Cisco Nexus 9000 Series NX-OS Release Notes, Release 7.0(3)I5(2)

This document describes the features, caveats, and limitations for Cisco NX-OS Release 7.0(3)I5(2) 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*.

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.
July 25, 2018	Added CSCuy08187 to the Open Caveats.
April 20, 2018	Added CSCvf40773 to the Open Caveats.
September 20, 2017	Moved CSCvc79642 to Resolved Caveats.
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).
August 9, 2017	Removed Intelligent Traffic Director from the Cisco Nexus 9200 and 9300-EX platform switches Unsupported section.
June 21, 2017	Added CSCve24965 to Open Caveats. Replaced X9564TX2 with X9464TX2.
May 12, 2017	Added Guidelines and Limitations for Fabric Extenders section.
May 11, 2017	Updated the Upgrade Instructions for ISSU.

Date	Description
April 6, 2017	Removed Cisco Plug-in for OpenFlow Compatibility Matrix table.
March 22, 2017	Updated the Unsupported Features section to remove 9300 from the FEX vPC item.
March 3, 2017	Removed “Ingress DROP_ACL_DROP is seen with Cisco Nexus 9272Q, 9236C and 92160YC-X Switches on an ASIC during congestion” from the Limitations section.
March 1, 2017	Removed “IGMP snooping is not supported on VXLAN VLANs” in the Unsupported Features section.
February 21, 2017	Added CSCvc90891 to the Open Caveats.
February 20, 2017	• Modified FEX Features section under New and Changed Information from 9000 Series switches to 9300 and 9300-EX Series switches. • Updated the Limitations section to include the N9K-X97160YC-EX line card to the supported breakout cable list.
February 16, 2017	Created the release notes for Release 7.0(3)I5(2).

Contents

Introduction 4
System Requirements 4
New and Changed Information 15
Caveats 19
Upgrade and Downgrade 23
Limitations 24
Guidelines and Limitations for Private VLANs 27
Guidelines and Limitations for Fabric Extenders 31
Unsupported Features 31
Related Documentation 36
Obtaining Documentation and Submitting a Service Request 37

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 Device Hardware
- Supported Optics
- Supported FEX Modules

Supported Device Hardware

The tables below list the Cisco Nexus 9000 Series hardware that Cisco NX-OS Release 7.0(3)I5(2) supports. For additional information about the supported hardware, see the *Hardware Installation Guide* for your Cisco Nexus 9000 Series device.

- Table 2 lists the Cisco Nexus 9000 Series fabric modules
- Table 3 lists the Cisco Nexus 9000 Series fans and fan trays
- Table 4 lists the Cisco Nexus 9000 Series line cards
- Table 5 lists the Cisco Nexus 9000 Series power supplies
- Table 6 lists the Cisco Nexus 9000 Series supervisor modules
- Table 7 lists the Cisco Nexus 9000 Series system controllers
- Table 8 lists the Cisco Nexus 9000 Series uplink modules
- Table 10 lists the 3232C and 3264Q switch hardware
- Table 11 lists the Cisco Nexus 3164Q switch hardware
- Table 12 lists the Cisco Nexus 31128PQ switch hardware

Table 2 Cisco Nexus 9000 Series Fabric Modules

Product ID	Hardware	Quantity

N9K-C9504-FM	Cisco Nexus 9504 40-Gigabit fabric module	3 to 6 depending on line cards
N9K-C9504-FM-E	100-Gigabit -E fabric module (for the Cisco Nexus 9504 chassis) that supports the 100-Gigabit (-EX) line cards. When used, there must be 4 of these fabric modules installed in fabric slots 22, 23, 24, and 26.	4
N9K-C9504-FM-S	100-Gigabit -S fabric module (for the Cisco Nexus 9504 chassis) that supports the 100-Gigabit (-S) line cards. When used, there must be 4 of these fabric modules installed in fabric slots 22, 23, 24, and 26.	4
N9K-C9508-FM	Cisco Nexus 9508 Series 40-Gigabit fabric module	3-6 depending on the line cards
N9K-C9508-FM-E	100-Gigabit -E fabric module (for the Cisco Nexus 9508 chassis) that supports the 100-Gigabit (-EX) line cards. When used, there must be 4 of these fabric modules installed in fabric slots 22, 23, 24, and 26.	4
N9K-C9508-FM-S	100-Gigabit -S fabric module (for the Cisco Nexus 9508 chassis) that supports the 100-Gigabit (-S) line cards. When used, there must be 4 of these fabric modules installed in fabric slots 22, 23, 24, and 26.	4
N9K-C9516-FM	Cisco Nexus 9500 platform 40-Gigabit fabric module	3-6 depending on the line cards

Table 3 Cisco Nexus 9000 Series Fans and Fan Trays

Product ID	Hardware	Quantity
N9K-C9300-FAN1	Cisco Nexus 9300 fan 1 module with port-side intake airflow (burgundy coloring) Note: Supports early versions of the Cisco Nexus 9396 switch (N9K-C9396PX).	3
N9K-C9300-FAN1-B	Cisco Nexus 9300 fan 1 module with port-side exhaust airflow (blue coloring) Note: Supports early versions of the Cisco Nexus 9396 switch (N9K-C9396PX).	3
N9K-C9300-FAN2	Cisco Nexus 9300 fan 2 module with port-side intake airflow (burgundy coloring) Note: Supports the Cisco Nexus 93128TX, 9396PX, and 9396TX switches.	3

N9K-C9300-FAN2-B	Cisco Nexus 9300 fan 2 module with port-side exhaust airflow (blue coloring) Note: Supports the Cisco Nexus 93128TX, 9396PX, and 9396TX switches.	3
N9K-C9300-FAN3	Cisco Nexus 9300 fan 2 module with port-side intake airflow (burgundy coloring) Note: Supports the Cisco Nexus 93120TX, 92304QC, and 9272Q switches.	2
N9K-C9300-FAN3-B	Cisco Nexus 9300 fan 2 module with port-side exhaust airflow (blue coloring) Note: Supports the Cisco Nexus 93120TX, 92304QC, and 9272Q switches.	2
N9K-C9504-FAN	Cisco Nexus 9504 fan tray	3
N9K-C9508-FAN	Cisco Nexus 9508 fan tray	3
NXA-FAN-30CFM-B	Cisco Nexus 9200 and 9300 fan module with port-side intake airflow (burgundy coloring) Note: Supports the Cisco Nexus 92160YC-X, 9236C, 93108TC-EX, 93180YC-EX, 9332PQ, 9372PX, 9372PX-E, 9372TX, and 9372TX-E switches.	4
NXA-FAN-30CFM-F	Cisco Nexus 9200 and 9300 fan module with port-side exhaust airflow (blue coloring) Note: Supports the Cisco Nexus 92160YC-X, 9236C, 93108TC-EX, 93180YC-EX, 9332PQ, 9372PX, 9372PX-E, 9372TX, and 9372TX-E switches.	4

