Cisco N9300 Series Smart Switch

Overview

This FAQ document is a resource designed to provide a high-level overview of the Cisco N9300 Series Smart Switch, covering its functions, key features, target audience, and competitive and development timelines. This document is intended to assist customers and partners in understanding the product's core elements and how it fits into Cisco's portfolio. However, this FAQ is not exhaustive and will be updated and amended regularly to include new details as they become available.

Cisco N9300 Series Smart Switch and Cisco Hypershield are two distinct products. The applicable Cisco Hypershield subscription must be purchased separately (when available) for Cisco N9300 Series Smart Switch. Cisco N9300 Series Smart Switch and Cisco Hypershield combined (network and security) represents both a compelling use case and value proposition, as well as a prime example of the power that is One Cisco.

Note: For any of the products and features described in this FAQ document that are not currently available, they remain in varying stages of development and will be offered on a when-and-if-available basis. The delivery timeline of any future products and features is subject to change at the sole discretion of Cisco, and Cisco will have no liability for delay in the delivery or failure to deliver any of the products or features set forth in this document.

Cisco N9300 Series Smart Switch

Q: What is the Cisco N9300 Series Smart Switch?

A: Since network switching hardware has evolved to include Data-Processing Units (DPUs)), we are transforming our switches into multifunctional, service-hosting devices. DPUs in the switches can offload complex data-processing tasks for high scale and performance while delivering advanced services beyond traditional networking functions.

The Cisco N9300 Series Smart Switch is the first value-driven use case for DPU-enhanced switching using Cisco's portfolio. The Cisco N9300 Series Smart Switch will be a network-based enforcer for Cisco Hypershield, offering L4 zone-based segmentation.

Q: What is Cisco Hypershield?

A: Cisco Hypershield is a distributed, AI-native security architecture that embeds security wherever it needs to be: in every software component of every application running on the network, on every server, and in public- or private-cloud deployments. It is a subscription-based software product that sits on top of the hardware with enforcement points that are workload- and network-based across public- or private- cloud deployments. The Cisco N9300 Series Smart Switch will be a network-based enforcer for Hypershield.

Hypershield is uniquely architected to implement an intent-based policy model that is centralized and easy to manage. No matter the form factor or location of the enforcement point, the policy being enforced is organized at a central location by Hypershield's cloud-based management console, Cisco Security Cloud Control.

Currently, Hypershield addresses the following use cases:

- Autonomous segmentation to control lateral movement across workloads in public and private clouds
- Distributed exploit protection to accelerate protection from vulnerability exploits while keeping applications up and running
- And with the Cisco N9300 Series Smart Switch, it will offer L4 zone-based segmentation

Q: When will Cisco N9300 Series Smart Switch be announced and released?

A: We will be announcing two (2) models on February 11, 2025, at Cisco Live! EMEA in Amsterdam:

N9324C-SE1U
Target Availability: March 2025 FCS

N9348Y2C6D-SE1U
Target Availability: May 2025 EFT, July 2025 GA

Note: Layer-4 zone-based segmentation capabilities are with appropriate licensing and will be coming soon.

Q: Why are we introducing the Cisco N9300 Series Smart Switch now?

A: The integration of Cisco® next-generation ASICs and AMD's high-performance DPUs is a significant advancement for modern data centers. This combination addresses the dual demands of high network performance and comprehensive security. By embedding security enforcement directly on the switch, the need for complex routing to external devices and reliance on CPU-intensive agents is minimized. This approach streamlines network operations, leading to enhanced performance and reliability while also reducing overall costs. Such a solution allows data center operators to manage workloads more efficiently, ensuring that security measures do not impede network speed or functionality. This innovation is particularly beneficial because data centers will continue to evolve and face increasing demands for speed, security, and cost-effectiveness.

Q: What are the first capabilities supported on a Cisco N9300 Series Smart Switch?

A: While DPUs are designed to be highly programmable and capable of supporting a wide range of services, of applications, our initial focus is on enhancing internal segmentation capabilities. Specifically, we are integrating Cisco Hypershield with the initial Cisco N9300 Series Smart Switches to provide protections in key areas such as the cloud-edge, zone-based segmentation, and Data Center Interconnect (DCI). This approach will offer a highly scalable and secure infrastructure for hybrid-cloud environments.

Q: What are the key products in the family of Cisco N9300 Series Smart Switches?

A. Currently, the two (2) products in the Cisco N9300 Series Smart Switches family are described in the table below:

Table 1. Cisco N9300 Series Smart Switches

Cisco N9300 Series Smart Switches		
Model	N9324C-SE1U	N9348Y2C6D-SE1U
Key specs	• 24x100G ports • 800G services throughput	• 48x25G ports, 6x400G ports, 2x100G ports • 800G services throughput
Switch details	• 4xAMD Elba DPU • 4.8T Cisco Silicon One® ASIC (E100)	• 2xAMD Giglio DPU • 4.8T Silicon One ASIC (E100)
Use cases	• Cloud-edge • Zone-based segmentation • Data center interconnect • Top of Rack (ToR)*	• Top of Rack (ToR)*
Management	• Cisco NX-OS, Nexus Dashboard, NX-API • Cisco Security Cloud Control (SCC)	• NX-OS, Nexus Dashboard, NX-API • Cisco Security Cloud Control (SCC)

*Post FCS

Q: What constitutes a Cisco N9300 Series Smart Switch?

