Cisco Nexus 9000 Series NX-OS Release Notes, Release 7.0(3)I4(1)

This document describes the features, caveats, and limitations for Cisco NX-OS Release 7.0(3)I4(1) software for use on the following switches:

- Cisco Nexus 9000 Series
- Cisco Nexus 31128PQ
- Cisco Nexus 3164Q
- Cisco Nexus 3232C
- Cisco Nexus 3264Q

Use this document in combination with documents listed in *Related Documentation*.

Note: Starting with Cisco NX-OS Release 7.0(3)I2(1), the Cisco NX-OS image filename has changed to start with "nxos" instead of "n9000."

Table 1 shows the online change history for this document.

Table 1 Online History Change

Date	Description
September 28, 2020	Upgrade and Downgrade section revised.
January 24, 2020	Added CSCvc95008 to Known Behaviors.
September 4, 2017	Updated the instructions for upgrading from Cisco NX-OS Releases 7.0(3)I1(2), 7.0(3)I1(3), or 7.0(3)I1(3a).
June 21, 2017	Replace X9564TX2 with X9464TX2.
February 6, 2017	Added CSCvc93246 to the Open Caveats.
October 20, 2016	Revised Upgrade Instructions about using the install all command.
July 15, 2016	Revised statement about fast reload in *Limitations* section
July 12, 2016	Added the following PID in *New Hardware Features*: N9K-C9504-FM-S
June 10, 2016	Specified that the issue with BCM (Broadcom) bits not being set applies only to FCoE VLANs in FCoE NPV mode

Date	Description
June 6, 2016	■ Updated Table 2 ■ Added link to Cisco Nexus 31128PQ Switch - Read Me First
June 2, 2016	Changed the description of the N9K-C9272Q
May 25, 2016	VTEP connected to FEX host interface ports is not supported
May 17, 2016	Added links to the configuration guides that are related to each new software feature
May 16, 2016	Created the release notes for Release 7.0(3)I4(1).

Contents

Introduction

Cisco NX-OS software is a data center-class operating system designed for performance, resiliency, scalability, manageability, and programmability at its foundation. The Cisco NX-OS software provides a robust and comprehensive feature set that meets the requirements of virtualization and automation in mission-critical data center environments. The modular design of the Cisco NX-OS operating system makes zero-impact operations a reality and enables exceptional operational flexibility.

The Cisco Nexus 9000 Series uses an enhanced version of Cisco NX-OS software with a single binary image that supports every switch in the series, which simplifies image management.

System Requirements

This section includes the following sections:

- Supported Cisco Software Releases
- Supported Device Hardware
- Supported Optics
- Supported FEX Modules

Supported Cisco Software Releases

Table 2 summarizes information about the Cisco Nexus platforms and software release versions that Cisco OpenFlow Plug-in supports.

Table 2 Cisco Plug-in for OpenFlow Compatibility Matrix

Switches	Cisco Plug-in for OpenFlow
Cisco Nexus 9300 Series switches and Cisco Nexus 31128PQ, 3232C, and 3264Q switches NX-OS 7.0(3)I3(1) and later	ofa-2.1.4-r2-nxos-SPA-k9.ova
Cisco Nexus 9300 Series switches and Cisco Nexus 31128PQ switches NX-OS 7.0(3)I2(1)	ofa-2.1.0-r1-nxos-SPA-k9.ova

Supported Device Hardware

Table 3 lists the Cisco Nexus 9000 Series hardware that Cisco NX-OS Release 7.0(3)I4(1) supports. For additional information about the supported hardware, see the Hardware Installation Guide for your Cisco Nexus 9000 Series device.

Table 3 Cisco Nexus 9000 Series Hardware

Product ID	Hardware	Quantity
N9K- X9464TX2	Cisco Nexus 9400 platform 48-port, 1-/10-Gbps BASE-T plus 4-port QSFP I/O module	■ Up to 8 in the Cisco Nexus 9508 ■ Up to 4 in the Cisco Nexus 9504 ■ Up to 16 in the Cisco Nexus 9516
N9K-X9564PX	Cisco Nexus 9500 platform 48-port, 1-/10-Gbps SFP+ plus 4-port QSFP I/O module	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 16 in the Cisco Nexus 9516
N9K-X9536PQ	Cisco Nexus 9500 36-port, 40 Gigabit Ethernet QSFP aggregation module	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 16 in the Cisco Nexus 9516
N9K-X9636PQ	Cisco Nexus 9500 platform 36-port 40-Gigabit QSFP I/O module Note: Not supported on the Cisco Nexus 9516 switch (N9K-C9516).	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508

Product ID	Hardware	Quantity
N9K-X9464PX	Cisco Nexus 9500 platform 48-port 10-Gigabit SFP+ plus 4-port QSFP I/O module	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 16 in the Cisco Nexus 9516
N9K-X9464TX	Cisco Nexus 9500 platform 48-port 10-GBASE-T plus 4-port QSFP I/O module	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 16 in the Cisco Nexus 9516
N9K-X9464TX2	Cisco Nexus 9500 platform 48-port 10GBASE-T plus 4-port QSFP I/O module	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 16 in the Cisco Nexus 9516
N9K-X9432C-S	Cisco Nexus 9500 platform line card with 32-port 100-Gigabit QSFP28 ports (supported by four 100-Gigabit –S fabric modules [N9K-C9504-FM-S and N9K-C9508-FM-S])	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508
N9K-X9432PQ	Cisco Nexus 9500 platform 32-port 40-Gigabit QSFP I/O module Note: The Cisco Nexus X9432PQ I/O module supports static breakout.	Up to 8 in the Cisco Nexus 9508

Product ID	Hardware	Quantity
N9K-X9408PC-CFP2	Cisco Nexus 9500 platform 8-port 100-Gigabit CFP2 I/O module for the Cisco Nexus 9504, 9508, and 9516 modular switches	■ Up to 4 in the Cisco Nexus ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 16 in the Cisco Nexus 9516
N9K-SC-A	Cisco Nexus 9500 platform System Controller Module	2
N9K-SUP-A	Cisco Nexus 9500 platform supervisor module	2
N9K-SUP-B	Cisco Nexus 9500 platform supervisor B module	2
N9K-PAC-3000W-B	Cisco Nexus 9500 platform 3000 W AC power supply	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 10 in the Cisco Nexus 9516
N9K-PDC-3000W-B	Cisco Nexus 9500 platform 3000 W DC power supply	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 10 in the Cisco Nexus 9516

