Cisco Nexus 7000 Series NX-OS 8.4, Release Notes

Modified Date: August 30, 2021
Current Release: 8.4(5)

This document describes the features, caveats, and limitations for Cisco NX-OS software for use on the Cisco Nexus 7000 Series Switches. Use this document in combination with documents listed in Related Documentation, page 94.

Note Release notes are sometimes updated with new information about restrictions and caveats. See the following website for the most recent version of the Cisco Nexus 7000 Series NX-OS Release Notes: http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-release-notes-list.html

Table 1 shows the online change history for this document.

Table 1 Change History

Date	Description
December 03, 2021	Added Cisco NX-OS Release 8.2(8) to the Upgrade and Downgrade Paths and Caveats section.
August 30, 2021	Created release notes for Cisco NX-OS Release 8.4(5).
July 12, 2021	Created release notes for Cisco NX-OS Release 8.4(4a).
July 02, 2021	Added Cisco NX-OS Release 7.3(8)D1(1) to the Upgrade and Downgrade Paths and Caveats section.
June 25, 2021	Added Cisco NX-OS Release 8.2(7a) to the Upgrade and Downgrade Paths and Caveats section.
February 22, 2021	Created release notes for Cisco NX-OS Release 8.4(4).
January 08, 2021	Added Cisco NX-OS Release 7.3(7)D1(1) to the Upgrade and Downgrade Paths and Caveats section.
October 06, 2020	Added N77-F312CK-26 to the "Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switches Hardware Support" table.

Cisco Systems, Inc.
www.cisco.com

Table 1 Change History

Date	Description
September 23, 2020	Created release notes for Cisco NX-OS Release 8.4(3).
July 24, 2020	Added Cisco NX-OS Release 8.2(6) to the Upgrade and Downgrade Paths and Caveats section.
April 17, 2020	Added Cisco NX-OS Release 7.3(6)D1(1) to the Upgrade and Downgrade Paths and Caveats section.
March 26, 2020	Created release notes for Cisco NX-OS Release 8.4(2).
July 10, 2019	Created release notes for Cisco NX-OS Release 8.4(1).

Contents

This document includes the following sections:

Introduction

The Cisco NX-OS software for the Cisco Nexus 7000 Series fulfills the routing, switching, and storage networking requirements of data centers and provides an Extensible Markup Language (XML) interface and a command-line interface (CLI) similar to Cisco IOS software.

Note The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

System Requirements

This section includes the following topic:

Supported Device Hardware

The Cisco NX-OS software supports the Cisco Nexus 7000 Series that includes Cisco Nexus 7000 switches and Cisco Nexus 7700 switches. You can find detailed information about supported hardware in the *Cisco Nexus 7000 Series Hardware Installation and Reference Guide*.

Note Cisco Nexus 7000 Supervisor 1 modules, M1 series modules (XL and non-XL modes), FAB-1 modules, F2 series modules are not supported in Cisco NX-OS Release 8.x.

Note There are no new hardware features introduced in Cisco NX-OS Release 8.4(1) and in Cisco NX-OS Release 8.4(2).

Table 2 shows the Cisco Nexus 7000 Series Switch and Cisco Nexus 7700 Switch hardware support details.

Table 3 shows the Fabric Extender (FEX) modules supported by the Cisco Nexus 7000 and Cisco Nexus 7700 I/O modules.

Table 4 shows the transceiver devices supported in each release of Cisco Nexus 7000 Series.

For a list of minimum recommended Cisco NX-OS software releases for use with Cisco Nexus 7000 Series switches, see the document titled *Minimum Recommended Cisco NX-OS Releases for Cisco Nexus 7000 Series Switches.*

Table 2 Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switches Hardware Support

Product ID	Hardware	Minimum Software Release
Cisco Nexus 7000 Series Hardware		
N7K-AC-3KW	3.0-kW AC power supply unit	6.1(2)
N7K-AC-6.0KW	6.0-kW AC power supply unit	4.0(1)
N7K-AC-7.5KW-INT N7K-AC-7.5KW-US	7.5-kW AC power supply unit	4.1(2) 4.1(2)
N7K-C7004	Cisco Nexus 7004 chassis	6.1(2)
N7K-C7004-FAN	Replacement fan for the Cisco Nexus 7004 chassis	6.1(2)
N7K-C7009	Cisco Nexus 7009 chassis	5.2(1)
N7K-C7009-FAB-2	Fabric module, Cisco Nexus 7000 Series 9-slot	5.2(1)
N7K-C7009-FAN	Replacement fan for the Cisco Nexus 7009 chassis	5.2(1)

Table 2 Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switches Hardware Support

Product ID	Hardware	Minimum Software Release
N7K-C7010	Cisco Nexus 7010 chassis	4.0(1)
N7K-C7010-FAB-2	Fabric module, Cisco Nexus 7000 Series 10-slot	6.0(1)
N7K-C7010-FAN-F	Fabric fan tray for the Cisco Nexus 7010 chassis	4.0(1)
N7K-C7010-FAN-S	System fan tray for the Cisco Nexus 7010 chassis	4.0(1)
N7K-C7018	Cisco Nexus 7018 chassis	4.1(2)
N7K-C7018-FAB-2	Fabric module, Cisco Nexus 7000 Series 18-slot	6.0(1)
N7K-C7018-FAN	Fan tray for the Cisco Nexus 7018 chassis	4.1(2)
N7K-DC-3KW	3.0-kW DC power supply unit	6.1(2)
N7K-DC-6.0KW N7K-DC-PIU N7K-DC-CAB=	6.0-kW DC power supply unit (cable included) DC power interface unit DC 48 V, -48 V cable (spare)	5.0(2) 5.0(2) 5.0(2)
N7K-F248XP-25E	Enhanced 48-port 1/10 Gigabit Ethernet SFP+ I/O module (F2E Series)	6.1(2)
N7K-F248XT-25E	Enhanced 48-port 1/10 GBASE-T RJ45 module (F2E Series)	6.1(2)
N7K-F306CK-25	Cisco Nexus 7000 6-port 100-Gigabit Ethernet CPAK I/O module (F3 Series)	6.2(10)
N7k-F312FQ-25	Cisco Nexus 7000 12-port 40-Gigabit Ethernet QSFP+ I/O module (F3 Series)	6.2(6)
N7K-F348XP-25	Cisco Nexus 7000 48-port 1/10-Gigabit Ethernet SFP+ I/O module (F3 Series)	6.2(12)
N7K-HV-3.5KW	3.5KW High Voltage Power Supply Unit	7.3(0)D1(1)
N7K-M202CF-22L	2-port 100-Gigabit Ethernet I/O module XL (M2 Series)	6.1(1)
N7K-M206FQ-23L	6-port 40-Gigabit Ethernet I/O module XL (M2 Series)	6.1(1)
N7K-M224XP-23L	24-port 10-Gigabit Ethernet I/O module XL (M2 Series)	6.1(1)

Table 2 Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switches Hardware Support

Product ID	Hardware	Minimum Software Release
N7K-M324FQ-25L	Cisco Nexus 7000 M3 Series 24-Port 40-Gigabit Ethernet I/O Module	8.0(1)
N7K-M348XP-25L	Cisco Nexus 7000 M3 Series 48-Port 1/10-Gigabit Ethernet I/O Module	8.0(1)
N7K-SUP2	Supervisor 2 module	6.1(1)
N7K-SUP2E	Supervisor 2 Enhanced module	6.1(1)
Cisco Nexus 7700 Series Hardware		
N77-AC-3KW	Cisco Nexus 7700 AC power supply	6.2(2)
N77-C7702	Cisco Nexus 7702 chassis	7.2(0)D1(1)
N77-C7702-FAN	Fan, Cisco Nexus 7702 chassis	7.2(0)D1(1)
N77-C7706	Cisco Nexus 7706 chassis	6.2(6)
N77-C7706-FAB-2	Fabric Module, Cisco Nexus 7706 chassis	6.2(6)
N77-C7706-FAB-3	Fabric Module, Cisco Nexus 7706 chassis	8.3(1)
N77-C7706-FAN	Fan, Cisco Nexus 7706 chassis	6.2(6)
N77-C7706-FAN-2	Generation 2 Fan Tray, Cisco Nexus 7706 Chassis	8.1(1)
N77-C7710	Cisco Nexus 7710 chassis	6.2(2)
N77-C7710-FAB-2	Fabric Module, Cisco Nexus 7710 chassis	6.2(2)
N77-C7710-FAB-3	Fabric Module, Cisco Nexus 7710 chassis	8.3(1)
N77-C7710-FAN	Fan, Cisco Nexus 7710 chassis	6.2(2)
N77-C7710-FAN-2	Fan, Cisco Nexus 7710 chassis	8.1(1)
N77-C7718	Cisco Nexus 7718 chassis	6.2(2)
N77-C7718-FAB-2	Fabric Module, Cisco Nexus 7718 chassis	6.2(2)
N77-C7718-FAN	Fan, Cisco Nexus 7718 chassis	6.2(2)
N77-C7718-FAN-2	Fan, Cisco Nexus 7718 chassis	8.1(1)
N77-DC-3KW	Cisco Nexus 7700 DC power supply	6.2(2)
N77-F248XP-23E	Cisco Nexus 7700 Enhanced 48-port 1/10 Gigabit Ethernet SFP+ I/O module (F2E Series)	6.2(2)

Table 2 Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switches Hardware Support

Product ID	Hardware	Minimum Software Release
N77-F312CK-26	Cisco Nexus 7700 12-port 100-Gigabit Ethernet CPAK I/O module (F3 Series)	7.3(2)D1(1)
N77-F324FQ-25	Cisco Nexus 7700 24-port 40-Gigabit Ethernet QSFP+ I/O module (F3 Series)	6.2(6)
N77-F348XP-23	Cisco Nexus 7700 48-port 1/10-Gigabit Ethernet SFP+ I/O module (F3 Series)	6.2(6)
N77-F430CQ-36	Cisco Nexus 7700 F4-Series 30-port 100-Gigabit Ethernet I/O module	8.3(1)
N77-HV-3.5KW	3.5KW High Voltage Power Supply Unit	7.3(0)D1(1)
N77-M312CQ-26L	12-Port 100-Gigabit Ethernet (M3 Series)	8.0(1)
N77-M348XP-23L	48-port 1/10-Gigabit Ethernet SFP+ I/O module (M3 series)	7.3(0)DX(1)
N77-M324FQ-25L	24-port 40-Gigabit Ethernet QSFP+ I/O module (M3 series)	7.3(0)DX(1)
N77-SUP2E	Cisco Nexus 7700 Supervisor 2 Enhanced module	6.2(2)
N77-SUP3E	Cisco Nexus 7700 Supervisor 3 Enhanced module	8.3(1)

Table 3 FEX Modules Supported by Cisco Nexus 7000 and 7700 Series Modules

Cisco Nexus 7000 Series Module	FEX Module	Minimum Software Release
FEX Modules Supported by Cisco Nexus 7000 Series Modules		
48-port 1-/10-Gigabit Ethernet SFP+ I/O M3 Series module (N7K-M348XP-25L) 24-port 40-Gigabit Ethernet QSFP+ I/O M3 Series module (N7K-M324FQ-25L)	N2K-C2232PP N2K-C2224TP N2K-C2248TP-E N2K-C2248PQ N2K-C2348UPQ N2K-C2348TQ N2K-C2332TQ	8.1(1)
	N2k-C2348TQ-E N2K-B22DELL-P	8.2(1)

Table 3 FEX Modules Supported by Cisco Nexus 7000 and 7700 Series Modules (continued)

Cisco Nexus 7000 Series Module	FEX Module	Minimum Software Release
12-port 40-Gigabit Ethernet QSFP I/O F3 Series module (N7k-F312FQ-25)	N2K-C2224TP-1GE N2K-C2248TP-1GE N2K-C2232PP-10GE N2K-C2232TM N2K-C2248TP-E N2K-C2232TM-E N2K-C2248PQ N2K-B22HP[1]	6.2(12)
	N2K-C2348UPQ N2K-C2348TQ N2K-B22IBM	7.2(0)D1(1)
	N2K-C2332TQ	8.1(1)
	N2k-C2348TQ-E N2K-B22DELL-P	8.2(1)
6-port 40-Gigabit Ethernet I/O M2 Series module XL (N7K-M206FQ-23L)	N2k-2348UPQ N2k-2348TQ	7.2(0)D1(1)
Breakout (4*10G) mode 40-Gigabit Ethernet I/O M2 Series module XL (N7K-M206FQ-23L)	N2k-2224TP N2k-2232PP N2k-2232TM N2k-2232TM-E N2k-2248PQ N2k-2248TP N2k-2248TP-E	7.2(0)D1(1)
24-port 10-Gigabit Ethernet I/O M2 Series module XL (N7K-M224XP-23L)	N2K-C2224TP-1GE N2K-C2248TP-1GE N2K-C2232PP-10GE N2K-C2232TM N2K-C2248TP-E	6.1(1)
	N2K-C2232TM-E N2K-C2248PQ N2K-B22HP	6.2(2)
	N2K-C2348UPQ N2K-C2348TQ N2K-B22IBM	7.2(0)D1(1)

