

Next Gen Data Centers Unleashed: Nexus Dashboard, Hypershield Smart Switches & Hyperfabric

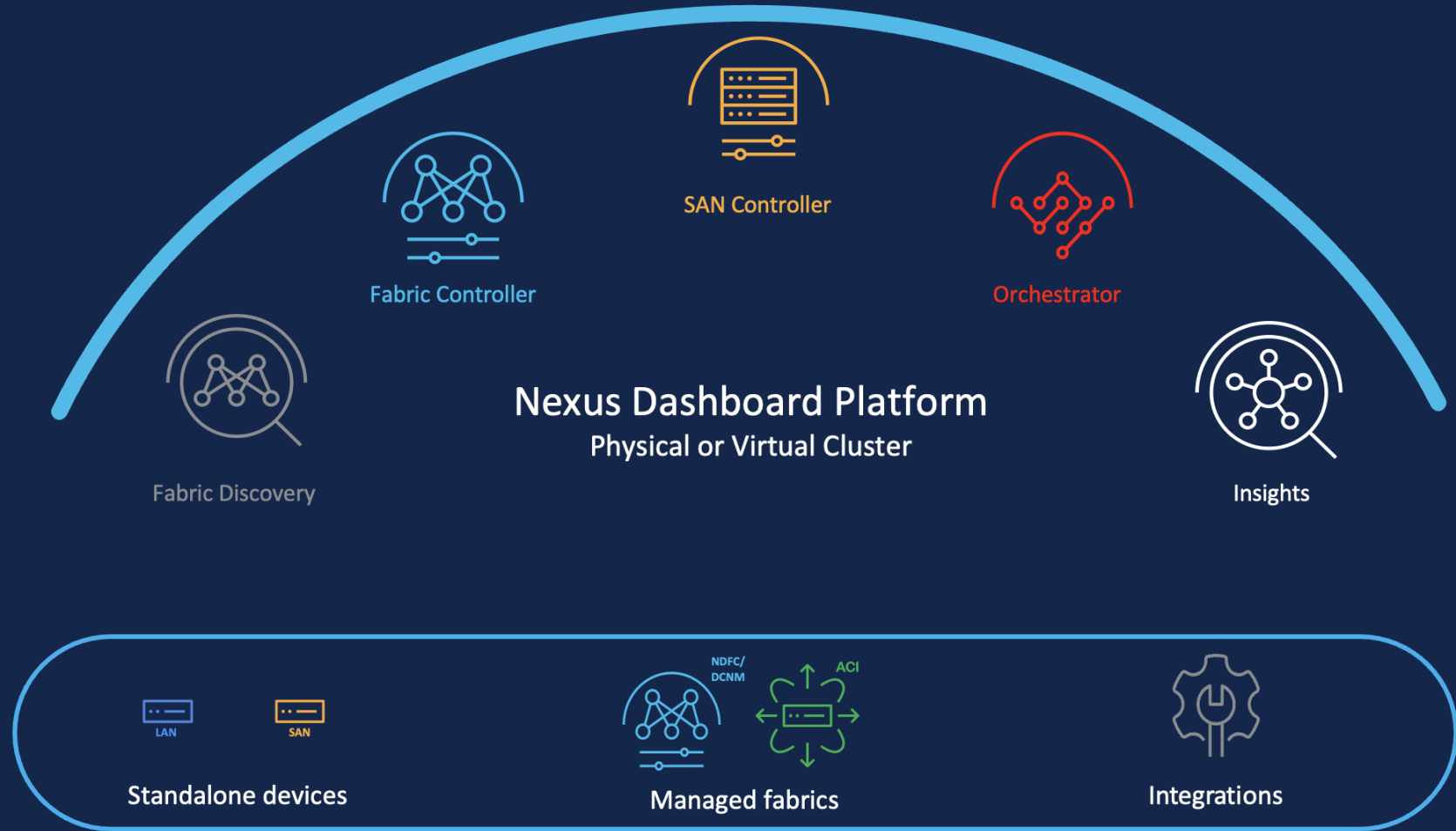
Raul Arias
Solutions Engineer



Agenda

1. Nexus Dashboard 4.1
2. Hyperfabric
3. Nexus Smart Switches

Cisco Nexus Dashboard



Nexus Dashboard Capabilities

Controller

For NX-OS based LAN or SAN

- VXLAN fabrics or classic L2/L3 LAN
- Greenfield, brownfield or read-only
- Automated LAN fabric provisioning
- Configuration automation
- Compliance monitoring
- NX-OS image & patch management
- Endpoint visibility & tracking
- MDS SAN management

Orchestration

For Multi-Site ACI Fabrics

- Policy coordination between fabrics
- Data center interconnect configuration automation
- Public cloud connectivity with Cloud Network Controller deployments

