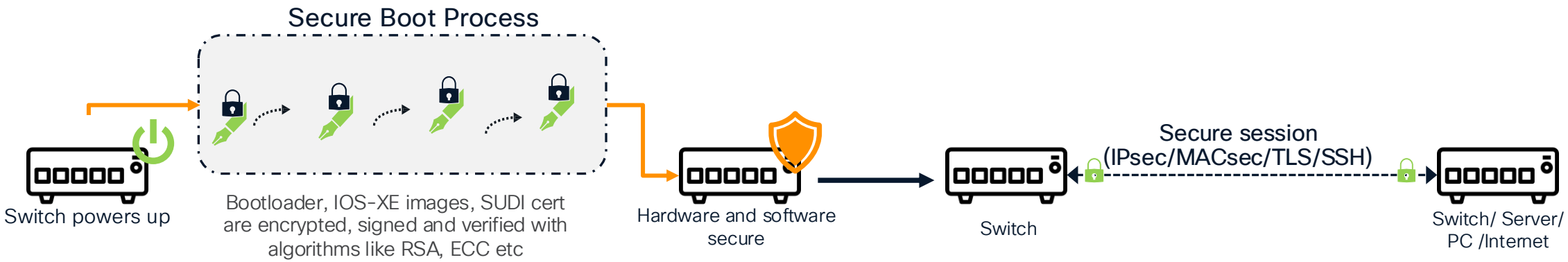
Detect and report on potential compromises

Protecting

Block and report on potential compromises

Cryptography in the Network Today

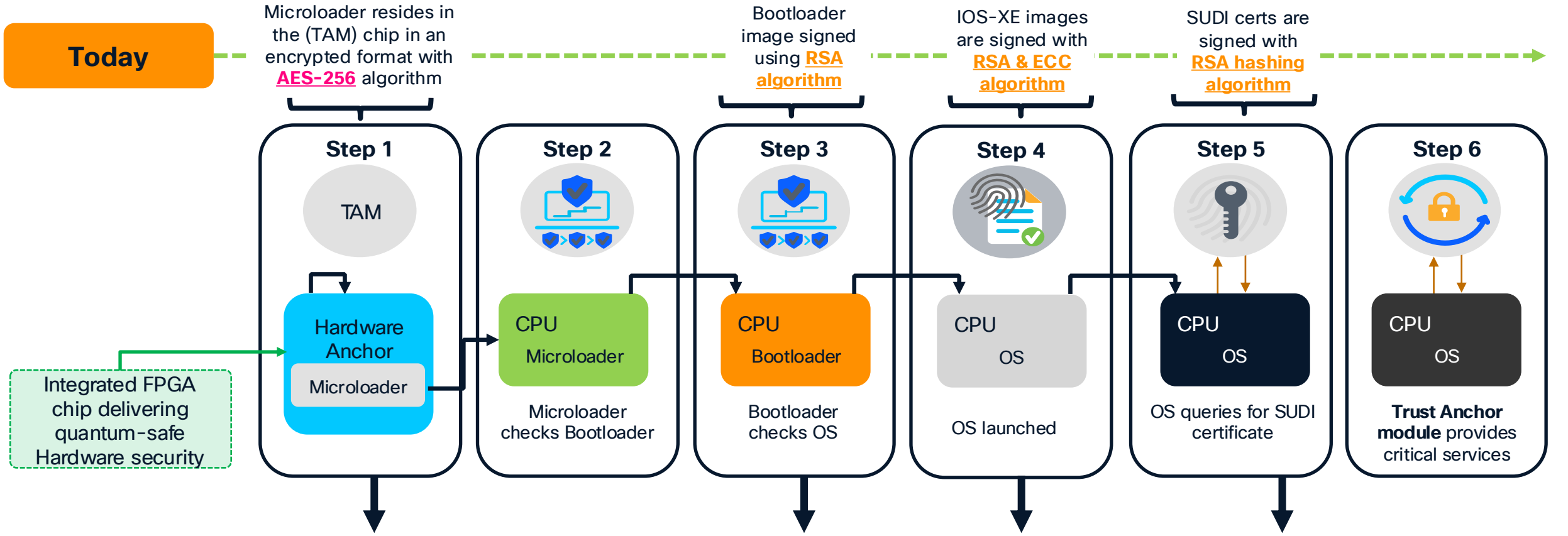
Hardware to Software



Security Feature	Cryptography	Use
IOS-XE image & bootloader image signing / verification	**Digital signatures** (using asymmetric cryptography)	Ensures authenticity and integrity of system software before booting.
SUDI Certificates / TLS Certificates / Root CA Certificates	**Digital certificates** (which use digital signatures & asymmetric cryptography)	Provide device identity and authentication, enable trust chaining (PKI).
Secure transportation sessions/ Key exchange	**Asymmetric encryption & symmetric encryption**	**Asymmetric encryption for key exchange**, then **symmetric encryption** for bulk data

