



Cisco Nexus 9000 Series NX-OS Release Notes, Release 7.0(3)I6(1)

This document describes the features, caveats, and limitations for Cisco NX-OS Release 7.0(3)I6(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*.

[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 Open Caveats .
April 20, 2018	Added CSCvf40773 to Open Caveats .
January 31, 2018	Update Limitations for IPv6 Multicast.
October 24, 2017	ISSU releases updated in the Upgrade Instructions .
October 2, 2017	Added upgrade issue for switches running vPC and connected to an IOS-based switch in Upgrade Instructions .
September 28, 2017	Added CSCvg05807 to Open Caveats .
September 26, 2017	Added REST API issue to the Limitations section.
September 7, 2017	Removed “50 Gb on the first 28 ports of the 93180LC-EX line card is not supported” from the Limitations section.
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).

Introduction

Date	Description
August 31, 2017	Removed Cisco Nexus 2000 Series Fabric Extenders from the Cisco Nexus 9200 and 9300-EX platform switches section. .
August 18, 2017	Updated the Unsupported FEX section for vPCs.
August 9, 2017	Removed Intelligent Traffic Director from the Cisco Nexus 9200 and 9300-EX platform switches Unsupported section.
July 7, 2017	Added a link to the Cisco Nexus 9000 Series Switch FEX Support in the Supported FEX Modules section.
June 22, 2017	Added the Container Tracker feature to New Software Features .
June 21, 2017	Added CSCve24965 to Resolved Caveats . Updated Upgrade Instructions .
June 14, 2017	Updated the Supported FEX Modules section.
June 8, 2017	Updated Multicast Routing Features for PIM and PIM6.
June 5, 2017	<ul style="list-style-type: none"> ■ Updated the Programmability Features section in New Software Features. ■ Updated the Limitations section when upgrading from Cisco NX-OS Release 7.0(3)I5(2) to Cisco NX-OS Release 7.0(3)I6(1).
May 25, 2017	Added FEX Layer 3 is not supported on the 2348TQ-E in the Unsupported Features section.
May 24, 2017	Added the LPM Internet-peering routing mode feature to Unicast Routing Features .
May 22, 2017	Added CSCvd61743 to the Resolved Caveats .
May 16, 2017	Created the release notes for Release 7.0(3)I6(1).

Introduction

Contents

Introduction	4
System Requirements	4
New and Changed Information	13
Caveats	19
Upgrade and Downgrade	23
Limitations	23
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)I6(1) 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 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) <i>Note:</i> 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) <i>Note:</i> Supports early versions of the Cisco Nexus 9396 switch (N9K-C9396PX).	3

System Requirements

N9K-C9300-FAN2	Cisco Nexus 9300 fan 2 module with port-side intake airflow (burgundy coloring) <i>Note:</i> 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) <i>Note:</i> 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) <i>Note:</i> 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) <i>Note:</i> 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) <i>Note:</i> Supports the Cisco Nexus 93180LC-EX, 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) <i>Note:</i> Supports the Cisco Nexus 93180LC-EX, 92160YC-X, 9236C, 93108TC-EX, 93180YC-EX, 9332PQ, 9372PX, 9372PX-E, 9372TX, and 9372TX-E switches.	4
NXA-FAN-35CFM-PE	Cisco Nexus 9200 fan module with port-side exhaust airflow (blue coloring) <i>Note:</i> Supports the Cisco Nexus 92300YC switch.	4
NXA-FAN-35CFM-PI	Cisco Nexus 9200 fan module with port-side intake airflow (burgundy coloring) <i>Note:</i> Supports the Cisco Nexus 92300YC switch.	4

- Table 4 lists the Cisco Nexus 9000 Series fans and fan trays
- [Table 5](#) Cisco Nexus 9000 Series Power Supplies

System Requirements

Product ID	Hardware	Quantity
N9K-PAC-500W-PE	500-W AC power supply, port-side exhaust airflow (blue coloring)	2
N9K-PAC-500W-PI	500-W AC power supply, port-side intake airflow (burgundy coloring)	2
N9K-PAC-650W	650-W AC power supply, port-side intake airflow (burgundy coloring)	2
N9K-PAC-650W-B	650-W AC power supply, port-side exhaust airflow (blue coloring)	2
N9K-PAC-1200W	1200-W AC power supply, port-side intake airflow (burgundy coloring)	2
N9K-PAC-1200W-B	1200-W AC power supply, port-side exhaust airflow (blue coloring)	2
N9K-PAC-3000W-B	3000-W AC power supply	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ 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)	2
N9K-PUV-3000W-B	3000-W Universal AC/DC power supply	<ul style="list-style-type: none"> ■ Up to 4 (Cisco Nexus 9504) ■ Up to 8 (Cisco Nexus 9508) Up to 10 (Cisco Nexus 9516)
NXA-PAC-500W-PE	Cisco Nexus 9300 500-W AC power supply, port-side exhaust airflow (blue coloring)	2
NXA-PAC-500W-PI	Cisco Nexus 9300 500-W AC power supply, port-side intake airflow (burgundy coloring)	2
NXA-PAC-650W	Cisco Nexus 9200 and 9300 650-W AC power supply (NEBS compliant), port-side intake airflow (burgundy coloring)	2

System Requirements

NXA-PAC-650W-B	Cisco Nexus 9200 and 9300 650 W AC power supply (NEBS compliant), port-side exhaust airflow (blue coloring)	2
NXA-PAC-650W-PE	Cisco Nexus 9200 650-W AC power supply, port-side exhaust airflow (white coloring)	2
NXA-PAC-650W-PI	Cisco Nexus 9200 650-W AC power supply, port-side intake airflow (burgundy coloring)	2
NXA-PAC-1200W	1200-W AC power supply, port-side intake airflow (burgundy coloring)	2
NXA-PAC-1200W-B	1200-W AC power supply, port-side exhaust airflow (blue coloring)	2
NXA-PDC-930W-PE	Cisco Nexus 9300 930-W DC power supply, port-side exhaust airflow (blue coloring)	2
NXA-PDC-930W-PI	Cisco Nexus 9300 930-W DC power supply, port-side intake airflow (burgundy coloring)	2
UCS-PSU-6332-DC	930-W DC power supply with port-side exhaust airflow (gray coloring)	2
UCSC-PSU-930WDC	930-W DC power supply with port-side intake airflow (green coloring)	2