Table 3 FEX Modules Supported by Cisco Nexus 7000 and 7700 Series Modules (continued)

Cisco Nexus 7000 Series Module	FEX Module	Minimum Software Release
48-port 1/10 Gigabit Ethernet SFP+ I/O F3 Series module (N7K-F348XP-25)	N2K-C2224TP-1GE N2K-C2248TP-1GE N2K-C2232PP-10GE N2K-C2232TM N2K-C2248TP-E N2K-2232TM-E N2K-2248PQ N2K-B22HP	6.2(12)
	N2K-C2348UPQ N2K-C2348TQ N2K-B22IBM	7.2(0)D1(1)
	N2K-C2332TQ	8.1(1)
	N2k-C2348TQ-E N2K-B22DELL-P	8.2(1)
Enhanced 48-port 1/10 Gigabit Ethernet SFP+ I/O module (F2E Series) (N7K-F248XP-25E)	N2K-C2224TP-1GE N2K-C2248TP-1GE N2K-C2232PP-10GE N2K-C2232TM N2K-C2248TP-E	6.1(2)
	N2K-2232TM-E N2K-C2248PQ N2K-B22HP	6.2(2)
	N2K-C2348UPQ N2K-C2348TQ N2K-B22IBM	7.2(0)D1(1)
	N2K-C2332TQ	8.1(1)
FEX Modules Supported by Cisco Nexus 7700 Series Modules		

Table 3 FEX Modules Supported by Cisco Nexus 7000 and 7700 Series Modules (continued)

Cisco Nexus 7000 Series Module	FEX Module	Minimum Software Release
48-port 1/10 Gigabit Ethernet SFP+ I/O module (F2E Series) (N77-F248XP-23E)	N2K-C2224TP-1GE N2K-C2248TP-1GE N2K-C2232PP-10GE N2K-C2232TM N2K-C2232TM-E N2K-C2248PQ N2K-C2248TP-E N2K-B22HP	6.2(2)
	N2K-C2348UPQ N2K-C2348TQ N2K-B22IBM	7.2(0)D1(1)
	N2K-C2332TQ	8.1(1)
24-port Cisco Nexus 7700 F3 Series 40-Gigabit Ethernet QSFP I/O module (N77-F324FQ-25)	N2K-C2224TP-1GE N2K-C2248TP-1GE N2K-C2232PP-10GE N2K-C2232TM N2K-C2248TP-E N2K-C2232TM-E N2K-C2248PQ N2K-B22HP[2]	6.2(8)
	N2K-C2348UPQ N2K-C2348TQ N2K-B22IBM	7.2(0)D1(1)
	N2K-C2332TQ	8.1(1)
	N2k-C2348TQ-E N2K-B22DELL-P	8.2(1)

Table 3 FEX Modules Supported by Cisco Nexus 7000 and 7700 Series Modules (continued)

Cisco Nexus 7000 Series Module	FEX Module	Minimum Software Release
48-port Cisco Nexus 7700 F3 Series 1/10-Gigabit Ethernet SFP+ I/O module (N77-F348XP-23)	N2K-C2224TP-1GE N2K-C2248TP-1GE N2K-C2232PP-10GE N2K-C2232TM N2K-C2248TP-E N2K-C2232TM-E N2K-C2248PQ N2K-B22HP	6.2(6)
	N2K-C2348UPQ N2K-C2348TQ N2K-B22IBM	7.2(0)D1(1)
	N2K-C2332TQ	8.1(1)
	N2k-C2348TQ-E N2K-B22DELL-P	8.2(1)
48-Port 1/10 Gigabit Ethernet SFP+ I/O M3 Series module (N77-M348XP-23L) 24-Port 40 Gigabit Ethernet QSFP+ I/O M3 Series module (N77-M324FQ-25L)	N2K-C2232PP N2K-C2224TP N2K-C2248TP-E N2K-C2248PQ N2K-C2348UPQ N2K-C2348TQ N2K-C2332TQ	8.1(1)
	N2k-C2348TQ-E N2K-B22DELL-P	8.2(1)

1. FEX server-facing interfaces should be configured in autonegotiate mode. Do not force a specific data rate.

Note The Cisco Nexus 7000 Enhanced F2 Series 48-port 1/10 GBASE-T RJ-45 Module (N7K-F248XT-25E) does not support Cisco Nexus 2000 FEXs.

Note FEX modules does not support M3 series modules in Cisco NX-OS Release 7.3(0)DX(1), Cisco NX-OS Release 7.3(1)D1, and in Cisco NX-OS Release 8.0(1).

Table 4 Transceivers Supported by Cisco NX-OS Software Releases

I/O Module	Product ID	Transceiver Type	Minimum Software Version
N77-F248XP-23E	FET-10G	Cisco Fabric Extender Transceiver (FET)	6.2(2)
	SFP-10G-AOCxM	10GBASE-AOC (Active Optical Cable) SFP+ Cable (1 m, 2 m, 3 m, 5 m, 7 m, 10 m)	6.2(2)
	SFP-10G-BXD-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, downstream	7.2(0)D1(1)
	SFP-10G-BXU-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, upstream	7.2(0)D1(1)
	SFP-10G-SR SFP-10G-SR-S	10GBASE-SR SFP+	6.2(2)
	SFP-10G-LR SFP-10G-LR-S	10GBASE-LR SFP+	6.2(2)
	SFP-10G-ER SFP-10G-ER-S	10GBASE-ER SFP+	6.2(2)
	SFP-10G-LRM	10GBASE-LRM SFP+	6.2(2)
	SFP-10G-ZR[1] SFP-10G-ZR-S	10GBASE-ZR SFP+	6.2(2)
	SFP-H10GB-CUxM	SFP-H10GB-CUxM Twinax Cable Passive (1 m, 3 m, 5 m)	6.2(2)
	SFP-H10GB-CUxM	SFP-H10GC-CUxM Twinax Cable Passive (1.5 m, 2 m, 2.5 m)	6.2(2)
	SFP-H10GB-ACUxM	SFP-H10GB-ACUxM Twinax Cable Active (7 m, 10 m)	6.2(2)
	SFP-GE-T	1000BASE-T SFP	6.2(2)
	SFP-GE-S	1000BASE-SX SFP (DOM)	6.2(2)
	SFP-GE-L	1000BASE-LX/LH SFP (DOM)	6.2(2)
	SFP-GE-Z	1000BASE-ZX SFP (DOM)	6.2(2)
	GLC-LH-SM	1000BASE-LX/LH SFP	6.2(2)
	GLC-LH-SMD	1000BASE-LX/LH SFP	6.2(2)
	GLC-SX-MM	1000BASE-SX SFP	6.2(2)
	GLC-SX-MMD	1000BASE-SX SFP	6.2(2)
	GLC-ZX-SM	1000BASE-ZX SFP	6.2(2)
	GLC-ZX-SMD	1000BASE-ZX SFP	6.2(2)
	GLC-T	1000BASE-T SFP	6.2(2)

Table 4 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	GLC-TE	1000BASE-T SFP	6.2(10)
	GLC-BX-D	1000BASE-BX10-D	6.2(2)
	GLC-BX-U	1000BASE-BX10-U	6.2(2)
	GLC-EX-SMD	1000BASE-EX SFP	6.2(2)
	CWDM-SFP-xxxx[2]	1000BASE-CWDM	6.2(2)
	DWDM-SFP10G-xx.xx[3]	10GBASE-DWDM SFP+	6.2(2)
	DWDM-SFP-xxxx[3]	1000BASE-DWDM	6.2(2)
N77-F312CK-26	CPAK-100G-SR4[4]	Multi-mode fiber (MMF)	7.3(2)D1(1)
	CPAK-100G-ER4L	Cisco 100GBASE-ER4L CPAK	7.2(1)D1(1)
	CPAK-100G-LR4[#]	Cisco 100GBASE-LR4 CPAK	6.2(6)
	CPAK-100G-SR10 [#]	Cisco 100GBASE-SR10 CPAK	6.2(6)
N77-F324FQ-25	CVR-QSFP-SFP10G (Only version V02 of the CVR-QSFP-SFP10G module is supported.)	QSFP 40G to SFP+ 10G Adapter Module	8.2(1)
	CVR-QSFP-SFP10G (This is supported only on F3 40G I/O modules with SFP-10G-SR or SFP-10G-SR-S optics. If the F3 I/O module is reloaded, the ports containing the CVR-QSFP-SFP10G adapter may remain down even after the F3 I/O module comes back up. If so, the CVR-QSFP-SFP10G adapter must be reseated.) (Only version V02 of the CVR-QSFP-SFP10G module is supported.)	Cisco 40G QSFP	6.2(14)
	QSFP-40G-SR-BD	Cisco 40G BiDi QSFP+	6.2(6)
	QSFP-40G-SR4 QSFP-40G-SR4-S	40GBASE-SR4 QSFP+	6.2(6)
	QSFP-40G-CSR4	40GBASE-CSR4 QSFP+	6.2(6)
	QSFP-40GE-LR4 QSFP-40G-LR4-S	40GBASE-LR4 QSFP+	6.2(6)
	FET-40G	Cisco 40G Fabric Extender Transceiver (FET)	6.2(8)
	QSFP-H40G-ACUxM	40GBASE-CR4 QSFP+ Direct Attach Copper Cable Active (7 m, 10 m)	6.2(8)
	QSFP-4X10G-ACxM	40GBASE-CR4 QSFP+ to 4x SFP+ Twinax Direct Attach Copper Breakout Cable Active (7 m, 10 m)	6.2(8)

Table 4 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	QSFP-4X10G-LR-S	Single-mode fiber (SMF)	7.3(1)D1(1)
	QSFP-H40G-AOCxM	40GBASE-AOC (Active Optical Cable) QSFP Cable (1 m, 2 m, 3 m, 5 m, 7 m, 10 m)	6.2(8)
	QSFP-H40G-AOC15M	40GBASE-AOC (Active Optical Cable) QSFP Cable (15m)	7.2(0)D1(1)
	QSFP-4X10G-AOCxM	40GBASE-AOC (Active Optical Cable) QSFP to 4x10G SFP+ Breakout Cable (1 m, 2 m, 3 m,5 m, 7 m, 10 m)	6.2(8)
	WSP-Q40GLR4L	40GBASE-LR4 lite (2km SMF) QSFP+	6.2(10)
	QSFP-40G-LR4	40GBASE-LR4 QSFP+ (Ethernet and OTU3 capable)	6.2(12)
	QSFP-40G-ER4	40GBASE-ER4 QSFP+ (40km)	6.2(12)
N77-F348XP-23	CWDM-SFP-xxxx[2]	1000BASE-CWDM	6.2(8)
	DWDM-SFP-xxxx[2]	1000BASE-DWDM	6.2(8)
	GLC-TE	1000BASE-T SFP	6.2(10)
	FET-10G	Cisco Fabric Extender Transceiver (FET)	6.2(6)
	SFP-10G-AOCxM	110GBASE-AOC (Active Optical Cable) SFP+ Cable (1 m, 2 m, 3 m, 5 m, 7 m, 10 m)	6.2(10)
	SFP-10G-BXD-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, downstream	7.2(0)D1(1)
	SFP-10G-BXU-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, upstream	7.2(0)D1(1)
	SFP-10G-SR SFP-10G-SR-S	10GBASE-SR SFP+	6.2(6)
	SFP-10G-LR SFP-10G-LR-S	10GBASE-LR SFP+	6.2(6)
	SFP-10G-ER SFP-10G-ER-S	10GBASE-ER SFP+	6.2(6)
	SFP-10G-ZR SFP-10G-ZR-S	10GBASE-ZR SFP+	6.2(6)
	DWDM-SFP10G-xx.xx	10GBASE-DWDM SFP+	6.2(6)
	SFP-10G-LRM[1]	10GBASE-LRM SFP+	6.2(8)

Table 4 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	SFP-H10GB-CUxM	SFP-H10GB-CUxM Twinax Cable Passive (1 m, 3 m, 5 m)	6.2(8)
	SFP-H10GB-CUxM	SFP-H10GC-CUxM Twinax Cable Passive (1.5 m, 2 m, 2.5 m)	6.2(8)
	SFP-H10GB-ACUxM	SFP-H10GB-ACUxM Twinax Cable Active (7 m, 10 m)	6.2(8)
	SFP-GE-T	1000BASE-T SFP	6.2(8)
	SFP-GE-S	1000BASE-SX SFP (DOM)	6.2(8)
	SFP-GE-L	1000BASE-LX/LH SFP (DOM)	6.2(8)
	SFP-GE-Z	1000BASE-ZX SFP (DOM)	6.2(8)
	GLC-LH-SM	1000BASE-LX/LH SFP	6.2(8)
	GLC-LH-SMD	1000BASE-LX/LH SFP	6.2(8)
	GLC-SX-MM	1000BASE-SX SFP	6.2(8)
	GLC-SX-MMD	1000BASE-SX SFP	6.2(8)
	GLC-ZX-SM	1000BASE-ZX SFP	6.2(8)
	GLC-ZX-SMD	1000BASE-ZX SFP	6.2(8)
	GLC-T	1000BASE-T SFP	6.2(8)
	GLC-BX-D	1000BASE-BX10-D	6.2(8)
	GLC-BX-U	1000BASE-BX10-U	6.2(8)
	GLC-EX-SMD	1000BASE-EX SFP	6.2(8)
	FET-10G	Cisco Fabric Extender Transceiver (FET)	6.2(8)
N77-F430CQ-36	QSFP-100G-DR-S and 100GBASE DR	QSFP Transceiver, 500m over Single-mode fiber (SMF)	8.4(5)
	QSFP-100G-FR-S and 100GBASE FR	QSFP Transceiver, 2km over Single-mode fiber (SMF)	8.4(5)
	QSFP-100G-SR4-S	Multi-mode fiber (MMF)	8.3(1)
	QSFP-40G-CSR4 QSFP-40G-SR4 QSFP-40G-SR4-S QSFP-40G-SR-BD QSFP-40G-BD-RX QSFP-40/100-SRBD	Multi-mode fiber (MMF)	8.3(2)