Product ID	Hardware	Quantity
N9K-PUV-3000W-B	Cisco Nexus 9500 3-kW Universal AC/DC power supply	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 10 in the Cisco Nexus 9516
N9K-C9516-FM	Cisco Nexus 9500 platform fabric module	3-6 depending on the line card
N9K-C9508	Cisco Nexus 9508 8-slot chassis	1
N9K-C9508-FAN	Cisco Nexus 9508 fan trays	3
N9K-C9508-FM	Cisco Nexus 9508 Series fabric module	3-6 depending on the line card
N9K-C9508-FM-S	A generation 2 fabric module that is required for the 100-Gigabit (-S) I/O modules. When used, there must be 4 of these fabric modules installed in fabric slots 22, 23, 24, and 26. Currently, this fabric module is supported on only the Cisco Nexus 9508 modular chassis.	4
N9K-C9504	Cisco Nexus 9504 4-slot chassis	1
N9K-C9504-FAN	Cisco Nexus 9504 fan trays	3
N9K-C9504-FM	Cisco Nexus 9504 fabric module	3 to 6 depending on line card
N9K-C9504-FM-S	Cisco Nexus 9504 100-Gigabit fabric module for the Cisco Nexus 9504 switch with 100-Gigabit I/O modules	4
N9K-C9396PX	Cisco Nexus 9300 48-port, 1/10-Gigabit Ethernet SFP+ and 12-port, 40-Gigabit Ethernet QSPF switch	1
N9K-C9396TX	Cisco Nexus 9300 48-port, 1/10-Gigabit Ethernet BASE-T and 12-port, 40-Gigabit Ethernet QSFP switch	1
N9K-C9372PX	Cisco Nexus 9300 48-port, 1/10-Gigabit Ethernet SFP+ and 6-port, 40-Gigabit Ethernet QSFP switch	1
N9K-C9372PX-E	An enhanced version of the N9K-C9372PX.	
N9K-C9372TX	Cisco Nexus 9300 48-port, 1/10-Gigabit Ethernet BASE-T and 6-port, 40-Gigabit Ethernet QSFP switch	1

Product ID	Hardware	Quantity
N9K-C9372TX-E	An enhanced version of the N9K-C9372TX.	1
N9K-C9332PQ	Cisco Nexus 9300 32-port, 40-Gigabit Ethernet QSFP switch with support for 4x10G breakout mode ■ Ports 1 to 26 (except 13 and 14) support 4x10G breakout mode. ■ Ports 27 to 32 (ALE uplink ports) support using QSA for 10G SFP/SFP+ transceivers in QSFP+ ports	1
N9K-C93128TX	Cisco Nexus 9300 switch with 96 1-/10-Gigabit BASE-T ports and eight 40-Gigabit Ethernet QSPF ports (The 1-/10-Gigabit BASE-T ports also support a speed of 100 Megabits.)	1
N9K-C93120TX	Cisco Nexus 93120TX switch with 96 1-/10-Gigabit BASE-T ports and 6 QSFP uplink ports	1
N9K-PAC-650W	Cisco Nexus 9300 650 W AC power supply, hot air out (red) Note: For use with the Cisco Nexus 9396 switch (N9K-C9396PX).	2 or less
N9K-PAC-650W-B	Cisco Nexus 9300 650 W AC power supply, cold air in (blue) Note: For use with the Cisco Nexus 9396 switch (N9K-C9396PX).	2 or less
N9K-PAC-1200W	Cisco Nexus 9300 1200 W AC power supply, hot air out (red) Note: For use with the Cisco Nexus 93128 switch (N9K-C93128TX).	2 or less
N9K-PAC-1200W-B	Cisco Nexus 9300 1200 W AC power supply, cold air in (blue) Note: For use with the Cisco Nexus 93128 switch (N9K-C93128TX).	2 or less
N9K-C9300-FAN1	Cisco Nexus 9300 fan 1, hot air out (red) Note: For use with the Cisco Nexus 9396 switch (N9K-C9396PX).	3
N9K-C9300-FAN1-B	Cisco Nexus 9300 fan 1, cold air in (blue) Note: For use with the Cisco Nexus 9396 switch (N9K-C9396PX).	3
N9K-C9300-FAN2	Cisco Nexus 9300 fan 2, port side intake (red) Note: For use with the Cisco Nexus 93128 switch (N9K-C93128TX).	3
N9K-C9300-FAN2-B	Cisco Nexus 9300 fan 2, port side exhaust (blue) Note: For use with the Cisco Nexus 93128 switch (N9K-C93128TX).	3
NXA-FAN-30CFM-F	Cisco Nexus 9300 fan, port-side exhaust Note: For use with the Cisco Nexus 9332PQ, 9372PX, and 9372TX switches (N9K-C9332PQ, N9K-C9372PX, and N9K-9372TX).	4

Product ID	Hardware	Quantity
NXA-FAN-30CFM-B	Cisco Nexus 9300 fan, port-side intake Note: For use with the Cisco Nexus 9332PQ, 9372PX, and 9372TX switches (N9K-C9332PQ, N9K-C9372PX, and N9K-9372TX).	4
N9K-M12PQ	Cisco Nexus GEM 9300 uplink module, 12-port, 40-Gigabit Ethernet QSPF Note: The front-panel ports on these GEM modules do not support auto negotiation with copper cables. Manually configure the speed on the peer switch.	1 (required)
N9K-C9272Q	Cisco Nexus 9200 2 rack unit switch with 72 40-Gigabit QSFP+ ports. Up to 35 of the ports (ports 37-71) also support breakout cables providing up to 140 10-Gigabit ports.	1
N9K-C9236C	Cisco Nexus 9200 1 rack unit (RU) switch with 7.2 Tbps of bandwidth, 36 40-to 100-Gbps ports (144 10- to 25-Gb ports with breakout cable), choice of port-side intake or port-side exhaust airflow, 1+1 redundant and hot-swappable 80-Plus Platinum-certified power supplies, and built-in EtherAnalyzer for monitoring and troubleshooting control-plane traffic.	1
N9K-C92304QC	Cisco Nexus 9200 1 rack unit (RU) switch with 6.08 Tbps of bandwidth, 56 40-Gbps ports (16 of which can use breakout cables for 64 10-Gigabit connections) and 8 100-Gbps ports, choice of port-side intake or port-side exhaust airflow, 1+1 redundant and hot-swappable 80-Plus Platinum-certified power supplies, built-in EtherAnalyzer for monitoring and troubleshooting control-plane traffic.	1
N9K-C92160YC-X	Cisco Nexus 9200 1 rack unit switch with 48 10-/25-Gigabit SFP+ downlink ports and 6 QSFP+ uplink ports with 4 of the uplink ports capable of supporting QSFP28 transceivers (100-Gigabits).	1
N9K-M6PQ	Cisco Nexus GEM 6-port 40-Gigabit Ethernet uplink module for the Cisco Nexus 9396PX, 9396TX, and 93128TX switches Note: The front-panel ports on these GEM modules do not support auto negotiation with copper cables. Manually configure the speed on the peer switch.	1
N9K-M6PQ-E	An enhanced version of the N9K-M6PQ.	
N9K-M4PC-CFP2	Cisco Nexus 9300 uplink module for the 93128TX (2 active ports), 9396PX (4 active ports), and 9396TX (4 active ports) Top-of-rack switches	1

Table 4 lists the 3232C and 3264Q switch hardware that Cisco NX-OS Release 7.0(3)I4(1) supports.