- lists the Cisco Nexus 9000 Series line cards
- [Error! Reference source not found.](#) lists the Cisco Nexus 9000 Series power supplies
- [Error! Reference source not found.](#) lists the Cisco Nexus 9000 Series supervisor modules
- [Error! Reference source not found.](#) lists the Cisco Nexus 9000 Series system controllers
- [Error! Reference source not found.](#) lists the Cisco Nexus 9000 Series uplink modules
- [Error! Reference source not found.](#) lists the 3232C and 3264Q switch hardware
- [Error! Reference source not found.](#) lists the Cisco Nexus 3164Q switch hardware
- [Error! Reference source not found.](#) lists the Cisco Nexus 31128PQ switch hardware

Table 2 Cisco Nexus 9000 Series Fabric Modules

Product ID	Hardware	Quantity

System Requirements

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-C9508-FM-Z	Fabric blank with Fan Tray Power Connector module used in place of a fabric module that has been removed from fabric slots 22, 24, or 26 during lab verification test.	1
N9K-C9516-FM	Cisco Nexus 9500 Series 40-Gigabit fabric module	3-6 depending on the line cards
N9K-C9516-FM-E	100-Gb -E fabric module (for the Cisco Nexus 9516 chassis_ that supports the 100-Gb (-EX) line cards. When used, there must be four of these fabric modules installed in fabric slots 22, 23, 24, and 26.	4
N9K-C9516-FM-Z	Fabric blank with Fan Tray Power Connector module used in place of a fabric module that has been removed from fabric slots 22, 24, or 26 during lab verification test.	1

Table 3 Cisco Nexus 9000 Series Fans and Fan Trays

Product ID	Hardware	Quantity
------------	----------	----------

System Requirements

N9K-C9300-FAN1	Cisco Nexus 9300 fan 1 module with port-side intake airflow (burgundy coloring) <i>Note:</i> 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) <i>Note:</i> 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) <i>Note:</i> 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) <i>Note:</i> 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) <i>Note:</i> 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) <i>Note:</i> 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) <i>Note:</i> Supports the Cisco Nexus 93180LC-EX, 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) <i>Note:</i> Supports the Cisco Nexus 93180LC-EX, 92160YC-X, 9236C, 93108TC-EX, 93180YC-EX, 9332PQ, 9372PX, 9372PX-E, 9372TX, and 9372TX-E switches.	4

System Requirements

NXA-FAN-35CFM-PE	Cisco Nexus 9200 fan module with port-side exhaust airflow (blue coloring) Note: Supports the Cisco Nexus 92300YC switch.	4
NXA-FAN-35CFM-PI	Cisco Nexus 9200 fan module with port-side intake airflow (burgundy coloring) Note: Supports the Cisco Nexus 92300YC switch.	4

Table 4 Cisco Nexus 9500 Series Line Cards

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])	<ul style="list-style-type: none"> ■ 1-4 (Cisco Nexus 9504) ■ 1-8 (Cisco Nexus 9508) ■ 1-16 (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])	<ul style="list-style-type: none"> ■ 1-4 (Cisco Nexus 9504) ■ 1-8 (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.	<ul style="list-style-type: none"> ■ 1-4 (Cisco Nexus 9504) ■ 1-8 (Cisco Nexus 9508) ■ 1-16 (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])	<ul style="list-style-type: none"> ■ 1-4 (Cisco Nexus 9504) ■ 1-8 (Cisco Nexus 9508) ■ 1-16 (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])	<ul style="list-style-type: none"> ■ 1-4 (Cisco Nexus 9504) ■ 1-8 (Cisco Nexus 9508) ■ 1-16 (Cisco Nexus 9516)
N9K-X9464TX2	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])	<ul style="list-style-type: none"> ■ 1-4 (Cisco Nexus 9504) ■ 1-8 (Cisco Nexus 9508) ■ 1-16 (Cisco Nexus 9516)

System Requirements

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])	<ul style="list-style-type: none"> ■ 1-4 (Cisco Nexus 9504) ■ 1-8 (Cisco Nexus 9508) ■ 1-16 (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])	<ul style="list-style-type: none"> ■ 1-4 (Cisco Nexus 9504) ■ 1-8 (Cisco Nexus 9508) ■ 1-16 (Cisco Nexus 9516)
N9K-X9564TX	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])	<ul style="list-style-type: none"> ■ 1-4 (Cisco Nexus 9504) ■ 1-8 (Cisco Nexus 9508) ■ 1-16 (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).	<ul style="list-style-type: none"> ■ 1-4 (Cisco Nexus 9504) ■ 1-8 (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, N9K-C9508-FM-E, and N9K-C9516-FM-E])	<ul style="list-style-type: none"> ■ 1-4 (Cisco Nexus 9504) ■ 1-8 (Cisco Nexus 9508) ■ 1-16 (Cisco Nexus 9516)
N9K-X9736C-EX	Line card with 36 40-/100 Gigabit Ethernet QSFP28 ports (supported by 100-Gigabit -E fabric modules [N9K-C9504-FM-E, N9K-C9508-FM-E, and N9K-9516-FM-E]).	<ul style="list-style-type: none"> ■ 1-4 (Cisco Nexus 9504) ■ 1-8 (Cisco Nexus 9508) ■ 1-16 (Cisco Nexus 9516)
N9K-X97160YC-EX	Line card with 48 10-/25-Gigabit Ethernet SFP28 ports and 4 40-/100-Gigabit Ethernet QSFP28 ports (supported by 100-Gigabit -E fabric modules [N9K-C9504-FM-E, N9K-C9508-FM-E, and N9K-9516-FM-E])	<ul style="list-style-type: none"> ■ 1-4 (Cisco Nexus 9504) ■ 1-8 (Cisco Nexus 9508) ■ 1-16 (Cisco Nexus 9516)

Table 5 Cisco Nexus 9000 Series Power Supplies

Product ID	Hardware	Quantity
N9K-PAC-500W-PE	500-W AC power supply, port-side exhaust airflow (blue coloring)	2
N9K-PAC-500W-PI	500-W AC power supply, port-side intake airflow (burgundy coloring)	2