Table 4 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	QSFP-100G-CWDM4-S QSFP-100G-PSM4-S QSFP-100G-LR4-S	Single-mode fiber (SMF)	8.3(1)
	QSFP-40G-ER4 QSFP-40G-LR4	Single-mode fiber (SMF)	8.3(2)
	QSFP-100G-AOC1M QSFP-100G-AOC2M QSFP-100G-AOC3M QSFP-100G-AOC5M QSFP-100G-AOC7M QSFP-100G-AOC10M QSFP-100G-AOC15M QSFP-100G-AOC20M QSFP-100G-AOC25M QSFP-100G-AOC30M	Active optical cable assembly	8.3(1)
	QSFP-H40G-AOC1M QSFP-H40G-AOC2M QSFP-H40G-AOC3M QSFP-H40G-AOC5M QSFP-H40G-AOC7M QSFP-H40G-AOC10M QSFP-H40G-AOC15M	Active optical cable assembly	8.3(2)
	QSFP-100G-ER4L-S	Single-mode fiber (SMF) (40km)	8.3(1)
N7K-F306CK-25	CPAK-100G-SR4[4]	Multi-mode fiber (MMF)	7.3(2)D1(1)
	CPAK-100G-ER4L	Cisco 100GBASE-ER4L CPAK	7.2(1)D1(1)
	CPAK-100G-LR4 #	Cisco 100GBASE-LR4 CPAK	6.2(10)
	CPAK-100G-SR10 #	Cisco 100GBASE-SR10 CPAK	6.2(10)
N7K-F312FQ-25	CVR-QSFP-SFP10G (Only version V02 of the CVR-QSFP-SFP10G module is supported.)	QSFP 40G to SFP+ 10G Adapter Module	8.2(1)

Table 4 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	CVR-QSFP-SFP10G (This is supported only on F3 40G I/O modules with SFP-10G-SR or SFP-10G-SR-S optics. If the F3 I/O module is reloaded, the ports containing the CVR-QSFP-SFP10G adapter may remain down even after the F3 I/O module comes back up. If so, the CVR-QSFP-SFP10G adapter must be reseated.) (Only version V02 of the CVR-QSFP-SFP10G module is supported.)	Cisco 40G QSFP	6.2(14)
	QSFP-40G-SR-BD	Cisco 40G BiDi QSFP+	6.2(6)
	QSFP-40G-SR4 QSFP-40G-SR4-S	40GBASE-SR4 QSFP+	6.2(6)
	QSFP-40G-CSR4	40GBASE-CSR4 QSFP+	6.2(6)
	QSFP-40GE-LR4 QSFP-40G-LR4-S	40GBASE-LR4 QSFP+	6.2(6)
	FET-40G	Cisco 40G Fabric Extender Transceiver (FET)	6.2(6)
	QSFP-H40G-ACUxM	40GBASE-CR4 QSFP+ Direct Attach Copper Cable Active (7 m, 10 m)	6.2(8)
	QSFP-4X10G-ACxM	40GBASE-CR4 QSFP+ to 4x SFP+ Twinax Direct Attach Copper Breakout Cable Active (7 m, 10 m)	6.2(8)
	QSFP-4X10G-LR-S	Single-mode fiber (SMF)	7.3(1)D1(1)
	QSFP-H40G-AOCxM	40GBASE-AOC (Active Optical Cable) QSFP Cable (1 m, 2 m, 3 m, 5 m, 7 m, 10 m)	6.2(8)
	QSFP-H40G-AOC15M	40GBASE-AOC (Active Optical Cable) QSFP Cable (15m)	7.2(0)D1(1)
	QSFP-4X10G-AOCxM	40GBASE-AOC (Active Optical Cable) QSFP to 4x10G SFP+ Breakout Cable (1 m, 2 m, 3 m, 5 m, 7 m, 10 m)	6.2(8)
	WSP-Q40GLR4L	40GBASE-LR4 lite (2km SMF) QSFP+	6.2(10)
	QSFP-40G-LR4	40GBASE-LR4 QSFP+ (Ethernet and OTU3 capable)	6.2(12)
	QSFP-40G-ER4	40GBASE-ER4 QSFP+ (40km)	6.2(12)
N7K-F348XP-25	CWDM-SFP-xxxx[2]	1000BASE-CWDM	6.2(12)

Table 4 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	DWDM-SFP-xxxx[2]	1000BASE-DWDM	6.2(12)
	GLC-TE	1000BASE-T SFP	6.2(12)
	FET-10G	Cisco Fabric Extender Transceiver (FET)	6.2(12)
	SFP-10G-AOCxM	110GBASE-AOC (Active Optical Cable) SFP+ Cable (1 m, 2 m, 3 m, 5 m, 7 m, 10 m)	6.2(12)
	SFP-10G-BXD-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, downstream	7.2(0)D1(1)
	SFP-10G-BXU-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, upstream	7.2(0)D1(1)
	SFP-10G-SR SFP-10G-SR-S	10GBASE-SR SFP+	6.2(12)
	SFP-10G-LR SFP-10G-LR-S	10GBASE-LR SFP+	6.2(12)
	SFP-10G-ER SFP-10G-ER-S	10GBASE-ER SFP+	6.2(12)
	SFP-10G-ZR SFP-10G-ZR-S	10GBASE-ZR SFP+	6.2(12)
	DWDM-SFP10G-xx.xx	10GBASE-DWDM SFP+	6.2(12)
	SFP-10G-LRM[1]	10GBASE-LRM SFP+	6.2(12)
	SFP-H10GB-CUxM	SFP-H10GB-CUxM Twinax Cable Passive (1 m, 3 m, 5 m)	6.2(12)
	SFP-H10GB-CUxM	SFP-H10GC-CUxM Twinax Cable Passive (1.5 m, 2 m, 2.5 m)	6.2(12)
	SFP-H10GB-ACUxM	SFP-H10GB-ACUxM Twinax Cable Active (7 m, 10 m)	6.2(12)
	SFP-GE-T	1000BASE-T SFP	6.2(12)
	SFP-GE-S	1000BASE-SX SFP (DOM)	6.2(12)
	SFP-GE-L	1000BASE-LX/LH SFP (DOM)	6.2(12)
	SFP-GE-Z	1000BASE-ZX SFP (DOM)	6.2(12)
	GLC-LH-SM	1000BASE-LX/LH SFP	6.2(12)
	GLC-LH-SMD	1000BASE-LX/LH SFP	6.2(12)
	GLC-SX-MM	1000BASE-SX SFP	6.2(12)
	GLC-SX-MMD	1000BASE-SX SFP	6.2(12)

Table 4 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	GLC-ZX-SM	1000BASE-ZX SFP	6.2(12)
	GLC-ZX-SMD	1000BASE-ZX SFP	6.2(12)
	GLC-T	1000BASE-T SFP	6.2(12)
	GLC-BX-D	1000BASE-BX10-D	6.2(12)
	GLC-BX-U	1000BASE-BX10-U	6.2(12)
	GLC-EX-SMD	1000BASE-EX SFP	6.2(12)
	FET-10G	Cisco Fabric Extender Transceiver (FET)	6.2(12)
N7K-F248XP-25	FET-10G	Cisco Fabric Extender Transceiver (FET)	6.0(1)
	SFP-10G-BXD-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, downstream	7.2(0)D1(1)
	SFP-10G-BXU-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, upstream	7.2(0)D1(1)
	SFP-10G-SR SFP-10G-SR-S	10GBASE-SR SFP+	6.0(1)
	SFP-10G-LR SFP-10G-LR-S	10GBASE-LR SFP+	6.0(1)
	SFP-10G-ER SFP-10G-ER-S	10GBASE-ER SFP+	6.0(1)
	SFP-10G-LRM	10GBASE-LRM SFP+	6.0(1)
	SFP-10G-ZR [2] SFP-10G-ZR-S	10GBASE-ZR SFP+	6.1(1)
	SFP-10G-AOCxM	10GBASE-AOC (Active Optical Cable) SFP+ Cable (1 m, 2 m, 3 m, 5 m, 7 m, 10 m)	6.2(2)
	SFP-H10GB-CUxM	SFP-H10GB-CUxM Twinax Cable Passive (1 m, 3 m, 5 m)	6.0(1)
	SFP-H10GB-CUxM	SFP-H10GC-CUxM Twinax Cable Passive (1.5 m, 2 m, 2.5 m)	6.2(2)
	SFP-H10GB-ACUxM	SFP-H10GB-ACUxM Twinax Cable Active (7 m, 10 m)	6.0(1)
	SFP-GE-T	1000BASE-T SFP	6.0(1)
	SFP-GE-S	1000BASE-SX SFP (DOM)	6.0(1)
	SFP-GE-L	1000BASE-LX/LH SFP (DOM)	6.0(1)
	SFP-GE-Z	1000BASE-ZX SFP (DOM)	6.0(1)

Table 4 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	GLC-TE	1000BASE-T SFP	6.2(10)
	GLC-LH-SM	1000BASE-LX/LH SFP	6.0(1)
	GLC-LH-SMD	1000BASE-LX/LH SFP	6.0(1)
	GLC-SX-MM	1000BASE-SX SFP	6.0(1)
	GLC-SX-MMD	1000BASE-SX SFP	6.0(1)
	GLC-ZX-SM	1000BASE-ZX SFP	6.0(1)
	GLC-ZX-SMD	1000BASE-ZX SFP	6.2(2)
	GLC-T	1000BASE-T SFP	6.0(1)
	GLC-BX-D	1000BASE-BX10-D	6.0(1)
	GLC-BX-U	1000BASE-BX10-U	6.0(1)
	GLC-EX-SMD	1000BASE-EX SFP	6.1(1)
	CWDM-SFP-xxxx [2]	1000BASE-CWDM	6.0(1)
	DWDM-SFP10G-xx.xx [3]	10GBASE-DWDM SFP+	6.1(1)
	DWDM-SFP-xxxx [3]	1000BASE-DWDM	6.0(1)
N7K-F248XP-25E	FET-10G	Cisco Fabric Extender Transceiver (FET)	6.1(2)
	SFP-10G-BXD-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, downstream	7.2(0)D1(1)
	SFP-10G-BXU-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, upstream	7.2(0)D1(1)
	SFP-10G-SR SFP-10G-SR-S	10GBASE-SR SFP+	6.1(2)
	SFP-10G-LR SFP-10G-LR-S	10GBASE-LR SFP+	6.1(2)
	SFP-10G-ER SFP-10G-ER-S	10GBASE-ER SFP+	6.1(2)
	SFP-10G-LRM	10GBASE-LRM SFP+	6.1(2)
	SFP-10G-ZR [1] SFP-10G-ZR-S	10GBASE-ZR SFP+	6.1(2)
	SFP-10G-AOCxM	10GBASE-AOC (Active Optical Cable) SFP+ Cable (1 m, 2 m, 3 m, 5 m, 7 m, 10 m)	6.2(2)
	SFP-H10GB-CUxM	SFP-H10GB-CUxM Twinax Cable Passive (1 m, 3 m, 5 m)	6.1(2)

