



Smart Switches

- [Smart Switch, on page 1](#)
- [Smart Switch architecture, on page 3](#)

Smart Switch

Smart Switch is a category of N9000 Series Switches that provides:

- embedded security with Hypershield
- advanced segmentation and connectivity, and
- hardware-accelerated architecture.

Embedded security with Hypershield—The N9300 Series Smart Switches provide service-accelerated performance and simplifies security architecture by integrating directly into the network, eliminating the need for separate Layer 4 stateful firewalls.

Advanced segmentation and connectivity—These switches facilitate secure segmentation and communication between security zones across the data center, interconnects, and cloud environments.

Hardware-accelerated architecture—Smart Switch integrates Data Processing Units (DPUs) with networking ASICs to enhance both data center networking throughput and security processing capabilities.

The Smart Switches that are currently available are the N9300 Series Smart Switches:

- N9324C-SE1U from 10.6(2)F
- N9348Y2C6D-SE1U from 10.6(2)F

The N9300 Series Smart Switches deliver an integrated solution for scalable, secure, and efficient data center operations, by combining advanced networking and security features with hardware acceleration and software flexibility.

The N9300 Series Smart Switches offer converged switching and routing services. These switches operate in network mode and DPU security mode. In the DPU security mode, features related to the network mode are also available.

The N9300 Smart Switches NX-OS Release 10.6(3s)F maintain functional parity with the N9000 Series NX-OS Release 10.6(3)F and additionally provides the capability to enable the DPU feature that inspects IP traffic. For more information on the software features supported in network mode, refer to [Cisco Nexus 9000 Series NX-OS Release Notes](#) of versions [10.6\(2\)F](#) and [10.6\(3\)F](#) and [Configuration Guides for Cisco NX-OS](#)

10.6(x). For more information about DPU security mode, refer to [Cisco Nexus 9000 Series NX-OS Release Notes, Release 10.6\(3s\)F](#) and this document.

Concepts

A few key concepts related to the architecture of the N9300 Smart Switch include:

- CPU—Central Processing Unit (CPU)—Controls and manages the switch; handles general control-plane tasks such as operating system processes, managing the device, routing protocols, logging, and system coordination.
- NPU—Network Processing Unit (NPU)—High-speed packet-forwarding engine; optimized for network traffic processing such as switching, routing, filtering, and traffic handling.
- DPU—Data Processing Unit (DPU)—Specialized programmable data processing engine; hosts services such as security, telemetry more efficiently.
- Modes—Two modes that the Smart Switch operates in, network and DPU security mode. The default mode is network mode. To use the DPU security mode, you need to enable feature service acceleration.
- Hypershield—A controller application designed to protect modern datacenters. Hypershield is a distributed security architecture that provides hardware-accelerated security policy enforcement using DPU technology. Hypershield centrally manages and distributes policies across all enforcement points, ensuring consistent security across the entire network.

The N9300 Smart switch serves as a Network-Based Enforcer for implementing and managing security policies across the network. You can view the N9300 Smart switch in Hypershield under Network-based enforcers in Hypershield. For more information, refer to the [Cisco Hypershield User Documentation](#).

- Hypershield Agent—A containerized agent that receives Security configurations and policies from Hypershield and pushes them to the DPU complex that in-turn configures security rules on DPUs. The Hypershield Agent constructs flow logs and exports them.
- Network Security Operations administrator role—A specialized role (netsecops-admin) available only on the N9300 Smart Switches that has the privileges to execute the commands within the DPU and the Hypershield agent container. For more information, refer to [User Accounts and RBAC for Smart Switches](#).
- DPU security mode—The N9300 Smart Switch DPU security mode differs from the Security Firewall product as well as the network security features in N9000 Series Switches. The Smart Switch, when used in DPU security mode, provides a distributed, stateful Layer-4 segmentation and DPU security enforcement directly within the switch using embedded Data Processing Units (DPUs).