System Requirements

N9K-PAC-650W	650-W AC power supply, port-side intake airflow (burgundy coloring)	2
N9K-PAC-650W-B	650-W AC power supply, port-side exhaust airflow (blue coloring)	2
N9K-PAC-1200W	1200-W AC power supply, port-side intake airflow (burgundy coloring)	2
N9K-PAC-1200W-B	1200-W AC power supply, port-side exhaust airflow (blue coloring)	2
N9K-PAC-3000W-B	3000-W AC power supply	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ 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)	2
N9K-PUV-3000W-B	3000-W Universal AC/DC power supply	<ul style="list-style-type: none"> ■ Up to 4 (Cisco Nexus 9504) ■ Up to 8 (Cisco Nexus 9508) Up to 10 (Cisco Nexus 9516)
NXA-PAC-500W-PE	Cisco Nexus 9300 500-W AC power supply, port-side exhaust airflow (blue coloring)	2
NXA-PAC-500W-PI	Cisco Nexus 9300 500-W AC power supply, port-side intake airflow (burgundy coloring)	2
NXA-PAC-650W	Cisco Nexus 9200 and 9300 650-W AC power supply (NEBS compliant), port-side intake airflow (burgundy coloring)	2
NXA-PAC-650W-B	Cisco Nexus 9200 and 9300 650 W AC power supply (NEBS compliant), port-side exhaust airflow (blue coloring)	2
NXA-PAC-650W-PE	Cisco Nexus 9200 650-W AC power supply, port-side exhaust airflow (white coloring)	2

System Requirements

NXA-PAC-650W-PI	Cisco Nexus 9200 650-W AC power supply, port-side intake airflow (burgundy coloring)	2
NXA-PAC-1200W	1200-W AC power supply, port-side intake airflow (burgundy coloring)	2
NXA-PAC-1200W-B	1200-W AC power supply, port-side exhaust airflow (blue coloring)	2
NXA-PDC-930W-PE	Cisco Nexus 9300 930-W DC power supply, port-side exhaust airflow (blue coloring)	2
NXA-PDC-930W-PI	Cisco Nexus 9300 930-W DC power supply, port-side intake airflow (burgundy coloring)	2
UCS-PSU-6332-DC	930-W DC power supply with port-side exhaust airflow (gray coloring)	2
UCSC-PSU-930WDC	930-W DC power supply with port-side intake airflow (green coloring)	2

Table 6 Cisco Nexus 9500 Series Supervisor Modules

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

Table 7 Cisco Nexus 9000 Series Switches

Product ID	Description
N9K-C9236C	<p>Cisco Nexus 9236C 1-RU switch with 36 40-/100-Gigabit QSFP28 ports (144 10-/25-Gigabit ports when using breakout cables).</p> <p>Note:</p> <ul style="list-style-type: none"> Beginning with Cisco NX-OS Release 7.0(3)I4(3), 25G CVR-2QSFP28-8SFP adapters are supported on the Cisco Nexus 9236C switches. <p>Beginning with Cisco NX-OS Release 7.0(3)I5(1), the switch supports 4x10G breakout cables.</p>
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)

System Requirements

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 for 10-Gigabit SFP/SFP+ transceivers in QSFP+ ports.
N9K-C9372PX	Cisco Nexus 9372PX 1-RU switch with 48 1-/10-Gigabit Ethernet SFP+ ports and 6 40-Gigabit Ethernet QSFP+ ports.
N9K-C9372PX-E	An enhanced version of the N9K-C9372PX switch.
N9K-C9372TX	Cisco Nexus 9372TX 1-RU switch with 48 1/10GBASE-T ports and 6 40-Gigabit Ethernet QSFP+ ports.
N9K-C9372TX-E	An enhanced version of the N9K-C9372TX switch.
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
N9K-C9396TX	Cisco Nexus 9396TX 1-RU switch with 48 1/10GBASE-T and an uplink module with up to 12 40-Gigabit Ethernet QSFP+ ports
N9K-C9504	Cisco Nexus 9504 4-slot modular switch
N9K-C9508	Cisco Nexus 9508 8-slot modular switch
N9K-C9516	Cisco Nexus 9516 16-slot modular switch
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).
N9K-C92300YC	Cisco Nexus 92300YC 1.5-RU switch with 48 downlink SFP28 ports that you can configure to work as 1- or 10- or 25-Gigabit ports, 18 fixed uplink QSFP28 ports that you can configure to work as 40- or 100-Gigabit ports.
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.
N9K-C93108TC-EX	Cisco Nexus 93108TC-EX 1-RU switch with 48 10GBASE-T ports and 6 40/100-Gigabit QSFP28 ports.
N9K-C93120TX	Cisco Nexus 93120TX 2RU switch with 96 1/10GBASE-T ports and 6 40-Gigabit QSFP+ uplink ports.
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.)
N9K-C93180LC-EX	Cisco Nexus 93180LC-EX 1-RU switch with 24 downlink QSFP+ ports that you can configure to work as 40- or 50-Gigabit ports, six fixed uplink QSFP28 ports that you can configure to work as 40- or 100-Gigabit ports.
N9K-C93180YC-EX	Cisco Nexus 93180YC-EX 1-RU switch with 48 10-/25-Gigabit Ethernet ports and 6 40/100-Gigabit QSFP28 ports.

System Requirements

Table 8 Cisco Nexus 9000 Series Uplink Modules

Product ID	Hardware
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.
N9K-M6PQ	Cisco Nexus 9300 uplink module with 6 40-Gigabit Ethernet QSFP+ ports for the Cisco Nexus 9396PX, 9396TX, and 93128TX switches.
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 QSFP+ ports.

Table 9 Cisco Nexus 9500 Series 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 40-Gb/100-Gb 2 x 10-Gb SFP+, 1-RU switch	1
N3K-C3264Q	Cisco Nexus 3264Q, 64 x 40-Gb 2 x 10-Gb SFP+, 2-RU switch	1

Table 11 Cisco Nexus 3164Q Switch Hardware

Product ID	Hardware	Quantity
N3K-C3164Q-40GE	Cisco Nexus 3164Q, 64 x 40-Gb SFP+, 2-RU switch	1

Table 12 Cisco Nexus 31128PQ Switch Hardware

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

Supported Optics

To determine which transceivers and cables are supported by this switch, see

<https://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 <https://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)I6(1) supports the following FEXes (Fabric extenders) on 93180YC-EX, 9332PQ, 9372PX, 9372PX-E, 9396PX, 93108TC-EX, and 9500 platform switches:

New and Changed Information

- 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 2348TQ-E
 - Cisco Nexus 2348UPQ
 - Cisco Nexus B22Dell
 - Cisco Nexus B22HP
 - Cisco Nexus NB22FTS
 - Cisco Nexus NB22IBM
 - For more information, see the [Cisco Nexus 9000 Series Switch FEX Support](#) page.
 -
-

Note: Please note the following:

- The N9K-X9408PC-CFP2 line card does not support the Cisco Nexus 2300 platform FEXs.
- Cisco Nexus 9300 platform switches do not support FEXs 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 Nexus 2248PQ, 2348TQ, and 2348UPQ FEXes support connections to the Cisco Nexus 9300 or 9500 platform switches by using supported breakout cables to connect a QSFP+ uplink on the FEX and an SFP+ link on the parent switch (4x10 G links).