Table 4 Cisco Nexus 9500 Platform Line Cards

Product ID	Description	Quantity

Product ID	Description	Quantity
N9K-X9408PC-CFP2	Line card with 8 100-Gigabit CFP2 ports (supported by 40-Gigabit fabric modules [N9K-C9504-FM, N9K-C9508-FM, and N9K-9516FM])	▪ 4 (Cisco Nexus 9504) ▪ 8 (Cisco Nexus 9508) ▪ 16 (Cisco Nexus 9516)
N9K-X9432C-S	Line card with 32 100-Gigabit QSFP28 ports (supported by four 100-Gigabit –S fabric modules [N9K-C9504-FM-S and N9K-C9508-FM-S])	▪ 4 (Cisco Nexus 9504) ▪ 8 (Cisco Nexus 9508)
N9K-X9432PQ	Line card with 32 40-Gigabit QSFP+ ports (supported by 40-Gigabit fabric modules [N9K-C9504-FM, N9K-C9508-FM, and N9K-9516FM]) Note: This line card supports static breakout.	▪ 4 (Cisco Nexus 9504) ▪ 8 (Cisco Nexus 9508) ▪ 16 (Cisco Nexus 9516)
N9K-X9464PX	Line card with 48 10-Gigabit SFP+ ports and 4 40-Gigabit QSFP+ ports (supported by 40-Gigabit fabric modules [N9K-C9504-FM, N9K-C9508-FM, and N9K-9516FM])	▪ 4 (Cisco Nexus 9504) ▪ 8 (Cisco Nexus 9508) ▪ 16 (Cisco Nexus 9516)
N9K-X9464TX	Line card with 48 10GBASE-T ports and 4 40-Gigabit QSFP+ ports (supported by 40-Gigabit fabric modules [N9K-C9504-FM, N9K-C9508-FM, and N9K-9516FM])	▪ 4 (Cisco Nexus 9504) ▪ 8 (Cisco Nexus 9508) ▪ 16 (Cisco Nexus 9516)
N9K- X9464TX2	Line card with 48 1-/10GBASE-T ports and 4 40-Gigabit QSFP+ ports (supported by 40-Gigabit fabric modules [N9K-C9504-FM, N9K-C9508-FM, and N9K-9516FM])	▪ 4 (Cisco Nexus 9504) ▪ 8 (Cisco Nexus 9508) ▪ 16 (Cisco Nexus 9516)

Product ID	Description	Quantity
N9K-X9536PQ	Line card with 36 40-Gigabit Ethernet QSFP+ ports (supported by 40-Gigabit fabric modules [N9K-C9504-FM, N9K-C9508-FM, and N9K-9516FM])	■ 4 (Cisco Nexus 9504) ■ 8 (Cisco Nexus 9508) ■ 16 (Cisco Nexus 9516)
N9K-X9564PX	Line card with 48 1-/10-Gigabit SFP+ ports and 4 40-Gigabit QSFP+ ports (supported by 40-Gigabit fabric modules [N9K-C9504-FM, N9K-C9508-FM, and N9K-9516FM])	■ 4 (Cisco Nexus 9504) ■ 8 (Cisco Nexus 9508) ■ 16 (Cisco Nexus 9516)
N9K-X9564TX	Line card with 48 1-/10-GBASE-T ports and 4 40-Gigabit QSFP+ ports (supported by 40-Gigabit fabric modules [N9K-C9504-FM, N9K-C9508-FM, and N9K-9516FM])	■ 4 (Cisco Nexus 9504) ■ 8 (Cisco Nexus 9508) ■ 16 (Cisco Nexus 9516)
N9K-X9636PQ	Line card with 36 40-Gigabit QSFP+ ports (supported by 40-Gigabit fabric modules [N9K-C9504-FM and N9K-C9508-FM]) Note: Not supported on the Cisco Nexus 9516 switch (N9K-C9516).	■ 4 (Cisco Nexus 9504) ■ 8 (Cisco Nexus 9508)
N9K-X9732C-EX	Line card with 32 40-/100-Gigabit Ethernet QSFP28 ports (supported by 100-Gigabit –E fabric modules [N9K-C9504-FM-E and N9K-C9508-FM-E])	■ 4 (Cisco Nexus 9504) ■ 8 (Cisco Nexus 9508)
N9K-X97160YC-EX	Line card with 48 10/25 Gigabit Ethernet SFP28 ports, 4 40/100 Gigabit Ethernet QSFP28 ports supported by the Cisco Nexus 9504 and 9508 modular switches.	■ 4 (Cisco Nexus 9504) ■ 8 (Cisco Nexus 9508)

Table 5 Cisco Nexus 9000 Series Power Supplies

Product ID	Hardware	Quantity
N9K-PAC-650W	650-W AC power supply, port-side intake airflow (burgundy coloring) Note: Supports the Cisco Nexus 9332PQ, 9372PX, 9372PX-E, 9372TX, 9372TX-E, 9396PX, and 9396TX switches.	■ 2
N9K-PAC-650W-B	650-W AC power supply, port-side exhaust airflow (blue coloring) Note: Supports the Cisco Nexus 9332PQ, 9372PX, 9372PX-E, 9372TX, 9372TX-E, 9396PX, and 9396TX switches.	■ 2
N9K-PAC-1200W	1200-W AC power supply, port-side intake airflow (burgundy coloring) Note: Supports the Cisco Nexus 93120TX switches.	■ 2
N9K-PAC-1200W-B	1200-W AC power supply, port-side exhaust airflow (blue coloring) Note: Supports the Cisco Nexus 93120TX switches.	■ 2
N9K-PAC-3000W-B	3000-W AC power supply Note: Supports the Cisco Nexus 9504, 9508, and 9516 switches.	■ Up to 4 (Cisco Nexus 9504) ■ Up to 8 (Cisco Nexus 9508) ■ Up to 10 (Cisco Nexus 9516)
N9K-PDC-3000W-B	3000-W DC power supply Note: Supports the Cisco Nexus 9504, 9508, and 9516 switches.	■ Up to 4 (Cisco Nexus 9504) ■ Up to 8 (Cisco Nexus 9508) ■ Up to 10 (Cisco Nexus 9516)
N9K-PUV-1200W	1200-W AC power supply (airflow direction determined by the installed fan modules) Note: Supports all of the Cisco Nexus 9200 and 9300 NX-OS mode switches.	2