Table 4 Cisco Nexus 3232C and 3264Q Switch Hardware

Product ID	Hardware	Quantity
N3K-C3232C	Cisco Nexus 3232C, 32 x 40G/100G 2 x 10G SFP+, 1-RU switch	1
N3K-C3264Q	Cisco Nexus 3264Q, 64 x 40G 2 x 10G SFP+, 2-RU switch	1

Table 5 lists the Cisco Nexus 3164Q switch hardware that Cisco NX-OS Release 7.0(3)I4(1) supports.

Table 5 Cisco Nexus 3164Q Switch Hardware

Product ID	Hardware	Quantity
N3K-C3164Q-40GE	Cisco Nexus 3164Q switch	1
N9K-C9300-FAN3	Cisco Nexus 3164Q fan module	3
N9K-PAC-1200W	Cisco Nexus 3164Q 1200W AC power supply	2

For additional information about the supported hardware, see the *Cisco Nexus 3000 Series Hardware Installation Guide*.

Table 6 lists the Cisco Nexus 31128PQ switch hardware that Cisco NX-OS Release 7.0(3)I4(1) supports.

Table 6 Cisco Nexus 31128PQ Switch Hardware

Product ID	Hardware	Quantity
N3K-C31128PQ-10GE	Nexus 31128PQ, 96 SFP+ ports, 8 QSFP+ ports, 2RU switch	1

Supported Optics

See the *Cisco 10-Gigabit Ethernet Transceiver Modules Compatibility Matrix* for a list of supported optical components.

Supported FEX Modules

Cisco NX-OS Release 7.0(3)I4(1) supports the following FEXes (Fabric extenders) on Cisco Nexus 9332PQ, 9372PX, 9372PX-E, 9396PX and 9500 platform Switches:

- Cisco Nexus 2224TP
- Cisco Nexus 2232PP

- Cisco Nexus 2232TM and 2232TM-E
- Cisco Nexus 2248PQ
- Cisco Nexus 2248TP and 2248TP-E
- Cisco Nexus 2348TQ
- Cisco Nexus 2348UPQ
- Cisco Nexus B22Dell
- Cisco Nexus B22HP
- Cisco Nexus NB22FTS
- Cisco Nexus NB22IBM

Note: Please note the following:

- The 9408 line card is not supported with the 2300 FEX.
- Cisco Nexus 9300 Series switches do not support FEX on uplink modules (ALE).
- For FEX HIF port channels, Cisco recommends that you enable STP port type edge using the spanning tree port type edge [trunk] command.
- The Cisco 2248PQ, 2348TQ, and 2348UPQ FEXes support connections to the Nexus 9300 or 9500 switches by using supported breakout cables to connect a QSFP+ uplink on the FEX and an SFP+ link on the parent switch (4x10G links).

  Note: For Cisco Nexus 9500 switches, 4x10G breakout for FEX connectivity is not supported.

New and Changed Information

This section lists the following topics:

- New Hardware Features in Cisco NX-OS Release 7.0(3)I4(1)
- New Software Features in Cisco NX-OS Release 7.0(3)I4(1)

New Hardware Features in Cisco NX-OS Release 7.0(3)I4(1)

Cisco NX-OS Release 7.0(3)I4(1) supports the following new hardware:

- Cisco Nexus 92304QC switch (N9K-C92304QC) – 1 rack unit (RU) switch with 6.08 Tbps of bandwidth, 56 40-Gbps ports and 8 100-Gbps ports, 64 10-Gb ports with a breakout cable, choice of port-side intake and port-side exhaust, 1+1 redundant and hot-swappable 80 Plus Platinum-certified power supplies, built-in EtherAnalyzer for monitoring and troubleshooting control-plane traffic.
- Cisco Nexus 9236C switch (N9K-C9236C) – 1 rack unit (RU) switch with 7.2 Tbps of bandwidth, 36 40 to 100-Gbps ports, 144 10 to 25-Gb ports with a breakout cable, the choice of port-side intake and port-side exhaust,

1+1 redundant and hot-swappable 80 Plus Platinum-certified power supplies, and built-in EtherAnalyzer for monitoring and troubleshooting control-plane traffic.

- Cisco Nexus 9504 100-Gigabit fabric module (N9K-C9504-FM-S) for the Cisco Nexus 9504 switch with 100-Gigabit I/O modules

New Software Features in Cisco NX-OS Release 7.0(3)I4(1)

Cisco NX-OS Release 7.0(3)I4(1) supports the following new software features:

FCoE Feature

- FCOE (Fiber Channel over Ethernet) over vPC–FCoE VLANs and virtual interfaces support. Includes support to shutdown LAN traffic on port-channels and individual Ethernet ports.

For more information see the *Cisco Nexus 9000 Series NX-OS FCOE Configuration Guide*.

FEX Feature

- FEX ISSU–Support for FEX ISSU.

For more information see the *Cisco Nexus 2000 Series NX-OS Fabric Extender Configuration Guide for Cisco Nexus 9000 Series Switches*.

Fundamentals Features

- POAP dynamic breakout – Dynamically breaks out ports in an effort to detect a DHCP (Dynamic Host Channel Protocol) server behind one of the broken-out ports. Previously, the DHCP server used for POAP (Power On Auto Provisioning) had to be directly connected to a normal cable because breakout cables were not supported.
- POAP personality – Enables user data, Cisco NX-OS and third-party patches, and configuration files to be backed up and restored. In previous releases, POAP can restore only the configuration.
- Variable support – Enables Cisco NX-OS CLI variables to contain hyphens and underscores.

For more information, see the *Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide*.