A: Cisco N9300 Series Smart Switches are the latest-generation of Nexus switches with Data Processing Units (DPUs) added to provide additional network services. The Cisco N9300 Series Smart Switch consists of:

- The Switch Components: Switch hardware and Cisco NX-OS, plus
- The Cisco Data Center Networking (DCN) licenses.

Note: Nexus Dashboard provides additional network functionality.

By default, the DPU is powered down. To enable network security services on the DPU, the following is required:

- The applicable Cisco Hypershield licenses
- Cisco Security Cloud Control (included with Cisco Hypershield)

Note: A DCN Premier license is required to utilize the DPU function.

Each Cisco N9300 Series Smart Switch supports the same automation and management capabilities as the current Cisco Nexus 9000 Series switches. This includes Nexus Dashboard and NX-OS Open APIs for integrating with existing network architectures. When running Cisco Hypershield on the DPUs, the Hypershield's cloud controller will provision and manage the security policies. At the same time, Nexus Dashboard 4.1 will be available to manage network policies on the switch.

Q: What Operating System (OS) does the Cisco N9300 Series Smart Switch run on?

A: The Cisco N9300 Series Smart Switch will be released with NX-OS only at FCS, The NX-OS image will include the software to activate/manage the DPU; install the Hypershield firmware load, and monitor the interfaces between DPUs and the NPU. All the security policies will be managed by Cisco Security Cloud Control.

Management of the switches by Cisco ACI® through the APIC is currently under consideration. Regardless, these switches can be used for zone, DCI, and Cisco Cloud Connect segmentation use cases.

Q: How does Cisco Hypershield work with the Cisco N9300 Series Smart Switch solution?

A: The Cisco N9300 Series Smart Switch adds to the growing family of Cisco Hypershield network-based enforcers (for example, the Hypershield VM appliance). The Cisco N9300 Series Smart Switch delivers on the Cisco Hypershield vision of embedding security capabilities into the networking infrastructure, simplifying operations, security, and network topologies.

Cisco Hypershield will provide L4 zone-based segmentation capabilities through the Cisco N9300 Series Smart switches. Self-qualifying updates are a core innovation of Hypershield, and a dual data plane for policy validation is included in the first release of the Cisco N9300 Series Smart Switch. Note: Hypershield's self-qualifying update capability for the Cisco N9300 Series Smart Switch is related to policy updates, and not applicable to Hypershield's own firmware update at GA.

Q: What are the benefits of the Cisco N9300 Series Smart Switch along with Cisco Hypershield?

A: There are several benefits provided by our Cisco N9300 Series Smart Switch with Cisco Hypershield that give customers a win-win solution.

- **Architecture simplification:** streamlines network and security architecture, reducing complexity and making it easier to manage and maintain.
- **Significant TCO savings:** reduces Total Cost of Ownership (TCO) for customers by minimizing the need for multiple, disparate security solutions and leveraging a unified platform.
- **Consistent security policies:** ensures uniform security policy testing and deployment across the entire network, reducing the risk of misconfigurations and enhancing overall security posture.

- **High throughput and scale:** by offloading compute intensive services to a high-performance DPU, the switch is able to provide high performance network functions at a higher scale than what can be done with an NPU alone.
- **Persona-driven operational models:** the Cisco N9300 Series Smart switches is designed for NetOps, SecOps, and NetSecOps, supporting both current and future operations. Network and security functions on the DPU switch are isolated: NetOps manages the switch lifecycle and network policy, while SecOps handles security policy. Smaller customers can have a unified NetSecOps team manage everything. We also provide a streamlined troubleshooting workflow for both network and security, surpassing traditional solutions. Security micro-frontend integration in Nexus Dashboard ensures compliance and health, while network health and analytics are shared with Cisco Security Cloud Control for security teams. This initiative integrates security directly into the network platform.
- **Hitless High Availability (HA):** ensures continuous operations without any downtime by seamlessly transitioning between active and standby systems, allowing for uninterrupted service even during maintenance or unexpected failures
- **Increased visibility:** enhances visibility across networking and security domains, enabling better monitoring, threat detection, and response capabilities.

Q: What use cases does the Cisco N9300 Series Smart Switch address?

A: **Zone-based segmentation:**

Cisco N9300 Series Smart Switch model: N9324C-SE1U (available at FCS)

Traditionally, security appliances are used to provide L3/L4 segmentation for intra-data center use cases. These zones can be based on networking functions (including subnets, VLANs, and bridge domains) or even represent independent business entities such as tenants and VRFs. In all cases, this forces the traffic to be redirected outside of the switch fabrics, which ultimately limits performance and increases cost and complexity. By integrating the ability to manage and enforce segmentation policies within the fabric, customers can improve their digital resiliency and time to market. In addition, the Cisco N9300 Series Smart Switch eliminates the need for expensive ingress/egress data center firewalls between security zones and extends Hypershield's capabilities while lowering TCO.