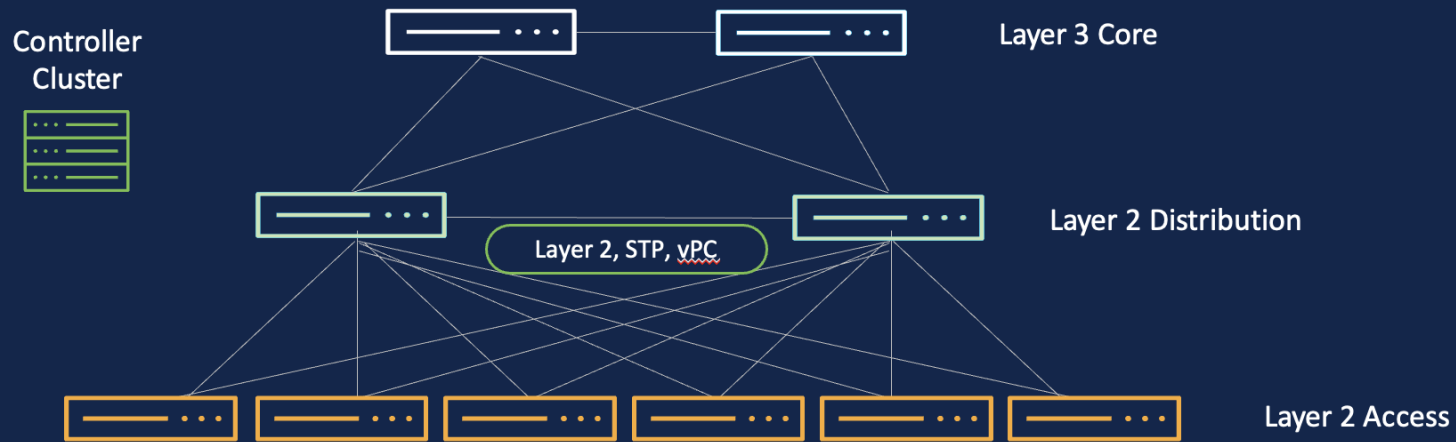
Telemetry

Visibility & Analytics

- Ingest & analyze switch configuration, telemetry, and flow data
- Config & traffic anomaly detection
- Config-based Bug & PSIRT scans
- Inventory, Power & EoSale reports
- Tailored Field Notice advisories
- Flow-level visibility & analytics w/ L4-L7 traffic path mapping
- Delta & What-if* analysis

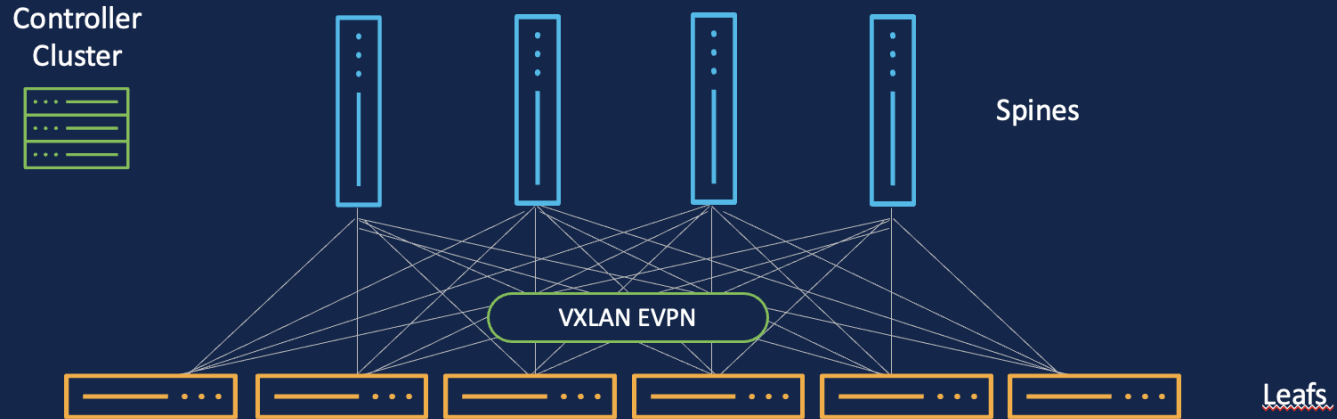
Fabric Deployment Options

Classic LAN Fabrics



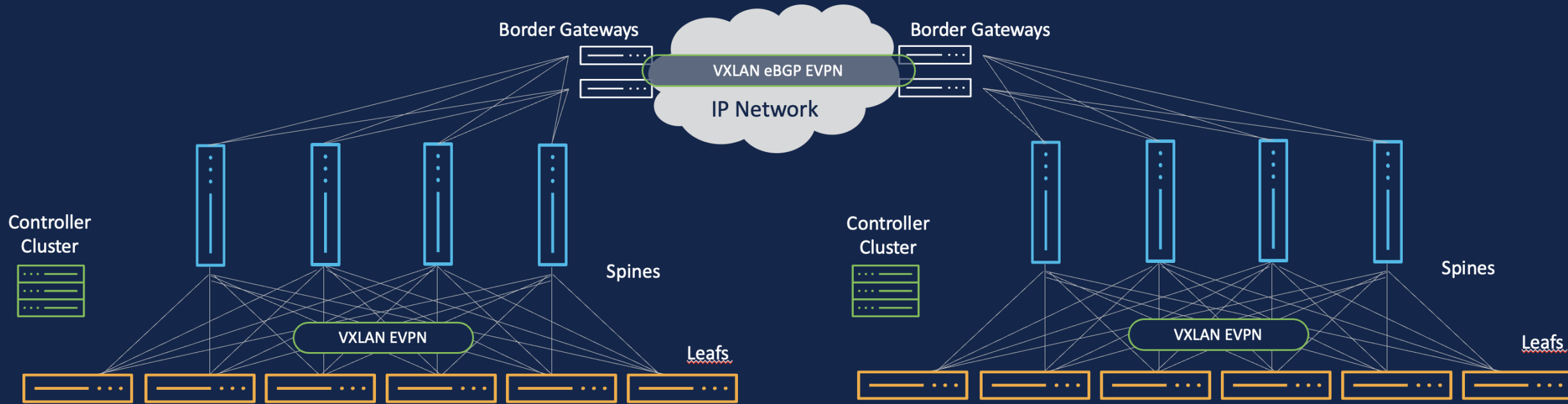
- Tiered Layer 2 / 3 Design
 - Access Layer for host connections
 - Distribution Layer for scale/services
 - Core Layer for all routing (default gateway)
- Optimized for North-South routed traffic
- Most connectivity is at Layer 2
 - Potentially large broadcast domains
 - Spanning Tree concerns
- Core becomes bottleneck for East-West routed traffic

VXLAN-based Fabrics



- Routed IP underlay (no Spanning Tree)
- VXLAN BGP EVPN overlay
 - Uses VXLAN encapsulation
 - Multiprotocol BGP EVPN control plane
 - L2 adjacency across entire fabric
 - Multitenancy support via VRF contexts
- Spine-Leaf topology
 - Take advantage of fixed 1-2RU spines
 - More endpoints = More leafs
 - More throughput = More spines
 - Deterministic Pathing w/ ECMP
 - Equal treatment of N-S and E-W traffic