To use the DPU security mode, you need to enable feature service acceleration. When the DPU is in a powered-on state, the switch works in both network and DPU security modes. When the DPU is in a powered-off state, the switch works in a network-only mode.

NX-OS and Hypershield

You can use the NX-OS command line interface or Nexus Dashboard and Hypershield to manage the operations on the N9300 Series Smart Switch.

From the NX-OS command line interface you can:

- manage the traffic redirection to the DPU

- configure network policies, and
- observe network analytics, and topology.

From the Hypershield, you can:

- manage and monitor security policies
- orchestrate the usage of security policies, and
- observe security policies and ensure security compliance.

References

The documents related to Smart Switches that provide additional references include:

- [Cisco N9324C-SE1U NX-OS-Mode Switch Hardware Installation Guide](#)
- [Cisco N9348Y2C6D-SE1U NX-OS Mode Switch Hardware Installation Guide](#)
- For Optics support on the N9300 Series Smart Switches, refer to [Cisco Optics-to-Device Compatibility Matrix](#)
- [N9300 Series Smart Switch Data Sheet](#)
- For network mode support features documentation, refer to [Cisco Nexus 9000 Series Switches](#)
- [Cisco Hypershield User Documentation](#)

Smart Switch architecture

Summary

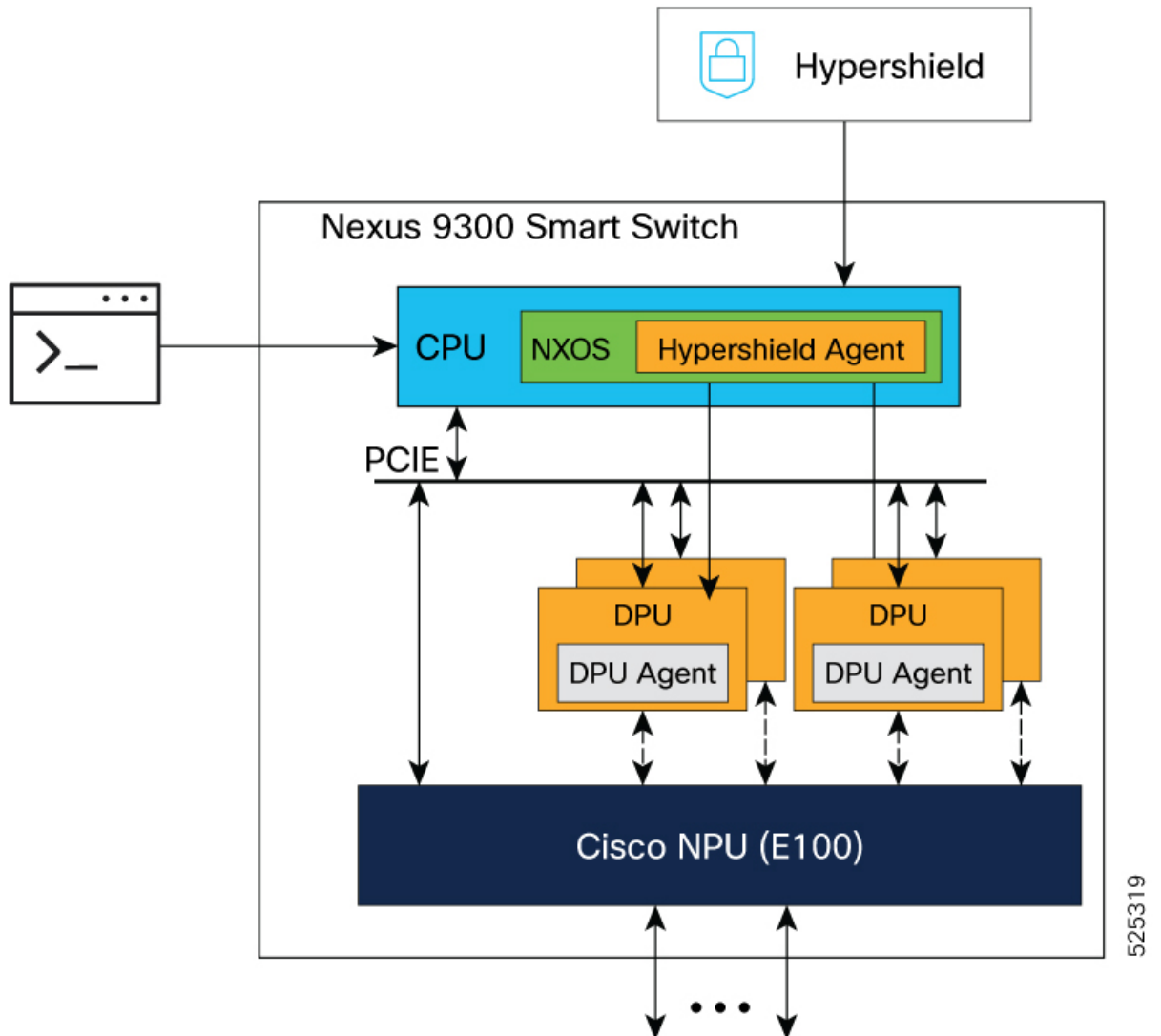
The Smart Switch architecture integrates several key components to manage and process network traffic. At the core is the Network Processing Unit (NPU) to perform routing and switching, and the Data Processing Units (DPUs) for traffic filtering. The CPU runs NX-OS and hosts the Hypershield Agent, which connects to the external Hypershield system. Management of networking configuration is performed using the NX-OS command line interface or Nexus Dashboard. The configuration of security policies is performed from Hypershield.