N9K-PUV-3000W-B	3000-W Universal AC/DC power supply	■ Up to 4 (Cisco Nexus 9504) ■ Up to 8 (Cisco Nexus 9508) ■ Up to 10 (Cisco Nexus 9516)
NXA-PAC-1200W	1200 W AC power supply, port-side intake airflow (burgundy coloring) Note: Supports the Cisco Nexus 9272Q switches.	2
NXA-PAC-1200W-B	1200 W AC power supply, port-side exhaust airflow (blue coloring) Note: Supports the Cisco Nexus 9272Q switches.	2
NXA-PAC-650W	Cisco Nexus 9200 and 9300 650 W AC power supply (NEBS compliant), port-side intake airflow (burgundy coloring) Note: Supports the Cisco Nexus 92160YC-X, 92304QC, 9236C, 93108TC-EX, and 93180YC-EX switches.	2
NXA-PAC-650W-B	Cisco Nexus 9200 and 9300 650 W AC power supply (NEBS compliant), port-side exhaust airflow (blue coloring) Note: Supports the Cisco Nexus 92160YC-X, 92304QC, 9236C, 93108TC-EX, and 93180YC-EX switches.	2
UCSC-PSU-930WDC	930-W DC power supply with port-side intake airflow Note: Supports all Cisco Nexus 9200 and 9300 NX-OS mode switches.	2
UCS-PSU-6332-DC	930-W DC power supply with port-side exhaust airflow Note: Supports all Cisco Nexus 9200 and 9300 NX-OS mode switches.	2

Table 6 Cisco Nexus 9500 Platform Supervisor Modules

Product ID	Hardware	Quantity
N9K-SUP-A	Cisco Nexus 9500 platform supervisor A module with 4 cores	2
N9K-SUP-B	Cisco Nexus 9500 platform supervisor B module with 6 cores	2

Table 7 Cisco Nexus 9000 Series Switches

Product ID	Description	Quantity
N9K-C9236C	Cisco Nexus 9236C 1-RU switch with 36 40-/100-Gigabit QSFP28 ports (144 10-/25-Gigabit ports when using breakout cables). Note: • Beginning with Cisco NX-OS Release 7.0(3)I4(3), 25G CVR-2QSFP28-8SFP adapters are supported on the Cisco Nexus 9236C switches. • Beginning with Cisco NX-OS Release 7.0(3)I5(1), the switch supports 4x10G breakout cables.	1
N9K-C9272Q	Cisco Nexus 9272Q 2-RU switch with 72 40-Gigabit Ethernet QSFP+ ports (up to 35 of the ports [ports 37-71] also support breakout cables providing up to 140 10-Gigabit connections)	1
N9K-C9332PQ	Cisco Nexus 9332PQ 1-RU switch with 32 40-Gigabit Ethernet QSFP+ ports and supports 4x10G breakout mode for ports 1 to 26 (except ports 13 and 14). Ports 27 to 32 (ALE uplink ports) support using the QSFP-to-SFP+ Adapter (QSA) for 10-Gigabit SFP/SFP+ transceivers in QSFP+ ports.	1
N9K-C9372PX	Cisco Nexus 9372PX 1-RU switch with 48 1-/10-Gigabit Ethernet SFP+ ports and 6 40-Gigabit Ethernet QSFP+ ports.	1
N9K-C9372PX-E	An enhanced version of the N9K-C9372PX switch.	1
N9K-C9372TX	Cisco Nexus 9372TX 1-RU switch with 48 1/10GBASE-T ports and 6 40-Gigabit Ethernet QSFP+ ports.	1
N9K-C9372TX-E	An enhanced version of the N9K-C9372TX switch.	1
N9K-C9396PX	Cisco Nexus 9396PX 1-RU switch with 48 1-/10-Gigabit Ethernet SFP+ ports and an uplink module with up to 12 40-Gigabit Ethernet QSPF+ ports	1
N9K-C9396TX	Cisco Nexus 9396TX 1-RU switch with 48 1/10GBASE-T and an uplink module with up to12 40-Gigabit Ethernet QSFP+ ports	1

N9K-C9504	Cisco Nexus 9504 4-slot modular switch	1
N9K-C9508	Cisco Nexus 9508 8-slot modular switch	1
N9K-C9516	Cisco Nexus 9516 16-slot modular switch	1
N9K-C92160YC-X	Cisco Nexus 92160YC-X 1-RU switch with 48 10-/25-Gigabit SFP+ ports and 6 40-Gigabit QSFP+ ports (4 of these ports support 100-Gigabit QSFP28 optics).	1
N9K-C92304QC	Cisco Nexus 92304QC 2-RU switch with 56 40-Gigabit Ethernet ports (64 10-Gigabit ports if using breakout cables) and 8 100-Gigabit ports.	1
N9K-C93108TC-EX	Cisco Nexus 93108TC-EX 1-RU switch with 48 10GBASE-T ports and 6 40/100-Gigabit QSFP28 ports. Note: The 40-Gigabit ports support 1/10-Gigabit Ethernet with SFP/SFP+ transceivers when used with a CVR-QSFP-SFP10G adapter.	N9K-C93108TC-EX
N9K-C93120TX	Cisco Nexus 93120TX 2RU switch with 96 1/10GBASE-T ports and 6 40-Gigabit QSFP+ uplink ports.	1
N9K-C93128TX	Cisco Nexus 93128TX 3-RU switch with 96 1/10GBASE-T ports and an uplink module that supports up to 8 40-Gigabit Ethernet QSPF+ ports (the 1/10GBASE-T ports also support a speed of 100 Megabits per second.)	1
N9K-C93180YC-EX	Cisco Nexus 93180YC-EX 1-RU switch with 48 10-/25-Gigabit Ethernet ports and 6 40/100-Gigabit QSFP28 ports. Note: The 40-Gigabit ports support 1/10-Gigabit Ethernet with SFP/SFP+ transceivers when used with a CVR-QSFP-SFP10G adapter.	1