Interface Features

- Port profiles–Support for port profiles. Beginning with 7.0(3)I4(1) on Cisco Nexus 9300 Series switches, you can create a port profile that contains many interface commands and apply that port profile to a range of interfaces.
- Changing SVI's VRF membership without losing configuration–Support for changing VRF membership for an SVI. Enables the retention of the Layer 3 configuration when the VRF member changes on the interface.
- PIM SSM over vPCs –Support for PIM SSM over vPCs (Virtual Port Channels).
- NAT ISSU – NAT support for ISSU.

For more information, see the *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*.

Multicast Routing Features

- PIM SSM over vPCs – Enables support for IGMPv3 joins and PIM S,G joins over vPC peers in the SSM range. This configuration is supported for orphan sources or receivers in the Layer 2 or Layer 3 domain.

For more information, see the *Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide*.

Security Features

- AAA enhancement − Adds the ability to log successful and failed login attempts.
- ACL detailed logging cache − Enables ACE (access control entry) and ACL (Access Control List) information to be displayed in the output of the show logging ip access-list cache command.
- CoPP enhancement − Changed the police CIR rate range to start with 0 to initiate a packet drop.

For more information, see the *Cisco Nexus 9000 Series NX-OS Security Configuration Guide*.

Software Upgrade and Downgrade Features

- In-service software upgrade enhancements − Adds ISSU support for FEX, NAT, segment routing, and VXLAN. An ISSU from Cisco NX-OS Release 7.0(3)I4(1) to a later release is non-disruptive for these features.

For more information, see the *Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Gui*de.

System Management Features

- SNMP IPv6 ACL support − Adds the ability to assign an IPv6 ACL to an SNMPv2 community or SNMPv3 user to filter SNMP requests.
- SPAN (Switch Port Analyzer) and ERSPAN (Encapsulated Remote Switch Port Analyzer) enhancements:
  - Adds the ability to span forward packet drops in the ingress pipeline for Cisco Nexus 9200 Series switches.
  - Adds the set-erspan-gre-proto and set-erspan-dscp actions to the ERSPAN ACL for Cisco Nexus 9200 Series switches.
  - Adds support for UDF (User-Defined Field)-based ERSPAN and UDF-based SPAN for Cisco Nexus 9200 Series switches.
  - Adds support for the CPU as a SPAN destination for Cisco Nexus 9200 Series switches only.
  - Adds support for configuring the same source in multiple ACL SPAN sessions.
  - Adds support for multiple ACL filters on the same source through configuring the same source in multiple ACL SPAN sessions (for all platforms except the Cisco Nexus 9200).

For more information, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide.*

Unicast Routing Features

- Prefix list filter for odd and even routes − Adds mask support for IP prefix lists. The mask is used to define a range of possible contiguous or non-contiguous routes to be compared to the prefix address.
- RPM match for OSPF area ID − Adds the match ospf-area command to match the OSPFv2 or OSPFv3 area ID for route maps.

For more information, see the *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*.

Virtual Fiber Channel

- Binding vFC (Virtual Fibre Channel) interfaces to the member of a port-channel is now supported.

Note: Binding VFC interfaces to the member of a port-channel is not supported if the port-channel has more than one member.

VXLAN Feature

- VXLAN ISSU – Support for VXLAN ISSU.
- suppress mac-route –Support for suppress mac-route command. Suppresses the BGP (Border Gateway Protocol) MAC route so that BGP only sends the MAC/IP route for a host.

For more information, see the *Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide.*

Caveats

This section includes the following topics:

- Resolved Caveats–Cisco NX-OS Release 7.0(3)I4(1)
- Open Caveats–Cisco NX-OS Release 7.0(3)I4(1)
- Known Behaviors–Cisco NX-OS Release 7.0(3)I4(1)

Resolved Caveats–Cisco NX-OS Release 7.0(3)I4(1)

Table 7 lists the Resolved Caveats in Cisco NX-OS Release 7.0(3)I4(1). Click the bug ID to access the Bug Search tool and see additional information about the bug.

Table 7 Resolved Caveats in Cisco NX-OS Release 7.0(3)I4(1)

Bug ID	Description
CSCuq94938	Show commands may take a long time to execute or may fail altogether. Configuration changes may also not be successful.
CSCus68543	Need to collect all show logging onboard CLIs as part of show tech.
CSCus73649	LACP PDUs are not received by the CPU. As a result, port-channel members are suspended.
CSCut81131	Add a drop capability on the CoPP CLI to conform on Cisco Nexus 9000 Series switches.
CSCuu44280	The output displayed for **show cdp neighbor detail** stops abruptly.
CSCuu72899	Display multicast in show hardware internal forwarding table utilization.
CSCuu91089	Do not allow fast rate LACP for vPC peerlinks.
CSCux69836	RIPng neighborship will not come-up between peers when configured above the Ipv4 tunnel.
CSCux71824	In the Cisco Nexus 9932 multi-chassis switch, entPhysicalTable is missing container entities for fan modules on the FEX chassis. The defect affects the Prime Network's ability to correctly model and display physical inventory.

Bug ID	Description
CSCux85390	Need support for different ACLs on different ERSPAN (Encapsulated Remote Switch Port Analyzer) sessions.
CSCux98907	DV: Ethpm changes to handle the conversion from 4c to 2c mode.
CSCuy15922	Cisco Nexus 9504 does not display NTP access-group information with the show ntp access-groups command.
CSCuy16277	In a setup with VTEP over vPC (budnode), remote VTEPs receive duplicate copies for BUM traffic.
CSCuy28590	The Cisco 9000 Series switch does not respond to incoming ARP request when the request contains “Vlan tag 0.”
CSCuy50611	A link goes up when inserting SFP without cables.
CSCuy88266	Line card .bin files are loaded in /tmp and are not removed by the standby SUP.
CSCuz01843	VXLAN decap ICMP packets are classified to class-default instead of copp-class-monitoring.
CSCuz05365	A vulnerability in a configured loopback interface of the Cisco Nexus 9000 Series Switch could allow an unauthenticated remote attacker to access certain sensitive data. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to having certain TCP and UDP ports listening on the loopback interface which are not required. An attacker could exploit this vulnerability by connecting to the affected device on one of the exposed TCP or UDP ports. An exploit could allow the attacker to discover certain sensitive data which could be used to conduct further attacks.
CSCuz01934	When trying to get the output for show logging last xxx, "Internal error in displaying logfile -40540001\n" is returned in NXAPI.
CSCuz14950	Cisco Nexus 9372 switches do not respond to MST proposals and take time to forward.
CSCuz18908	ICMPv6 Neighbor Discovery between a Cisco Nexus 9000 Series switch and a neighboring IPv6 enabled device fails.
CSCuz25423	Interface ingress and egress rate counters fluctuate..
CSCuz12560	Upgrading to 7.0(3)I2(2c) displays “Incompatible image.”
CSCuz47463	After performing an ISSU, the VNI mode removes the MCT (Multichassis Etherchannel Trunk) port from the encap list for FEX VXLAN.
CSCuz67490	sFlow should be disabled on an ALE port channel before adding or removing a member of the port channel. Note: Disabling sFlow on one ALE uplink port could cause the rest of the sFlow-enabled ALE uplink ports to stop sampling. To work around this issue, disable and then re-enable sFlow on one of the other sFlow-enabled ALE uplink ports.