Note: For Cisco Nexus 9500 platform switches, 4x10-Gb breakout for FEX connectivity is not supported.
- The 93180LC-EX only supports the following FEXes only on down links (1-27):
 - Cisco Nexus 2348TQ
 - Cisco Nexus 2348TQ-E
 - Cisco Nexus 2348UPQ

New and Changed Information

This section lists the following topics:

- New Hardware Features in Cisco NX-OS Release 7.0(3)I6(1)

- New Software Features in Cisco NX-OS Release 7.0(3)I6(1)

New Hardware Features in Cisco NX-OS Release 7.0(3)I6(1)

Cisco NX-OS Release 7.0(3)I6(1) supports the following new hardware:

- Cisco Nexus 2348TQ-E—48 x 100MBase-T and 1/10GBase-T port host interfaces (RJ-45) and up to 6 QSFP+ 10/40 Gigabit Ethernet fabric interfaces; FCoE support up to 30 m with Category 6a and 7 cables.

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

- The Cisco Nexus 92300YC switch (N9K-C92300YC) is a 1.5-RU, fixed-port switch designed for Top-of-Rack (ToR) deployment in data centers. This switch has 48 downlink SFP28 ports that you can configure to work as 1- or 10- or 25-Gigabit ports, and it has 18 fixed uplink QSFP28 ports that you can configure to work as 40- or 100-Gigabit ports. The 48 downlink ports are arranged in 3 rows of 16, in such a way that one row is upside down to optimize connections. To remove a transceiver, without a pull-tab, you need to insert a standard (flat) screwdriver to press the release tab to free it from the port.

For more information, see the [Cisco Nexus 92300YC NX-OS Mode Hardware Installation Guide](#).

- The Cisco Nexus 93180LC-EX switch (N9K-C93180LC-EX) is a 1-RU, fixed-port switch designed for top-of-rack (ToR), middle-of-rack (MoR), and end-of-rack (EoR) deployment in data centers. This switch has 28 downlink QSFP+ ports that you can configure to work as 40- or 50-Gigabit ports, and it has 4 fixed uplink QSFP28 ports that you can configure to work as 40- or 100-Gigabit ports, as well as breakout to 4x10G/4x25G/2x50G.

For more information, see the [Cisco Nexus 93180LC-EX NX-OS Mode Hardware Installation Guide](#).

- The Cisco Nexus 9516-FM-E is a fabric module for the Cisco Nexus 9516 switch.

For more information, see the [Cisco Nexus 9516 NX-OS Mode Switch Hardware Installation Guide](#).

- The Cisco Nexus 9736C-EX line card for Cisco Nexus 9500 platform switch. This line card has 36 40/100 Gb QSFP28 ports.

For more information, see the [Cisco Nexus 9508 NX-OS Mode Switch Hardware Installation Guide](#).

New Software Features in Cisco NX-OS Release 7.0(3)I6(1)

Cisco NX-OS Release 7.0(3)I6(1) supports the following new software features:

FCoE Features

- FCoE NPV—Added support for the Cisco Nexus 93180LC-EX switch.

For more information, see the [Cisco Nexus 9000 Series NX-OS FCoE Configuration Guide, Release 7.x](#)

FEX Features

New and Changed Information

- FEX—Added support for the Cisco Nexus 93108TC-EX and 93180LC-EX switches. Support includes straight-through and dual-homed (active/active) FEX topologies.

NOTE: Breakout ports do not support FEX. FEX connected in 40-Gb ports only works with 40-Gb native mode.

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

Fundamentals Features

- POAP—Introduced a single POAP script and the ability to start a service on boot across 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 Fundamentals Configuration Guide, Release 7.x](#).

Interfaces Features

- Smart channel—Added the ability where the load-balancing algorithm is determined by the software and a resilient load balancing is provided. Smart channel can be used for traffic distribution, load balancing, and redirection on the Cisco Nexus devices. This feature is supported for the Cisco Nexus 9372PX, 93108TC-EX, and 9516 switches.
- Tunnel enhancements—Introduced the tunnel source direct and tunnel mode ipv6ipv6 decapsulate-any CLI commands to configure IP-in-IP tunnel decapsulation on directly connected IP addresses and to support IPv6 payload over IPv6 transport (IPv6inIPv6 packets) respectively. This feature is supported for all Cisco Nexus 9000 Series switches except Cisco Nexus 9500 platform switches.

For more information, see the [Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 7.x](#).

IP SLAs Features

- HTTP Probe—Added support for HTTP operation requests on Cisco Nexus 9000 Series switches. HTTP probe is not supported with Intelligent Traffic Director (ITD).
- IPv6 SLA—Added support for Internet Control Message Protocol (ICMP) Echo operation on Cisco Nexus 9300 and 9500 platform switches.

For more information, see the [Cisco Nexus 9000 Series NX-OS IP SLAs Configuration Guide, Release 7.x](#).

Label Switching Features

- L3-EVPN over segment routing MPLS—Introduced the feature mpls evpn CLI command to enable L3-EVPN over segment routing MPLS and encapsulation mpls CLI command to send EVPN type-5 route updates to the neighbors. This feature is supported on all Cisco Nexus 9000 Series switches.
- MPLS segment routing OAM—Added support for MPLS OAM for NIL FEC type on Cisco Nexus 9000 Series switches. Introduced the feature mpls oam CLI command to enable MPLS OAM. This feature is supported on all Cisco Nexus 9000 Series switches.

For more information, see the [Cisco Nexus 9000 Series NX-OS Label Switching Configuration Guide, Release 7.x](#).