Table 8 Cisco Nexus 9000 Series Uplink Modules

Product ID	Hardware	Quantity
N9K-M4PC-CFP2	Cisco Nexus 9300 uplink module with 4 100-Gigabit Ethernet CFP2 ports. For the Cisco Nexus 93128TX switch, only two of the ports are active. For the Cisco Nexus 9396PX and 9396TX switches, all four ports are active.	1

N9K-M6PQ	Cisco Nexus 9300 uplink module with 6 40-Gigabit Ethernet QSFP+ ports for the Cisco Nexus 9396PX, 9396TX, and 93128TX switches. Note: The front-panel ports on these uplink modules do not support auto negotiation with copper cables. You can manually configure the speed on the peer switch.	1
N9K-M6PQ-E	An enhanced version of the Cisco Nexus N9K-M6PQ uplink module.	
N9K-M12PQ	Cisco Nexus 9300 uplink module with 12 40-Gigabit Ethernet QSPF+ ports. Note: The front-panel ports on these uplink modules do not support auto negotiation with copper cables. You can manually configure the speed on the peer switch.	1 (required)

Table 9 Cisco Nexus 9500 Platform System Controller

Product ID	Hardware	Quantity
N9K-SC-A	Cisco Nexus 9500 Platform System Controller Module	2

Table 10 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 Note: The 40-Gigabit ports support 1/10-Gigabit Ethernet with SFP/SFP+ transceivers when used with a CVR-QSFP-SFP10G adapter.	1
N3K-C3264Q	Cisco Nexus 3264Q, 64 x 40G 2 x 10G SFP+, 2-RU switch Note: The 40-Gigabit ports support 1/10-Gigabit Ethernet with SFP/SFP+ transceivers when used with a CVR-QSFP-SFP10G adapter.	1

Note: Beginning with Cisco NX-OS Release 7.0(3)I4(3), 25G CVR-2QSFP28-8SFP is supported on the Cisco Nexus 3232C switches.

Table 11 Cisco Nexus 3164Q Switch Hardware

Product ID	Hardware	Quantity
N3K-C3164Q-40GE	Cisco Nexus 3164Q, 64 x 40G SFP+, 2-RU switch	1
N9K-C9300-FAN3	Cisco Nexus 3164Q fan module	3
N9K-PAC-1200W	Cisco Nexus 3164Q 1200W AC power supply	2

Table 12 Cisco Nexus 31128PQ Switch Hardware

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

Note: The Cisco Nexus M6PQ-E uplink module and the Cisco Nexus 9372PX-E and 9372TX-E switches need to run the following minimum Cisco NX-OS releases:

- 7.0(3)I2(2d)
- 7.0(3)I2(2e)
- 7.0(3)I3(2)
- 7.0(3)I4(1)

Supported Optics

To determine which transceivers and cables are supported by this switch, see http://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html.
To see the transceiver specifications and installation information, see http://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-installation-guides-list.html.

Supported FEX Modules

Cisco NX-OS Release 7.0(3)I5(2) supports the following FEXes (Fabric extenders) on 93180YC-EX, 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 and 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, we recommend 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)I5(2)
- New Software Features in Cisco NX-OS Release 7.0(3)I5(2)

New Hardware Features in Cisco NX-OS Release 7.0(3)I5(2)

Cisco NX-OS Release 7.0(3)I5(2) supports the following new hardware:

- 48-port 10/25-Gigabit Ethernet SFP28 and 4-port 40/100-Gigabit Ethernet QSFP28 line card (N9K–X97160YC-EX), which is supported by the Cisco Nexus 9504 and 9508 modular switches.

New Software Features in Cisco NX-OS Release 7.0(3)I5(2)

Cisco NX-OS Release 7.0(3)I5(2) supports the following new software features:

ACL Features

- Cisco Tetration Analytics filtering support has been added for N9K-C93180YC-EX and N9K-C92160YC-X.
- New NX-API REST commands have been added.

For more information, see the Cisco Nexus 3000 and 9000 Series NX-API REST SDK User Guide and API Reference.

FCoE Features

- FCoE-NPV–Added support for N9K-X9732C-EX line cards.

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

FEX Features

- FEX–Added Layer 3 FEX port-channel support for Cisco Nexus 9300 Series switches.
- Each FEX is dual-homed with two Cisco Nexus 9300 and Nexus 9300-EX Series switches. The FEX fabric interfaces for each FEX are configured as vPCs on both peer switches, and the host interfaces on the FEX appear on both peer switches.

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

- New NX-API REST commands have been added.

For more information, see the *Cisco Nexus 3000 and 9000 Series NX-AP REST SDK User Guide and API Reference*.

Interfaces Features

- Port profiles are supported on Cisco Nexus 9500 platform switches.
- You can use a QSFP-to-SFP adapter on Cisco Nexus 9200 and 9300-EX Series switches and Cisco Nexus 3232C and 3264Q Series switches.

For more information, see the *Cisco Nexus 2000 Series NX-OS Interfaces Configuration Guide.*

Label Switching Features

- MPLS label stack imposition–Enables an outgoing label stack with one or more labels to be statically provisioned. This feature is supported for all Cisco Nexus 9000 Series switches and the Cisco Nexus 3164Q, 31128PQ, 3232C, and 3264Q switches.

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

Layer 2 Switching Features

- PVLAN-Added PVLAN support over vPNs and port channels for Cisco Nexus 9500 platform switches.

Multicast Routing Features

- Protocol Independent Multicast (PIM)–Added PIM sparse mode support for Layer 3 port-channel subinterfaces on Cisco Nexus 9300 Series switches.

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

NX-OSv 9000 Features

- Cisco Virtual Appliance Configuration (CVAC)–Introduced this out-of-band configuration mechanism, which is similar to the POAP autoconfiguration. However, instead of downloading the configuration across the network as POAP does, CVAC receives the configuration injected into the Cisco NX-OSv 9000 environment on a CD-ROM.
- KVM/QEMU hypervisor–Added support for KVM/QEMU environment networking.
- vNICs–Increased support from 9 to 64 data port interfaces.

For more information, see the *Cisco NX-OSv 9000 Guide.*

QoS Features

- The global CLI hardware qos classify ns-only command is introduced to enable configuration of the QoS policy on the NS ports without carving the T2 QoS region, for example, qos and l3-qos regions. This command is only supported on Cisco Nexus 9000 Series switches with Application Leaf Engine (ALE). Policing and marking are not supported on the NS ports if this CLI command is used..

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

- New NX-API REST commands have been added.

For more information, see the *Cisco Nexus 3000 and 9000 Series NX-AP REST SDK User Guide and API Reference*.