Open Caveats–Cisco NX-OS Release 7.0(3)I4(1)

Table 8 lists the open caveats in the Cisco NX-OS Release 7.0(3)I4(1). Click the bug ID to access the Bug Search tool and see additional information about the bug.

Table 8 Open Caveats in Cisco NX-OS Release 7.0(3)I4(1)

Bug ID	Description
CSCun26726	HSRP packet decoding fails with an assertion error.
CSCun34856	All VLANs are suspended if one has a QoS policy, but the TCAM is not configured.
CSCuq03168	Microsoft NLB traffic being routed into the destination VLAN is experiencing packet loss.
CSCur30555	The show policy-map type queuing command does not show statistics for FEX HIF interfaces.
CSCur37816	When QoS Lite TCAM is configured, policer violated statistics shown as part of the show policy-map interface command is reported as 0 instead of NA (Not-Applicable).
CSCur46879	When copying the tunnel configuration file to running, the tunnel may flap before stabilizing.
CSCur59482	Policer action is not supported when a QoS policy of type “qos” is applied with the no-stats keyword.
CSCur61647	Even though there are no QoS classification policies currently active on any of the FEX HIF interfaces, the show incompatibility command still reports FEX QoS incompatibility during downgrade from 3.2 to earlier versions of software.
CSCur87839	Traffic cannot be routed using policy-based routing if the next-hop reachability is across the vPC peer link and the local vPC leg is down.
CSCus06693	ERPSAN sessions with a destination on the port-channel sub-interface are not supported.

Bug ID	Description
CSCus07061	When a remote end of a vPC port channel member is shut down, the local end takes ~10 seconds to shut down. This only occurs when the port channel is 'active' (i.e., has LACP enabled).
CSCus58475	Vntag-mgr times out after changing VLANS for a range of 20 vPC port-channels.
CSCus63613	When a user reloads the active supervisor, the standby supervisor also reloads. During the reload process, the Service Policy Manager (SPM) cannot send data to the standby supervisor. A syslog is observed, notifying the active supervisor that the SPM has not successfully updated its data base to the standby supervisor. The active supervisor reloads the standby supervisor again, and the standby supervisor eventually reaches a good standby state.
CSCuu31392	ERSPAN packets are dropped on the intermediate switches if more than one ERSPAN session resolves over 40 Gig uplinks on a ToR.
CSCuu33640	An ITD policy is shown in no shut state. However, no policy is actually applied to the ingress policy if an invalid ACL is used for "exclude."
CSCuu87126	When access-list is configured for ITD service, this error is received: "ACL cannot apply when more than one node is active."
CSCuv04072	Using a port channel range command for pv mapping causes VLAN membership to not get programmed for all the member ports.
CSCuv90152	Packets are accepted on HIFPC members in suspended state.
CSCuv96382	For single label mpls/stripped tap-agg packets, when the mpls strip dest-mac xxxx.xxxx.xxxx CLI is configured, dmac is not re-written on the modular (EOR) setup. The same will work on ToRs.
CSCuv97661	A generic error occurs in response to many CLIs when volatile gets full.
CSCux15156	When policy-map is copied through qos copy policy-map, the newly created policy-map cannot be modified or deleted.

Bug ID	Description
CSCux36390	Not able to move FEX PO to base port.
CSCux39229	Multicast Bidir Protocol: If the SVI is designated as a router on the switch, and also happens to be a non-designated forwarder to the RP and for the traffic coming onto this SVI, bridged multicast traffic is not forwarded to the receivers on the SVI.
CSCux42376	Packets entering on NS-PO ports are encapped with inner dot1q.
CSCux52183	Install may fail with following message on Nexus 9500 switches if previous install attempts were terminated. sys03-eor1(config)# install all nxos bootflash:nxos.7.0.3.I2.2a.bin parallel Installer will perform compatibility check first. Please wait. Installer is forced disruptive Pre-upgrade check failed. Return code 0x40930062 (free space in the filesystem is below threshold). sys03-eor1(config)# sys03-eor1(config)#
CSCux68819	NAT CLI Command clear ip nat translation all takes more than 5 minutes in scale setup where number of nat translations are at the maximum limit 1023.
CSCuy08187	Cisco NX-OS Release 7.0(3)I3(1) is backwards compatible with EPLD versions of the previous NxOS releases. However, 7.0(3)I3(1) establishes base versions of Bios and EPLD images for non-disruptive upgrade to work. In 7.0(3)I3(1), when customer tries non-disruptive upgrade, the baseline EPLD version check is not enforced and the non-disruptive upgrades is allowed to proceed. This may result in customer experiencing issues with non-disruptive upgrades with symptoms like link down or traffic failures.
CSCuy90292	256K PV (Port VLAN): Need optimization for 64-ports with 4k VLANs.
CSCuz12723	switchport isolate 4k vlan - vpc peer reload takes 70 secs convergence.
CSCuz25770	Need to add a CLI that displays the PV count.

Bug ID	Description
CSCvc93246	Nexus 93108TC-EX stops RX/TX after negotiating down to 100Mbps in I4(1)

Known Behaviors–Cisco NX-OS Release 7.0(3)I4(1)

Table 9 lists the known behaviors in the Cisco NX-OS Release 7.0(3)I4(1). Click the bug ID to access the Bug Search tool and see additional information about the bug.

Table 9 Known Behaviors in Cisco NX-OS Release 7.0(3)I4(1)

Bug ID	Description
CSCvc95008	On Cisco Nexus 9300-EX switches, when 802.1q EtherType has changed on an interface, the EtherType of all interfaces on the same slice will be changed to the configured value. This change is not persistent after a reload of the switch and will revert to the EtherType value of the last port on the slice.
CSCuw64066	FET-40G transceivers show unreliable connectivity on Tomahawk-based systems.
CSCux24692	Routed ACLs will not match for packets with Multicast Ethernet MAC addresses as the destination.
CSCuy85644	VXLAN access and network ports have been added to the broadcast (BCAST) and multicast (MCAST) domains; this causes packets to flood on all VXLAN ports attached to the MCAST and BCAST domains, including the source port. However, packets are dropped on the egress of the source port. As a result, unknown unicast and broadcast traffic is incremented in the Out-Discard counter without affecting the Xmit-Err counter.