VXLAN EVPN Multi-Site/Fabric



- Extends VXLAN encap across WAN
 - Maintains traffic segmentation
 - Potential for L2 extension between sites
- Uses Border Gateways or Border Gateway Spines
 - Each site/fabric is an availability zone
 - Possible traffic engineering challenges
 - Policy, ID consistency required
 - Offered by Nexus Dashboard

Policy Based Configuration

Filter by attributes

☐ Template	Description	Content type	Switch	Entity name	Entity type	Source			
☐ feature_lacp	-	TEMPLATE_CLI	SJC-NDI-NXOS-Leaf-1	SWITCH	SWITCH	UNDERLAY	50	false	false
☐ feature_ngoam	-	TEMPLATE_CLI	SJC-NDI-NXOS-Leaf-1	SWITCH	SWITCH	UNDERLAY	50	false	false
☐ feature_pim	-	TEMPLATE_CLI	SJC-NDI-NXOS-Leaf-1	SWITCH	SWITCH	UNDERLAY	50	false	false
☐ feature_dhcp	-	TEMPLATE_CLI	SJC-NDI-NXOS-Leaf-1	SWITCH	SWITCH				
☐ copp_policy	-	TEMPLATE_CLI	SJC-NDI-NXOS-Leaf-1	SWITCH	SWITCH				
☐ switch_freeform	Additional Feature Configuration	PYTHON	SJC-NDI-NXOS-Leaf-1	SWITCH	SWITCH				
☐ copp_policy	-	TEMPLATE_CLI	SJC-NDI-NXOS-Leaf-2	SWITCH	SWITCH				
☐ switch_freeform	Additional Feature Configuration	PYTHON	SJC-NDI-NXOS-Leaf-2	SWITCH	SWITCH				
☐ feature_ospf	-	TEMPLATE_CLI	SJC-NDI-NXOS-Leaf-2	SWITCH	SWITCH	UNDERLAY	50	false	false

All changes to device configuration is performed using policy templates, which can be easily backed out if needed. Templates can be customized or can apply free-form CLI commands if desired.

Fabric Overview - Multi-Site

Generated Config Details for Site1-BGW1

Generated Config Before

Generated Config After

```
1 router bgp 65111
2   neighbor 10.2.0.6
3     remote-as 65111
4     update-source loopback0
5     address-family l2vpn evpn
6       send-community
7       send-community extended
8
9
10
```

Software Upgrades

Fabric Software

NX-OS/IOS-XE

ACI

Automate NX-OS software image upgrades across the fabric, with support for customized upgrade groups for staged deployments.

Overview

Images

Image Policies

Devices

History

Filter by attributes

Actions

☐	Device name	IP address	Fabric	Software version	Policy	Status	Model	View Details	Image Staged	Validated	
☐	SJC-NDI-NXOS-Leaf-2	198.19.253.214	sjc-nxos1	10.4(2)	sjc-nxos1_policy_1_N9K_All	Out-Of-Sync	N9K-C93180YC-FX3	Validate			
☐	SJC-NDI-NXOS-Spine-1	198.19.253.211	sjc-nxos1	10.4(2)	sjc-nxos1_policy_1_N9K_All	Out-Of-Sync	N9K-C93180YC-FX3	Validate			
☐	SJC-NDI-NXOS-Spine-2	198.19.253.212	sjc-nxos1	10.4(2)	sjc-nxos1_policy_1_N9K_All	Out-Of-Sync	N9K-C93180YC-FX3	Validate			
☐	SJC-NDI-NXOS-	198.19.253.213	sic-nxos1	10.4(2)	sjc-	Out-Of-Sync	N9K-C93180YC-FX3	Validate			

Endpoint Tracking

sjc-nxos1

🕒 Current ▾

Anomaly level

22

Critical0

Healthy22

Major0

Minor0

Warning0

Change summary ⓘ

0 Endpoint New or modified

+

0 Endpoint Deleted

↓

Filter By attributes

MAC	IP addresses	Hostname	Anomaly level	Switches	Interface	Status	VRF	VLAN	
00:50:56:8E:84:3E	198.18.11.55	-	Healthy	SJC-NDI-NXOS-Leaf-1	eth1/2	Active	siwapp_vrf	2300	...
00:50:56:8E:77:72	198.18.11.58	-	Healthy	SJC-NDI-NXOS-Leaf-1	eth1/2	Active	siwapp_vrf	2300	...
00:50:56:99:72:37	198.19.254.1	-	Healthy	SJC-NDI-NXOS-Leaf-1	eth1/48	Active	nddata_vrf	-	...
00:50:56:94:05:F0	192.168.192.250	-	Healthy	SJC-NDI-NXOS-Leaf-1	eth1/2	Active	pingerapp_vrf	1711	...
	172.16.0.10								
00:50:56:82:48:3E	172.16.0.11	-	Healthy	SJC-NDI-NXOS-Leaf-1	eth1/2	Active	nditfgen_vrf	2302	...

Telemetry on Nexus Dashboard

Anomalies

Service Endpoint Traffic Score Unhealthy

What's wrong?

Service endpoint 172.16.1.7:3260 (TCP), traffic score is not healthy; Congestion occurred

Anomaly level

Warning

Status active

Last seen

Last seen: Aug 13, 2025, 06:30:09 PM

Category	Fabric	Nodes	Initial detection time
Connectivity	sjc-nxos1	SJC-NDI-NXOS-Leaf-2	Aug 13 2025 06:20:08 PM

What triggered this anomaly?

Service endpoint 172.16.1.7:3260 (TCP), traffic score is not healthy; Congestion occurred

What's the impact?

- 1 service endpoint's communication with 4 clients is impacted
- [View report](#)

How do I fix it?

Cisco recommended solution (1/2)

Congestion occurred. Consider increasing buffer allocation for traffic class and rate of traffic

<

>

Detect issues impacting single switch or fabric-wide connectivity.

Requires **Advantage** license.