Security Features

- DHCP relay–Introduced the ip dhcp relay sub-option circuit-id format-type string command to configure Option 82 to use encoded string format instead of the default binary ifindex format. This feature is supported for all Cisco Nexus 9000 Series switches and the Cisco Nexus 3164Q, 31128PQ, 3232C, and 3264Q switches.
- IPv4 ACLs–Added support for user-defined filtering (UDF)-based port ACLs on Cisco Nexus 9200, 9300, and 9300-EX Series switches.
- IPv6 router advertisement (RA) guard–Drops all incoming IPv6 RA packets on a Layer 2 interface. This feature is supported for the Cisco Nexus 9200, 9300, and 9300-EX Series switches and the N9K-X9732C-EX line card.

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

System Management Features

- ERSPAN and SPAN–Added Tx broadcast and multicast support for Layer 2 port sources on Cisco Nexus 9300-EX Series switches and the Cisco Nexus N9K-X9732C-EX line card. These features are not supported for Layer 3 port sources, FEX sources with non-unicast traffic, and VLAN sources.
- UDF-based TAP aggregation–Adds the ability to apply a TAP aggregation policy to an IPv4 ACL with UDF-based match for Cisco Nexus 9200, 9300, and 9300-EX Series switches.

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

Cisco Tetration Analytics Features

- Selective flow monitoring capability on Cisco Nexus N9K-C92160YC-X, N9K-93180YC-EX, and N9K-C93108TC-EX switches.

For more information, see http://www.cisco.com/c/en/us/support/data-center-analytics/tetration-analytics/tsd-products-support-series-home.html

Unicast Routing Features

- BGP Monitoring Protocol (BMP)–Monitors BGP updates and peer statistics. BMP is supported for all Cisco Nexus 9000 Series switches and the Cisco Nexus 3164Q, 31128PQ, 3232C, and 3264Q switches.

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

VXLAN Features

- Configuring FHRP over VXLAN is supported on the Cisco Nexus 9200, 9300, and 9300-EX Series switches.

- VXLAN EVPN multihoming is supported on cisco Nexus 9300 Series switches only. Cisco Nexus platforms support vPC-based multihoming, where a pair of switches act as a single device for redundancy and both switches function in an active mode. Cisco NX-OS allows either vPC based EVPN multihoming or ESI based EVPN multihoming. Both features should not be enabled together. ESI based multihoming is enabled using the evpn esi multihoming CLI command.

  NOTE: The command for ESI multihoming enables the Ethernet-segment configurations and generation of Ethernet-segment routes on the switches.

  The receipt of Type-1 and Type-2 routes with valid ESI and the path-list resolution are not tied to the evpn esi multihoming command. If the switch receives MAC/MAC-IP routes with a valid ESI and the command is not enabled, the ES based path resolution logic still applies to these remote routes. It is required for interoperability between the vPC-enabled switches and the ESI enabled switches.
  ARP suppression and VLAN consistency checking with EVPN multihoming are supported on Cisco Nexus 9300 Series switches only.

  New Sub-features:

  - L2 Gateway STP and EVPN ESI MH-EVPN multihoming is supported with the Layer 2 Gateway Spanning Tree Protocol (L2G-STP). The Layer 2 Gateway Spanning Tree Protocol (L2G-STP) builds a loop-free tree topology. However, the Spanning Tree Protocol root must always be in the VXLAN fabric.

    The Layer 2 Gateway Spanning Tree Protocol (L2G-STP) is disabled by default on EVPN ESI multihoming VLANs. Use the spanning-tree mode <rapid-pvst, mst> CLI command to enable it on all VTEPs. With L2G-STP enabled, the VXLAN fabric (all VTEPs) emulates a single pseudo root switch for the customer access switches. The L2G-STP is initiated to run on all VXLAN VLANs by default on boot up and the root is fixed on the overlay. With L2G-STP, the root-guard gets enabled by default on all the access ports.
  - ARP suppression and EVPN ESI MH- ESI ARP suppression is an extension of already available ARP suppression solution in VXLAN-EVPN. This feature is supported on top of ESI multihoming solution, that is on top of VXLAN-EVPN solution. ARP suppression is an optimization on top of BGP-EVPN multihoming solution. ARP broadcast is one of the most significant part of broadcast traffic in data centers. ARP suppression significantly cuts down on ARP broadcast in the data center.

    ARP request from host is normally flooded in the VLAN. You can optimize flooding by maintaining an ARP cache locally on the access switch. ARP cache is maintained by the ARP module. ARP cache is populated by snooping all the ARP packets from the access or server side. Initial ARP requests are broadcasted to all the sites. Subsequent ARP requests are suppressed at the first hop leaf and they are answered locally. In this way, the ARP traffic across overlay can be significantly reduced.

    ARP suppression is only supported with BGP-EVPN (distributed gateway). ESI ARP suppression is a per-VNI (L2-VNI) feature. ESI ARP suppression is supported in both L2 (no SVI) and L3 modes. Beginning with Cisco NX-OS Release 7.0(3)I5(2), only L3 mode is supported.

  - ESI VLAN CC and EVPN ESI MH- In a typical multihoming deployment scenario, host 1 belonging to VLAN X sends traffic to the access switch and then the access switch sends the traffic to both the uplinks towards VTEP1 and VTEP2. The access switch does not have the information about VLAN X configuration on VTEP1 and VTEP2. VLAN X configuration mismatch on VTEP1 or VTEP2 results in a partial traffic loss for host 1. VLAN consistency checking helps to detect such configuration mismatch.

For VLAN consistency checking, CFSoIP is used. Cisco Fabric Services (CFS) provides a common infrastructure to exchange the data across the switches in the same network. CFS has the ability to discover CFS capable switches in the network and to discover the feature capabilities in all the CFS capable switches. You can use CFS over IP (CFSoIP) to distribute and synchronize a configuration on one Cisco device or with all other Cisco devices in your network.

CFSoIP uses multicast to discover all the peers in the management IP network. For EVPN multihoming VLAN consistency checking, it is recommended to override the default CFS multicast address with the cfs ipv4 mcast-address <mcast address> CLI command. To enable CFSoIP, the cfs ipv4 distribute CLI command should be used.

- VXLAN selective Q-in-VNI is supported on Cisco Nexus 9300-EX Series switches. Selective Q-in-VNI is a VXLAN tunneling feature that allows a user specific range of customer VLANs on a port to be associated with one specific provider VLAN. Packets that come in with a VLAN tag that matches any of the configured customer VLANs on the port are tunneled across the VXLAN fabric using the properties of the service provider VNI.