Table 4 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	SFP-H10GB-CUxM	SFP-H10GC-CUxM Twinax Cable Passive (1.5 m, 2 m, 2.5 m)	6.2(2)
	SFP-H10GB-ACUxM	SFP-H10GB-ACUxM Twinax Cable Active (7 m, 10 m)	6.1(2)
	SFP-GE-T	1000BASE-T SFP	6.1(2)
	SFP-GE-S	1000BASE-SX SFP (DOM)	6.1(2)
	SFP-GE-L	1000BASE-LX/LH SFP (DOM)	6.1(2)
	SFP-GE-Z	1000BASE-ZX SFP (DOM)	6.1(2)
	GLC-LH-SM	1000BASE-LX/LH SFP	6.1(2)
	GLC-LH-SMD	1000BASE-LX/LH SFP	6.1(2)
	GLC-SX-MM	1000BASE-SX SFP	6.1(2)
	GLC-SX-MMD	1000BASE-SX SFP	6.1(2)
	GLC-ZX-SM	1000BASE-ZX SFP	6.1(2)
	GLC-ZX-SMD	1000BASE-ZX SFP	6.1(2)
	GLC-T	1000BASE-T SFP	6.1(2)
	GLC-TE	1000BASE-T SFP	6.2(10)
	GLC-BX-D	1000BASE-BX10-D	6.1(2)
	GLC-BX-U	1000BASE-BX10-U	6.1(2)
	GLC-EX-SMD	1000BASE-EX SFP	6.1(2)
	CWDM-SFP-xxxx[2]	1000BASE-CWDM	6.1(2)
	DWDM-SFP10G-xx.xx [3]	10GBASE-DWDM SFP+	6.1(2)
	DWDM-SFP-xxxx[3]	1000BASE-DWDM	6.1(2)
N7K-M108X2-12L	SFP-10G-SR[1] SFP-10G-SR-S	10GBASE-SR SFP+	5.2(3a)
	SFP-10G-LR[1] SFP-10G-LR-S	10GBASE-LR SFP+	5.2(3a)
	SFP-10G-LRM[1]	10GBASE-LRM SFP+	5.2(1)
	SFP-H10GB-CUxM[1]	SFP-H10GB-CUxM Twinax Cable Passive (1 m, 3 m, 5 m)	5.2(1)
	CVR-X2-SFP10G	OneX Converter Module - X2 to SFP+ Adapter	5.2(1)
	X2-10GB-CX4	10GBASE-CX4 X2	5.1(1)
	X2-10GB-ZR	10GBASE-ZR X2	5.1(1)
	X2-10GB-LX4	10GBASE-LX4 X2	5.1(1)
	X2-10GB-SR	10GBASE-SR X2	5.0(2a)
	X2-10GB-LR	10GBASE-LRX2	5.0(2a)

Table 4 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	X2-10GB-LRM	10GBASE-LRM X2	5.0(2a)
	X2-10GB-ER	10GBASE-ERX2	5.0(2a)
	DWDM-X2-xx.xx=[3]	10GBASE-DWDM X2	5.0(2a)
N7K-M148GS-11L	SFP-GE-S	1000BASE-SX	5.0(2a)
	GLC-SX-MM		5.0(2a)
	SFP-GE-L	1000BASE-LX	5.0(2a)
	GLC-LH-SM		5.0(2a)
	SFP-GE-Z	1000BASE-ZX	5.0(2a)
	GLC-ZX-SM		5.0(2a)
	GLC-EX-SMD	1000BASE-EX SFP	6.2(2)
	GLC-ZX-SMD	1000BASE-ZX SFP	6.2(2)
	GLC-T	1000BASE-T	5.0(2a)
	SFP-GE-T		5.0(2a)
	GLC-BX-D	1000BASE-BX10-D	5.2(1)
	GLC-BX-U	1000BASE-BX10-U	5.2(1)
	GLC-SX-MMD	1000BASE-SX	5.2(1)
	GLC-LH-SMD	1000BASE-LX	5.2(1)
	GLC-TE	1000BASE-T SFP	6.2(10)
	DWDM-SFP-xxxx [3]	1000BASE-DWDM	5.0(2a)
	CWDM-SFP-xxxx [2]	1000BASE-CWDM	5.0(2a)
N7K-M132XP-12L	FET-10G	Cisco Fabric Extender Transceiver (FET)	5.1(1)
	SFP-10G-BXD-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, downstream	7.2(0)D1(1)
	SFP-10G-BXU-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, upstream	7.2(0)D1(1)
	SFP-10G-SR SFP-10G-SR-S	10GBASE-SR SFP+	5.1(1)
	SFP-10G-LR SFP-10G-LR-S	10GBASE-LR SFP+	5.1(1)
	SFP-10G-ER SFP-10G-ER-S	10GBASE-ER SFP+	5.1(1)
	SFP-10G-LRM	10GBASE-LRM SFP+	5.1(1)

Table 4 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	SFP-10G-ZR [1] SFP-10G-ZR-S	10GBASE-ZR SFP+	6.1(1)
	SFP-10G-AOCxM	10GBASE-AOC (Active Optical Cable) SFP+ Cable (1 m, 2 m, 3 m, 5 m, 7 m, 10 m)	6.2(2)
	SFP-H10GB-ACUxM	SFP-H10GB-ACUxM Twinax Cable Active (7 m, 10 m)	5.1(1)
	SFP-H10GB-CUxM[1]	SFP-H10GB-CUxM Twinax Cable Passive (1 m, 3 m, 5 m)	5.1(2)
	SFP-H10GB-CUxM	SFP-H10GC-CUxM Twinax Cable Passive (1.5 m, 2 m, 2.5 m)	6.2(2)
	DWDM-SFP10G-xx.xx [3]	10GBASE-DWDM SFP+	6.1(1)
N7K-M224XP-23L	SFP-10G-BXD-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, downstream	7.2(0)D1(1)
	SFP-10G-BXU-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, upstream	7.2(0)D1(1)
	FET-10G	Cisco Fabric Extender Transceiver (FET)	6.1(1)
	SFP-10G-SR SFP-10G-SR-S	10GBASE-SR SFP+	6.1(1)
	SFP-10G-LR SFP-10G-LR-S	10GBASE-LR SFP+	6.1(1)
	SFP-10G-ER SFP-10G-ER-S	10GBASE-ER SFP+	6.1(1)
	SFP-10G-ZR [3] SFP-10G-ZR-S	10GBASE-ZR SFP+	6.1(1)
	SFP-10G-LRM	10GBASE-LRM SFP+	6.1(1)
	SFP-10G-AOCxM	10GBASE-AOC (Active Optical Cable) SFP+ Cable (1 m, 2 m, 3 m, 5 m, 7 m, 10 m)	6.2(2)
	SFP-H10GB-ACUxM	SFP-H10GB-ACUxM Twinax Cable Active (7 m, 10 m)	6.1(1)
	SFP-H10GB-CUxM [1]	SFP-H10GB-CUxM Twinax Cable Passive (1m, 3m, 5m)	6.1(1)
	SFP-H10GB-CUxM	SFP-H10GC-CUxM Twinax Cable Passive (1.5 m, 2 m, 2.5 m)	6.2(2)
	DWDM-SFP10G-xx.xx [3]	10GBASE-DWDM SFP+	6.1(1)

Table 4 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
N77-M312CQ-26L	QSFP-100G-DR-S and 100GBASE DR	QSFP Transceiver, 500m over Single-mode fiber (SMF)	8.4(5)
	QSFP-100G-FR-S and 100GBASE FR	QSFP Transceiver, 2km over Single-mode fiber (SMF)	8.4(5)
	CPAK-100G-SR4	Multi-mode fiber (MMF)	8.1(1)
	QSFP-100G-CSR4-S	100G extended short reach 300m OM3 400m OM4	8.2(1)
	QSFP-100G-ER4L-S	100G-ER4 lite SMF (40km)	8.2(1)
	QSFP-100G-SM-SR	100G Short Reach over dual SMF (2km)	8.2(1)
	QSFP-100G-SR4-S QSFP-40G-CSR4 QSFP-40G-SR4 QSFP-40G-SR4-S QSFP-40G-SR-BD	Multi-mode fiber (MMF)	8.0(1)
	QSFP-100G-CWDM4-S QSFP-100G-PSM4-S QSFP-100G-LR4-S QSFP-40G-LR4-S QSFP-40G-ER4 QSFP-40G-LR4	Single-mode fiber (SMF)	8.0(1)
	QSFP-H40G-ACU7M QSFP-H40G-ACU10M	Direct attach copper, active	8.0(1)

Table 4 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	QSFP-100G-AOC1M QSFP-100G-AOC2M QSFP-100G-AOC3M QSFP-100G-AOC5M QSFP-100G-AOC7M QSFP-100G-AOC10M QSFP-100G-AOC15M QSFP-100G-AOC20M QSFP-100G-AOC25M QSFP-100G-AOC30M QSFP-H40G-AOC1M QSFP-H40G-AOC2M QSFP-H40G-AOC3M QSFP-H40G-AOC5M QSFP-H40G-AOC7M QSFP-H40G-AOC10M QSFP-H40G-AOC15M	Active optical cable assembly	8.0(1)
	WSP-Q40G-LR4L	40GBASE-LR4 QSFP40G (for Single-mode Fiber (SMF))	8.0(1)

Table 4 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
N77-M324FQ-25L	CVR-QSFP-SFP10G FET-10G SFP-10G-SR SFP-10G-SR-S DWDM-SFP10G-xx.xx[3] SFP-10G-BXD-I SFP-10G-BXU-I SFP-10G-LRM SFP-10G-ER SFP-10G-ER-S SFP-10G-LR SFP-10G-LR-S SFP-10G-ZR SFP-10G-ZR-S SFP-H10GB-CU1M SFP-H10GB-CU1-5M SFP-H10GB-CU2M SFP-H10GB-CU2-5M SFP-H10GB-CU3M SFP-H10GB-CU5M SFP-H10GB-ACU7M SFP-H10GB-ACU10M SFP-10G-AOC1M SFP-10G-AOC2M SFP-10G-AOC3M SFP-10G-AOC5M SFP-10G-AOC7M SFP-10G-AOC10M	QSFP 40G to SFP+ 10G Adapter Module	8.2(1)
	FET-40G	Cisco Fabric Extender Transceiver (FET)	8.1(1)
	QSFP-40G-CSR4 QSFP-40G-SR4 QSFP-40G-SR4-S QSFP-40G-SR-BD	Multi-mode fiber (MMF)	7.3(0)DX(1)

Table 4 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	QSFP-40G-ER4 QSFP-40G-LR4 QSFP-40G-LR4-S QSFP-4X10G-LR-S WSP-Q40G-LR4L	Single-mode fiber (SMF)	7.3(0)DX(1)
	QSFP-H40G-ACU7M QSFP-H40G-ACU10M	Direct attach copper, active	7.3(0)DX(1)
	QSFP-4X10G-AC7M QSFP-4X10G-AC10M	Direct attach breakout copper, active	8.0(1)
	QSFP-H40G-AOC1M QSFP-H40G-AOC2M QSFP-H40G-AOC3M QSFP-H40G-AOC5M QSFP-H40G-AOC7M QSFP-H40G-AOC10M QSFP-H40G-AOC15M	Active optical cable assembly	7.3(0)DX(1)
	QSFP-4X10G-AOC1M QSFP-4X10G-AOC2M QSFP-4X10G-AOC3M QSFP-4X10G-AOC5M QSFP-4X10G-AOC7M QSFP-4X10G-AOC10M	Active optical breakout cable assembly	8.0(1)
N77-M348XP-23L	FET-10G	Cisco Fabric Extender Transceiver (FET)	8.1(1)
	GLC-TE	Category 5	7.3(0)DX(1)
	GLC-LH-SMD GLC-SX-MMD	Multi-mode fiber (MMF)	7.3(0)DX(1)
	CWDM-SFP-xxxx[2] DWDM-SFP-xxxx GLC-BX-U GLC-BX-D GLC-EX-SMD GLC-LH-SMD GLC-ZX-SMD	Single-mode fiber (SMF)	7.3(0)DX(1)

Table 4 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	SFP-10G-SR	Multi-mode fiber (MMF)	7.3(0)DX(1)
	SFP-10G-SR-S	10G BASE-SR SFP+ transceiver module for Multi-mode fiber (MMF)	8.0(1)
	DWDM-SFP10G-xx.xx[3] SFP-10G-BXD-I SFP-10G-BXU-I SFP-10G-LRM	Single-mode fiber (SMF)	7.3(0)DX(1)
	SFP-10G-ER	10G BASE-LR SFP+ transceiver module for Single-mode fiber (SMF)	7.3(0)DX(1)
	SFP-10G-ER-S	10G BASE-LR SFP+ transceiver module for Single-mode fiber (SMF)	8.0(1)
	SFP-10G-LR	10G BASE-LR SFP+ transceiver module for Single-mode fiber (SMF)	7.3(0)DX(1)
	SFP-10G-LR-S	10G BASE-LR SFP+ transceiver module for Single-mode fiber (SMF)	8.0(1)
	SFP-10G-ZR	10G BASE-LR SFP+ transceiver module for Single-mode fiber (SMF)	7.3(0)DX(1)
	SFP-10G-ZR-S	10G BASE-LR SFP+ transceiver module for Single-mode fiber (SMF)	8.0(1)
	SFP-H10GB-CU1M SFP-H10GB-CU1-5M SFP-H10GB-CU2M SFP-H10GB-CU2-5M SFP-H10GB-CU3M SFP-H10GB-CU5M	Twinax cable assembly, passive	7.3(0)DX(1)
	SFP-H10GB-ACU7M SFP-H10GB-ACU10M	Twinax cable assembly, active	7.3(0)DX(1)