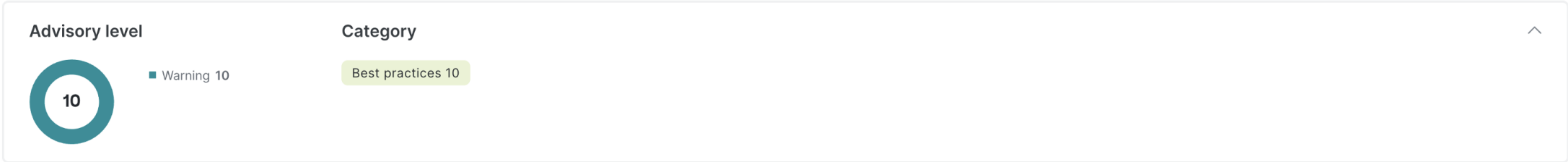
Best Practices Advisories

sjc-nxos1

OverviewInventoryConnectivitySegmentation and securityConfiguration policiesAnomaliesAdvisoriesHistory

Active nowUnacknowledged

Filter by attributes



☐ Title	Advisory level	Category	Nodes	
☐ Disable IP source routing	Warning	Best practices	SJC-NDI-NXOS-Spine-2 sjc-nxos1 View all (4 total)	...
☐ Configure NTP with authentication	Warning	Best practices	SJC-NDI-NXOS-Spine-2 sjc-nxos1 View all (4 total)	...
☐ Use AAA for authentication	Warning	Best practices	SJC-NDI-NXOS-Spine-2 sjc-nxos1 View all (4 total)	...

Refer toView in TableAction

Alerts you to any switch configuration items that do not follow Cisco best practices.

Requires **Advantage** license.

Not yet available for ACI.

Delta Analysis

Target Fabrics:

ACI

NDFC

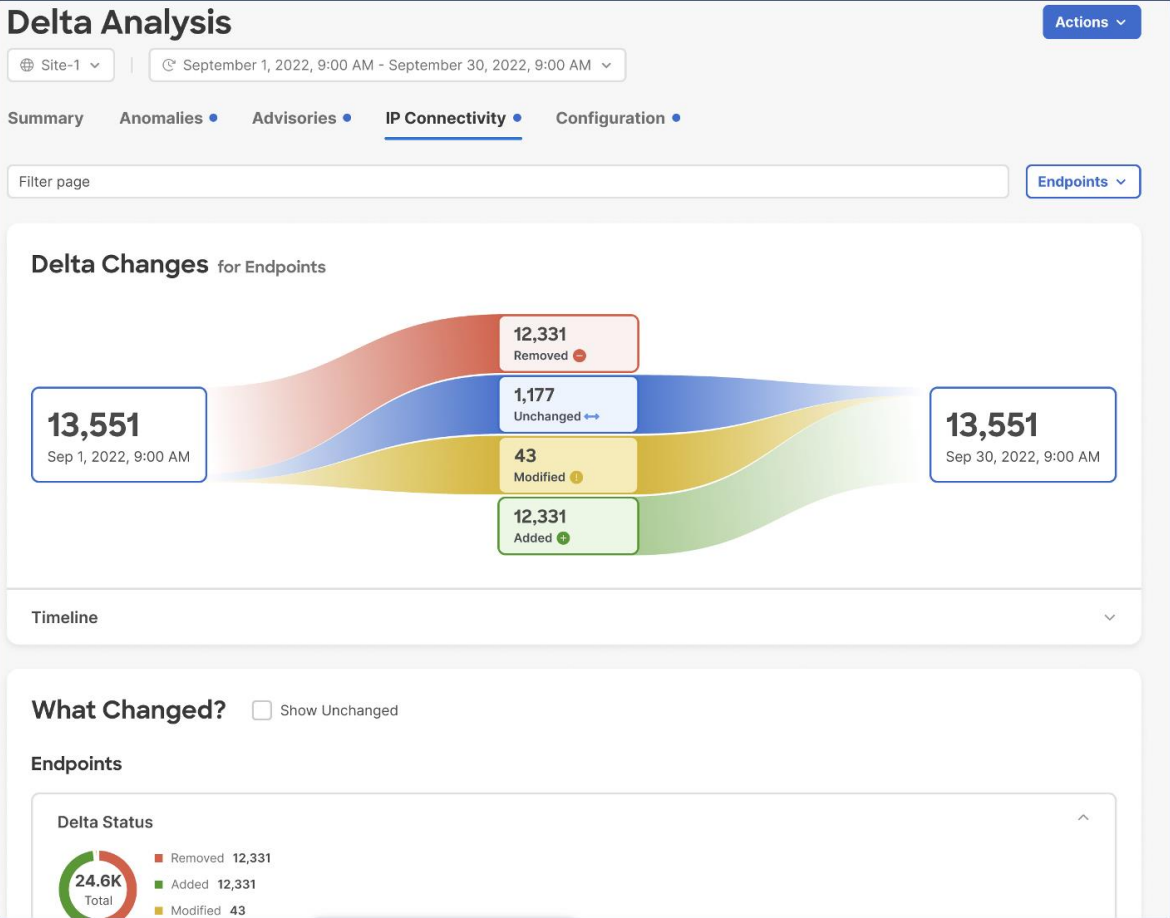
NX-OS

License Tiers:

Prem.

Compare Fabric configuration and connectivity between two points in time to see what changed.

Requires **Premier** license.



Traffic Analytics

Target Fabrics:

NDFC

NX-OS

License Tiers:

Prem.

Analysis Hub > Traffic Analytics

Traffic Analytics

Data shown is based on telemetry-monitored hardware. You can [learn more about our methodology here](#).

Actions

Site 1

Last 2 Hours

Summary



Traffic Analytics Score is Critical

Three service endpoint categories have critical Traffic Analytics Scores.

Traffic Analytic Metrics



Latency Critical

Amount of time it takes for a data packet to go from one place to another.



Congestion Warning

Reduced quality of service that occurs when a network node or link is carrying more data than it can handle.



Drops Healthy

Lost packets not reaching destination due to congested faulty cables/devices or other problems.