Secure Boot Process on C9000 Smart Switches

Hardware PQC support with Trust Anchor Module

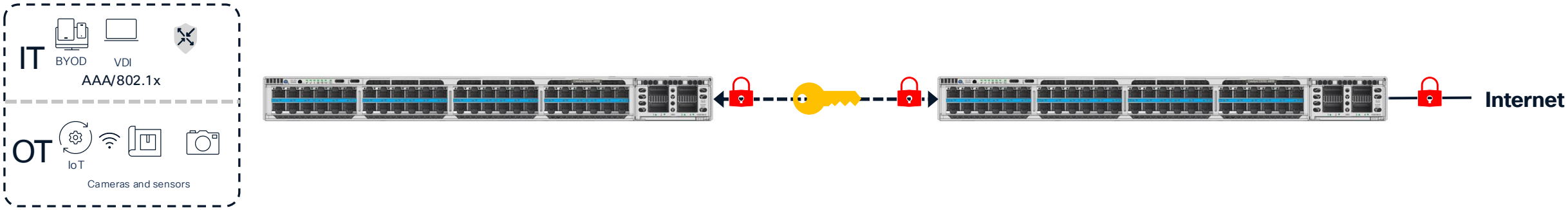


With PQC

Microloader resides in the (TAM) chip in an encrypted format with AES-256 algorithm, which is PQC-resistant	Bootloader image signed and verified with LMS (Leighton-Micali Signature) algorithm, a PQC-resistant standard.	All Cisco IOS-XE images will be signed and verified using the ML-DSA-87, a PQC approved algorithm	SUDI cert residing in TAM for HW authentication will be signed with ML-DSA-87, a PQC approved algorithm

Software PQC Support on C9000 Switches for Transport Encryption

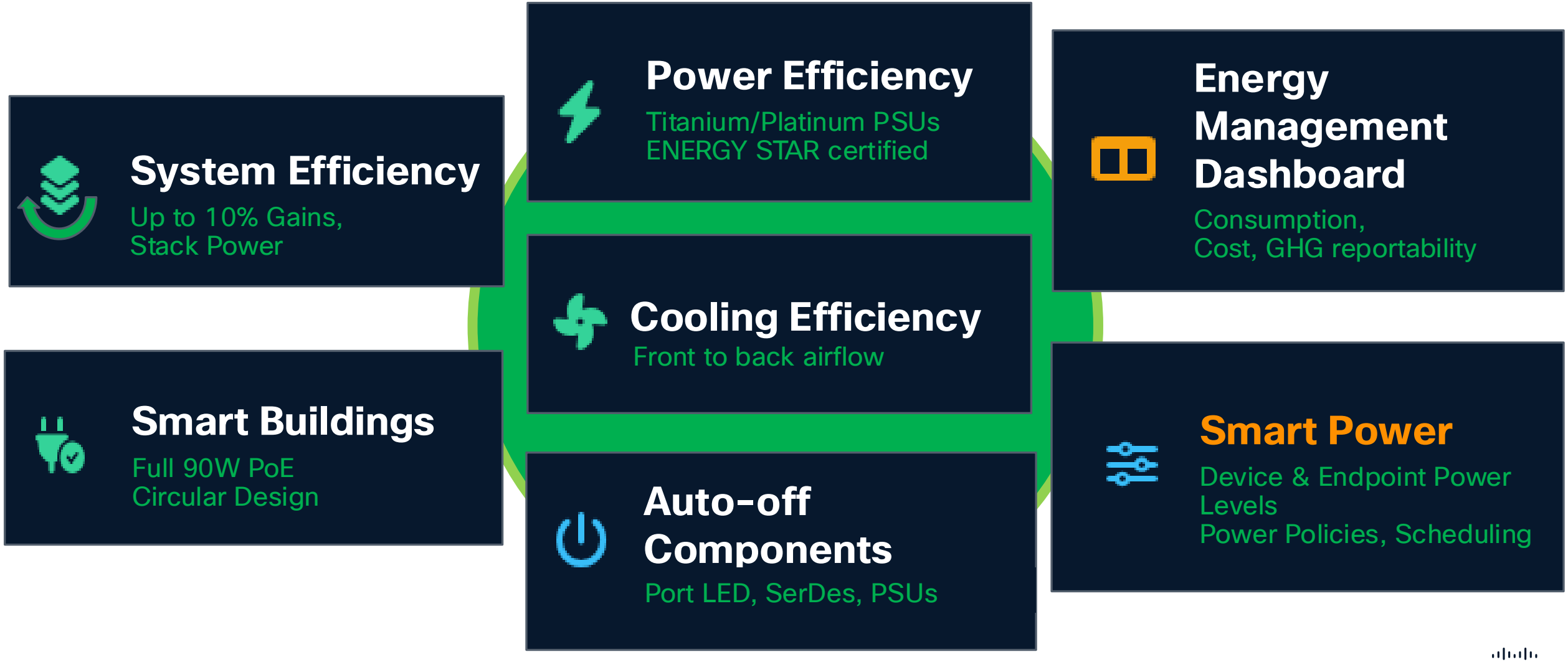
Data Protection with Transport Security in the Network



