Overview

This chapter introduces the Cisco N9300 Series Smart switches.

Introduction

The Cisco N9300 Series Smart switches provide 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 Cisco N9300 Series Smart switches provide embedded security that is powered with Hypershield. The switches offer service-accelerated performance and simplify security by integrating into the network, eliminating the need for separate firewall structures.

The Cisco N93000 Series Smart switches securely segments and connects security zones within the data center, across interconnects and Cloud.

Cisco N9300 Series Smart Switches

The Cisco N9300 Series Smart switches integrate Data Processing Units (DPUs) with networking ASICs to enhance data center networking and security. Hypershield manages the DPU to provide the security functions, while the NPU provides the N9000 routing and switching functions.

The integration of Cisco NX-OS and Hypershield software into a single software image simplifies deployment and enhances operational flexibility.

The Cisco N9300 Series Smart switches offer converged switching, routing, and Layer 4 - Layer 7 services, and has a programmable software-defined pipeline for Layer 2 -Layer 7 services with these features:

- Hardware-enhanced Layer 4- Layer 7 services

- Scalable stateful firewall for millions of connections
- Centralized control of network services
- Connection state management
- Instrumentation and analytics for services

Cisco N9324C-SE1U switch

The Cisco N9324C-SE1U switch is a 1-RU solution designed to deliver high-performance networking capabilities. Its features include:

- 24-port 100G ports
- Cisco Silicon One E100 ASIC offering high-speed connectivity and scalability
- 4 DPUs offering software-defined stateful services
- Services such as distributed Layer-4 segmentation and DoS protection

Port speed on Cisco N9324C-SE1U switch

The Cisco N9324C-SE1U supports 40G and 100G native port speeds.

Cisco N9324C-SE1U supports breakout on

- 4x25G
- 4x10G
- 2x50G

Cisco N9324C-SE1U supports 10G with QSA on the ports.

Optics support

Cisco N9324C-SE1U supports these optics.

- 100G Optics
  - QSFP28-100G-SR4
  - QSFP28-100G-PSM4
  - QSFP28-100G-CWDM4
  - QSFP28-100G-LR4
  - QSFP28 AOC, 1, 3, 5, 7, 10, 15, 30m
  - QSFP28 – 100G DR, 100G FR
- 40G Optics
  - QSFP-40G-LR4

- QSFP AOC, 1, 3, 5, 7, 10, 15, 30m
- QSFP-40G-LR4-S
- QSFP-40G-SR-BD
- QSFP-40G-SR4-S
- QSFP-40G-SR4

Service-Ethernet ports

Service-Ethernet Ports are a unique type of NXOS 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, 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.

Use the **show interface service-ethernet** *slot/port* command to view the status of the interfaces.

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

Use the **show interface hardware-mappings** to view the DPU to interface mapping.

```
Switch# show interface hardware-mappings
:
--------------------------------------------------------------------------------
Name       Ifindex  Smod Unit HPort NPort Slice Ifg   VPort Serdes_id  service
--------------------------------------------------------------------------------
Eth1/1     1a000000 1    0    16    0     0     0     -1    12
Eth1/2     1a000200 1    0    20    4     0     0     -1    16
Eth1/3     1a000400 1    0    24    8     0     0     -1    20
:
SEth1/1    65000000 1    0    24    8     0     0     -1    20          DPU/1
SEth1/2    65002000 1    0    24    8     0     0     -1    20          DPU/1
SEth1/3    65004000 1    0    24    8     0     0     -1    20          DPU/2
SEth1/4    65006000 1    0    24    8     0     0     -1    20          DPU/2
```

Cisco NX OS and Security Cloud Control

You can use the Cisco NX OS command line interface (CLI) and Security Cloud Control to manage the operations on the Cisco N9300 Series Smart switch.

This table list the operations of the Cisco NX OS CLI and the Security Cloud Control.

Cisco NX OS CLI	Security Cloud Control
Manage the traffic redirection on the DPU	Manage and monitor security policy lifecycle
Configure the network policies	Orchestrate the usage of security policies
Observe network analytics, and topology	Observe security policies and ensure security compliance
Troublehsoot connectivity and provide assurance	Upgrade and downgrade Hypershield Agent on the smart switches.

