Cisco N9300 Series Smart Switches

Overview

This FAQ document is a resource designed to provide a high-level overview of the Cisco N9300 Series Smart Switch. It covers product capabilities, available models, licensing and management, integration with Cisco Hypershield™, supported use cases, and operational considerations.

Cisco N9300 Series Smart Switches and Cisco Hypershield are two distinct products.
An applicable Cisco Hypershield subscription must be purchased separately (when available) to enable Cisco Hypershield security services on the switches. Cisco N9300 Series Smart Switches and Cisco Hypershield combined (network and security) represent both a compelling use case and value proposition, as well as a prime example of the power that is One Cisco. Security is now fused directly into the network, and customers have a seamless way to protect their infrastructure without compromising performance.

Note: Any of the products and features described in this FAQ document that are not currently available are 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.



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

Cisco N9300 Series Smart Switches

Q: What is the Cisco N9300 Series Smart Switch?

A: The Cisco N9300 Series Smart Switches are Cisco® Silicon One®-based data-center switches enhanced with Data Processing Units (DPUs) and designed to deliver advanced services beyond traditional networking functions. DPUs can offload complex data processing tasks, enabling high scale and performance for services such as stateful segmentation.

By combining high-performance networking and DPU-based service acceleration in a single platform, Cisco is evolving the role of the switch into a multifunctional, service-hosting devices. Cisco N9300 Series Smart Switch is the first in Cisco's portfolio to leverage DPU-enhanced switching. When used with Cisco Hypershield, they can serve as a network-based enforcement point with L3/L4 stateful segmentation, the initial use case. Additional services may be delivered in the future.

Q: What is Cisco Hypershield?

A: Cisco Hypershield is a distributed 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 with workload- and network-based enforcement points across public- or private-cloud deployments. The Cisco N9300 Series Smart Switch can serve as a network-based enforcer for Cisco Hypershield.

Cisco 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 controlled by Cisco Hypershield's on-premises controller, manageable through its on-premises UI, an API, or the cloud-based security console, Cisco Cloud Control (CCC).

Q: Why the Cisco N9300 Series Smart Switch?

A: The integration of Cisco's next-generation Silicon One 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 that impose a performance tax, or the 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 as data centers 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, or applications, our initial focus is on enhancing east/west segmentation capabilities. Specifically, Cisco Hypershield is integrated with the initial Cisco N9300 Series Smart Switches to provide protections in key areas such as fabric-wide L3/L4 stateful segmentation, zone-based segmentation, Data Center Interconnect (DCI) with integrated routing, segmentation and encryption, and secure hybrid-cloud connectivity at the cloud-edge. This approach offers a highly scalable and secure infrastructure for hybrid-cloud environments.

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

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 Table 1.

Table 1. Cisco N9300 Series Smart Switches

Model	Cisco N9324C-SE1U	N9348Y2C6D-SE1U
Key specs	• 24x100G ports • 800G services throughput	• 48x25G ports, 2x100G ports, 6x400G ports • 800G services throughput
Switch details	• AMD Elba DPU • Cisco Silicon One ASIC (E100)	• AMD Giglio DPU • Silicon One ASIC (E100)
Use cases	• Zone-based segmentation • Secure Data Center Interconnect • Top-of-rack (ToR) Segmentation	• Top-of-rack (ToR) Segmentation
Management (network)	• Cisco NX-OS, Nexus® Dashboard, NX-API	• Cisco NX-OS, Nexus Dashboard, NX-API
Management (security)	• Cisco Hypershield Controller (on-premises) • Cisco Cloud Control	• Cisco Hypershield Controller (on-premises) • Cisco Cloud Control

Q: What are the main architectural components of a Cisco N9300 Series Smart Switch?

A: Cisco N9300 Series Smart Switches are the latest-generation of Nexus switches combining a Cisco Silicon One ASIC (NPU) with Data Processing Units (DPUs) in a single platform. Each component serves a distinct function:

Network (NPU):

- Provides routing, switching, and VXLAN fabric capabilities powered by Cisco Silicon One
- Managed by NetOps through Cisco NX-OS CLI, Nexus Dashboard, and NX-OS Open APIs
- Requires Cisco Data Center Networking (DCN) licenses

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

Security (DPU):

- Provides advanced security services such as L4 stateful segmentation
- Managed by SecOps through the Cisco Hypershield on-premises controller, its UI, API, or Cisco Cloud Control
- Requires 12 Cisco Cloud Protection Suite (CPS) units per switch

By default, the DPU is powered down until Cisco Hypershield services are enabled.