Encryption Algorithms today		PQC compliance	Remediation
MACSec	Pre-shared Key	PQC resilient	NA
	Certificate based (MKA EAP-TLS)	PQC vulnerable	**EAP-TLS 1.3 with ML-KEM** • C9350 – IOS-XE 26.1.1* • C9610 – IOS-XE 26.2.1*
IPSec	IKEv2 Initial Key Exchange	PQC vulnerable	**IKEv2 with ML-KEM and TLS 1.3 with ML-KEM** • C9350 – IOS-XE 26.2.1* • C9610 – Roadmap

*Features release timelines are not final and subject to change

Sustainability Innovations with C9000 Smart switches



Introducing Smart Power : IOS XE 17.18.2

Policy-Driven Power Management and Optimization Framework

Smart Power Domain: Devices are grouped into Smart Power domain with a unique domain name and security credentials

Neighbor Discovery: via UDP port 43440 broadcasts and CDP extensions, **Queries/Replies:** TCP or UDP unicast

Attributes: finetune policies with metadata like *Importance, Role, Keyword, Level, Name*

SDK Interoperability: Provides an SDK for interoperability with non-Cisco devices and facility management systems

Power Levels

Granular endpoint control with defined states ranging from 0 (Off) to 10 (Fully On).
Operates at Layer 2.

Policies

Apply schedules by role, location, or tag. Uses attribute-based logic and conditional activation.

Schedules

Recurring policies with comprehensive time parameters (e.g., "5:30 PM, Mon-Fri").

Smart Power Policy – How to

1. Target & Action

Select Ports or device groups/tags

Select Desired Action: Power Level: 0 (Off).

2. Condition

Set the trigger condition for the policy to run: Importance = 100.

3. Schedule

Use a simple calendar and clock to Set the recurrence: At 5:30 PM, Every Day.

Example Policy (CLI)

```
Interface gi1/0/1
smartpower level 0 recurrence importance 100 at 30 17 1-31 1-12 0-7
```

</> What It Means

This policy targets port **gi1/0/1**.

It sets the power level to **0 (Off)**.

It runs at **5:30 PM** (17:30), **every day** (1-31), **every month** (1-12), on **all days of the week** (0-7).

This *only* applies if the device's **importance** is **100**.

System
Power Levels

Endpoint
Power Levels

switch specific power optimizations

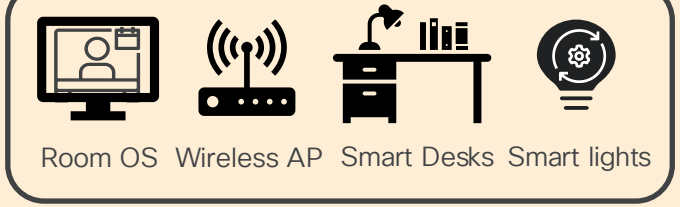
Endpoint specific power optimizations

Power Optimization 0 to 100%

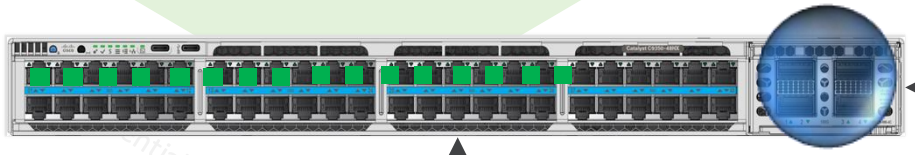
Level 1	Power off
Level 2	Hibernation*
Level 3	Deep sleep*
Level 4	NA
Level 5	NA
Level 6	NA
Level 7	Auto off – LED, PSU and SFP
Level 8	Auto off – LED and SFP
Level 9	Auto off – SFP
Level 10	Full Power

Auto-Off PSU - StackPower

Partner Device integrations*



Smart Power Packet



Example: Set Smart Power level to 7
All port LED, SFP and unused PSUs can be turned off

Example: Smart Power level # 7on IP phone turns off screen to save power

Catalyst Center/ Meraki Cloud Policy Management*

9800 & 8875 series IP Phones with PhoneOs supports Smart Power Level 10,7 & 2

Achieving NetZero Goals with the Smart Power Framework

Example: Shifting 1,000 phones from level 10 to level 7 during off-hours can reduce up to 35% power draw