Multicast Routing Features

- Multicast counters—Added the ability to display the bytes and rate for every multicast S,G route in the output of the show ip mroute command. Only Cisco Nexus 9300-EX platform switches support this feature.
- PIM and PIM6—Added Protocol Independent Multicast (PIM) IPv4 and IPv6 sparse mode support for Layer 3 port-channel subinterfaces on the following hardware:

New and Changed Information

- o Cisco Nexus 9500 platform switches with N9K-X9732C-EX, N9K-X9736C-EX, and N9K-X97160YC-EX line cards
- o Cisco Nexus 9300-EX platform switches
- o Cisco Nexus 3232C and 3264Q switches

For more information, see the [Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 7.x](#).

NX-API Features

- New NX-API REST commands have been added. The following table describes the markdown files and the name of the corresponding section in the Cisco Nexus 3000 and 9000 Series NX-API REST SDK User Guide and API Reference that were edited to include the Data Management Engine (DME)-ized commands made available for the 7.0(3)I6(1) release.

Markdown File Name	Section Name
_acl.md	Configuring ACLs Added commands for configuring ACE, MAC ACLs, and time ranges and for applying access control to a list of VLANs.
_bgp.md	Configuring BGP Added commands for specifying and configuring BGP routers, IPv4 unicast address families, template peers, and neighbors
_ifconfig.md	Configuring Interfaces Added commands for configuring source-interface.
_nd.md	Configuring IPv6 Neighbor Discovery and ICMPv6 Added operation, action, and configuration commands
_netstack.md	Configuring Netstack Added operation, action, and configuration commands
_nfm.md	Configuring NFM Added commands for configuring TCAM.
_qos.md	Configuring QoS Added commands for applying policy maps
_staticrt.md	Configuring Static Routes Added operation, action, and configuration commands
_tunnel.md	Configuring Tunnel Interfaces Added commands for configuring tunneling.
_vrrp.md	Configuring VRRP Added commands for configuring VVRPv3.
_vxlan.md	Configuring VXLAN BGP EVPN Added commands for enabling and configuring the NGOAM feature

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

NX-OSv 9000 Features

- CML—Added the ability to run the VM in the Cisco Modeling Lab (CML) environment.
- Memory footprint reduction (VIRL)—Added the ability to use either 4-G or 8-G memory to launch the VM.
- VXLAN—Added support for the VXLAN BGP Ethernet VPN (EVPN) control plane.

For more information, see the [Cisco NX-OSv 9000 Guide](#).

Programmability Features

- **The device model's namespace has been changed to <https://cisco.com/ns/yang/cisco-nx-os-device>** and the module name to Cisco-NX-OS-device.
- **Container tracker**—Cisco NX-OS is configured to communicate with the Kubernetes API Server to understand the capabilities of the containers behind a given switch port.
- **Dynamic logging**—Changes can be made to the logging behavior without restarting.
- **NETCONF candidate**—The NETCONF agent supports updates to the configuration using a candidate configuration file without affecting the running configuration. Configuration changes to the candidate configuration file are only applied once the candidate configuration has been committed.
- **NX-SDK**— Provides users access to infrastructure APIs to streamline NX-OS application development.
- **REST2CLI**—The Cisco Nexus 9000 NX-API Sandbox feature supports conversions from a JSON REST payload to the equivalent CLI commands.
- **Telemetry**
 - Can be configured using the NX-API REST API.
 - Supports data encoding using the Google Protocol Buffers (GPB) and JSON.
 - Supports secure data transport using the Google remote procedure call (gRPC).

For more information, see the [Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 7.x](#).

QoS Features

- **Egress policing per VLAN**—Added support on the Cisco Nexus 93108TC-EX and 93180LC-EX switches, and the N9K-X97160YC-EX, N9K-X9732C-EX, and N9K-X9736C-EX line cards.
- **PFC watchdog interval**—Added support to detect whether packets in a no-drop queue are being drained within a specified time period. This feature is supported on Cisco Nexus 9200 platform switches, Cisco Nexus 93108TC-EX and 93180YC-EX switches, and Cisco Nexus 9508 switches with the N9K-X9732C-EX line cards.
- **WRED**—Added support to configure drop thresholds for non-ECN flows.

For more information, see the [Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide, Release 7.x](#).

Security Features

- **Catena**—Added support for service chaining for Cisco Nexus 92160YC-X, 9372TX, and 93180YC-EX switches.

Catena is a multi-Tbps application chaining, security, analytics, segmentation and L4-L7 applications integration solution, natively on the switch/router. The solution works with all L4-L7 virtual and physical devices, such as, Firewalls, IPS, IDS, WAAS, DDoS protection, load-balancers, SSL offload engines, network monitoring, network switches/routers, etc.

Catena allows user to create multiple chains with multiple elements in each chain. User can configure security policies to configure which traffic goes through which chain. An element could be a cluster of devices, in which case Catena load-balances to the cluster. Catena performs health monitoring and failure handling of devices. Catena performs sophisticated analytics.

The devices are inserted in the data path in such a way that there are no topological changes needed, and no changes to existing configuration. This feature can support scalability with many number of appliances in the data path.

- **Egress rate-limiter**—Added support for the hardware rate-limiter to show statistics for outbound traffic on SPAN egress ports. This rate-limiter is supported for all Cisco Nexus 9000 Series switches and the Cisco Nexus 3164Q, 31128PQ, 3232C, and 3264Q switches.

New and Changed Information

- IPv4 ACLs—Added support for user-defined filtering (UDF)-based port ACLs on Cisco Nexus 9200, 9300, and 9300-EX platform switches.
- IPv6 ACL/UDF ERSPAN—Added support for IPv6 ACLs with UDF-based match for Cisco Nexus 9300-EX platform switches.
- Port security over vPC—Added support for security on vPCs for Cisco Nexus 9300-EX platform switches.
- Storm control—Added support for configuring the traffic storm control rate for ARP packets entering a port channel for Cisco Nexus 3232C and 3264Q switches only. You can configure traffic storm control so that ARP packets conform to the configured rate.
- VACL redirect—Added support for Cisco Nexus 9200 and 9300-EX platform switches.

For more information, see the [Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 7.x](#).

Software Upgrade and Downgrade Features

- In-service software upgrade (ISSU)—Added ISSU support for the following platforms:
 - Cisco Nexus 3232C and 3264Q switches
 - Cisco Nexus 9236C, 9272Q, 92160YC-X, 92300YC, and 92304QC switches
 - Cisco Nexus 93108TC-EX and 93180YC-EX switches (Note: The Cisco Nexus 93180LC-EX switch does not support ISSU.)