The main benefits to customers include the following: having extensible and consistent policies across zones and workloads, testing and staging policies before production rollout using Hypershield's dual data plane feature, and providing a cloud-based SaaS model that frees up time normally needed for software maintenance.

Data Center Interconnect (DCI):

Cisco N9300 Series Smart Switch model: N9324C-SE1U (available at FCS)

Communication between data centers (whether routed, through dense wavelength- division multiplexing [DWDM], dark fiber, etc.) needs to be fast and secure. Currently, customers use multiple routers and security devices to ensure that communication will be protected and redundant.

With Cisco's new solution, customers can deploy the Cisco N9300 Series Smart Switch as an IP border gateway with the capability to provide segmentation and MACsec encryption to secure their DCIs.

The main benefits in this use case are reducing TCO by reducing the number of devices to provide routing, segmentation, and encryption. Digital resiliency is improved by reducing complex routing rules to multiple external firewalls.

Cloud-edge use cases:

Cisco N9300 Series Smart Switch model: N9324C-SE1U (available at FCS)

Public cloud on-ramps from data centers and colocations require secure high performance and low-latency connections due to the volume of traffic between them. Customers treat this connection as an external site that puts them in a DMZ Zone protecting their environments. The Cisco N9300 Series Smart Switch provides for much higher performance while also reducing complexity and expense compared to using traditional firewall clusters. In addition, it provides a custom routing-point eliminating the need for additional L3 devices at the on ramps.

The main benefits in cloud-edge use cases are simplified hybrid-cloud connectivity by optimizing routing and eliminating the need for DMZ traffic to trombone; elimination of the DMZ firewall as a single point of failure; reduced costs with scale-out vs. scale-up using firewall appliances; and consistent security-policy enforcement with Hypershield.

ToR segmentation and enforcement:

Cisco N9300 Series Smart Switch models: N9348Y4C6D-SE1U and N9324C-SE1U (available post-FCS)

Major innovation compared to existing ToR switches and network segmentation tools. The Cisco N9300 Series Smart Switch can be deployed as a leaf switch with integrated features such as autonomous and stateful segmentation enforcement on every port, which can be synchronized across all the Cisco N9300 Series Smart Switches. Hypershield can then follow a continuous and dynamic process to update policies as the application changes or moves. Additionally, microsegmentation policies can be enforced outside of any workload, providing another layer of security with fewer points of management.

The main benefits in this use case include: a physical-space-saving alternative to current firewall devices, simplified management with Nexus Dashboard for common network and security visibility, pervasive segmentation, and 25G and 100G top-of- rack switching with stateful microsegmentation regardless of workload type.

Q: How will customers troubleshoot workflows between the ASIC and DPU?

A: The packet-flow tracer is a tool designed for the Cisco N9300 Series Smart Switch. It will help with end-to-end dataplane troubleshooting and traffic assurance. It can be launched from Nexus Dashboard or NX-API. Packet capture is available from the NPU (ASIC) and in DPU Hypershield service.

Q: What other third-party security policy tools are we considering integrating?

A: AlgoSec and Tufin are being evaluated as part of the roadmap.

Q: Will the Cisco N9300 Series Smart Switch be VRF-aware or support contexts/instances?

A: At FCS, we will support VRF(s) redirect through the NPU and DPU for security policy enforcement. Inter-VRF is not supported at FCS but is expected to be added in NX-OS QR1F (July/August 2025). The security policies defined by Cisco Hypershield are not VRF-aware at FCS.

Q: Can customers purchase the Cisco N9300 Series Smart Switch without Hypershield?

A: Yes, the Cisco N9300 Series Smart Switch can be purchased without the Cisco Hypershield subscription. When NX-OS is installed, all DPUs are powered down by default until Cisco Hypershield services are turned on. Customers can deploy the Cisco N9300 Series Smart Switch as a regular switch and then enable services at a later point. This provides flexibility and helps make the customer's network future-ready. Cisco Hypershield allows for flexible reallocation of Hypershield protection units. These units can be purchased before, during, or after acquisition of the Cisco N9300 Series Smart Switch hardware and can be allocated toward the Cisco N9300 Series Smart Switch at any time.

Q: How does the Cisco N9300 Series Smart Switch support sustainability initiatives?

A: Cisco's sustainability initiatives and new capabilities will be supported through regular updates in each software release, integrated with the Nexus Dashboard.

Customers can save up to 77 percent in power consumption and 89 percent in rack space due to the reduction of required infrastructure.

Additional resources

Cisco N9300 Series Smart Switch Data Sheet

Cisco N9300 Series Smart Switch At-a-Glance

Cisco N9300 Series Smart Switch Web Page

Cisco Hypershield

Cisco Hypershield Web Page

C67-4878201-00 02/25