  Selective Q-in-VNI is supported on both vPC and non-vPC ports on Cisco Nexus 9300-EX Series switches. This feature is also supported with flood and learn.

- VXLAN IGMP snooping is supported on Cisco Nexus 9300 Series switches and Cisco Nexus 9500 platform switches with N9K-X9732C-EX line cards.
- Configuring FHRP over VXLAN is supported on the Cisco Nexus 9200, 9300, and 9300-EX Series switches.

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)I5(2)
- Open Caveats—Cisco NX-OS Release 7.0(3)I5(2)
- Known Behaviors—Cisco NX-OS Release 7.0(3)I5(2)

Resolved Caveats—Cisco NX-OS Release 7.0(3)I5(2)

Table 13 lists the Resolved Caveats in Cisco NX-OS Release 7.0(3)I5(2). Click the bug ID to access the Bug Search tool and see additional information about the bug.

Table 13 Resolved Caveats in Cisco NX-OS Release 7.0(3)I5(2)

Bug ID	Description
CSCvb04193	N9000 acl redirect does not work between uplink ports
CSCvb44301	pimNeighborLoss trap send with reverse IP in trap varbind
CSCvb52582	N9K-C93108TC-EX MAC speed mismatch between ingress and egress ports can lead to Underrun/CRC errors.

CSCvb63195	Python broken with Cisco SSL
CSCvb75526	peer adj pointing to 0xfffff though route is present in RIB
CSCvb78782	Switchport flag not set in kernel for port-channel
CSCvb81335	DHCP packets punted to CPU when feature is disabled on transit dut
CSCvb85116	SPAN TX source tags output with vlan 4095 (TOR/intra-asic)
CSCvb85449	PS display fail/shut but operate fine
CSCvb93730	Traffic not forwarded out of FEX HIF interface
CSCvb94475	VXLAN: Higher convergence time during vPC primary reload
CSCvc00351	N9K - New vrf with "default" keyword in name break connectivity on interface using it
CSCvc03500	EOBC/EPC heartbeat failure with no stack trace
CSCvc04301	copy ftp command is rejected if it has password with special characters
CSCvc06939	VPC peer-keepalive config check not triggering
CSCvc07028	Service "vpc" crash after NX-OS upgrade
CSCvc09586	N9200s, N931xx: Need "show hardware internal errors module X" to show which ports are dropping
CSCvc11535	Nexus 9000 -> Not able to modify vlan after PO is imported via config sync
CSCvc11632	N3K- generates syslog recurringly ->%USER-3-SYSTEM_MSG: user delete failed for userid:userdel:
CSCvc18092	Traffic impact when adding VLAN under port-profile
CSCvc18155	Reloading N9300 with VxLan and Fex config breaks vPC HIF
CSCvc18323	VRF config not applied on L3 port
CSCvc18353	show tech tah-usd to incorporate l2 hardware forwarding verification commands
CSCvc28941	Make member-vni sub-commands config-profile aware
CSCvc29451	cannot establish bgp session with static route underlay
CSCvc29999	Incorrect power redundancy reported

CSCvc33783	Layer 2 forwarded VPLS Packets are dropped when internal DMAC starts with 4 or 6
CSCvc34664	Switch returns 502 Bad Gateway on multiple API requests
CSCvc36090	N93180/N9200 NAT w/ pool overload blackholes icmp traffic
CSCvc36935	Service "tahusd" crash with core saved
CSCvc39097	FIB misprogramming for /32 host route
CSCvc41631	EOBC/EPC heartbeat failure causes module reset with no core or stack traces
CSCvc42931	N9396/N3232C NAT may fail after reboot due to RACL overriding NAT ACL
CSCvc44015	address-family ipv4 multicast path invalid in BGP but present in URIB
CSCvc44478	N9K: After upgrade to 7.0(3)I5(1) NETCONF port [TCP/830] is listening.
CSCvc46369	UDP transit traffic is incorrectly CPU punted due to BFD over LACP ACL
CSCvc49621	vsh sessions hang after ssh session termination
CSCvc54618	N9K: 'show interface Ethx/x' takes 10 to 20 sec to output if QSA/SFP-10GSR are inserted.
CSCvc56379	N9K Crash when Standby is inserted with ACI image and active has n9k standalone image
CSCvc58714	Incorrect placement of OSPF rfc1583compatibility command under VRF configuration
CSCvc59118	N9K:Default interface not clearing duplex configs under interface
CSCvc62087	MAC move on same T2 instance might cause MTS buffer exhausted
CSCvc65350	Nexus 9K Switch Crashes Due to "ACLQOS" Process with NAT and DHCP
CSCvc69230	for 7.0(3)I5(1) for N9k command "no send-community both" removes only standard community
CSCvc69750	N9K-C92160YC-X: VLAN add to pre-existing trunk fails after upgrade to 7.0(3)I5(1)
CSCvc70778	"Fatal Upgrade Error" HW reset reason printed by mistake in "show logging onboard int reset-reason"
CSCvc71792	implement a knob to allow weak ciphers
CSCvc72646	post-routed unknown unicast flooding broken on same T2 instance
CSCvc74591	Backend processing error when nxapi receives 60s+ requests

CSCvc75047	memory leak in ipfib process due to duplicate ip in vxlan environment
CSCvc79642	Switch running 7.0(3)I5(1) reloads with pktmgr hap reset when vPC-peered with older release
CSCvc84014	Need to bypass accounting logs from EEM
CSCvc92124	"show ptp corrections | json" returns "output conversion failed"
CSCvc92246	"show ptp corrections | json" has incorrect correction-val values
CSCvc92265	NX-OS NTP and HSRP: replies with the wrong source IP
CSCvd01493	cdp and stp bpdu packets getting looped in vpc setup through l2pt
CSCvd03141	Inability to Remove Type Config Causes Config to be Stuck And Cannot Install different FEX
CSCvd03501	Kernel panic - not syncing: Fatal exception-Nexus9
CSCvd04392	F&L: NVE loopback IP next-hop incorrectly programmed as Null0 in FIB

Open Caveats–Cisco NX-OS Release 7.0(3)I5(2)

Table 14 lists the open caveats in the Cisco NX-OS Release 7.0(3)I5(2). Click the bug ID to access the Bug Search tool and see additional information about the bug.