Table 4 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	SFP-10G-AOC1M SFP-10G-AOC2M SFP-10G-AOC3M SFP-10G-AOC5M SFP-10G-AOC7M SFP-10G-AOC10M	Active optical cable assembly	7.3(0)DX(1)
N7K-M202CF-22L	CFP-40G-SR4	40GBASE-SR4 CFP	6.1(2)
	CFP-40G-LR4	40GBASE-LR4 CFP	6.1(2)
	CFP-100G-SR10	100GBASE-SR10 CFP	6.1(3)
	CFP-100G-LR4	100GBASE-LR4 CFP	6.1(1)
	CFP-100G-ER4	100GBASE-ER4 CFP	6.2(10)
N7K-M206FQ-23L	FET-40G	Cisco 40G Fabric Extender Transceiver (FET)	6.2(6)
	QSFP-40G-SR-BD	Cisco 40G BiDi QSFP+	6.2(6)
	QSFP-40G-SR4 QSFP-40G-SR4-S	40GBASE-SR4 QSFP+	6.1(1)
	QSFP-40G-CSR4	40GBASE-CSR4 QSFP+	6.2(2)
	QSFP-40GE-LR4 QSFP-40G-LR4-S	40GBASE-LR4 QSFP+	6.1(4)
	QSFP-H40G-ACUxM	40GBASE-CR4 QSFP+ Direct Attach Copper Cable Active (7 m, 10 m)	6.2(2)
	QSFP-4X10G-ACxM	40GBASE-CR4 QSFP+ to 4x SFP+ Twinax Direct Attach Copper Breakout Cable Active (7 m, 10 m)	6.2(8)
	QSFP-H40G-AOCxM	40GBASE-AOC (Active Optical Cable) QSFP Cable (1 m, 2 m, 3 m, 5 m, 7 m, 10 m)	6.2(8)
	QSFP-H40G-AOC15M	40GBASE-AOC (Active Optical Cable) QSFP Cable (15m)	7.2(0)D1(1)
	QSFP-4X10G-AOCxM	40GBASE-AOC (Active Optical Cable) QSFP to 4x10G SFP+ Breakout Cable (1 m, 2 m, 3 m, 5 m, 7 m, 10 m)	6.2(8)
	WSP-Q40GLR4L	40GBASE-LR4 lite (2km SMF) QSFP+	62(10)

Table 4 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	QSFP-40G-LR4	40GBASE-LR4 QSFP+ (Ethernet and OTU3 capable)	6.2(12)
	QSFP-40G-ER4	40GBASE-ER4 QSFP+ (40km)	6.2(12)
N7K-M324FQ-25L	CVR-QSFP-SFP10G FET-10G SFP-10G-SR SFP-10G-SR-S DWDM-SFP10G-xx.xx[3] SFP-10G-BXD-I SFP-10G-BXU-I SFP-10G-LRM SFP-10G-ER SFP-10G-ER-S SFP-10G-LR SFP-10G-LR-S SFP-10G-ZR SFP-10G-ZR-S SFP-H10GB-CU1M SFP-H10GB-CU1-5M SFP-H10GB-CU2M SFP-H10GB-CU2-5M SFP-H10GB-CU3M SFP-H10GB-CU5M SFP-H10GB-ACU7M SFP-H10GB-ACU10M SFP-10G-AOC1M SFP-10G-AOC2M SFP-10G-AOC3M SFP-10G-AOC5M SFP-10G-AOC7M SFP-10G-AOC10M	QSFP 40G to SFP+ 10G Adapter Module	8.2(1)
	FET-40G	Cisco Fabric Extender Transceiver (FET)	8.1(1)
	QSFP-H40G-ACUxM	Direct attach copper, active	8.0(1)

Table 4 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	QSFP-H40G-AOCxM	Active optical cable assembly	8.0(1)
	QSFP-4X10G-AC7M	Direct attach breakout copper, active	8.0(1)
	QSFP-4X10G-AC10M	Direct attach breakout copper, active	8.0(1)
	QSFP-4X10G-ACUxM	Direct attach breakout copper, active	8.0(1)
	QSFP-4X10G-AOC1M	Active optical breakout cable assembly	8.0(1)
	QSFP-4X10G-AOC2M	Active optical breakout cable assembly	8.0(1)
	QSFP-4X10G-AOC3M	Active optical breakout cable assembly	8.0(1)
	QSFP-4X10G-AOC5M	Active optical breakout cable assembly	8.0(1)
	QSFP-4X10G-AOC7M	Active optical breakout cable assembly	8.0(1)
	QSFP-4X10G-AOC10M	Active optical breakout cable assembly	8.0(1)
	QSFP-40G-CSR4	Multi-mode fiber (MMF)	8.0(1)
	QSFP-40G-ER4	Single-mode fiber (SMF)	8.0(1)
	QSFP-4x10G-LR-S	Single-mode fiber (SMF)	8.0(1)
	QSFP-40G-LR4	Single-mode fiber (SMF)	8.0(1)
	QSFP-40G-LR4-S	Single-mode fiber (SMF)	8.0(1)
	QSFP-40G-SR4	Multi-mode fiber (MMF)	8.0(1)
	QSFP-40G-SR4-S	Multi-mode fiber (MMF)	8.0(1)
	QSFP-40G-SR-BD	Multi-mode fiber (MMF)	8.0(1)
N7K-M348XP-25L	CWDM-SFP-xxxx[2]	Single-mode fiber (SMF)	7.3(0)DX(1)
	CWDM-SFP 10G-1xxx	Single-mode fiber (SMF)	8.0(1)
	DWDM-SFP-xxxx	Single-mode fiber (SMF)	7.3(0)DX(1)
	DWDM-SFP 10G-xx.xx	Single-mode fiber (SMF)	8.0(1)
	FET-10G	Cisco Fabric Extender Transceiver (FET)	8.1(1)

Table 4 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	GLC-BX-U GLC-BX-D GLC-EX-SMD GLC-LH-SMD GLC-ZX-SMD	Single-mode fiber (SMF)	7.3(0)DX(1)
	GLC-LH-SMD GLC-SX-MMD	Multi-mode fiber (MMF)	7.3(0)DX(1)
	GLC-TE	Category 5	7.3(0)DX(1)
	SFP-10G-AOCxM	Active optical cable assembly	8.0(1)
	SFP-10G-BXU-I	Single-mode fiber (SMF)	8.0(1)
	SFP-10G-BXD-I	Single-mode fiber (SMF)	8.0(1)
	SFP-10G-ER	Single-mode fiber (SMF)	8.0(1)
	SFP-10G-LR	Single-mode fiber (SMF)	8.0(1)
	SFP-10G-LRM	Single-mode fiber (SMF)	8.0(1)
	SFP-10G-SR	Multi-mode fiber (MMF)	8.0(1)
	SFP-10G-ZR	Single-mode fiber (SMF)	8.0(1)
	SFP-H10GB-ACU7M	Twinax cable assembly, active	8.0(1)
	SFP-H10GB-ACU10M	Twinax cable assembly, active	8.0(1)
	SFP-H10GB-CU1M	Twinax cable passive	8.0(1)
	SFP-H10GB-CU1-5M	Twinax cable passive	8.0(1)
	SFP-H10GB-CU2M	Twinax cable passive	8.0(1)
	SFP-H10GB-CU2-5M	Twinax cable passive	8.0(1)
	SFP-H10GB-CU3M	Twinax cable passive	8.0(1)
	SFP-H10GB-CU5M	Twinax cable passive	8.0(1)

[1]Minimum version supported is -02.

[2]CWDM-SFP-xxxx is supported only with 1-Gigabit Ethernet I/O modules.

[3]DWDM-SFP10G-C is not supported.

[4]For Cisco NX-OS 8.x releases, CPAK-100G-SR4 is supported from Cisco NX-OS Release 8.1(1).

[#]If you remove and reinsert a CPAK, reinsertion must be delayed by at least 30 seconds. This enables the device to discharge completely and power up properly upon reinsertion.

Note For a complete list of supported optical transceivers, see the Cisco Transceiver Module Compatibility Information page.

Guidelines and Limitations

This section includes the following topics:

Guidelines and Limitations—Cisco NX-OS Release 8.4(5)

There are no specific guidelines and limitations applicable to Cisco NX-OS Release 8.4(5). The guidelines listed for Cisco NX-OS Release 8.4(1) is also applicable to Cisco NX-OS Release 8.4(5).

Guidelines and Limitations—Cisco NX-OS Release 8.4(4a)

There are no specific guidelines and limitations applicable to Cisco NX-OS Release 8.4(4a). The guidelines listed for Cisco NX-OS Release 8.4(1) is also applicable to Cisco NX-OS Release 8.4(4a).

Guidelines and Limitations—Cisco NX-OS Release 8.4(4)

There are no specific guidelines and limitations applicable to Cisco NX-OS Release 8.4(4). The guidelines listed for Cisco NX-OS Release 8.4(1) is also applicable to Cisco NX-OS Release 8.4(4).

Guidelines and Limitations—Cisco NX-OS Release 8.4(3)

There are no specific guidelines and limitations applicable to Cisco NX-OS Release 8.4(3). The guidelines listed for Cisco NX-OS Release 8.4(1) is also applicable to Cisco NX-OS Release 8.4(3).

Guidelines and Limitations—Cisco NX-OS Release 8.4(2)

There are no specific guidelines and limitations applicable to Cisco NX-OS Release 8.4(2). The guidelines listed for Cisco NX-OS Release 8.4(1) is also applicable to Cisco NX-OS Release 8.4(2).

Guidelines and Limitations—Cisco NX-OS Release 8.4(1)

The following guidelines and limitations are applicable to Cisco NX-OS Release 8.4(1):

- A system configured with EIGRP 64bit metric version and having 32bit metric version neighbors precision in delay conversion from 64bit metric to 32bit metric and from 32bit metric to 64bit metric is improved. It implies that the 32bit metric of prefixes in the 64bit EIGRP system and 64bit metric of prefixed in 32bit EIGRP system changes from previous releases. This is not applicable for the 32bit metric EIGRP system or if all neighbors are the 64bit metric version.
- Support for the RISE feature has been deprecated in Cisco NX-OS Release 8.4(1).
- In a system with large routing table of approximately 250K routes and over, a M3 module upon reload may go online before the full routing table is populated in its TCAM. This issue is fixed in CSCvn25428.However, even with the fix in CSCvn25428, if multiple M3 modules reload in tandem, some of the modules may go online without the full routing table in TCAM. There is no fix for this case. This is a known limitation.
- Beginning with Cisco NX-OS Release 8.4(1), it is recommended to use agent-less configuration management systems such as Puppet or Ansible with the Cisco Nexus 7000 Series switches; as the Open Agent Container (OAC) support will be deprecated in the future releases. This OAC feature was added in the Cisco NX-OS Release 7.3(0)D1(1) with the purpose of providing and execution space for configuration management. For more details see Cisco Nexus 7000 Series NX-OS Programmability Guide.
- Cisco NX-OS Release 8.4(1) addresses a vulnerability, CVE-2019-1649 in N77-SUP3E platform. After upgrading or booting to Cisco NX-OS Release 8.4(1), an explicit EPLD upgrade needs to be done to address this vulnerability effectively. EPLD upgrade can be initiated using the **install module** *sup_module_no* **epld system** *path_of_system_image* command. This step is not needed if the setup has a**uto epld upgrade** option enabled.
- When you upgrade Supervisor 2, Supervisor 2E, and Supervisor 3E to Cisco NX-OS Release 8.4(1) with dual supervisors, the management interface of the of HA-Standby supervisor flaps every 30 minutes. The flap is detected on the peer switch interface, which is connected to the mgmt 0 interface of HA-Standby as link down event.
  The flap occurs because of the new feature introduced in Cisco NX-OS Release 8.4(1) where the management loopback test is run periodically on the HA-Standby supervisor. This is an expected behaviour.
  In order stop the link flap on peer switch this loopback test has to be disabled. To disable the loopback test for standby supervisor run the **no diagnostic monitor module <***standby sup module number***> test 15** command on the active supervisor.
- With the new BIOS, the image name length for Supervisor 2, Supervisor 2E, and Supervisor 3E modules is changed to a maximum of 256 characters. Meanwhile, the image name length is still restricted to 128 characters for kick start and system images. Hence make sure that you do not use more than 128 characters in image names.
- During the supervisor 2 to supervisor 3 module migration do not disturb the testbed, i.e., do not plug in or plug out, power down, reload, and reset the modules and ports. If you do any of these tasks the migration might fail or might give undesirable results. You can use only the show commands during the migration.
- The default max-bundle value has been enhanced to 32 for Cisco Nexus 7000 Series switch from Cisco NX-OS Release 8.4(1). The previous max-bundle value of 16 is now considered as non-default and this value is displayed in the show running configuration and show running all configuration output after the upgrade to Cisco NX-OS Release 8.4(1). You can configure no lacp max-bundle 16 on previously configured port-channel to reflect system default to 32.

For information on features related to Cisco NX-OS Release 8.4(1) see New and Enhanced Software Features - Cisco NX-OS Release 8.4(1), page 68.

Guidelines and Limitations Common for Cisco NX-OS Release 8.x

The following guidelines and limitations are applicable to Cisco NX-OS Release 8.0(1) and later releases.