For more information, see the [Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.x](#).

System Management Features

- Ingress Timestamping—Added the ability to configure timestamp tagging on Layer 2 and Layer 3 ingress interfaces. This feature enables you to track in real time when packets arrive at remote devices. It is supported for the Cisco Nexus 9200 and 9300-EX platform switches.
- NTP—Added the ability to scan the access group options in the following order, from least restrictive to most restrictive: peer, serve, serve-only, query-only. This feature is supported for all Cisco Nexus 9000 Series switches and the Cisco Nexus 3164Q, 31128PQ, 3232C, and 3264Q switches.
- PTP—Added the ability to increase the number of PTP sessions by offloading timers to the line card. This feature is supported for the Cisco Nexus 9500 platform switches with N9K-X9732C-EX, N9K-X9736C-EX, and N9K-X97160YC-EX line cards.
- PTP—Added support for a unicast and mixed mode communication. This feature is supported on the Cisco Nexus 93108TC-EX and 93180YC-EX switches.
- SNMP—Added the ability to configure the SNMP local engine ID. This feature is supported on 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 System Management Configuration Guide, Release 7.x](#).

Unicast Routing Features

- Hot Standby Routing Protocol (HSRP)—Added the ability to configure an HSRP subnet virtual IP address (VIP) in a different subnet than that of the SVI IP address. This feature enables you to conserve public IPv4 addresses by using a VIP as a public IP address and an interface IP as a private IP address. It is supported for all Cisco Nexus 9000 Series switches and the Cisco Nexus 3164Q, 31128PQ, 3232C, and 3264Q switches.
- LPM Internet-peering routing mode—You can configure this LPM routing mode in order to support IPv4 and IPv6 LPM Internet route entries. This mode supports dynamic Trie (tree bit lookup) for IPv4 and IPv6 prefixes. Only the Cisco Nexus 9300-EX Series switches and Cisco Nexus 9500 Series switches with X9700-EX line cards

Caveats

support this routing mode. For LPM Internet-peering routing mode scale numbers, see the [Cisco Nexus 9000 Series NX-OS Verified Scalability Guide, Release 7.0\(3\)I6\(1\)](#).

For more information, see the [Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 7.x](#).

VXLAN Features

- lACP vpc-convergence CLI command—Introduced this command for better convergence on Layer 2 unicast traffic and vPC port-channel events. This feature is supported on all Cisco Nexus 9000 Series switches.
- NGOAM authentication—NGOAM authenticates the pathtrace requests to provide the statistics by using the HMAC MD5 authentication mechanism. This feature is supported on all Cisco Nexus 9000 Series switches.
- Port VLAN Mapping with VXLAN—Added support for configuring port VLAN with VXLAN on Cisco Nexus 9300-EX and 9500 platform switches with -EX line cards with the following exceptions:
 - Only Layer 2 (no routing) is supported with port VLAN with VXLAN on these switches.
 - No inner VLAN mapping is supported.
- VXLAN—Added support for configuring VXLAN on Cisco Nexus 3232C and 3264Q switches.

For more information, see the [Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 7.x](#).

Caveats

This section includes the following topics:

- Resolved Caveats—Cisco NX-OS Release 7.0(3)I6(1)
- Open Caveats—Cisco NX-OS Release 7.0(3)I6(1)
- Known Behaviors—Cisco NX-OS Release 7.0(3)I6(1)_

Resolved Caveats—Cisco NX-OS Release 7.0(3)I6(1)

Table 3 lists the Resolved Caveats in Cisco NX-OS Release 7.0(3)I6(1). Click the bug ID to access the Bug Search tool and see additional information about the bug.

Table 3 Resolved Caveats in Cisco NX-OS Release 7.0(3)I6(1)

Bug ID	Description
CSCue73984	Object tracking shows wrong state of switchport (L2) interface
CSCur66930	FTP not showing any progress indication
CSCuz55002	SSTE:Reliance Sol:BGP table with no nexthop when nexthop learnt thro LU
CSCvb93995	Nessus Scan removes ACL from VTY interface.
CSCvc03558	N9K drops transient BFD and LACP BFD frames on uplink ports due to BFD ACL

Caveats

CSCvc05559	fex:continuous logs-Parent netdev NULL for FEX port ifindex:0x1600008d, parent ifindex: 0x0
CSCvc14918	9500 Modular:Tahusd crash if LC modules N9K-X97*EX and N9K-X96/X95/X94* present in same chassis
CSCvc61275	N9k MAC address out of sync in HW/SW after added a new VLAN
CSCvc86068	Unable to add SSH key to a user due to sys/userext/remoteuser-XXX record stuck in DME
CSCvc86738	VLAN creation on the Nexus 9K flap the interface on the standby ASR9K in MLAG
CSCvc86759	Unable to change the power to insrc-redundant from different modes.
CSCvc90891	Nexus 9k - Smart Call Home Inventory Failure with SHA256 Certificate
CSCvc94606	Evaluation of N9k/N7k/N5k/N3k/MDS for OpenSSL Jan 2017
CSCvd01076	'dir json' doesn't provide output
CSCvd10781	Ping to g/w fails - Native-VLAN + VPC
CSCvd17852	PIM BDir DF election issue
CSCvd19119	Multi Fan failure timer is not reset
CSCvd20720	Service crashes with nginx_f
CSCvd29639	High convergence for L2 or L3 multicast traffic with large oiflist
CSCvd29898	DNS probes are failing with type cname in the dns response
CSCvd31530	N9K: var/tmp is full with csm_sh_run_acfg files
CSCvd35319	N3232C static NAT packet loss with AU enabled
CSCvd37435	N9000 models N31108, N31128, N3232C, N3164, N3264 show version should show Nexus9000
CSCvd39440	N9K ITD Reflecting TTL 1 packets
CSCvd41645	Unable to change/remove "route-target" from I2 VNI
CSCvd42032	In pure BGP environment, all next hops are not added to ECMP
CSCvd45870	N9000 vrf aware static NAT black holing traffic due to incorrect translation
CSCvd45908	N9000 NAT TS does not include correct vrf specific output