Q: What is the management model of the Smart Switch?

A: Network operations and security operations are separated, with each management solution designed for the needs and focus of its respective persona (NetOps vs. NetSecOps). Whereas management consoles are independent, integration and context sharing between Nexus Dashboard and Cisco Hypershield exist for consistent operations and faster troubleshooting, with Data Processing Units (DPUs) added to provide additional network services.

Each Cisco N9300 Series Smart Switch supports the same automation and management capabilities as the current Cisco Nexus 9000 Series Switches, enabling seamless integration with existing network architectures.

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

A: The Cisco N9300 Series Smart Switch runs on Cisco NX-OS. Cisco NX-OS 10.6.x is the first software release train supported on these switches. The NX-OS image includes the software for switch operations as well as the components to activate, manage, and monitor the DPUs.

The DPU runs its own firmware, which includes the Cisco Hypershield agent responsible for receiving security policies from the Cisco Hypershield on-premises controller and programming them into the DPU. During initial deployment, the NX-OS image bundles both the switch software and the DPU firmware. After initial deployment, the Cisco Hypershield agent and DPU firmware can be upgraded independently from Cisco Hypershield, without requiring a full switch software upgrade.

Q: How are Cisco Hypershield policies enforced on Cisco N9300 Series Smart Switches?

A: 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.

The Cisco N9300 Series Smart Switch serves as a hardware enforcement point for Cisco Hypershield, leveraging the DPU to enforce L3/L4 stateful segmentation policies locally and at line rate within the network fabric.

Security policies are managed centrally through the Cisco Hypershield on-premises controller. The on-premises controller provides the policy control plane, while policies can be defined through its on-premises UI or API, or through Cisco Cloud Control.

Q: What are the benefits of using Cisco N9300 Series Smart Switch 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 by integrating security into the fabric itself, whether the fabric is a classic LAN fabric, a modern VXLAN EVPN fabric, or a routed fabric
- **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. Additionally, consolidating functions into fewer devices reduces power consumption, cooling, and rack space, further contributing to lower operational costs.

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

- **Consistent security policies:** ensures uniform security policy deployment across the entire infrastructure, including network and workloads, reducing the risk of misconfigurations and enhancing overall security posture.
- **High throughput and scale:** offloads compute intensive services to the high-performance DPU, achieving reduced latency (compared to solutions relying on CPU) and higher scale for security enforcement.
- **Persona-driven operational models:** separates network operations and security operations, with management solutions designed for the needs and focus of different personas (NetOps vs. NetSecOps). Although management consoles are independent, integration and context sharing exist for consistent operations and faster troubleshooting.
- **Increased visibility:** through integration between Cisco Hypershield and Nexus Dashboard, yields improved end-to-end 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: There are three (3) initial use cases for Cisco N9300 Series Smart Switches together with Cisco Hypershield:

Top-of-rack segmentation and enforcement:

The Cisco N9300 Series Smart Switches can be deployed as a top-of-rack leaf, bringing the enforcement point closer to the workloads and distributing segmentation across the fabric.

Every port on the N9300 Series smart switch becomes an enforcement point, enabling L3/L4 stateful segmentation for all connected workloads regardless of type (VMs, bare-metal, or containers). Policies are managed centrally through the Cisco Hypershield on-premises controller (or through Cisco Cloud Control) and enforced locally on the DPU, reducing reliance on external firewalls or host-based agents for use cases where L4 stateful segmentation is sufficient. The switch also supports line-rate MACsec on all ports, providing link-level encryption where connected devices support MACsec. This results in fewer devices to manage, reduced complexity, and consistent security enforcement at the access layer.

Zone-based segmentation:

Traditionally, security appliances such as Next-Generation Firewalls (NGFWs) are used to provide L3/L4 segmentation between data-center zones (based on subnets, VLANs, bridge domains, tenants, or VRFs). For use cases where L4 stateful segmentation is sufficient, using an NGFW introduces unnecessary latency, cost, and scale limitations.

The Cisco N9300 Series Smart Switch can replace external firewalls in these scenarios, delivering L3/L4 stateful segmentation with higher throughput, lower latency, improved scale, and reduced TCO. Additionally, the integration between Nexus Dashboard and Cisco Hypershield provides enhanced end-to-end visibility across network and security domains.