Beginning with Cisco NX-OS Release 8.0(1), the following M1-Series I/O modules are not supported:

- Cisco Nexus 7000 M1-Series 48-port Gigabit Ethernet Module with XL Option (SFP optics) (N7K-M148GS-11L)
- Cisco Nexus 7000 M1-Series 48-port 10/100/1000 Ethernet Module with XL Option (RJ45) (N7K-M148GT-11L)
- Cisco Nexus 7000 M1-Series 32 Port 10GbE with XL Option, 80G Fabric (requires SFP+) (N7K-M132XP-12L)
- Cisco Nexus 7000 M1-Series 8-Port 10 Gigabit Ethernet Module with XL Option (requires X2) (N7K-M108X2-12L)

Beginning with Cisco NX-OS Release 8.0(1), the following F2-Series I/O modules are not supported:

- Nexus 7000 F2-Series 48 Port 1G/10G Ethernet Module, SFP/SFP+ (and spare) (N7K-F248XP-25, N7K-F248XP-25=)

VXLAN BGP EVPN in VDCs having M3 modules

The following features are not supported for VXLAN BGP EVPN in VDCs having M3 modules:

- EVPN VXLAN leaf functionality (except Border Leaf functionality) is not supported.
- LISP hand off is not supported.
- Hosts connected behind FEX is not supported.

EVPN Border Leaf Hand Off Limitation in M3 Module

This limitation is on the EVPN to VRF lite hand off.

If EVPN fabric connected interface is on a M3 module and VRF lite interface is on F3 module, south to north traffic will be dropped on the border leaf.

Smart Licensing Show Commands are Missing on Non-Default VDC Context

Smart Licensing show commands are missing on the non-default VDC context. The work around is to use the default VDC to verify license related show outputs.

OTV Traffic Fails on VXLAN EVPN Border Leaf Due To ARP Resolution Failure

OTV traffic fails on VXLAN EVPN border leaf due to ARP resolution failure. This issue occurs on the following conditions:

- Dual switch VPC Border Leaf
- M3 only VDC setup
- vPC legs connected to OTV VDC
- Reloading the switch
- Using **shutdown** and **no shutdown** commands on the port-channel logical interface

The workaround to his issue is to do a ‘shutdown’ and ‘no shutdown’ of vPC port-channel member interfaces from both the vPC switches and then re-send the ARP for the flows.

Note Port-channel interface shut and no shut may not work,

Native VLAN Change Causes Link Flap

Changing the native VLAN on an access port or trunk port will flap the interface. This behavior is expected.

Passive Copper Optic Cables are not Supported on the Non EDC Ports

Passive copper optic cables are not supported on the non-EDC ports.

The delay in link up event in SFP+ implementation is due to a factor called Electronic Dispersion Compensation (EDC). EDC ports mitigate power penalties associated with optical link budgets. Receivers without EDC (for example - SFP, where there is no delay in bringing the port up) can recover an optical signal only if the dispersion is less than approximately one-half Unit Interval (UI) over the length of fiber.

QSFP passive copper (QSFP-H40G-CU1M, QSFP-H40G-CU3M, QSFP-H40G-CU5M), and copper breakout cables (QSFP-4SFP10G-CU1M, QSFP-4SFP10G-CU3M, QSFP-4SFP10G-CU5M) are not supported on the following modules:

– N7K-M206FQ-23L

– N7K-F312FQ-25

– N77-F324FQ-25

The workaround to this limitation is to use active optical cables (QSFP-H40G-AOC1M, QSFP-H40G-AOC3M, QSFP-H40G-AOC5M) and active optical breakout cables (QSFP-4X10G-AOC1M, QSFP-4X10G-AOC3M, QSFP-4X10G-AOC5M).

The passive optics (N7K M3 40G, N77 M3 40G, and N77 M3 100G) are not supported on the following modules:

– N7K-M324FQ-25L

– N77-M324FQ-25L

– N77-M312CQ-26L

MPLS over GRE

MPLS over GRE is not supported on F3 modules.

VLAN Translation on Fabric Extender Is Not Supported

VLAN translation on fabric extender is not supported. If you need to map a VLAN, you must move the interface to the parent switch and then configure the VLAN translation on the switches directly. The VLAN translation configuration is applicable for trunk ports connecting two data centers.

The no hardware ejector enable Command is Not Recommended for Long-Term Use

The **no hardware ejector enable** command cannot be configured and persistently saved in the startup configuration. This command is intended for temporary usage.

To work around this limitation, do not physically remove an active supervisor. Instead, use the **system switchover** command to switch to the standby supervisor.

This applies only to the Cisco Nexus 7700 Series switches.

Saving VLAN Configuration Information

Because a VLAN configuration can be learned from the network while the VLAN Trunking Protocol (VTP) is in a server/client mode, the VLAN configuration is not stored in the running configuration. If you copy the running configuration to a file and apply this configuration at a later point, including after a switch reload, the VLANs will not be restored. However, the VLAN configuration will be erased if the switch is the only server in the VTP domain.

To work around this limitation, perform one of the following tasks:

- Configure one of the clients as the server.
- Complete these steps:
  1. Copy the VTP data file to the bootflash: data file by executing the **copy vtp-datafile bootflash:vtp-datafile** command.
  2. Copy the ASCII configuration to the startup configuration by executing the **copy ascii-cfg-file startup-config** command.
  3. Reload the switch.

This limitation does not apply to a binary configuration, which is the recommended approach, only for an ASCII configuration.

Behavior of Control Plane Packets in an F2e Series Module

To support the coexistence of an F2e Series module with an M Series module in the same VDC, the F2e Series module operates in a proxy mode so that all the Layer 3 traffic is sent to an M Series module in the same VDC. For F2e proxy mode, having routing adjacencies connected through F2e interfaces with an M1 Series module is not supported. However, routing adjacencies connected through F2e interfaces with an M2 Series module is supported.

Error Appears When Copying a File to the Running Configuration

Copying a file to the running configuration can trigger an error and the following message is displayed:

```
"WARNING! there is unsaved configuration"
```

This issue might occur if the configuration contains SNMP-related configurations to send traps or notifications, and if the file that is to be copied to the running configuration contains only EXEC **show** commands.

When the following message is displayed, enter **y**.

```
"This command will reboot the system. (y/n)? [n] y."
```

Note that there is no operational impact and no configuration loss when the switch reloads.

PONG in a vPC Environment

PONG is not supported in a vPC environment in the following scenarios:

- In a vPC environment, a PONG to an access switch or from an access switch might fail. To work around this issue, use the interface option while executing a PONG from an access switch to a vPC peer. The interface can be one that does not have to go over the peer link, such as an interface that is directly connected to the primary switch.

- When FabricPath is enabled and there are two parallel links on an F2 Series module, PONG might fail. To work around this issue, form a port channel with the two links as members.

For more details on PONG, refer to the *Cisco Nexus 7000 Series NX-OS Troubleshooting Guide*.

LISP Traffic

A Layer 3 link is required between aggregation switches when deploying LISP host mobility on redundant LISP Tunnel Routers (xTRs) that are a part of a vPC. In rare (but possible) scenarios, failure to deploy this Layer 3 link might result in traffic being moved to the CPU and potentially dropped by the Control Plane Policing (CoPP) rate limiters.

Standby Supervisor Might Reset with a Feature-Set Operation

The standby supervisor might reload when a feature-set operation (install, uninstall, enable, or disable) is performed if the high availability (HA) state of the standby supervisor is not "HA standby" at the time of the feature-set operation. To prevent the reload, ensure that the state of the standby supervisor is "HA standby." To check the HA state for the specific virtual device context (VDC) where the feature-set operation is performed, enter the **show system redundancy ha status** command on the active supervisor.

A reload of the standby supervisor has no operational impact because the active supervisor is not affected.

In addition, if you perform a feature-set operation while modules are in the process of coming up, then those modules are power cycled. Modules that are up and in the OK state are not power cycled when you perform a feature-set operation.

Unfair Traffic Distribution for Flood Traffic

Uneven load balancing of flood traffic occurs when you have a seven-member port channel. This behavior is expected, and occurs on all M Series and F Series modules. In addition, M Series modules do not support Result Bundle Hash (RBH) distribution for multicast traffic.

BFD Not Supported on the MTI Interface

If bidirectional forwarding detection (BFD) on Protocol Independent Multicast (PIM) is configured together with MPLS multicast VPN (MVPN), the following error might appear:

```
2012 Jan 3 15:16:35 dc3_sw2-dc3_sw2-2 %PIM-3-BFD_REMOVE_FAIL: pim [22512] Session remove
request for neighbor 11.0.3.1 on interface Ethernet2/17 failed (not enough memory)
```

This error is benign. To avoid the error, disable BFD on the multicast tunnel interface (MTI) interface.

For every multicast domain of which an multicast VRF is a part, the PE router creates a MTI. MTI is an interface the multicast VRF uses to access the multicast domain.

Role-Based Access Control

You can configure role-based access control (RBAC) in the Cisco Nexus 7000 storage VDC using Cisco NX-OS CLI commands. You cannot configure RBAC in the Cisco Nexus 7000 storage VDC using Cisco Data Center Network Manager (DCNM). Note that RBAC in the storage VDC and in the Cisco Nexus 7000 Series switches is the same, which is different from that for the Cisco MDS 9500 Series Multilayer Directors.

RBAC CLI scripts used in Cisco MDS 9500 Series Multilayer Directors cannot be applied to the storage VDC configured for a Cisco Nexus 7000 Series switch.

You cannot distribute the RBAC configuration between a Cisco MDS 9500 Series switch and the storage VDC configured for a Cisco Nexus 7000 Series switch. To prevent this distribution, assign RBAC in Cisco MDS and the Cisco Nexus 7000 storage VDC to different Cisco Fabric Services (CFS) regions.

Limitation on the Level 4 Protocol Entries on the M Series Modules

The M Series modules support only 7 entries for Layer-4 protocols (L4Ops).

Network Analysis Module (NAM-NX1)

Cisco Nexus 7000 Series Network Analysis Module (NAM-NX1) is not supported.

SVI Statistics on an F2 Series Module

F2 Series I/O modules do not support per-VLAN statistics. Therefore, the **show interface** command will not display per-VLAN Rx or Tx counters or statistics for switch virtual interfaces (SVIs).

TrustSec SGT on the F3 Series Modules

F3 Series I/O modules require a dot1q header to be present for proper processing and transport of SGT-tagged packets. For Layer 2 switch ports use trunked interfaces instead of an access VLAN. Layer 3 interfaces should be configured as an L3 subinterface to force the dot1q over the L3 interconnection.

Fabric Module Removal on the Cisco Nexus 7700 Switches

When a fabric module is power cycled or removed momentarily during an online insertion and removal (OIR) from slot 5 or slot 6 on a Fabric 2 module in a Cisco Nexus 7700 switch, packet drops can occur. This limitation is not applicable to Cisco Nexus 7702 Switches.

Fabric Utilization on the Cisco Nexus 7700 Switches

When traffic ingresses from a module on the Cisco Nexus 7700 switch at a rate much below the line rate, uniform fabric utilization does not occur across the fabric modules. This behavior is expected and reflects normal operation based on the fabric autospreading technology used in the Cisco Nexus 7700 switch.

MTU Changes do not Take Effect on FEX Queues

When you change the interface MTU on a fabric port, the configured MTU on the FEX ports are not configured to the same value. This issue occurs when the interface MTU changes on a fabric port.

The configured MTU for the FEX ports is controlled by the network QoS policy. To change the MTU that is configured on the FEX ports, modify the network QoS policy to also change when the fabric port MTU is changed.

Multicast Traffic is Forwarded to FEX Ports

Multicast traffic that is sent to Optimized Multicast Flooding (OMF) Local Targeting Logic (LTL) is forwarded to FEX ports that are not a part of the bridge domain (BD). This issue occurs when multicast traffic is sent to OMF LTL, which occurs if an unknown unicast flooding occurs when OMF is enabled.

FEX interfaces can support multicast routers, but OMF must be disabled on those VLANs. If there is a multicast MAC address mismatch on the VLAN, traffic will be flooded in the VLAN and will eventually reach the router behind the FEX port.

F2 Connectivity Restrictions on Connecting Ports to an FEX

If an ASCII configuration has incompatible ports, such as when the configuration is created with ports that are added to an FEX from different modules or VDC types, the ports might be added without warnings.

When connecting F2 Series ports to the same FEX, make sure the VDC type is the same as in the source configuration that is being replicated.

DHCP Snooping and vPC+ FEX

DHCP snooping is not supported when the vPC+ FEX feature is enabled.

Upgrade and Downgrade Paths and Caveats

This section includes information about upgrading and downgrading Cisco NX-OS software on Cisco Nexus 7000 Series switches. It includes the following sections:

Supported Upgrade and Downgrade Paths

Before you upgrade or downgrade your Cisco NX-OS software, we recommend that you read the complete list of caveats in this section to understand how an upgrade or downgrade might affect your network, depending on the features that you have configured.

Note Do not change any configuration settings or network settings during a software upgrade. Changes to the network settings might cause a disruptive upgrade.

Releases that are not listed for a particular release train do not support a direct ISSU.

Non-disruptive in-service software downgrades (ISSD) are not supported in the Cisco NX-OS 8.x releases.

Note For a nondisruptive upgrade dual supervisor modules are required.

ISSU Paths for Cisco NX-OS Release 8.4(5)

See Table 5 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.4(5).

Note Only the ISSU paths/combinations in Table 5 have been tested and are supported.