Table 14 Open Caveats in Cisco NX-OS Release 7.0(3)I5(2)

Bug ID	Description
CSCuy08187	If EPLD is not latest, terminate non-disruptive ISSU
CSCvb57299	Hardcoding the Cisco Nexus 9500 platform line card module speed to 100 causes the duplex full port to go down.
CSCvb64127	N3K-C3048TP-1GE sometimes fails to reboot with 7.0(3) images because of an MD5Sum mismatch.
CSCvb82259	Cisco Nexus 3000 Series switches take more than 10 secs to populate the S,G entry.
CSCvb90306	CoPP copy to already existing policy does not reprogram the modified classes.
CSCvc18548	show feature | json generates more elements in each row of the cfcFeatureCtrlTable table and misses the row delimiter: ROW_cfcFeatureCtrlTable. Because of this, the output of show feature is not backward compatible.
CSCvc61275	N9k MAC address out of sync in HW/SW after adding a new VLAN

CSCvc90891	Nexus 9k - Smart Call Home Inventory Failure with SHA256 Certificate.
CSCvd01076	The dir | json command doesn't provide output.
CSCvd06973	PVLAN: Secondary VLAN traffic will not hit ACL on primary VLAN's SVI.
CSCvd08039	Copying an ACL into an SSH session of N9K fails, random lines are dropped.
CSCvd11242	After write-erase, reload and copy config, seeing flood traffic egress both legs of STvpc po
CSCvd15172	N9K-C92304QC/N9K-C9236 100 Mbps ARP packets not reaching CPU due to wrong BD on packets.
CSCve24965	From 7.0(3)I5(2) to 7.0(3)I6(1) bios upgrade is not happening with install all
CSCvf40773	Configuration Won't Apply To FEX Ports After Upgrade.

Known Behaviors–Cisco NX-OS Release 7.0(3)I5(2)

Table 15 Known Behaviors in Cisco NX-OS Release 7.0(3)I5(2)

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.

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)I5(2).

- Ingress queuing policy is supported only at the system level (and not at the interface level) for Cisco Nexus 9508 switches with the X9732C-EX line card and Cisco Nexus 93108TC-EX and 93180YC-EX switches.
- Ingress queuing policy is supported only at the system level (and not at the interface level) for Cisco Nexus 9508 switches with the X9732C-EX line card and Cisco Nexus 93108TC-EX and 93180YC-EX switches.
- Q-in-VNI has the following limitations:
  - Single tag is supported on Cisco Nexus 9300 Series switches. It can be enabled by unconfiguring the overlay-encapsulation vxlan-with-tag command from interface nve:

```
N9564PX-2(config)# int nve 1
N9564PX-2(config-if-nve)# no overlay-encapsulation vxlan-with-tag
N9564PX-2# sh run int nve 1

!Command: show running-config interface nve1
!Time: Wed Jul 20 23:26:25 2016

version 7.0(3u)I4(2u)

interface nve1
  no shutdown
  source-interface loopback0
  host-reachability protocol bgp
  member vni 900001 associate-vrf
  member vni 2000980
    suppress-arp
    mcast-group 225.4.0.1
```

  - Single tag is not supported on Cisco Nexus 9500 platform switches; only double tag is supported.
  - Double tag is not supported on Cisco Nexus 9300-EX Series switches, only single tag is supported.
  - When upgrading from Cisco Nexus 7.0(3)I3(1) or Release 7.0(3)I4(1) to Release 7.0(3)I5(2) with Cisco Nexus 9300 Series switches without the overlay-encapsulation vxlan-with-tag command under interface nve, you should add overlay-encapsulation vxlan-with-tag under the nve interface in the older release before starting the ISSU upgrade. We were only supporting double tag in Cisco Nexus 7.0(3)I3(1) and Release 7.0(3)I4(1) . We now support single tag also in Release 7.0(3)I5(2).
  - We do not support traffic between ports configured for Q-in-VNI and ports configured for trunk on Cisco Nexus 9300-EX Series switches.
- 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)I5(2), 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)I5(2). 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
- Flooding for Microsoft Network Load Balancing (NLB) unicast mode is supported only on Cisco Nexus 9500 platform switches. However, if the NLB servers are connected on FEX HIFs, the flooding does not work. NLB is not supported in max-host system routing mode, and NLB multicast mode is not supported.

  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.
- 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
    - N9K-C93108TC-EX
    - N9K-C93180YC-EX

- 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
    - N9K-C93180YC-EX
    - N9K-C93108TC-EX
    - N9K-X9732C-EX line card
    - N9K-X97160YC-EX

- Weighted ECMP (Equal-Cost Multi-Path) Nexus 3000 feature is not supported on the Cisco Nexus 9000 Series switch.
- When upgrading from N9K-X94*xx*, N9K-X95*xx*, and N9K-X96*xx* line cards to N9K-X9732C-EX line cards and their fabric modules, upgrade the Cisco NX-OS software before inserting the line cards and fabric modules. Failure to do so can cause a diagnostic failure on the line card and no TCAM space to be allocated. You must use the write_erase command followed by the reload command.
- 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

For more information, see the *Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*.

Private VLANs have the following configuration guidelines and limitations:

- When changing Private port mode to non-private VLAN port mode, you need to enter the default interface command and then configure non-private VLAN port modes under the interface.
- 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.
- PVLANs 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.
- PVLANs are mapped or associated depending on the PVLAN trunk mode.
- PVLANs 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)
- PVLANs 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
- PVLANs support STP as follows:
  - MST (Multiple Spanning Tree)
  - RSTP (Rapid Spanning Tree Protocol)
- PVLANs port mode is not supported on the following:
  - 40G interfaces of the Cisco Nexus ALE ports on Cisco Nexus 9300 Series switches.
  - Cisco Nexus 3164Q
- PVLANs are supported on breakout ports for the Cisco Nexus 9200 and 9300-EX Series switches.
- PVLANs 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 on Cisco Nexus 9500 platform switches' 40 G ports with the following line cards:

  - N9K-X9636PQ
  - N9K-X9564PX
  - N9K-X9564TX
  - N9K-X9536PQ
  - N9K-X9432PQ
  - N9K-X9464PX
  - N9K-X9464TX
- For more details, see the *Cisco Nexus 9000 Series NX-OS Layer 2 Switching 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 PVLANs.
- 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: We recommend that you enable BPDU Guard on all ports that you configure as a host port; do not enable this feature on promiscuous ports.

