Revised: September 7, 2026

System Management for Network Mode

System management features

This article outlines the supported system management features, their functions, and associated limitations for the N9324C-SE1U and N9348Y2C6D-SE1U smart switches. The features cover traffic observation, neighbor discovery, time synchronization, flow monitoring, hardware diagnostics, and graceful maintenance operations. Use the related articles for configuration requirements and feature-specific limitations.

Generic Online Diagnostics

Generic Online Diagnostics (GOLD) tests hardware components and verifies data paths and control signals while a smart switch is operating on a live network. This topic covers the breakout-port behavior that applies to N9324C-SE1U and N9348Y2C6D-SE1U smart switches.

For more information, refer to Online Diagnostics.

Guidelines and limitations for Generic Online Diagnostics

- BootupPortLoopback is not supported on breakout ports during bootup on N9324C-SE1U and N9348Y2C6D-SE1U smart switches.
- The BootupPortLoopback test can display as Untested (U) or Fail (F) for breakout subports.
- On-demand PortLoopback tests are supported on breakout ports after bootup.
- Disruptive online diagnostic tests cannot be run on demand.

LLDP

Link Layer Discovery Protocol (LLDP) is a vendor-neutral, one-way device discovery protocol defined by the IEEE 802.1AB standard. It enables network devices to advertise information about themselves to other devices on the same local network segment, facilitating device discovery and network topology mapping.

Beginning with NX-OS Release 10.6(2)F, LLDP is supported on the N9324C-SE1U and N9348Y2C6D-SE1U smart switches.

For information on LLDP, refer to Configuring LLDP.

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) enables network management systems to monitor and manage the N9324C-SE1U and N9348Y2C6D-SE1U smart switches. Beginning with NX-OS Release 10.6(2)F, these smart switches support SNMPv1, SNMPv2c, and SNMPv3.

For more information, refer to Simple Network Management Protocol.

Sampled flow

Sampled Flow (sFlow) is a standards-based network traffic monitoring technology that enables real-time monitoring of traffic in data networks containing switches and routers.

Beginning with NX-OS Release 10.6(2)F, sampled flow is supported on the N9324C-SE1U and N9348Y2C6D-SE1U smart switches.

For information on sFlow, refer to Configuring sFlow.

Limitations for sampled flow

- For egress sampled packet, re-written information is not available in sFlow record.
- Egress Layer 2 source interface is not supported.
- sFlow is not supported on the sub-interface traffic.
- sFlow is not supported on Service-Ethernet or Service-Port-channels.

NetFlow

NetFlow monitors ingress traffic and exports IPv4 and IPv6 flow records using NetFlow version 9 to an external collector, with support for up to 64,000 flow records per second and a cache of up to 1,000,000 flow records.

Beginning with NX-OS Release 10.6(2)F, ingress NetFlow is supported on the N9324C-SE1U and N9348Y2C6D-SE1U smart switches.

For more information, refer to NetFlow.

Guidelines and limitations for NetFlow

- Egress NetFlow is not supported on these smart switches.

Switched Port Analyzer

Switched Port Analyzer (SPAN) duplicates traffic from specified source ports and sends a copy to a designated destination port for analysis on N9300 Series smart switches.

Beginning with NX-OS Release 10.6(2)F, SPAN is supported on N9324C-SE1U and N9348Y2C6D-SE1U smart switches.

For information on SPAN, refer to Switched Port Analyzer.

Guidelines and limitations for SPAN

These guidelines and limitations apply when you configure SPAN on these smart switches:

- **Sessions**—Each smart switch supports a maximum of 10 active monitor sessions at a time, regardless of whether the sessions are local SPAN or ERSPAN.
- **Packet mirroring**—The smart switch mirrors packets on a subinterface when the parent service-port-channel interface is configured as the source. SPAN mirrored packets use the default egress queue (Q0) on the SPAN destination interface and do not have a dedicated SPAN egress queue. SPAN can mirror traffic entering or leaving a service-port-channel interface.

