Revised: September 2, 2026

Interfaces configuration for Network Mode

Interfaces

This article outlines the supported interface features, their functions, and associated limitations for N9324C-SE1U and N9348Y2C6D-SE1U Smart switches. The features include port profiles, Layer 2 access and trunk ports, native VLAN tagging, reserved VLAN handling, Layer 3 routed interfaces and subinterfaces, and switch virtual interfaces (SVIs) for traffic segmentation and routing. Single-hop BFD, LACP, port channels, virtual port channels, Q-in-Q VLAN tunnels, and unidirectional link detection provide connectivity, redundancy, traffic encapsulation, and link protection.

Interface concepts and relationships

Interface features define how devices connect to the switch and how the switch carries, routes, aggregates, and protects traffic.

Table 1: Interface terminology

Term	Definition	Relationship
Port profile	A reusable group of interface commands.	Applies consistent settings to multiple interfaces.
Access port	A Layer 2 port that carries traffic for one VLAN.	Connects an endpoint to a single VLAN.
Trunk port	A Layer 2 port that carries traffic for multiple VLANs.	Extends VLAN connectivity between switches or other VLAN-aware devices.
Native VLAN and reserved VLAN	A native VLAN carries untagged traffic, and a reserved VLAN is allocated for internal switch functions.	Controls VLAN selection for untagged traffic and prevents use of VLANs reserved for internal functions.
Switch Virtual Interface (SVI)	A logical interface associated with a VLAN.	Connects Layer 2 VLAN forwarding to Layer 3 services.
Routed interface and subinterface	A Layer 3 interface and a logical Layer 3 interface derived from a parent interface.	Forwards routed traffic through physical, native, or port-channel interfaces.
Port channel and Virtual Port Channel (vPC)	A port channel aggregates physical links, and a vPC presents links from two switches as one logical port channel.	Provides link redundancy, aggregated bandwidth, and multichassis connectivity.
Q-in-Q VLAN tunnel	A Layer 2 tunnel that adds an outer 802.1Q tag to an already tagged frame.	Preserves customer VLAN information across a provider or shared network.
Link failure detection	Unidirectional Link Detection (UDLD) detects one-way Ethernet links, and Single-Hop Bidirectional Forwarding Detection (BFD) detects failures between directly connected Layer 3 devices.	Helps protect links and accelerate recovery from detected failures.

Port profiles

You can create a port profile that contains many interface commands and apply that port profile to a range of interfaces.

Beginning with NX-OS Release 10.6(2)F, port profiles are supported on the N9324C-SE1U and N9348Y2C6D-SE1U Smart switches.

For information on port profiles, refer to Port Profiles

Layer 2 access and trunk ports

A Layer 2 port can be configured as an access port, which carries traffic for a single VLAN, or as a trunk port, which carries traffic for two or more VLANs simultaneously.

Beginning with NX-OS Release 10.6(2)F, you can configure VLAN access and trunk modes on the N9324C-SE1U and N9348Y2C6D-SE1U Smart switches.

For information on access and trunk ports, refer to About Access and Trunk Interfaces.

Native VLAN ID and tagging native VLAN traffic

A native VLAN carries untagged traffic on a trunk port. The trunk can also carry tagged traffic for other VLANs.

NX-OS supports the IEEE 802.1Q standard on trunk ports. You can configure the switch to retain or strip 802.1Q tags on native VLAN traffic on all trunk ports.

Beginning with NX-OS Release 10.6(2)F, you can configure native VLAN traffic and tagging on the N9324C-SE1U and N9348Y2C6D-SE1U Smart switches.

For more information, refer to Configuring Layer 2 Interfaces.

Reserved VLAN

A reserved VLAN is a VLAN that NX-OS allocates for internal switch functions.

By default, NX-OS reserves VLANs 3968 through 4095 for internal use. You can change the reserved range in groups of 128 VLANs, but VLANs 4093 through 4095 remain reserved for internal use. Save the configuration and reload the switch for a changed range to take effect.

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

For more information, refer to Configuring VLANs.