Hypershield

Cisco Hypershield is an AI-native Security Cloud based Controller application designed to protect modern datacenters and cloud environments. Hypershield provides enhanced security measures to protect from unauthorized access and potential threats by implementing robust security protocols.

Hypershield is built with AI from the ground up, enabling it to analyze large amounts of security data, generate insights, and make intelligent recommendations. Its hyper distributed enforcement makes sure that security mechanisms are integrated into servers and network infrastructure, providing protection across various locations and environments. Hypershield centrally manages and distributes policies across all enforcement points, ensuring consistent security across the entire network. Its kernel level enforcement provides deep visibility and control at the operating system level, allowing for granular security actions. Its distributed exploit protection can quickly identify and deploy compensating controls for new vulnerabilities, providing protection within minutes.

Hypershield manages these assets:

- **Tesseract Security Agent**: this is an agent that is installed on any server running linux inside the datacenter, and it provides the ability to perform the enforcement of security policies. The agent monitors network connections, file and system calls, and kernel functions. It generates event-based telemetry for observing and analyzing security events. It also can add in AI automated compensating controls for any security event or PSIRTs on NXOS and Servers.
- **Network-Based Enforcer**: these are devices implementing traffic filtering while forwarding the traffic. The smart switch is a network enforcer. With a network enforcer you can create Layer 3 and Layer 4 policies to protect network segments like VRFs and VLANs.

The Cisco N9300 Smart switch serves as a Network-Based Enforcer for implementing and managing security policies across the network. You can view the Cisco N9300 Smart switch in Security Cloud Control under Network-based enforcers in Hypershield.

How the N9324C-SE1U switch works

Summary

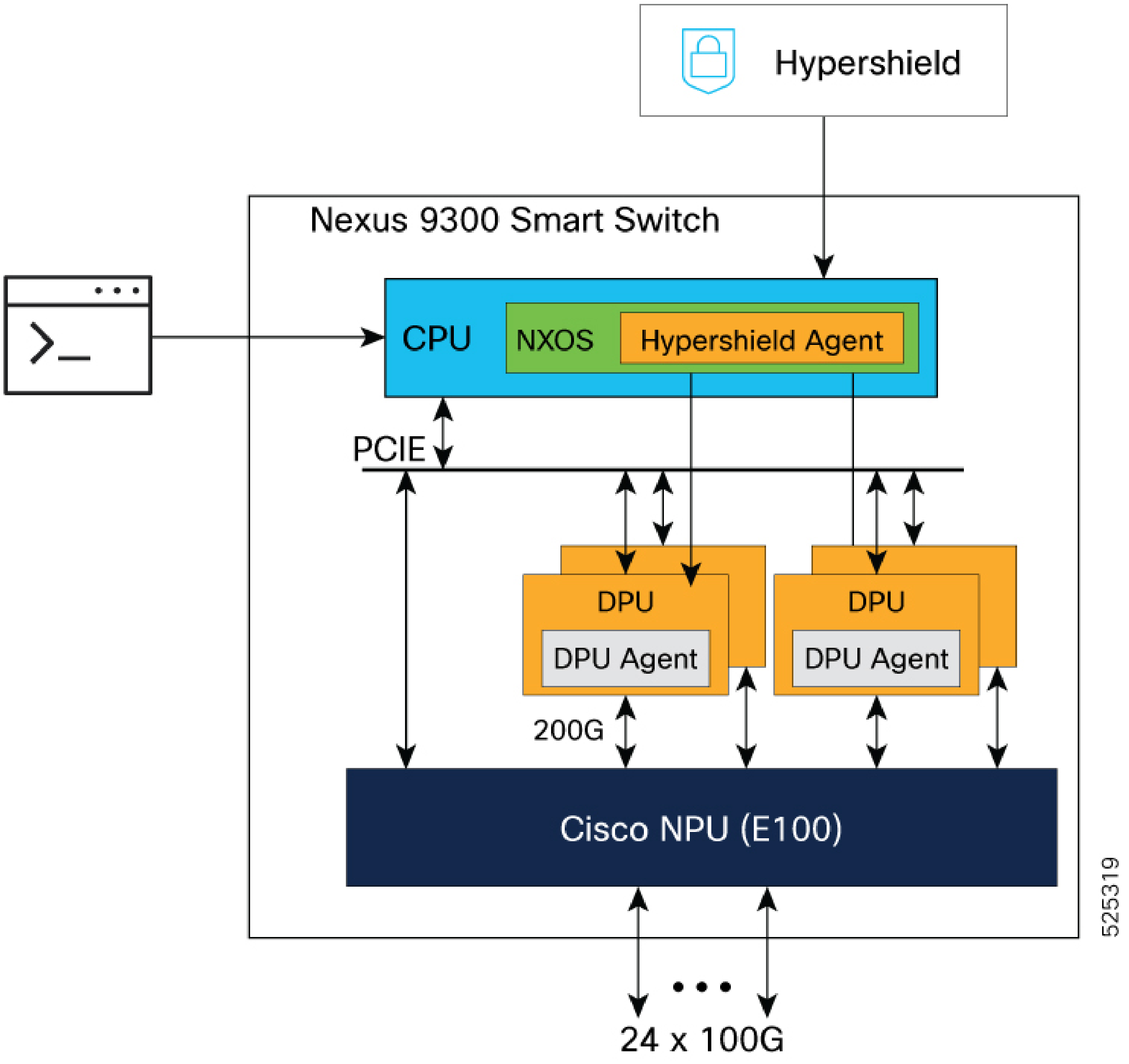
The Cisco N9324C-SE1U switch architecture integrates several key components to manage and process network traffic. At the core is the Network Processing Unit (NPU) to perform routing and switching, and the Data Processing Units (DPUs) for traffic filtering. The CPU runs the NXOS operating system and hosts the