Endpoint Service Categories by Score



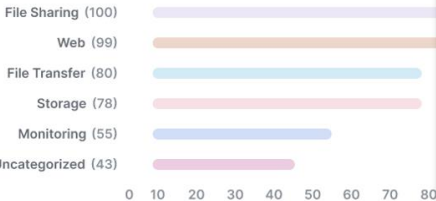
Critical 3
Web
File Transfer
Monitoring

Healthy 2
Storage
File Sharing

Warning 1
Uncategorized

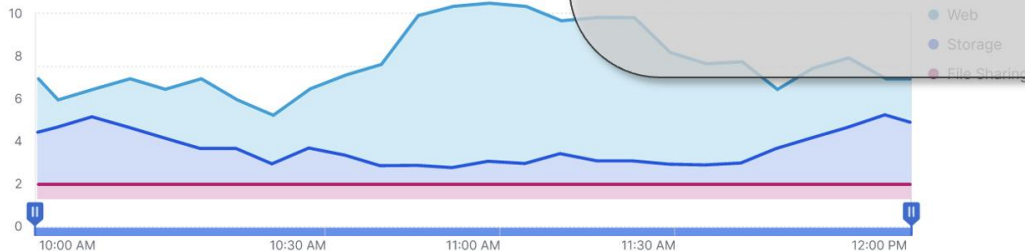
[Manage Service Endpoint Categories](#)

Number of Service Endpoints by Category



View Endpoint Service Categories by Traffic Analytics Score

Filter



Endpoint Service	Traffic Score	Category	Protocol	Client Count	Session Count	Avg Tx Rate	Avg Rx Rate	Connected To	
1.2.34.50:80	Critical	Web	TCP	20	100	0.5 Tb	1.5 Tb	Leaf101 and 2 more	...
122.2.3.33:3260	Critical	Storage	TCP	20	100	0.5 Tb	1.5 Tb	Leaf101 and 2 more	...
144.4.4.44:21	Warning	File Transfer	TCP	20	100	0.5 Tb	1.5 Tb	Leaf101 and 2 more	...
155.5.55.5:443	Warning	Web	TCP	20	100	0.5 Tb	1.5 Tb	Leaf101 and 2 more	...
191.91.91.91:85	Healthy	Uncategori	TCP	20	100	0.5 Tb	1.5 Tb	Leaf101 and 2 more	...

Machine learning categorizes endpoints and flows into specific service categories based on well-known and customizable TCP ports, allowing for better analysis of traffic flows. Switch Flow Table (FT) telemetry can be set to catch all flows for specific services during a specified time window.

Requires **Premier** license.

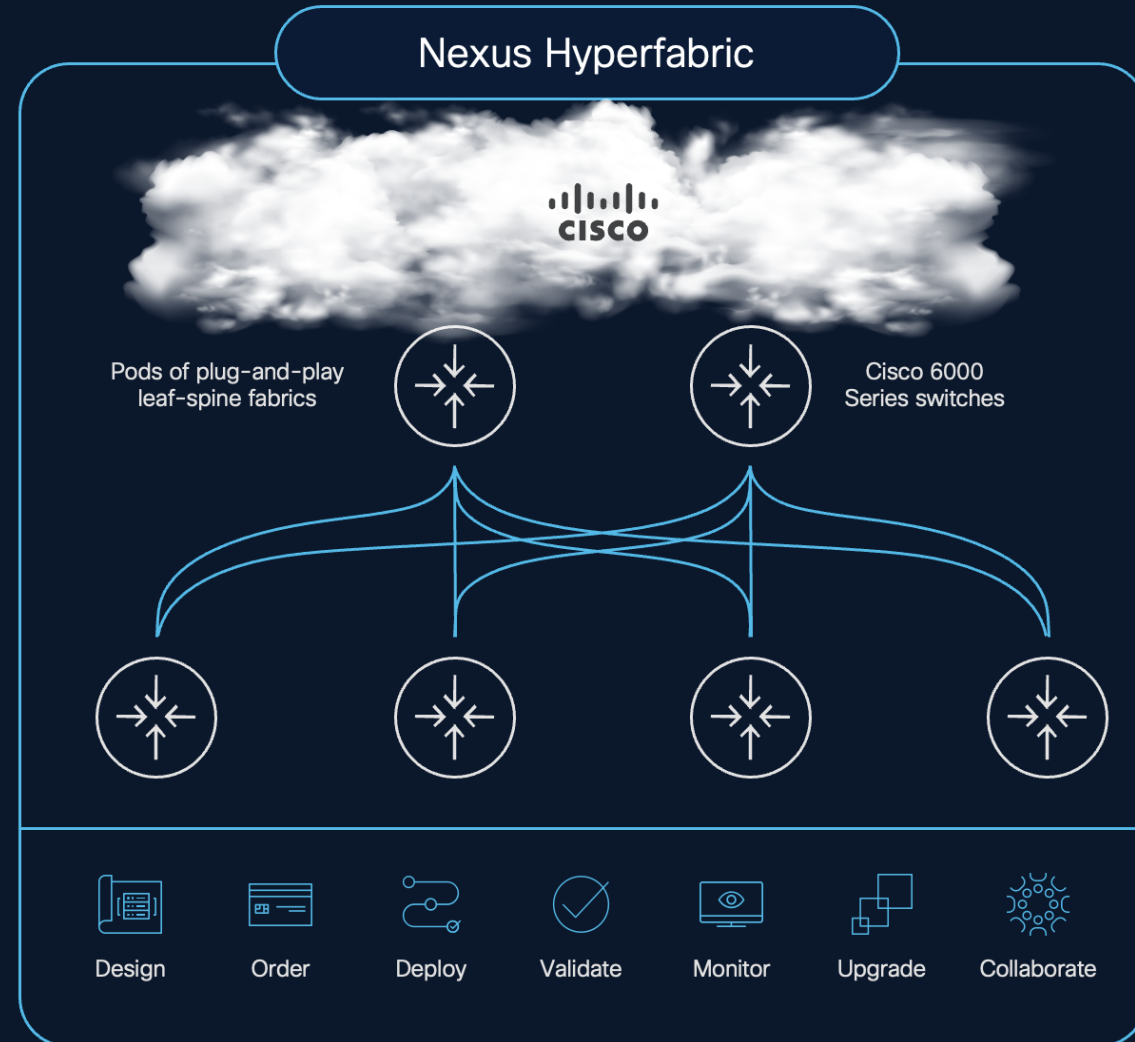
Nexus Dashboard Demo!