- PVLAN promiscuous trunk ports allow you to configure a maximum of 16 private VLAN primary and secondary VLAN pairs on each promiscuous trunk port.
- For PVLAN 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 PVLAN ports configured to a release that does not support PVLAN 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 PVLAN configuration causes PVLAN 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 PVLAN configuration. Layer 2 trunk interfaces, which may carry PVLANs, are active and remain part of the STP database.
- Use only the PVLAN configuration commands to assign ports to primary, isolated, or community VLANs.

Limitations with Other Features

Consider these configuration limitations with other features when configuring PVLAN:

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 PVLANs, STP controls only the primary VLAN.
- PVLAN host or promiscuous ports cannot be SPAN destination ports.

- PVLAN 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.

Guidelines and Limitations for Fabric Extenders

This section list configuration guidelines and limitations for the Cisco Nexus 2000 Series Fabric Extenders:

- Post-routed flood is not supported.
- The configuration is purged when:
  - Straight-through FEXes are converted to dual-homed
  - Dual-homed FEXes are converted to Straight-through.
- Conversion from dual-homed FEX to straight-through or straight-through to dual-homed FEX requires a reload of the parent switch.

  There are two cases for dual-home to straight-through conversion:

  - While the FEX is online: the FEX goes down as a dual-homed FEX on conversion and comes back up a straight-through FEX. The configuration is purged on bringup.
  - While the FEX is offline: the FEX goes down as a dual-homed FEX, then the no vpc id command is entered on the fabric port channel. No configuration purge takes place. In this scenario, default the configuration on FEX interfaces while toggling the mode from active-active to straight-through.

For more information, see the *Cisco Nexus 2000 Series NX-OS Fabric Extender Configuration Guide for Cisco Nexus 9000 Series Switches, Release 7.x*.

Unsupported Features

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

- Cisco Nexus 3232C and 3264Q Switches
- Cisco Nexus 9200 and 9300-EX Series Switches
- Cisco Nexus 9408 Line Card and 9300 Series Switches
- Cisco Nexus 9732C-EX Line Card
- DHCP
- FEX
- Other Unsupported Features
- PVLAN
- VXLAN

Cisco Nexus 3232C and 3264Q Switches

- The following features are not supported for the Cisco Nexus 3232C and 3264Q switches:
- 3264Q 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 (regular and enhanced)
- MLD
- PIM6
- 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
- VXLAN IGMP snooping

Cisco Nexus 9200 and 9300-EX Series Switches

The following features are not supported for the Cisco Nexus 9200 Series switches and the Cisco Nexus 93108TC-EX and 93180YC-EX 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
- Egress port ACLs
- Egress QoS policer or marking
- FEX (supported for Cisco 93180YC-EX switches but not for Cisco Nexus 93108TC-EX and Cisco Nexus 9200 Series switches)
- GRE v4 payload over v6 tunnels
- Host to LPM spillover
- IP length-based matches
- IP-in-IP on 92160
- ISSU
- Layer 2 Q-in-Q is supported only on Cisco Nexus 9300-EX Series switches (93108TC-EX and 93180YC-EX) and Cisco Nexus 9500 platform switches with the X9732C-EX line card.
- MTU (Multi Transmission Unit) checks for packets received with an MPLS header
- Packet-based statistics for traffic storm control (only byte-based statistics are supported)
- PV routing for VXLAN
- PVLANs (supported on Cisco Nexus 9300 and 9300-EX Series switches but not on Cisco Nexus 9200 Series switches)
- Q-in-VNI is not supported on Cisco Nexus 9200 Series switches. Beginning with Cisco NX-OS Release 7.0(3)I5(1), Q-in-VNI is supported on Cisco Nexus 9300-EX Series switches.
- Q-in-Q for VXLAN is not supported on Cisco Nexus 9200 and 9300-EX Series switches
- Q-in-VNI is not supported on Cisco Nexus 9200 Series switches (supported on Cisco Nexus 9300-EX Series switches)
- 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 slice
- SVI uplinks with Q-in-VNI are not supported with Cisco Nexus 9300-EX Series switches
- 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 Switches

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

- 802.3x
- Breakout ports
- FEX (this applies to the 9408 and –EX switches, not all 9300 switches)
- MCT (Multichassis EtherChannel Trunk)
- Only support 40G flows
- Port-channel (No LACP)
- PFC/LLFC
- PTP (Precision Time Protocol)
- PVLAN (supported on Cisco Nexus 9300 Series switches)
- Shaping support on 100g port is limited
- SPAN destination/ERSPAN destination IP
- Storm Control
- vPC
- VXLAN access port.

Cisco Nexus 9732C-EX Line Card

The following features are not supported for Cisco Nexus 9508 switches with an N9K-X9732C-EX line card:

- FEX
- IPv6 support for policy-based routing
- LPM dual-host mode
- SPAN port-channel destinations
- TAP aggregation

DHCP

DHCP subnet broadcast is not supported.

FEX

- 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, 93180YC-EX, and 9500 platform switches (FEX is not supported on the N9K-X9732C-EX line card, 93108TC-EX switches, and Cisco Nexus 9200 platforms).
- FEX vPC is not supported between any model of FEX and the Cisco Nexus 9500 platform switches as the parent switches.
- IPSG (IP Source Guard) is not supported on FEX ports.
- VTEP connected to FEX host interface ports is not supported.

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

PVLAN

This section lists PVLAN features that are not supported.

- PVLAN PO/VPN PO is not supported on N9K-X9632PC-QSFP100, N9K-X9432C-S.

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.
- IPv6 for VXLAN EVPN ESI MH is not supported.
- Native VLANs for VXLAN are not supported on Cisco Nexus 9300 Series switches. All traffic on VXLAN Layer 2 trunks need to be tagged.

NOTE: This limitation does not apply to the Cisco Nexus 9300-EX Series switches.

- 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:
- 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: We recommend that you use a PACL or VACL on the access side to filter out traffic entering the overlay network.

- 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).

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

The Cisco Nexus 3232C/3264Q Switch - Read Me First is available at the following URL:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3232and3264/sw/7x/readme/b_Cisco_Nexus_3232C_and_3264Q_Switch_Read_Me_First.html

The *Cisco Nexus 3000 and 9000 Series NX-API REST SDK User Guide and API Reference* is available at the following URL:

https://developer.cisco.com/site/nx-os/docs/n3k-n9k-api-ref/

New Documentation

There is no new documentation for Release 7.0(3)I5(2).

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 Nexus 9000 Series NX-OS Release Notes, Release 7.0(3)I5(2)