Upgrade and Downgrade

To perform a software upgrade or downgrade, follow the instructions in the *Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.x*.

For information about an In Service Software Upgrade (ISSU), see the Cisco NX-OS ISSU Support application.

Note: Upgrading from Cisco NX-OS 7.0(3)I1(2), 7.0(3)I1(3), or 7.0(3)I1(3a) requires installing a patch for Cisco Nexus 9500 platform switches only. For more information on the upgrade patch, see Upgrade Patch Instructions.

Limitations

This section lists limitations related to Cisco NX-OS Release 7.0(3)I4(1).

- In Cisco NX-OS Release 7.0(3)I4(1), resilient hashing (port-channel load-balancing resiliency) and VXLAN configurations are not compatible with VTEPs using ALE uplink ports. Please note that resilient hashing is disabled by default.
- Fast reload is not supported for any Cisco Nexus 3000 or 9000 Series switches starting with Cisco NX-OS Release 7.0(3)I4(1).
- CoPP (Control Plane Policing) cannot be disabled. If you attempt to disable it in Cisco NX-OS Release 7.0(3)I4(1), an error message appears. In previous releases, attempting to disable CoPP causes packets to be rate limited at 50 packets per seconds.
- Skip CoPP policy option has been removed from the Cisco NX-OS initial setup utility because using it can impact the control plane of the network.
- hardware profile front portmode command is not supported on the Cisco Nexus 9000 Series switches.
- PV (Port VLAN) configuration through an interface range is not supported.
- Layer 3 routed traffic for missing Layer 2 adjacency information is not flooded back onto VLAN members of ingress units when the source MAC address of routed traffic is a non-VDC (Virtual Device Context) MAC address. This limitation is for hardware flood traffic and can occur when the SVI (Switched Virtual Interface) has a user-configured MAC address.
- neighbor-down fib-accelerate command is supported in a BGP-only environment.
- Uplink modules should not be removed from a Cisco Nexus 9300 Series switch that is running Cisco NX-OS Release 7.0(3)I4(1). The ports on uplink modules should be used only for uplinks.
- PortLoopback and BootupPortLoopback tests are not supported.
- PFC (Priority Flow Control) and LLFC (Link-Level Flow Control) are supported for all Cisco Nexus 9300 and 9500 platform hardware except for the 100G 9408PC line card and the 100G M4PC generic expansion module (GEM).
- FEXes configured with 100/full-duplex speed, without explicitly configuring the neighboring device with 100/full-duplex speed, will not pass data packet traffic properly. This occurs with or without the link appearing to be “up.”
  - no speed–Auto negotiates and advertises all speeds (only full duplex).
  - speed 100–Does not auto negotiate; pause cannot be advertised. The peer must be set to not auto negotiate (only 100 Mbps full duplex is supported).
  - speed 1000–Auto negotiates and advertises pause (advertises only for 1000 Mbps full duplex).
- Eight QoS groups are supported only on modular platforms with the Cisco Nexus 9300 N9K-M4PC-CFP2 uplink module, and the following Cisco Nexus 9500 platform line cards:
  - N9K-X9432PQ
  - N9K-X9464PX
  - N9K-X9464TX

- N9K-X9636PQ

- Cisco NX-OS Release 7.0(3)|4(1) supports flooding for Microsoft Network Load Balancing (NLB) unicast mode on Cisco Nexus 9500 platform switches but not on Cisco Nexus 9300 Series switches. NLB is not supported in max-host system routing mode. NLB multicast mode is not supported on Cisco Nexus 9500 or 9300 Series switches.

Note: To work around the situation of Unicast NLB limitation, Cisco can statically hard code the *address resolution protocol* (*ARP*) and MAC address pointing to the correct interface. Please refer to bug ID CSCuq03168 in detail in the Open Caveats section.

- TCAM resources are not shared when:
  - Applying VACL (VLAN ACL) to multiple VLANs
  - Routed ACL (Access Control List) is applied to multiple SVIs in the egress direction
- Cisco Nexus 9000 Series switch hardware does not support range checks (layer 4 operators) in egress TCAM. Because of this, ACL/QoS policies with layer 4 operations-based classification need to be expanded to multiple entries in the egress TCAM. Egress TCAM space planning should take this limitation into account.
- Applying the same QoS policy and ACL on multiple interfaces requires applying the `qos-policy` with the `no-stats` option to share the label.
- Multiple port VLAN mappings configured on an interface during a rollback operation causes the rollback feature to fail.
- The following switches support QSFP+ with the QSA (QSFP to SFP/SFP+ Adapter) (40G to 10G QSA):
  - N9K-C93120TX
  - N9K-C93128TX
  - N9K-C9332PQ
  - N9K-C9372PX
  - N9K-C9372PX-E
  - N9K-C9372TX
  - N9K-C9396PX

Note: The Cisco Nexus 9300 support for the QSFP+ breakout has the following limitations:

- Only 10G can be supported using QSA on 40G uplink ports on Cisco Nexus 9300 switches in NX-OS.
- 1G with QSA is not supported.
- For the Cisco Nexus 9332PQ switch, all ports except 13-14 and 27-32 can support breakout
- All ports in the QSA speed group must operate at the same speed (see the configuration guide)

- The following switches support the breakout cable (40G ports to 4x10G ports):

  - N9K-C9332PQ
  - N9K-X9436PQ
  - N9K-X9536PQ

- Weighted ECMP (Equal-Cost Multi-Path) Nexus 3000 feature is not supported on the Cisco Nexus 9000 Series switch.
- Limitations for ALE (Application Link Engine) uplink ports are listed at the following URL:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/ale_ports/b_Limitations_for_ALE_Uplink_Ports_on_Cisco_Nexus_9000_Series_Switches.html

Guidelines and Limitations for Private VLANs

This section provides guidelines and limitations for configuring private VLANs.