The Hypershield Agent in the N9300 Series Smart Switch establishes connectivity to the Hypershield system through the front panel ports and uses the IP address of a loopback interface as the source-interface.

Workflow

This flow describes how the N9300 Smart Switch works.

Figure 1: Architecture of a Smart Switch



1. When a security administrator configures a security policy in the Hypershield system, this is pushed to the Hypershield agent in the N9300 Smart switch. The Hypershield agent programs it on the DPUs.
2. The NPU performs routing and switching like any other NX-OS device. It is connected with links (for example 200G, based on the platform) to multiple DPUs (for example, the N9324C-SE1U supports 4 DPUs).
3. When you enable the required configuration on the NPU, it redirects the traffic to the DPUs, for traffic inspection. After traffic inspection, traffic is forwarded as usual by the NPU.

This architecture allows the DPU to accelerate the data plane processing for traffic filtering.

The N9300 Smart Switch works both as a network device and a security device as it includes:

- NPU, which provides the N9000 routing and switching functions that is managed using the command line interface, programmability, or Nexus Dashboard.

- DPU, which provides security functions that are managed using Hypershield.

Service-Ethernet ports

Service-Ethernet Ports are a unique type of NX-OS ethernet interface assigned to DPUs to carry traffic from the NPU to the DPU. These ports are distinct from inband or front-panel interfaces, to clearly differentiate them from other existing interface types.

The service-ethernet ports are created with default values for basic interface settings like MTU, speed, and bandwidth similar to the front-panel ports. The service-ethernet ports are always administratively UP.

The service-ethernet ports are operational only when the DPU comes online and is detected. If the DPU goes offline, or when the service acceleration feature is unconfigured, the link may go down, and the ports corresponding to the DPU(s) are impacted.



Note These ports are configured by DPU agent every time the device is rebooted, including ISSU upgrades.

To view the status of the interfaces and DPUs they map to, use the `show interface service-ethernet slot/port` command.

```
switch# show interface service-ethernet 1/1
admin state is up, Connected to DPU-1
```

The service-ethernet interfaces are added to service-port-channel interfaces which can be observed in the output of the **show port-channel summary** command. The membership of the service port-channel interfaces may vary based on the platform and the load-balance configuration discussed in [Configure load-balance mode](#).