the Hypershield Agent, which connects to the external Hypershield system. Management of networking configuration is performed via the NXOS CLI. The configuration of security policies is performed from Hypershield.

The Hypershield Agent in the Cisco N9300 Smart switch establishes connectivity to the Hypershield system via the front panel ports, and uses the IP address of the loopback interface for the source-interface.

Workflow

Figure 1: Working of the Cisco N9300 Smart Switch



These stages describe the working of the Cisco N9300 Smart switch.

1. When a security administrator configures a security policy in the Hypershield system, this is pushed to the Hypershield agent in the Cisco N9300 Smart switch. The Hypershield agent programs it on the DPUs.

2. The Cisco NPU performs routing and switching like any other NXOS device. It is connected with 200G links to multiple DPUs (the Cisco N9324C-SE1U supports 4 DPUs) and, on configuration the Cisco NPU can also redirect traffic to the DPUs for traffic inspection.

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

Software management

NXOS manages the software images for both the Cisco NXOS operating system and the DPUs.

- A specific NXOS image is released that bundles both the NXOS component and the Hypershield Management Software. The format for such image names follows a pattern like `nxos64-s1-dpu.10.5.3s.F.bin`.

Updates to the Hypershield agent are possible via Hypershield.

Supported software features

Cisco Nexus NX-OS Release 10.5(3s)F introduces the support for the Cisco N9324C-SE1U and for these software features with the DPU enabled:

- Layer 3 IPv4/IPv6 forwarding with multi-VRF support
- VRF-based redirection
- DPU based traffic inspection for unicast IPv4 and IPv6 routed traffic, routed ports, subinterfaces, routed port channels, and port-channel subinterfaces
- Routing protocols such as BGP , IS-IS, OSPF, EIGRP , and static
- DPU lifecycle management (software upgrade, and DPU health monitoring)

Additional references

Table 1: Related Documentation

For infromation on...	see...
Cisco Nexus 9000 Series Switches	https://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.html
Hypershield	https://www.cisco.com/c/en/us/products/collateral/security/hypershield/hypershield-so.html