- Configuring Private VLANs
- Secondary and Primary VLAN Configuration
- Private VLAN Port Configuration
- Limitations with Other Features

Configuring Private VLANs

Private VLANs have the following configuration guidelines and limitations:

- Private VLANs must be enabled before the device can apply the private VLAN functionality.
- VLAN interface feature must be enabled before the device can apply this functionality.
- VLAN network interfaces for all VLANs that you plan to configure as secondary VLANs should be shut down before being configured.
- When a static MAC is created on a regular VLAN, and then that VLAN is converted to a secondary VLAN, the Cisco NX-OS maintains the MAC that was configured on the secondary VLAN as the static MAC.
- Private VLANs support port modes as follows:
  - Community host
  - Isolated host
  - Isolated host trunk
  - Promiscuous
  - Promiscuous trunk
- When configuring PVLAN promiscuous or PVLAN isolated trunks, it is recommended to allow non-private VLANs in the list specified by the switchport private-vlan trunk allowed id command.
- Private VLANs are mapped or associated depending on the PVLAN trunk mode.

- Private VLANs support the following:
  - Layer 2 forwarding
  - PACLs (Port Access Control Lists)
  - Promiscuous trunk
  - PVLAN across switches through a regular trunk port
  - RACLs (Router Access Control Lists)
- Private VLANs support SVIs as follows:
  - HSRP (Hot Standby Router Protocol) on the primary SVI
  - Primary and secondary IPs on the SVI
  - SVI allowed only on primary VLANs
- Private VLANs support STP as follows:
  - MST (Multiple Spanning Tree)
  - RSTP (Rapid Spanning Tree Protocol)
- Private VLANs port mode is not supported on the following:
  - 40G interfaces of the Cisco Nexus C9396PX or Cisco Nexus C93128TX
  - Cisco Nexus 3164Q
- Private VLANs do not provide port mode support for the following:
  - Port channels
  - vPC (Virtual Port Channel) interfaces
- Private VLANs do not provide support on breakout.
- Private VLANs do not provide support for the following:
  - DHCP (Dynamic Host Channel Protocol) snooping
  - IP multicast or IGMP snooping
  - PVLAN QoS
  - SPAN (Switch Port Analyzer) when the source is a PVLAN VLAN
  - Tunnels
  - VACLs
  - VTP (VLAN Trunk Protocol)
  - VXLANs

- Shared interfaces cannot be configured to be part of a private VLAN. For more details, see the *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*.
- Configuring multiple isolated VLAN configurations per PVLAN group is allowed by the Cisco NX-OS CLI. However, such a configuration is not supported. A PVLAN group can have at most one isolated VLAN.

Secondary and Primary VLAN Configuration

Follow these guidelines when configuring secondary or primary VLANs in private VLANs:

- Default VLANs (VLAN1), or any of the internally allocated VLANs, cannot be configured as primary or secondary VLANs.
- VLAN configuration (config-vlan) mode must be used to configure private VLANs.
- Primary VLANs can have multiple isolated and community VLANs associated with it. An isolated or community VLAN can be associated with only one primary VLAN.
- Private VLANs provide host isolation at Layer 2. However, hosts can communicate with each other at Layer 3.
- PVLAN groups can have one isolated VLAN at most. Multiple isolated VLAN configurations per primary VLAN configurations are not supported.
- When a secondary VLAN is associated with the primary VLAN, the STP parameters of the primary VLAN, such as bridge priorities, are propagated to the secondary VLAN. However, STP parameters do not necessarily propagate to other devices. You should manually check the STP configuration to ensure that the spanning tree topologies for the primary, isolated, and community VLANs match exactly so that the VLANs can properly share the same forwarding database.
- For normal trunk ports, note the following:
  - Separate instances of STP exist for each VLAN in the private VLAN.
  - STP parameters for the primary and all secondary VLANs must match.
  - Primary and all associated secondary VLANs should be in the same MST instance.
- For non-trunking ports, STP is aware only of the primary VLAN for any private VLAN host port; STP runs only on the primary VLAN for all private VLAN ports.

Note: Cisco recommends that you enable BPDU Guard on all ports that you configure as a host port; do not enable this feature on promiscuous ports.

- Private VLAN promiscuous trunk ports allow you to configure a maximum of 16 private VLAN primary and secondary VLAN pairs on each promiscuous trunk port.
- For private VLAN isolated trunk ports, note the following:
  - You can configure a maximum of 16 private VLAN primary and secondary VLAN pairs on each isolated trunk port.
  - The native VLAN must be either a normal VLAN or a private VLAN secondary VLAN. You cannot configure a private VLAN primary port as the native VLAN for a private VLAN isolated trunk port.
- Downgrading a system that has private VLAN ports configured requires unconfiguring the ports.

- Before configuring a VLAN as a secondary VLAN, you must shut down the VLAN network interface for the secondary VLAN.

Private VLAN Port Configuration

Follow these guidelines when configuring private VLAN ports:

- Deleting a VLAN used in the private VLAN configuration causes private VLAN ports (promiscuous ports or host ports, not trunk ports) that are associated with the VLAN to become inactive.
- Layer 2 access ports that are assigned to the VLANs that you configure as primary, isolated, or community VLANs are inactive while the VLAN is part of the private VLAN configuration. Layer 2 trunk interfaces, which may carry private VLANs, are active and remain part of the STP database.
- Use only the private VLAN configuration commands to assign ports to primary, isolated, or community VLANs.

Limitations with Other Features

Consider these configuration limitations with other features when configuring private VLANs:

Note: In some cases, the configuration is accepted with no error messages, but the commands have no effect.

- After configuring the association between the primary and secondary VLANs and deleting the association, all static MAC addresses that were created on the primary VLANs remain on the primary VLAN only.
- After configuring the association between the primary and secondary VLANs:
  - Static MAC addresses for the secondary VLANs cannot be created.
  - Dynamic MAC addresses that learned the secondary VLANs are aged out.
- Destination SPAN ports cannot be isolated ports. However, a source SPAN port can be an isolated port.
- Ensure consistent PVLAN type, states, and configuration across vPC peers. There is currently no PVLAN consistency check for vPC. Inconsistent PVLAN configs across vPV peers may end up in incorrect forwarding and impacts.
- In private VLANs, STP controls only the primary VLAN.
- Private VLAN host or promiscuous ports cannot be SPAN destination ports.
- Private VLAN ports can be configured as SPAN source ports.
- vPC pairing between T2 and TH platforms is not recommended.

Note: See the *Cisco Nexus 9000 Series NX-OS Security Configuration Guide* for information on configuring static MAC addresses.

Unsupported Features

This section lists features that are not supported in the current release.

- VXLAN

- DHCP
- FEX
- Cisco Nexus 3232C and 3264Q Switches
- Cisco Nexus 9200 Series switches
- Cisco Nexus 9408 Line Card and 9300 Series Leaf Switches
- Other Unsupported Features

VXLAN

This section lists VXLAN features that are not supported.