In this use case, the Cisco N9300 Series Smart Switch is not part of the underlying fabric, allowing it to work with any fabric solution, including Cisco NX-OS fabrics, Cisco ACI®, Cisco Hyperfabric™, and fabrics from sources other than Cisco.

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

Secure Data Center Interconnect (DCI):

Communication between data centers (whether routed, through DWDM, dark fiber, etc.) needs to be fast and secure. Customers often deploy multiple routers and security devices to ensure protection and redundancy, adding cost and complexity.

The Cisco N9300 Series Smart Switch can be deployed as an IP border gateway or VXLAN border gateway, combining routing, L3/L4 stateful segmentation, and MACsec encryption in a single device to secure Data Center Interconnects. This reduces TCO by consolidating multiple functions, simplifies the architecture by eliminating complex routing to external firewalls, and improves digital resiliency.

Cloud-edge connectivity and segmentation:

Public-cloud on-ramps from data centers and colocation facilities require secure, high-performance, low-latency connectivity because of the volume of traffic exchanged between environments. Customers often treat these connections as external sites and place them in a DMZ to protect their environments.

The Cisco N9300 Series Smart Switch can provide higher performance while reducing complexity and cost compared with traditional firewall clusters. It can also provide an integrated routing point at the cloud on-ramp, reducing the need for additional Layer 3 devices.

For use cases where L4 stateful segmentation is sufficient, this architecture simplifies hybrid-cloud connectivity by optimizing routing and eliminating DMZ traffic tromboning. It also reduces reliance on centralized DMZ firewalls as potential single points of failure, lowers costs through a scale-out rather than scale-up architecture, and provides consistent security policy enforcement through Cisco Hypershield.

Q: How can customers troubleshoot workflows between the NPU and DPU?

A: Cisco Nexus Dashboard includes a feature called connectivity analysis, which provides end-to-end path visibility and traffic assurance. This feature has been extended to leverage packet tracer, a tool available on the Silicon One NPU, to provide visibility into traffic forwarding between the NPU and the DPU within the N9300 Series smart switch. This enables visual troubleshooting across both networking and security domains, and can be launched from Nexus Dashboard or NX-API.

Q: Is the Cisco N9300 Series Smart Switch be VRF-aware, VLAN-aware, or does it support contexts/instances?

A: Yes, the switch is both VRF- and VLAN-aware and it supports contexts/instances. Through Nexus Dashboard (and also through NX-OS CLI), administrators can select which VRFs or VLANs are redirected to the DPU for security policy enforcement. Security policies can be defined on a per-VRF or per-VLAN basis, and Cisco Hypershield will deploy the corresponding rules to the N9300 Series smart switches where that VRF or VLAN is redirected. Inter-VRF DPU filtering is also supported as a foundational use case.

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

A: Yes, the Cisco N9300 Series Smart Switch can be deployed with DPUs powered down, operating as a regular Cisco Nexus switch. The DPUs are powered down by default. Customers can enable DPU security services at a later point by acquiring the Cisco Cloud Protection Suite (CPS) licenses. This provides flexibility and makes the customer's network future-ready.

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

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

A: By consolidating switching and security functions into a single device, the Cisco N9300 Series Smart Switch reduces the number of devices required in the data center, resulting in lower power consumption, reduced cooling requirements, and less rack space.

Customers will reduce power, cooling, and space by collapsing multiple switches and firewalls into smart switches running Cisco Hypershield because the latter switches consume less power and cooling compared to traditional designs that require multiple L3 devices and firewalls.

Q: What are the differences between the Cisco N9300 Series Smart Switches and the Cisco C® 9000 Series Smart Switches?

A: The Cisco Catalyst 9000 Series Switches are primarily campus devices that offer the ASA virtual firewall capabilities as a container and encryption in addition to classic routing and switching: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000-switches/upgrade-9350-series-smart-switches-br.html. The Cisco C9300 stateful filtering performance is up to 900 Mbps on Cisco Catalyst 9300X Fiber Switches and 500 Mbps on Cisco C9300 Series Smart Switches. The Cisco N9300 Series Smart Switches, instead, provides stateful firewalling capabilities for the data center at 800Gbps of throughput thanks to a dedicated ASIC.

Additional resources

- Cisco N9300 Series Smart Switch Data Sheet
- Cisco N9300 Series Smart Switch At-a-Glance
- Cisco N9300 Series Smart Switch
- Cisco Hypershield



© 2026 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

C67-4878201-02 09/26