Nexus Hyperfabric

SHIPPING

Nexus Hyperfabric

- ✓ Design, deploy and operate on-premises fabrics located anywhere
- ✓ Easy enough for IT generalists, application and DevOps teams
- ✓ Outcome driven by a purpose-built vertical stack



Nexus Hyperfabric Components

Cloud Controller

- Scalable, globally distributed multi-tenant cloud service
- Design, plan, control, upgrade, and monitor your fabrics
- Browser, API, and mobile access



Cloud-managed 6000 Switch

- Boot-strapped from cloud
- Full visibility and control from the cloud



High-performance Fabrics

- Initially thousands of 10/25/100/400 GbE host ports
 - VXLAN EVPN, layer 2 VLANs, IPv4/IPv6 routing
 - Mesh and spine leaf fabrics



Helping Hands Web Portal

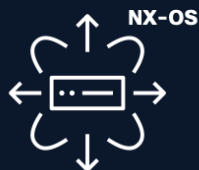
- Step-by-step deployment tasks
- Registration and cabling
- Real-time validation

Data Center Networking Portfolio



Nexus Dashboard

On-Premises Delivered



Powered by Nexus 9000 Series

Day 2 Ops

Visibility



Analytics



Troubleshooting



Compliance



Nexus Hyperfabric

Cloud Delivered



Powered by Cisco 6000 Series

Delivering networking at speed from the cloud

Hyperfabric is closing an operational
model gap, not replacing a product.

Building Flexible Architectures

Hyperfabric 6000 Switches



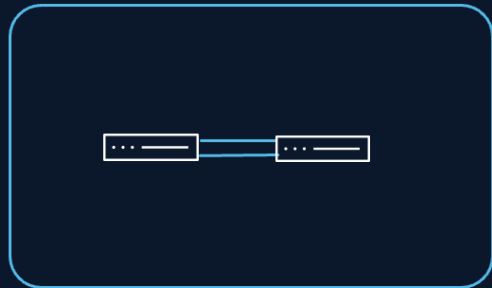
Leaf: HF6100-60L4D

- 4x 100/400GbE QSFP56-DD (16x 100G breakout)
- 60x 10/25/50GbE SFP56



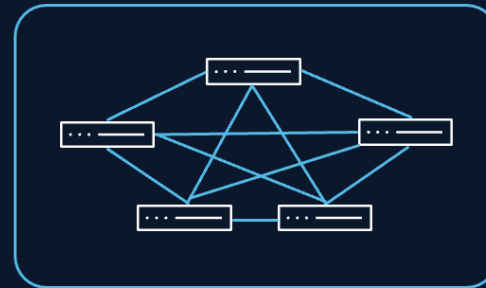
Spine/Leaf: HF6100-32D

- 32x 100/400GbE QSFP56-DD
- 128x 100GbE via 400:100 breakout



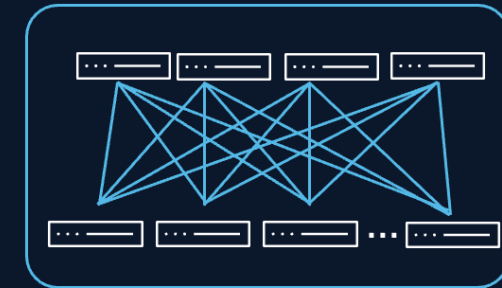
2-Switch Fabric

- Host Ports: 120x 10/25/50GbE
- Fabric Links: 2x400GbE
- Gateway Ports: 4x 100/400GbE



5-Switch Fabric

- Host Ports: 300x 10/25/50GbE
- Fabric Links: 10x400GbE
- Gateway: Host ports only (10/25/50GbE)



Spine Leaf Designs

Cisco 6000 Series Hardware Platforms at FCS

Spine or Leaf

Cisco HF6100-32D (Q200)



- 32x 100/400GbE QSFP56-DD
- 128x 100GbE via 400:100 breakout

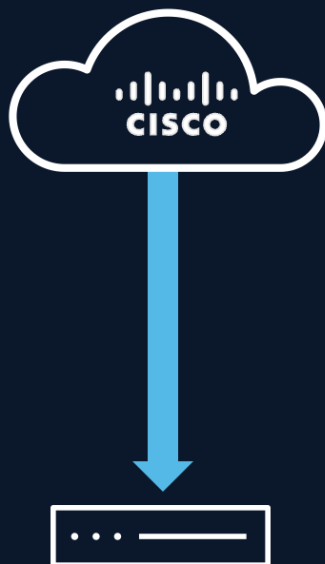
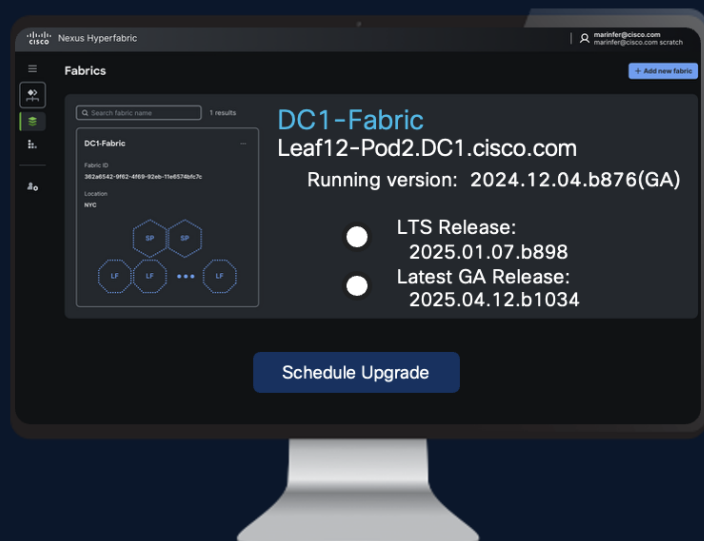
Leaf / Edge

Cisco HF6100-60L4D (Q200)