Caveats

CSCvd59350	Crash in the hsrp_engine process after removing HSRP Group
CSCvd59759	SNMP counters displays zero on specific uplink interfaces E1/50,E1/52 with IF-MIB::ifOutDiscards
CSCvd60104	will enable "feature bash-shell" by tac-pac
CSCvd60407	CLIs crash due to maximum number of OSPF process being breached
CSCvd61743	PIM config restore causes tamnw process and system crash
CSCvd62376	Sysmgr core does not have kernel trace logs
CSCvd64493	Setting the console authentication method to "Local" is not being applied.
CSCvd67148	N9K: "udld aggressive" is not set to interface, even though "sh udld" is set to udld-aggressive
CSCvd68147	Nexus 9200/9300 switches don't forward UDP port 6784 with feature BFD disabled.
CSCvd70698	N9k + PXE BOOT - VPC check flag is not cleared when the interface goes from up to Individual state
CSCvd73818	9564PX linecard resets due to an MTM crash
CSCvd74188	config-sync switch-profile configuration for active-active fex ports is lost after 9K VPC reload
CSCvd86332	EIGRP routers stopped propagating default route.
CSCvd88370	7.0(3)I4(6) SSH Weak MAC Algorithms Enabled
CSCvd90140	Mac Addressed learned over MCT with Vxlan-Fex environment not in HW.
CSCvd91204	pktmgr keeps crashing
CSCvd93850	Service "I2fm" cores on both VPC switches when VLAN deleted
CSCvd96147	N9K // Unable to modify port-channel parameters
CSCvd99713	Guest shell default route in mgmt VRF lost after re-configuring mgmt intf IP addr
CSCve00092	N9K Service "aclqos" crash
CSCve03416	cVpcDualActiveDetectionStatus returns 0 instead of 2 for FALSE
CSCve04084	ETHPM LINK UP event delayed randomly during N9K-C9236C bootup
CSCve05166	N3K-C3232C / ipv6 prefix-list with ge 128 not applied / 7.0.3.I4.1 thru 7.0.3.I4.6

Caveats

CSCve09154	Cli "system nve infra-vlans" has extra space
CSCve11058	N9K VLAN match for IPv6 ACLs not working
CSCve12424	Traffic crossing MCT fail for PV(Translated Vlan) if localleg is down .
CSCve12612	N9k: user created in setup script with "\" in password not honored.
CSCve13039	Implement single knob for ICMPv6 actions in IPv6 ACL.
CSCve15453	[n9k+fex] Converting AA-fex to ST is breaking flow-through connectivity
CSCve19619	system fabric-mode full-rate command causes N9K-C950x-FM-E to powerdown
CSCve19697	LSE based n9k mac learn not occur if smac is different in ARP mapping table
CSCve20830	Configuring range of port-channel corrupts TCAM resulting in traffic drop
CSCve24672	BGP routes not advertised to peer after shut/no shut of interface connected to peer
CSCve24965	From 7.0(3)I5(2) to 7.0(3)I6(1) bios upgrade is not happening with install all
CSCve25506	VXLAN-ARP-SUPPRESSION TCAM is not programmed after upgrade to 7.0(3)I5(2)
CSCve29794	FEX 2348 goes offline on N9K-X9636PQ specific port 32
CSCve32883	N9K - MAC Learning disabled.

Open Caveats—Cisco NX-OS Release 7.0(3)I6(1)

Table 4 lists the open caveats in the Cisco NX-OS Release 7.0(3)I6(1). Click the bug ID to access the Bug Search tool and see additional information about the bug.

Table 4 Open Caveats in Cisco NX-OS Release 7.0(3)I6(1)

Bug ID	Description
CSCuy08187	If EPLD is not latest, terminate non-disruptive ISSU
CSCvb57299	Hardcoding the Cisco Nexus 9500 Series line card module speed to 100 causes the duplex full port to go down.
CSCvb82259	Cisco Nexus 3000 Series switches take more than 10 secs to populate the S,G entry.
CSCvd06973	PVLAN: Secondary VLAN traffic will not hit ACL on primary VLAN's SVI.

CSCvf40773	Configuration Won't Apply To FEX Ports After Upgrade.
CSCvg05807	N9K: IOS attached VPCs err-disabled during upgrade to 7.0.3.I6.1 or newer

Known Behaviors—Cisco NX-OS Release 7.0(3)I6(1)

Table 5 Known Behaviors in Cisco NX-OS Release 7.0(3)I6(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.

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)I6(1).

- IPv6 multicast is not supported on Cisco Nexus 9500 platform switches.
- A delay of 10 to 15 seconds occurs when applying certain configurations to interfaces through the REST API. If you try to configure a port as a switch port and make it either an access or trunk port, a delay occurs in applying either the access or trunk VLANs to the port. This delay is only seen when trying to apply all of the configuration at once. If the port is already a switch port, the issue is not seen. This behavior is due to how NXAPI REST is programmed which concurrently sends requested changes to different processes.
- If you are upgrading from Cisco NX-OS Release 7.0(3)I5(2) to Cisco NX-OS Release 7.0(3)I6(1) and Straight Through FEX with vPC is shut, VXLAN virtual ports are not created for that port channel. When the upgrade to Cisco NX-OS Release 7.0(3)I6(1) is complete, missing VXLAN virtual ports cause MAC deletion.
- SFP management port on the 93180LC-EX line card is not supported.
- Line rate cannot be sustained across all 36 ports on the 9736C-EX line card.