- ACL and QoS for VXLAN traffic in the network-to-access direction are not supported.
- Consistency checkers are not supported for VXLAN tables.
- DHCP snooping and DAI features are not supported on VXLAN VLANs.
- IGMP snooping is not supported on VXLAN VLANs.
- Native VLANs for VXLAN are not supported. All traffic on VXLAN Layer 2 trunks needs to be tagged.
- QoS buffer-boost is not applicable for VXLAN traffic.
- QoS classification is not supported for VXLAN traffic in the network-to-access direction.
- Static MAC pointing to remote VTEP (VXLAN Tunnel End Point) is not supported with BGP EVPN (Ethernet VPN).
- TX SPAN (Switched Port Analyzer) for VXLAN traffic is not supported for the access-to-network direction.
- VXLAN routing and VXLAN Bud Nodes features on the 3164Q platform are not supported.

VXLAN ACL Limitations

The following ACL related features are not supported:

- Ingress RACL that is applied on an uplink Layer 3 interface that matches on the inner or outer payload in the network-to-access direction (decapsulated path).
- Egress RACL that is applied on an uplink Layer 3 interface that matches on the inner or outer payload in the access-to-network direction (encapsulated path).
- Egress VACL for decapsulated VXLAN traffic.

Note: Cisco recommends that you use a PACL or VACL on the access side to filter out traffic entering the overlay network.

DHCP

DHCP subnet broadcast is not supported.

FEX

- VTEP connected to FEX host interface ports is not supported.
- ASCII replay with FEX needs be done twice for HIF configurations to be applied. The second time should be done after the FEXs have come up.
- Cisco Nexus 9300 Series switches do not support FEX on uplink modules (ALE).
- FEX is supported only on the Cisco Nexus 9332PQ, 9372PX, 9372PX-E, 9396PX, and 9500 platform switches.
- FEX vPC is not supported between any model of FEX and the Nexus 9300 (TOR) and 9500 Switches (EOR) as the parent switches.
- IPSG (IP Source Guard) is not supported on FEX ports.

Cisco Nexus 3232C and 3264Q Switches

The following features are not supported for the Cisco Nexus 3232C and 3264Q switches:

- 3264PX and 3232C platforms do not support the PXE boot of the NXOS image from the loader.
- Automatic negotiation support for 25G and 50G ports on the Cisco Nexus 3232C switch
- Cisco Nexus 2000 Series Fabric Extenders (FEX)
- Cisco NX-OS to ACI conversion (The Cisco Nexus 3232C and 3264Q switches operate only in Cisco NX-OS mode.)
- DCBXP
- Designated router delay
- DHCP subnet broadcast is not supported
- Due to a Poodle vulnerability, SSLv3 is no longer supported
- FCoE NPV
- Intelligent Traffic Director (ITD)
- ISSU
- Policy-based routing (PBR)
- Port loopback tests
- Resilient hashing
- SPAN on CPU as destination
- Virtual port channel (vPC) peering between Cisco Nexus 3232C or 3264Q switches and Cisco Nexus 9300 Series switches or between Cisco Nexus 3232C or 3264Q switches and Cisco Nexus 3100 Series switches
- VXLAN

Cisco Nexus 9200 Series switches

The following features are not supported for the Cisco Nexus 9200 Series switches:

- 64-bit ALPM routing mode
- 9272PQ and 92160YC platforms do not support the PXE boot of the NXOS image from the loader.
- ACL filters to span subinterface traffic on the parent interface
- Cisco Nexus 2000 Series Fabric Extenders
- DCBXP for LLDP
- Egress port ACLs
- Egress QoS policer or marking
- FCoE NPV
- GRE v4 payload over v6 tunnels
- Intelligent Traffic Director
- IP length-based matches
- IPinIP on 92160
- ISSU
- Layer 2 Q-in-Q, due to a hardware limitation
- Micro-burst detection
- MTU (Multi Transmission Unit) checks for packets received with an MPLS header
- OpenFlow, due to a hardware limitation
- Packet-based statistics for traffic storm control (only byte-based statistics are supported)
- Policy-based routing
- PV routing for VXLAN
- PVLANs
- Q-in-VNI and Q-in-Q for VXLAN, due to a hardware limitation
- Resilient hashing for ECMP
- Resilient hashing for port-channel
- Rx SPAN for multicast if the SPAN source and destination are on the same slice and no forwarding interface is on the slicet
- sFlow
- Traffic storm control for copy-to-CPU packets
- Traffic storm control with unknown multicast traffic

- Tx SPAN for multicast, unknown multicast, and broadcast traffic
- VACL redirects for TAP aggregation

Cisco Nexus 9408 Line Card and 9300 Series Leaf Switches

The following features are not supported for the Cisco Nexus line card (N9K-X9408PC-CFP2) and Cisco Nexus 9300 Series leaf switches with generic expansion modules (N9K-M4PC-CFP2):

- Breakout ports
- Port-channel (No LACP)
- vPC
- MCT (Multichassis EtherChannel Trunk)
- FEX
- PTP (Precision Time Protocol)
- PFC/LLFC
- 802.3x
- PVLAN
- Storm Control
- VXLAN access port.
- SPAN destination/ERSPAN destination IP
- Shaping support on 100g port is limited
- Only support 40G flows

Other Unsupported Features

The following lists other features not supported in the current release:

- Cisco Nexus 9300 Series switches do not support the 64-bit ALPM routing mode.
- Due to a Poodle vulnerability, SSLv3 is no longer supported.
- IPSG is not supported on the following:
  - The last six 40G physical ports on the 9372PX, 9372TX, and 9332PQ switches
  - All 40G physical ports on the 9396PX, 9396TX, and 93128TX switches

Related Documentation

The entire Cisco Nexus 9000 Series NX-OS documentation set is available at the following URL:

http://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/tsd-products-support-series-home.html

The Cisco Nexus 3164Q Switch - Read Me First is available at the following URL:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3164/sw/6x/readme/b_Cisco_Nexus_3164Q_Switch_Read_Me_First.html

The Cisco Nexus 31128PQ Switch - Read Me First is available at the following URL:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus31128/sw/readme/b_Cisco_Nexus_31128PQ_Switch_Read_Me_First.html

New Documentation

This release does not include new documentation.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus9k-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Open a service request online at:

https://tools.cisco.com/ServiceRequestTool/create/launch.do

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

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)

Cisco Nexus 9000 Series NX-OS Release Notes, Release 7.0(3)I4(1)

© 2016-2020 Cisco Systems, Inc. All rights reserved.