Switch Virtual Interface

An SVI provides the logical connection between a VLAN bridging function and the routing function. Its operational state follows the forwarding state of ports in the corresponding VLAN: the SVI comes up when at least one port is in the Spanning Tree Protocol forwarding state and goes down when the last forwarding port goes down or changes STP state.

Beginning with NX-OS Release 10.6(2)F, SVI and VLAN logical interfaces are supported on on the N9324C-SE1U and N9348Y2C6D-SE1U Smart switches.

For more information, refer to Configuring Layer 2 Interfaces.

Layer 3 routed interface and subinterface support

Layer 3 routed interfaces provide routed connectivity between the smart switches and attached networks. Routed subinterfaces provide logical Layer 3 interfaces on native and port-channel interfaces.

Beginning with NX-OS Release 10.6(2)F, you can configure Layer 3 routed interfaces and routed subinterfaces (native and port-channel) on the N9324C-SE1U and N9348Y2C6D-SE1U Smart switches.

For information about configuring Layer 3 interfaces and routed subinterfaces, refer to Configuring Layer 3 Interfaces.

Single-Hop BFD

Single-Hop Bidirectional Forwarding Detection (BFD) is a protocol that provides rapid detection of failures in the path between two directly connected network devices, enabling fast convergence and improved network reliability.

Beginning with NX-OS Release 10.6(2)F, Single-Hop BFD is supported on the N9324C-SE1U and N9348Y2C6D-SE1U Smart switches.

For more information, refer to Configuring Bidirectional Forwarding Detection.

LACP and port channels

A port channel is an aggregation of multiple physical interfaces that creates a logical interface.

Link Aggregation Control Protocol (LACP) for Ethernet is defined in IEEE 802.1AX and IEEE 802.3ad. This protocol controls how physical ports are bundled together to form one logical channel.

Beginning with NX-OS Release 10.6(2)F, port channels and LACP are supported on the N9324C-SE1U and N9348Y2C6D-SE1U Smart switches.

For more information on LACP and port channels, refer to Configuring Port Channels

Virtual Port Channel

A Virtual Port Channel (vPC) allows links connected to two devices to function as a single logical port channel to a third device, enabling Layer 2 multipathing for redundancy, higher bandwidth, and load balancing.

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

For information on vPC, refer to Configuring vPCs.

Q-in-Q VLAN tunnels

A Q-in-Q VLAN tunnel enables a service provider to segregate the traffic of different customers in their infrastructure, while still giving the customer a full range of VLANs for their internal use by adding a second 802.1Q tag to an already tagged frame.

For information on configuring Q-in-Q VLAN tunnels, refer to Configuring Q-in-Q VLAN Tunnels.

Q-in-Q VLAN tunnel guidelines and limitations

Beginning with NX-OS Release 10.6(2)F, you can configure Q-in-Q on the N9324C-SE1U and N9348Y2C6D-SE1U Smart switches with these limitations:

- You cannot configure a range of allowed VLANs by using **switchport trunk allowed vlan** *vlan_list* command.

```
..!
interface Ethernet1/1  switchport mode trunk
switchport vlan mapping all dot1q-tunnel 30
switchport trunk allowed vlan 30-40
 ..!
```

  In the configuration example, trunk VLAN 30 is the provider VLAN. The VLANs 31 through 40 filter regular trunk traffic; these VLANs operate in sparse mode.

- You cannot use VLAN ACL with Q-in-Q.
- Multicast is not supported, and IGMP snooping is not supported.
- Custom EtherType is not supported.
- Variations of QinQ are not supported:
  - Q-in-VNI and Selective Q-in-VNI are not supported.
  - Selective Q-in-Q is not supported.
- You do not need the **system dot1q-tunnel transit** command for Q-in-Q tunneling when the switch acts as a transit device.
- Auto-negotiation is not supported.

Unidirectional Link Detection

Unidirectional Link Detection (UDLD) is a Cisco-proprietary protocol that enables devices connected by fiber-optic or copper Ethernet cables to detect and disable unidirectional links by periodically exchanging UDLD frames, thereby preventing network issues caused by misconnected or faulty cabling.

Beginning with NX-OS Release 10.6(2)F, UDLD feature is supported on N9300 Series smart switches.

For information on UDLD, refer to Unidirectional Link Detection Parameter.