- 4x 100/400GbE QSFP56-DD (16x via 100GbE breakout)
- 60x 10/25/50GbE SFP56

Software Lifecycle Management



On-prem switch software

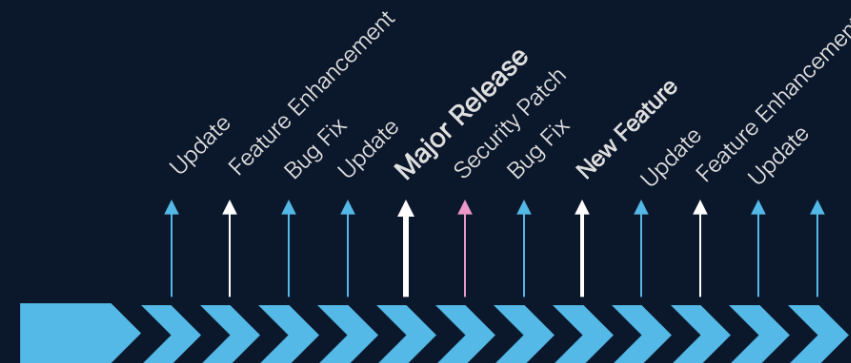
Cloud-delivered Software Upgrades: User-Driven Update Schedule

- Schedule firmware updates
- Software rollback support

Cloud SaaS controller:

Continuous delivery model: always up-to-date

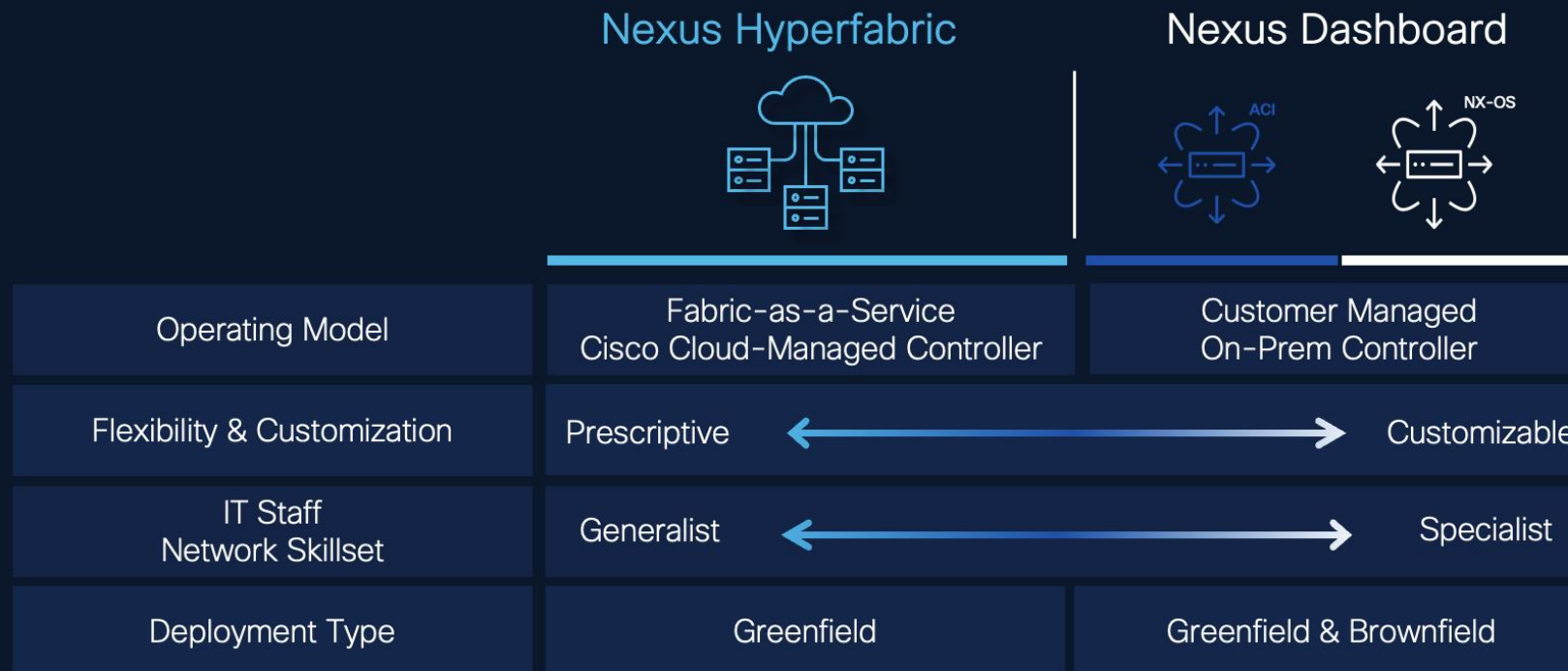
- Continuous delivery of new features and software updates to the production cloud service.
- No user testing or software maintenance required



Hyperfabric Demo!!!

What to position and when

Choice is good



Nexus Smart Switches

Nexus Smart Switch

Unmatched Flexibility, Performance, and Efficiency

Networking



- Rich NX-OS Features and Services
- High-speed connectivity and scalable performance
- Optimized for latency and power efficiency



Routing
Switching



EVPN/MPLS/
VLAN/SR



Rich
Telemetry



Line-rate
Encryption



Power
Efficiency

Cisco
Smart Switches



Cisco Nexus 9300 Services Accelerated Switch

Hypershield



- Software-defined Stateful Services
- Programmable at all layers: add new services without HW change
- Scale-out services with wire-rate performance
- Power down DPU complex when not used