- **SPAN to CPU**—Monitor statistics are not displayed for SPAN to CPU. Both Rx and Tx mirroring are supported for SPAN to CPU.
- **Multicast traffic**—When local SPAN mirrors multicast traffic from a front-panel interface, the monitor port accounts for the traffic as multicast.
- **Port-channel interface**—When a port-channel interface with multiple member ports is configured as a SPAN destination, only one member interface is used for mirrored traffic. Member selection is handled in software, which results in packet loss when membership changes.
- **MTU truncation**—SPAN MTU truncation supports 144 bytes. Rx mirrored packets are truncated to 144 bytes, excluding FCS, and Tx mirrored packets are truncated to 80 bytes, excluding FCS.
- **Unsupported features**—The features that are not supported include:
  - Mirroring packets on Layer 3 subinterfaces or Layer 3 port-channel subinterfaces when the respective parent interface is configured as the source.
  - Sharing the same source port or interface across sessions.
  - Using tunnel ports, VLAN, SUP Ethernet, or a management interface as a source.
  - Using UDF or a SPAN ACL filter.

Encapsulated Remote Switched Port Analyzer

Encapsulated Remote Switched Port Analyzer (ERSPAN) transports mirrored traffic over an IP network from source ports or VLANs on one device to destination ports or analyzers on another device for remote monitoring on N9300 Series smart switches.

Beginning with NX-OS Release 10.6(2)F, ERSPAN is supported on N9324C-SE1U and N9348Y2C6D-SE1U smart switches.

For information on ERSPAN, refer to Configuring ERSPAN.

Guidelines and limitations for ERSPAN

These guidelines and limitations apply when you configure ERSPAN on these smart switches:

- **Sessions**—Each smart switch supports a maximum of 10 active monitor sessions at a time, regardless of whether the sessions are local SPAN or ERSPAN.
- **Packet mirroring**—The smart switch mirrors packets on a subinterface when the parent service-port-channel interface is configured as the source. ERSPAN mirrored packets use the default egress queue (Q0) on the ERSPAN destination interface and do not have a dedicated ERSPAN egress queue. ERSPAN can mirror traffic entering or leaving a service-port-channel interface.
- **MTU truncation**—ERSPAN MTU truncation supports 144 bytes. Rx mirrored packets are truncated to 144 bytes, excluding FCS, and Tx mirrored packets are truncated to 80 bytes, excluding FCS.
- **Port-channel interface**—When a port-channel interface with multiple member ports is configured as an ERSPAN destination, only one member interface sends mirrored traffic. Member selection is handled in software, which can cause packet loss when membership changes.
- **Unsupported features**—The features that are not supported include:
  - Mirroring packets on Layer 3 subinterfaces or Layer 3 port-channel subinterfaces when the respective parent interface is configured as the source.

- Sharing the same source port or interface across sessions.
- Using tunnel ports, VLAN, SUP Ethernet, or a management interface as a source.
- Using an ERSPAN Type 3 header.
- ERSPAN destination or termination.
- Using UDF or an ERSPAN ACL filter.

Precision Time Protocol

Precision Time Protocol (PTP) synchronizes distributed clocks over Ethernet on the N9324C-SE1U and N9348Y2C6D-SE1U smart switches.

Beginning with NX-OS Release 10.6(3)F, PTP is supported on these smart switches.

For more information, refer to Precision Time Protocol.

Guidelines and limitations for Precision Time Protocol

- IEEE 1588v2 and the media profile are supported.
- The 8275.1 PTP profile is not supported.
- PTP is not supported on an interface when MACsec is enabled.

Graceful Insertion and Removal

Graceful Insertion and Removal (GIR) places a smart switch in maintenance mode, isolates configured Layer 3 control-plane protocols, and removes the smart switch from the regular forwarding path. Graceful insertion restores the protocols and returns the smart switch to normal operation.

Beginning with NX-OS Release 10.6(2)F, GIR is supported on N9324C-SE1U and N9348Y2C6D-SE1U smart switches.

For more information, refer to Configuring Graceful Insertion and Removal.

GIR workflow

Complete the GIR workflow in this order:

1. Optionally create the maintenance-mode profile.
2. Optionally create the normal-mode profile.
3. Create a snapshot before graceful removal.
4. Trigger graceful removal to place the smart switch in maintenance mode.
5. Perform the maintenance or debugging operation.
6. Trigger graceful insertion to return the smart switch to normal mode.
7. Create a second snapshot and compare it with the first snapshot.

Guidelines and limitations for GIR

- Remove existing custom profiles before creating new maintenance-mode or normal-mode profiles.
- Layer 2 GIR in a vPC environment does not provide zero packet loss during the transition to maintenance mode.
- When only one vPC smart switch is isolated, traffic to SVI hosts can use the vPC peer during OSPF maintenance behavior.
- During a binary reload, interfaces remain shut until the smart switch completes booting and declares system readiness.