* roadmap

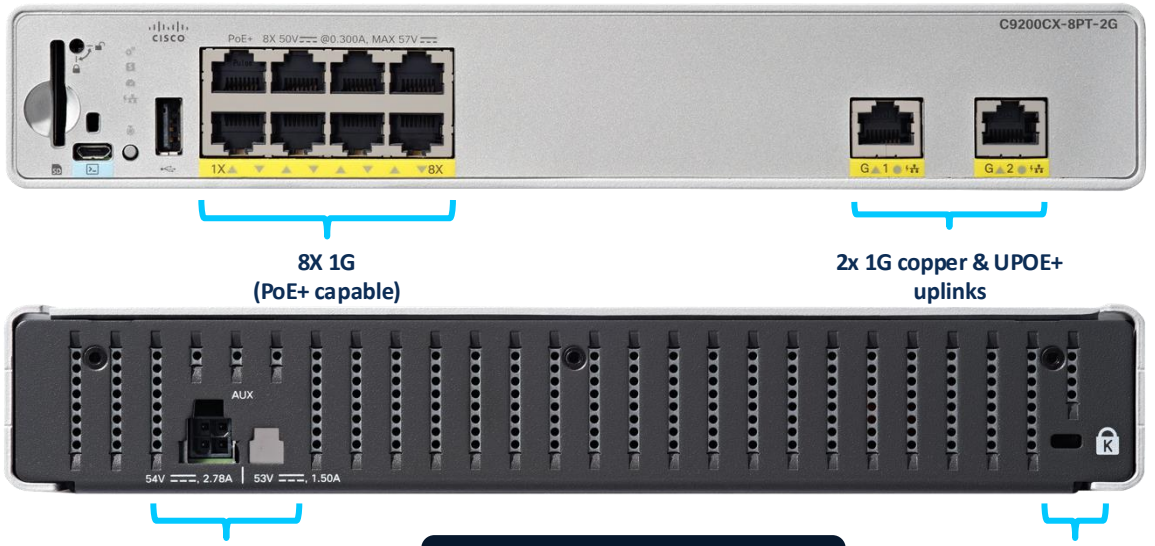
Cisco Catalyst 9200CX Pass-through SKU

For Flexible Powering Deployments Requiring PoE Downlinks

IOS-XE 17.18.1

10MB/100MB/1G Speeds

Power via PoE+/UPOE/UPOE+ and/or External Power Adapter*



Power budget details

Aux 80W	Aux 150W	PD1	PD2	POE Power Available	Number of 30W PSE Ports	Number of High Priority Ports
-	Present	Class 8	Class 8	249.5	8	3
-	Present	Class 4	Class 8	210	7	2
Present	-	Class 8	Class 8	179.5	6	2
-	Present	Class 6	Class 6	208.5	6	1
	Present	Class 4	Class 4	168.5	5	0
Present		Class 6	Class 6	138.5	4	1
	Present			129.5	3	0
		Class 8	Class 8	99.5	3	1
Present		Class 4		78.5	2	0
		Class 8	Class 6	79	2	0
Present				59.5	1	0
		Class 8	Class 4	30 **	1	0

All Downlink Ports PoE+ Capable

240W Max PoE Power Budget**

Powered by the UADP 2 Mini ASIC

* Class 4 30W minimum needed to power C9200CX-8PT-2G

** When Powered by 2x 802.3bt UPOE+ uplinks in addition to the 150W External Power Adapter

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

C9000 Smart Switches upcoming features

Bridging parity gaps

C9350 Smart Switch

Upcoming features
IOS-XE 17.18.2 and 26.1.1

IOS-XE 17.18.2	IOS-XE 26.1.1
L3-Multicast IPv6 Full Key Support	High Availability-ISSU (xFSU)
Full key Multicast support	Fabric-EVPN (Leaf role)
Fabric-SDA (Fabric Edge role)	QoS-AVC
NetFlow (FNF Byte Counter)	L3 Switching-BFD
Security-ACL (ACL Logging)	Security-FHS (IPv6 FHS)
Security-CTS/SGT	L3 Switching-PBR
L3 VPN - MPLS-MPLS	ISIS SA bit support
QOS-MPLS	RACL Multicast
Netflow-Advanced	SGACL Cell Counter Scale
L2 Switching-STP	4K SVI
	MacSec – Switch to Switch

C9610 Smart Switch

Upcoming features
IOS-XE 17.18.2 and 26.1.1

IOS-XE 17.18.2	IOS-XE 26.1.1
SVL/ISSU	Fabric-SDA border
Full key Multicast support	L3 Switching-NAT
NetFlow Base support	Multicast global resource synchronization
L3 Switching-PBR	L3 Switching-BFD
L3 VPN - MPLS-MPLS	Secure boot
Security-ACL	
Security-CTS/SGT	
DHCP Snooping	
QOS - MPLS	
1G support (Fiber)	
50G support	

Thank you