Limitations

- You must use either the CLI or SNMP to configure a feature on your switch. Do not configure a feature using both interfaces to the switch.
- Ingress DROP_ACL_DROP is seen with Cisco Nexus 9272Q, 9236C, and 92160YC-X switches on an ASIC during congestion. However, these drops do not impact the performance of the switch. For more details on this, see the [CSCvb53216](#) bug.
- 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 platform switches. It can be enabled by unconfiguring the overlay-encapsulation vxlan-with-tag command from interface nve:

```
switch(config)# int nve 1
switch (config-if-nve)# no overlay-encapsulation vxlan-with-tag
switch # 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 platform switches, only single tag is supported.
 - When upgrading from Cisco NX-OS Release 7.0(3)I3(1) or 7.0(3)I4(1) to Cisco NX-OS Release 7.0(3)I6(1) with Cisco Nexus 9300 platform 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 NX-OS Release 7.0(3)I3(1) and 7.0(3)I4(1). We now support single tag also in Release 7.0(3)I6(1).
 - We do not support traffic between ports configured for Q-in-VNI and ports configured for trunk on Cisco Nexus 9300-EX platform 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)I6(1), an error message appears. In previous releases, attempting to disable CoPP causes packets to be rate limited at 50 packets per seconds.

Limitations

- 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 platform switch that is running Cisco NX-OS Release 7.0(3)I6(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 switches except for the 100 Gb 9408PC line card and the 100 Gb 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

Limitations

- 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 QSFP to SFP/SFP+ Adapter (40 Gb to 10 Gb):
 - 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 platforms support for the QSFP+ breakout has the following limitations:
 - Only 10 Gb can be supported using the QSFP-to-SFP Adapter on 40-Gb uplink ports on Cisco Nexus 9300 platform switches in NX-OS.
 - 1 Gb with QSFP-to-SFP Adapter is not supported.
 - For the Cisco Nexus 9332PQ switch, all ports except 13-14 and 27-32 can support breakout.
 - All ports in the QSFP-to-SFP Adapter speed group must operate at the same speed (see the configuration guide).
-
- The following switches support the breakout cable (40 Gb ports to 4x10-Gb ports):
 - N9K-C9332PQ
 - N9K-X9436PQ
 - N9K-X9536PQ
 - N9K-C93180LC-EX—last four ports are breakout capable (10x4, 24x4, 50x2)
 - N9K-C93180YC-EX

Guidelines and Limitations for Private VLANs

- N9K-C93108TC-EX
- N9K-X9732C-EX line card
- N9K-X97160YC-EX
- Weighted ECMP (Equal-Cost Multi-Path) Cisco Nexus 3000 Series feature is not supported on the Cisco Nexus 9000 Series switch.
- When upgrading from N9K-X94xx, N9K-X95xx, and N9K-X96xx 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:

- 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

Guidelines and Limitations for Private VLANs

- 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 vlan 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:
 - 40-Gb interfaces of the Cisco Nexus ALE ports on Cisco Nexus 9300 platform switches.
 - Cisco Nexus 3164Q
- PVLANS are supported on breakout ports for the Cisco Nexus 9200 and 9300-EX platform 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

- Breakout ports 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](#)

Unsupported Features

- [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 NX-OS image from the loader.
- Automatic negotiation support for 25-Gb and 50-Gb 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)
- Enhanced ISSU. NOTE: Check the appropriate guide to determine which platforms support Enhanced ISSU.
- 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 platform switches or between Cisco Nexus 3232C or 3264Q switches and Cisco Nexus 3100 Series switches
- VXLAN IGMP snooping

Cisco Nexus 9200 and 9300-EX Platform Switches

The following features are not supported for the Cisco Nexus 9200 platform switches and the Cisco Nexus 93108TC-EX and 93180YC-EX switches:

- 64-bit ALPM routing mode
- Cisco Nexus 9272PQ and Cisco Nexus 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

Unsupported Features

- Egress port ACLs
- Egress QoS policer or marking
- FEX (supported for Cisco Nexus 9300-EX platform switches but not for Cisco Nexus 9200 platform switches.)
- GRE v4 payload over v6 tunnels
- Host to LPM spillover
- IP length-based matches
- IP-in-IP on Cisco Nexus 92160 switch
- ISSU enhanced
- Layer 2 Q-in-Q is supported only on Cisco Nexus 9300-EX platform 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 platform switches but not on Cisco Nexus 9200 platform switches)
- Q-in-VNI is not supported on Cisco Nexus 9200 platform switches. Beginning with Cisco NX-OS Release 7.0(3)I5(1), Q-in-VNI is supported on Cisco Nexus 9300-EX platform switches.
- Q-in-Q for VXLAN is not supported on Cisco Nexus 9200 and 9300-EX platform switches
- Q-in-VNI is not supported on Cisco Nexus 9200 platform switches (supported on Cisco Nexus 9300-EX platform 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 platform 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

Unsupported Features

Cisco Nexus 9500 Platform N9K-X9408PC-CFP2 Line Card and 9300 Platform Switches

The following features are not supported for the Cisco Nexus 9500 platform N9K-X9408PC-CFP2 line card and Cisco Nexus 9300 platform switches with generic expansion modules (N9K-M4PC-CFP2):

- 802.3x
- Breakout ports
- FEX (this applies to the N9K-X9408PC-CFP2 and -EX switches, not all Cisco Nexus 9300 platform 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 platform switches)
- Shaping support on 100g port is limited
- SPAN destination/ERSPAN destination IP
- Storm Control
- vPC
- VXLAN access port.

N9K-X9732C-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 platform 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, 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.
- FEX Layer 3 is not supported on the Cisco Nexus 2348TQ-E fabric.

Other Unsupported Features

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

- Cisco Nexus 9300 platform 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 40-Gb physical ports on the Cisco Nexus 9372PX, 9372TX, and 9332PQ switches
 - All 40G physical ports on the Cisco Nexus 9396PX, 9396TX, and 93128TX switches

PVLAN

This section lists PVLAN features that are not supported.

- PVLAN PO/VPC PO is not supported on Cisco Nexus N9K-X9632PC-QSFP100, N9K-X9432C-S.

VXLAN

This section lists VXLAN features that 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. 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-host direction as ingress policy on uplink interface.

Related Documentation

- 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).
- 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:

<https://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:

https://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:

https://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:

https://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

The *Cisco Nexus 9000 Series and Cisco Nexus 3000 Series FPGA/EPLD Upgrade Release Notes, Release 7.0(3)I6(1)* is available at the following URL.

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/epld_rn/guide/nxos_epldRN_703i61.html

The Cisco Nexus 9000 Series NX-OS Verified Scalability Guide, Release 7.0(3)I6(1) is available at the following URL:

https://www-author.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/scalability/guide_703i61/b_Cisco_Nexus_9000_Series_NX-OS_Verified_Scalability_Guide_703i61.html

The Cisco Nexus 93180LC-EX NX-OS Mode Hardware Installation Guide is available at the following URL:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/n93180lcex_hig/guide/b_c93180lcex_nxos_mode_hardware_install_guide.html

The Cisco Nexus 92300YC NX-OS Mode Hardware Installation Guide is available at the following URL:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/n92300yc_hig/guide/b_c92300yc_nxos_mode_hardware_install_guide.html

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:

<https://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)I6(1)

© 2017-2020 Cisco Systems, Inc. All rights reserved.