Distributed
Security



IPSEC
Encryption



Large-Scale
NAT



Event-Based
Telemetry



DoS
Protection

Future Use Cases

Cisco Smart Switches Integrated with Hypershield Security

Ultra Ethernet Consortium

Cisco N9300 Series Smart Switches

Shipping



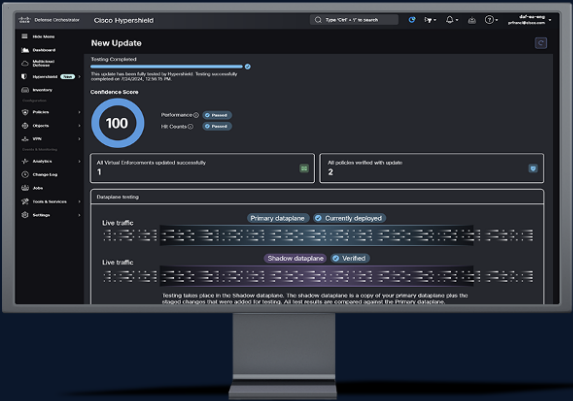
N9324C-SE1U
24-port 100G
800G Services Throughput

Orderable



N9348Y2C6D-SE1U
48-port 1G/10G/25G, 6-port 400G, 2-port 100G
800G Services Throughput

Cisco Hypershield



Use Cases

Top of Rack segmentation and enforcement

Cloud Edge

Zone-based segmentation

Smart Switch “Networking Mode” Use Cases

Available Now

September 2025

Single Fabric Use Case

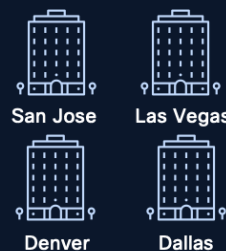


Single Fabric
• VXLAN-EVPN
• BGP

ToR Smart Switch
Deschutes | Dansberg

- ✓ **Role: Leaf, Border Leaf**
- ✓ Comprehensive fabric features (L2, L3, QoS, Multicast, VPC, L2 mobility, L2/L3 stretch, etc ...)

Multi-Fabric Use Case



Multi-Site
VXLAN-EVPN

ToR Smart Switch
Deschutes | Dansberg

- ✓ **Role: Leaf, Border Gateway**
- ✓ Active-Active & DR continuity
- ✓ Multi-site features (L2/L3 stretch, anycast border gateway, TRMv4, etc...)

Position Futureproofing :

- Prioritize LDOS and competitive refresh
- Target new builds, RFP, expansions against competition
- Brown field insertion

Product Highlights:

September 2025

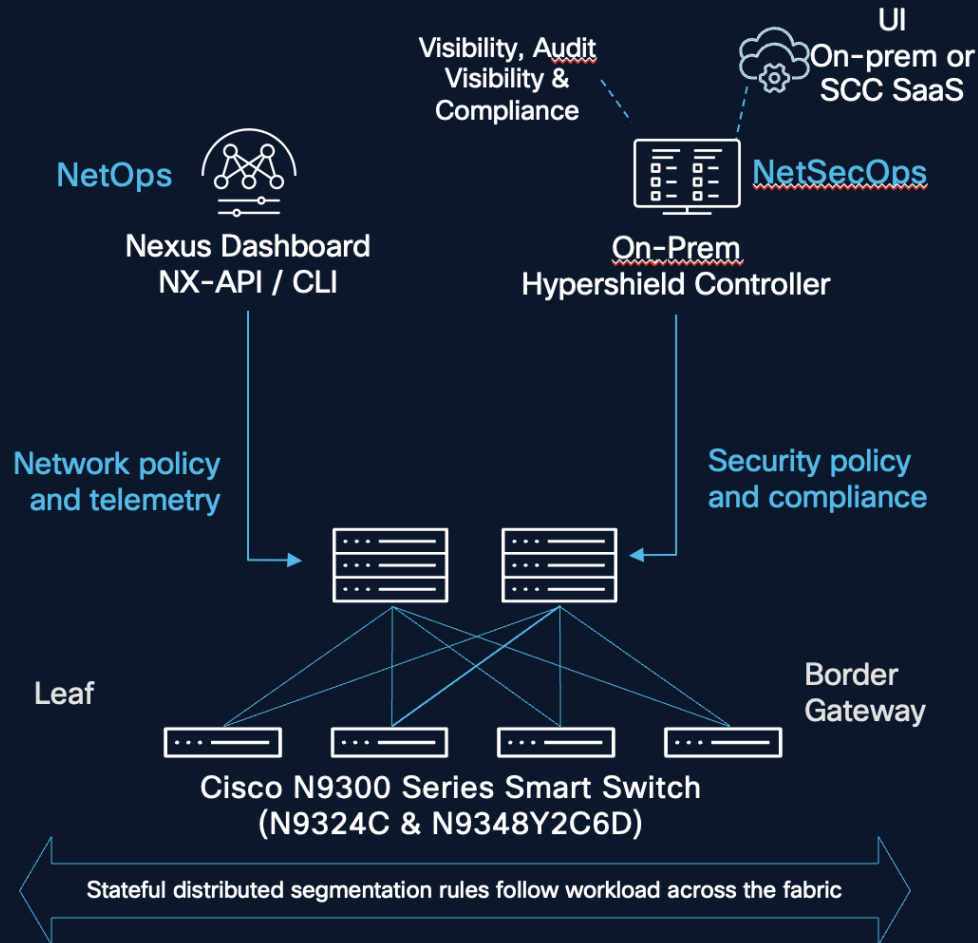
- N9324C-SE1U and N9348Y2C6D-SE1U
Networking mode GA on September 1st week
- 10G to 400G fiber and copper support

November 2025

- Nexus Dashboard 4.1.x support
- 1G support
- VXLAN vPC, BGW
- Netflow

Smart Switch “Networking & Security” Use Case

Top of Rack L4 Segmentation – November GA



Security Infused in Data Center Fabric

Version: NXOS 10.6(2), Hypershield 1.2

Smart Switches: N9348Y2C6D-SE1U, N9324C-SE1U

Fabric: VXLAN-EVPN, VXLAN-multi-site, BGP fabric, brownfield

Segmentation: VRF/VLAN + CIDR rules, stateful/stateless, 100K rules, 800G throughput (final scale based on benchmarking)

Policy: CRD schema, policy validation and canary rollout/rollback

Hypershield: Air-gap ready on-prem controller* and optional Security Cloud Control SaaS

Upgrade: NXOS CLI for DPU load, SMU for Hypershield agent

Observability: Nexus Dashboard, Splunk, Prometheus/Grafana

Thank you