Table 5 Supported ISSU Paths for Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switch (Cisco NX-OS Release 8.4(4a))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 8.4(5)	8.4(4a)
	8.4(4)
	8.4(3)
	8.4(2)
	8.4(1)
	8.3(2)
	8.3(1)
	8.2(8)
	8.2(7a)
	8.2(6)
	8.2(5)
	8.2(4)
	8.2(3)
	8.2(2)
	8.2(1)
	8.1(2a)
	8.1(2)
	7.3(8)D1(1)
	7.3(7)D1(1)
	7.3(6)D1(1)
	7.3(5)D1(1)
	7.3(4)D1(1)
	7.3(3)D1(1)
	7.3(2)D1(3a)
	7.3(2)D1(3)
	7.3(2)D1(2)

Note ISSU from 8.2(8) to any higher releases like 8.3(1), 8.3(2), 8.4(1), 8.4(2), 8.4(3), 8.4(4), 8.4(4a) will be disruptive if M3 linecards are present.

ISSU Paths for Cisco NX-OS Release 8.4(4a)

See Table 6 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.4(4a).

Note Only the ISSU paths/combinations in Table 6 have been tested and are supported.

Table 6 Supported ISSU Paths for Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switch (Cisco NX-OS Release 8.4(4a))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 8.4(4a)	8.4(4)
	8.4(3)
	8.4(2)
	8.4(1)
	8.3(2)
	8.3(1)
	8.2(8)
	8.2(7a)
	8.2(6)
	8.2(5)
	8.2(4)
	8.2(3)
	8.2(2)
	8.2(1)
	8.1(2a)
	8.1(2)
	7.3(8)D1(1)
	7.3(7)D1(1)
	7.3(6)D1(1)
	7.3(5)D1(1)
	7.3(4)D1(1)
	7.3(3)D1(1)
	7.3(2)D1(3a)
	7.3(2)D1(3)
	7.3(2)D1(2)

Note ISSU from 8.2(8) to any higher releases like 8.3(1), 8.3(2), 8.4(1), 8.4(2), 8.4(3), 8.4(4), 8.4(4a) will be disruptive if M3 linecards are present.

Note After ISSU from 8.2(7) or 8.4(4) to 8.4(4a) and if SCALABLE_SERVICES_PKG is installed and in use, you must reload M2 linecard.

ISSU Paths for Cisco NX-OS Release 8.4(4)

See Table 7 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.4(4).

Note Only the ISSU paths/combinations in Table 7 have been tested and are supported.

Table 7 Supported ISSU Paths for Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switch (Cisco NX-OS Release 8.4(4))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 8.4(4)	8.4(3)
	8.4(2)
	8.4(1)
	8.3(2)
	8.3(1)
	8.2(8)
	8.2(7a)
	8.2(6)
	8.2(5)
	8.2(4)
	8.2(3)
	8.2(2)
	8.2(1)
	8.1(2a)
	8.1(2)
	7.3(8)D1(1)
	7.3(7)D1(1)
	7.3(6)D1(1)
	7.3(5)D1(1)
	7.3(4)D1(1)
	7.3(3)D1(1)
	7.3(2)D1(3a)
	7.3(2)D1(3)
	7.3(2)D1(2)

Note ISSU from 8.2(8) to any higher releases like 8.3(1), 8.3(2), 8.4(1), 8.4(2), 8.4(3), 8.4(4), 8.4(4a) will be disruptive if M3 linecards are present.

ISSU Paths for Cisco NX-OS Release 8.4(3)

See Table 8 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.4(3).

Note Only the ISSU paths/combinations in Table 8 have been tested and are supported.

Table 8 Supported ISSU Paths for Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switch (Cisco NX-OS Release 8.4(3))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 8.4(3)	8.4(2)
	8.4(1)
	8.3(2)
	8.3(1)
	8.2(8)
	8.2(7a)
	8.2(6)
	8.2(5)
	8.2(4)
	8.2(3)
	8.2(2)
	8.2(1)
	8.1(2a)
	8.1(2)
	7.3(8)D1(1)
	7.3(7)D1(1)
	7.3(6)D1(1)
	7.3(5)D1(1)
	7.3(4)D1(1)
	7.3(3)D1(1)
	7.3(2)D1(3a)
	7.3(2)D1(3)
	7.3(2)D1(2)

Note ISSU from 8.2(8) to any higher releases like 8.3(1), 8.3(2), 8.4(1), 8.4(2), 8.4(3), 8.4(4), 8.4(4a) will be disruptive if M3 linecards are present.

Note Multi hop ISSU is not supported. If you are upgrading from a release other than the nondisruptive upgrade releases listed in Table 8, a reload is required.

ISSU Paths for Cisco NX-OS Release 8.4(2)

See Table 9 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.4(2).

Note Only the ISSU paths/combinations in Table 9 have been tested and are supported.

Table 9 Supported ISSU Paths for Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switch (Cisco NX-OS Release 8.4(2))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 8.4(2)	8.4(1)
	8.3(2)
	8.3(1)
	8.2(8)
	8.2(7a)
	8.2(6)
	8.2(5)
	8.2(4)
	8.2(3)
	8.2(2)
	8.2(1)
	8.1(2a)
	8.1(2)
	7.3(8)D1(1)
	7.3(7)D1(1)
	7.3(6)D1(1)
	7.3(5)D1(1)
	7.3(4)D1(1)
	7.3(3)D1(1)
	7.3(2)D1(3a)
	7.3(2)D1(3)
	7.3(2)D1(2)

Note ISSU from 8.2(8) to any higher releases like 8.3(1), 8.3(2), 8.4(1), 8.4(2), 8.4(3), 8.4(4), 8.4(4a) will be disruptive if M3 linecards are present.

Note Multi hop ISSU is not supported. If you are upgrading from a release other than the nondisruptive upgrade releases listed in Table 9, a reload is required.

ISSU Paths for Cisco NX-OS Release 8.4(1)

See Table 10 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.4(1).

Note Only the ISSU paths/combinations in Table 10 have been tested and are supported.

Table 10 Supported ISSU Paths for Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switch (Cisco NX-OS Release 8.4(1))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 8.4(1)	8.3(2)
	8.3(1)
	8.2(8)
	8.2(7a)
	8.2(6)
	8.2(5)
	8.2(4)
	8.2(3)
	8.2(2)
	8.2(1)
	8.1(2a)
	8.1(2)
	7.3(8)D1(1)
	7.3(7)D1(1)
	7.3(6)D1(1)
	7.3(5)D1(1)
	7.3(4)D1(1)
	7.3(3)D1(1)
	7.3(2)D1(3a)
	7.3(2)D1(3)
	7.3(2)D1(2)

Note ISSU from 8.2(8) to any higher releases like 8.3(1), 8.3(2), 8.4(1), 8.4(2), 8.4(3), 8.4(4), 8.4(4a) will be disruptive if M3 linecards are present.

Note Multi hop ISSU is not supported. If you are upgrading from a release other than the nondisruptive upgrade releases listed in Table 10, a reload is required.

ISSU Upgrade

To perform an ISSU to Cisco NX-OS Release 8.0(1) and later releases, follow these steps:

1. Enter the **show running-config aclmgr inactive-if-config** command for all VDCs.
2. Enter the **clear inactive-config acl** command for all VDCs.
3. If the configuration has any mac packet-classify configurations on any interfaces, remove all of the configurations by entering the **no mac packet-classify** command.
4. Start the ISSU procedure.

In-Service Software Upgrade (ISSU) Caveats

- **ISSU upgrade from Cisco NX-OS 7.3.x releases to Cisco NX-OS Release 8.0(1)and later releases with RISE configuration:**
  - RISE configuration must be removed prior to starting your upgrade to Cisco NX-OS Release 8.0(1) and later releases. ISSU performs compatibility check and blocks the upgrade if RISE is configured.
    - If the RISE feature is not configured, there is no impact on the ISSU.
    - If the RISE feature is configured you will be prompted to remove this feature in order to proceed with the ISSU. You can proceed with the upgrade only after you disable this feature.
      - Sample CLI output:

```
"Running-config contains configuration that is incompatible with the new
image (strict incompatibility).
Please run 'show incompatibility-all system <image>' command to find out
which feature needs to be disabled.".
Pre-upgrade check failed. Return code 0x40930029 (Current running-config is
not supported by new image).
switch# show incompatibility-all system n7000-s2-dk9.8.0.1.bin

Checking incompatible configuration(s) for vdc 'switch':
--------------------------------------------------------
No incompatible configurations

Checking dynamic incompatibilities for vdc 'switch':
----------------------------------------------------
Service : iscm , UUID: 1144
Description : Rise ISSU script
Compatibility requirement: STRICT
Workaround:
ISSU from version < 8.0(1) not supported when Rise feature is enabled.
```

- **ISSU upgrade from Cisco NX-OS 7.3.x releases to Cisco NX-OS Release 8.0(1) and later releases with VXLAN configuration in a vPC setup**:

  ISSU upgrade from Cisco NX-OS 7.3.x releases to Cisco NX-OS Release 8.0(1) and later releases with VXLAN configuration in a vPC setup can result in a traffic loss when the second vPC peer is upgraded.

  The following upgrade steps are recommended as the workaround for this issue:

  - Shutdown vPC on the vPC secondary and reload with 8.0(1).
  - Perform no shut vpc after the system is operational,
  - Perform a vPC role change so that vPC secondary becomes a vPC primary.

  - Shutdown vPC on the other peer that is still running 7.3 release and reload with 8.0(1).
  - Perform no shut vpc after the system is operational,
  - Optionally, a vPC role change can be performed to get the latest peer back to vPC primary.
- If ISSU fails during a FEX module upgrade, you need to clear the flash as per the following steps and then proceed with the upgrade:
  - rlogin to the failing FEX—rlogin 192.0.2.<FEX-ID> -l root
  - umount /mnt/cfg
  - flash_eraseall /dev/mtd5
  - mount -t jffs2 -rw /dev/mtdblock5 /mnt/cfg

    The **mount** command enables you to mount a file from a source folder to a destination folder.
- FCoE FEX
  - After ISSU upgrade, you must change the port-channel load balance for FEX, that is, from default VDC, in order to apply load balancing for SAN traffic:

    Device(config)# **port-channel load-balance src-dst mac fex 101**
  - You can revert back to the default load balance after changing the load balance for FEX.
- For details on ISSU for other earlier releases refer to the following: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/7_x/nx-os/release/notes/7x_nx-os_release_note.html
- For multihop ISSU scenario for releases earlier than Cisco NX-OS Release 7.2(0) refer to the following:

  http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/release/notes/62_nx-os_release_note.html#pgfId-812362.

Non-ISSU Upgrade/Cold Boot Upgrade

Cisco NX-OS Release 8.4(5) supports the following cold boot support matrix:

Table 11 Supported Cold Boot Matrix in Cisco NX-OS Release 8.4(5)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
8.4(5)	8.4(4a)
	8.4(4)
	8.4(3)
	8.4(2)
	8.4(1)
	8.3(2)
	8.3(1)
	8.2(8)
	8.2(7a)
	8.2(6)
	8.2(5)
	8.2(4)
	8.2(3)
	8.2(2)
	8.2(1)
	8.1(2a), 8.1(2)
	8.1(1), 8.0(1)
	7.3(8)D1(1)
	7.3(7)D1(1)
	7.3(6)D1(1)
	7.3(5)D1(1)
	7.3(4)D1(1)
	7.3(3)D1(1)
	7.3(2)D1(3a), 7.3(2)D1(3)
	7.3(2)D1(2)
	7.3(2)D1(1)
	7.3(1)D1(1)
	7.3(0)DX(1), 7.3(0)D1(1)
	7.2(2)D1(2), 7.2(2)D1(1)
	7.2(1)D1(1), 7.2(0)D1(1)
	6.2(24a), 6.2(24)
	6.2(22), 6.2(20a), 6.2(20)
	6.2(18), 6.2(16), 6.2(14)
	6.2(12), 6.2(10)

Cisco NX-OS Release 8.4(4a) supports the following cold boot support matrix:

Table 12 Supported Cold Boot Matrix in Cisco NX-OS Release 8.4(4a)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
8.4(4a)	8.4(4)
	8.4(3)
	8.4(2)
	8.4(1)
	8.3(2)
	8.3(1)
	8.2(8)
	8.2(7a)
	8.2(6)
	8.2(5)
	8.2(4)
	8.2(3)
	8.2(2)
	8.2(1)
	8.1(2a), 8.1(2)
	8.1(1), 8.0(1)
	7.3(8)D1(1)
	7.3(7)D1(1)
	7.3(6)D1(1)
	7.3(5)D1(1)
	7.3(4)D1(1)
	7.3(3)D1(1)
	7.3(2)D1(3a), 7.3(2)D1(3)
	7.3(2)D1(2), 7.3(2)D1(1)
	7.3(1)D1(1)
	7.3(0)DX(1), 7.3(0)D1(1)
	7.2(2)D1(2), 7.2(2)D1(1)
	7.2(1)D1(1)
	7.2(0)D1(1)
	6.2(24a), 6.2(24)
	6.2(22), 6.2(20a), 6.2(20)
	6.2(18), 6.2(16), 6.2(14)
	6.2(12), 6.2(10)

Cisco NX-OS Release 8.4(4) supports the following cold boot support matrix:

Table 13 Supported Cold Boot Matrix in Cisco NX-OS Release 8.4(4)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
8.4(4)	8.4(3)
	8.4(2)
	8.4(1)
	8.3(2)
	8.3(1)
	8.2(8)
	8.2(7a), 8.2(6)
	8.2(5)
	8.2(4)
	8.2(3)
	8.2(2)
	8.2(1)
	8.1(2a), 8.1(2)
	8.1(1), 8.0(1)
	7.3(8)D1(1)
	7.3(7)D1(1)
	7.3(6)D1(1)
	7.3(5)D1(1)
	7.3(4)D1(1)
	7.3(3)D1(1)
	7.3(2)D1(3a), 7.3(2)D1(3)
	7.3(2)D1(2)
	7.3(2)D1(1)
	7.3(1)D1(1)
	7.3(0)DX(1), 7.3(0)D1(1)
	7.2(2)D1(2), 7.2(2)D1(1)
	7.2(1)D1(1)
	7.2(0)D1(1)
	6.2(24a), 6.2(24)
	6.2(22), 6.2(20a), 6.2(20)
	6.2(18), 6.2(16), 6.2(14)
	6.2(12), 6.2(10)

Cisco NX-OS Release 8.4(3) supports the following cold boot support matrix:

Table 14 Supported Cold Boot Matrix in Cisco NX-OS Release 8.4(3)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
8.4(3)	8.4(2)
	8.4(1)
	8.3(2)
	8.3(1)
	8.2(8)
	8.2(7a), 8.2(6)
	8.2(5)
	8.2(4)
	8.2(3)
	8.2(2)
	8.2(1), 8.1(2a)
	8.1(2)
	8.1(1)
	8.0(1)
	7.3(8)D1(1)
	7.3(7)D1(1)
	7.3(6)D1(1)
	7.3(5)D1(1)
	7.3(4)D1(1)
	7.3(3)D1(1)
	7.3(2)D1(3a), 7.3(2)D1(3)
	7.3(2)D1(2), 7.3(2)D1(1)
	7.3(1)D1(1), 7.3(0)DX(1)
	7.3(0)D1(1)
	7.2(2)D1(2)
	7.2(2)D1(1)
	7.2(1)D1(1)
	7.2(0)D1(1)
	6.2(24a), 6.2(24)
	6.2(22), 6.2(20a)
	6.2(20), 6.2(18)
	6.2(16), 6.2(14)
	6.2(12), 6.2(10)

Cisco NX-OS Release 8.4(2) supports the following cold boot support matrix:

Table 15 Supported Cold Boot Matrix in Cisco NX-OS Release 8.4(2)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
8.4(2)	8.4(1)
	8.3(2)
	8.3(1)
	8.2(8)
	8.2(7a), 8.2(6)
	8.2(5)
	8.2(4)
	8.2(3)
	8.2(2)
	8.2(1)
	8.1(2a), 8.1(2)
	8.1(1)
	8.0(1)
	7.3(8)D1(1)
	7.3(7)D1(1)
	7.3(6)D1(1)
	7.3(5)D1(1)
	7.3(4)D1(1)
	7.3(3)D1(1)
	7.3(2)D1(3a), 7.3(2)D1(3)
	7.3(2)D1(2), 7.3(2)D1(1)
	7.3(1)D1(1)
	7.3(0)DX(1), 7.3(0)D1(1)
	7.2(2)D1(2)
	7.2(2)D1(1)
	7.2(1)D1(1)
	7.2(0)D1(1)
	6.2(24a), 6.2(24)
	6.2(22)
	6.2(20a), 6.2(20)
	6.2(18), 6.2(16)
	6.2(14), 6.2(12)
	6.2(10)

Cisco NX-OS Release 8.4(1) supports the following cold boot support matrix:

Table 16 Supported Cold Boot Matrix in Cisco NX-OS Release 8.4(1)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
8.4(1)	8.3(2)
	8.3(1)
	8.2(8)
	8.2(7a)
	8.2(6)
	8.2(5)
	8.2(4)
	8.2(3)
	8.2(2)
	8.2(1)
	8.1(2a), 8.1(2)
	8.1(1)
	8.0(1)
	7.3(8)D1(1)
	7.3(7)D1(1)
	7.3(6)D1(1)
	7.3(5)D1(1)
	7.3(4)D1(1)
	7.3(3)D1(1)
	7.3(2)D1(3a), 7.3(2)D1(3)
	7.3(2)D1(2)
	7.3(2)D1(1)
	7.3(1)D1(1)
	7.3(0)DX(1), 7.3(0)D1(1)
	7.2(2)D1(2)
	7.2(2)D1(1)
	7.2(1)D1(1)
	7.2(0)D1(1)
	6.2(24a), 6.2(24)
	6.2(22), 6.2(20a), 6.2(20)
	6.2(18), 6.2(16)
	6.2(14), 6.2(12), 6.2(10)
	6.2(8b), 6.2(8a), 6.1(5a)

Note Non-ISSU upgrades are also referred to as cold boot upgrade.

To perform a non-ISSU upgrade (cold boot upgrade) to Cisco NX-OS Release 8.0(1) and later releases from any prior supported releases in Table 15 and Table 10 follow these steps:

1. Change the boot variable, as shown here:

   Example for Cisco NX-OS Release 8.4(1)

```
boot kickstart bootflash:/n7000-s2-kickstart.8.4.1.bin sup-2
boot system bootflash:/n7000-s2-dk9.8.4.1.bin sup-2
boot kickstart bootflash:/n7000-s2-kickstart.8.4.1.bin sup-2e
boot system bootflash:/n7000-s2-dk9.8.4.1.bin sup-2e
```

2. Enter the **copy running-config startup-config vdc-all** command.
3. Enter the **reload** command to reload the switch.

Note Allow some time after the reload for the configuration to be applied.

Reload based NXOS downgrades involve rebuilding the internal binary configuration from the text-based startup configuration. This is done to ensure compatibility between the binary configuration and the downgraded software version. As a result, certain specific configuration may be missing from the configuration, after downgrade, due to ASCII replay process. This would include FEX HIF port configuration and VTP database configuration. Furthermore, NX-OS configurations that require VDC or switch reload to take effect may require additional reload when applied during the downgrade process. Examples of this include URIB/MRIB shared memory tuning, custom reserved VLAN range and Fabricpath Transit Mode feature. In order to mitigate this during downgrade, you should copy your full configuration to bootflash/tftpserver.

Feature Support:

Any features introduced in a release must be disabled before downgrading to a release that does not support those features.

Unsupported Modules:

When manually downgrading from a Cisco NX-OS Release to an earlier release, first power down all modules that are unsupported in the downgrade image. Then, purge the configuration of the unsupported modules using the **purge module** *module_number* **running-config** command.

For complete instructions on upgrading your software, see the *Cisco Nexus 7000 Series NX-OS Upgrade Downgrade Guide*.

Non-In-Service Software Upgrade (Non-ISSU)/Cold Boot Upgrade Caveats

Cold boot/Reload upgrades from Cisco NX-OS 7.3.x releases to Cisco NX-OS Release 8.0(1) and later releases with RISE Configuration:

- RISE configuration must be removed prior to starting your upgrade to Cisco NX-OS Release 8.0(1)/Cisco NX-OS Release 8.1(1) and later releases. ISSU performs compatibility check and blocks the upgrade if RISE is configured. There is no warning displayed or prevention for the reload upgrade. Therefore make sure to remove RISE configuration before the reload upgrade.

- There is no system check to block this upgrade path.
- Ensure that the RISE feature is disabled before attempting to upgrade to Cisco NX-OS Release 8.0(1) or later releases. After upgrading to Cisco NX-OS Release 8.0(1)/later releases, configure RISE services as required. The RISE feature configuration can be verified by using the **show rise** and **show run services sc_engine** commands.
- If you upgrade to Cisco NX-OS Release 8.0(1)/later releases with the RISE configuration, RISE services will become unstable and unmanageable.
  - Steps to identify the error condition:
    Even if the **show feature** command output shows RISE as enabled, no output will be displayed if you run the **show rise** and **show run services sc_engine** commands.
  - Steps to recover:
    The only way to recover from this condition is to do a **reload ascii** on the switch.

ASCII Configuration Replay

Saving VLAN Configuration Information:

Because a VLAN configuration can be learned from the network while the VLAN Trunking Protocol (VTP) is in a server/client mode, the VLAN configuration is not stored in the running configuration. If you copy the running configuration to a file and apply this configuration at a later point, including after a switch reload, the VLANs will not be restored. However, the VLAN configuration will be erased if the switch is the only server in the VTP domain.

The following steps list the workaround for this limitation:

- Configure one of the clients as the server.
- Complete the following steps:
  - Copy the VTP data file to the bootflash: data file by entering the **copy vtp-datafile bootflash: vtp-datafile** command.
  - Copy the ASCII configuration to the startup configuration by entering the **copy ascii-cfg-file startup-config** command.
  - Reload the switch with Cisco NX-OS Release 6.2(2) or a later release.

This limitation does not apply to a binary configuration, which is the recommended approach, but only to an ASCII configuration. In addition, this limitation applies to all Cisco NX-OS software releases for the Cisco Nexus 7000 series.

Rebind Interfaces command is not automatically executed when Replaying ASCII configuration in Cisco NX-OS Release 6.2(x):

The **rebind interfaces** command introduced in Cisco NX-OS Release 6.2(2) is needed to ensure the proper functionality of interfaces in certain circumstances. The command might be required when you change the module type of a VDC. However, because of the disruptive nature of the **rebind interfaces** command, for Cisco NX-OS Release 6.2(x) prior to Cisco NX-OS Release 6.2(8), this limitation applies only when all of the following conditions are met:

- The ASCII configuration file is replayed in the context of the default VDC or the admin VDC, and at least one VDC has an F2e Series or an F3 Series module listed as supported module types either before or after the replay.
- The **limit-resource module-type** commands listed in the ASCII configuration file requires that **rebind interfaces** command be executed.

The following steps list the workaround for this limitation:

- Manually enter the **rebind interfaces** command wherever needed to the ASCII configuration file for replay.
- Enter the **rebind interfaces** command immediately after you enter the **limit-resource module-type** command.
- Ensure that the ASCII replay properly applies all interface configurations for all interfaces in the relevant VDCs.

Note If you boot up the switch without any startup configuration, this limitation might apply to an ASCII replay. The reason is that without a startup configuration, the default VDC might still have certain interfaces automatically allocated. Because of this possibility, follow the approaches to work around the limitation.

Non-ISSU/Cold Boot Downgrade

Instructions provided below list the steps for the cold boot (non-ISSU) downgrade. The example provided below is for a cold boot downgrade for the following:

- A switch that is running Cisco NX-OS Release 8.3(1), Cisco NX-OS Release 8.2(1), and Cisco NX-OS Release 8.1(1) and needs to reload with Cisco NX-OS Release 6.2(8a).
- A switch that is running Cisco NX-OS Release 8.0(1) and needs to reload with Cisco NX-OS Release 6.2(12).

Refer to the ASCII Configuration Replay caveats section for specific configuration caveats.

- Save the switch configuration.
  - Enter **copy running-config bootflash:<config.txt> vdc-all** command.
- Change the boot variable to boot the target release.
- Enter **copy running-config startup-config vdc-all** command to save the boot variable.
- Enter **write erase** command to erase running configuration on the switch.
- Enter **reload** command.

Once the switch and all the modules are up with the target image, do the following:

- Enter the **copy bootflash:<config.txt> running-config** command.
- Verify that the switch is configured correctly.
- Replay the configuration copy to check if fex interfaces exist.
  - Enter the **copy bootflash:<config.txt> running-config** command.

Erasable Programmable Logic Device Images

Cisco NX-OS Release 8.4(3) includes the following Erasable Programmable Logic Device (EPLD) images:

- n7000-s2-epld.8.4.3.img
- n7700-s2-epld.8.4.3.img
- n7700-s3-epld.8.4.3.img

Table 17 shows the modules that are supported in Cisco NX-OS Release 8.4(3):

Table 17 Supported Modules with the FPGA in Cisco NX-OS Releases 8.4(3)

Module	FPGA Type	Version
Cisco Nexus 7000 Supervisor 2	PMFPGA	38.000
	IOFPGA	1.013
Cisco Nexus 7700 Supervisor 2E	PMFPGA	22.000
Cisco Nexus 7700 Switch Supervisor 3 Enhanced Module	PMFPGA	22.000
Fan-10 slot chassis (Cisco Nexus 7000 Series)	FAN	0.007
Fan-18 slot chassis (Cisco Nexus 7000 Series)	FAN	0.002
Fan-9 slot chassis (Cisco Nexus 7000 Series)	FAN	0.009
Fan-4 slot chassis (Cisco Nexus 7000 Series)	FAN	0.005
Fan-18 slot chassis (Cisco Nexus 7700 Series)	FAN	0.006
Fan-10 slot chassis (Cisco Nexus 7700 Series)	FAN	0.006
Fan-6 slot chassis (Cisco Nexus 7700 Series)	FAN	0.006
Fan-2 slot chassis (Cisco Nexus 7700 Series)	FAN	0.016
9 slot chassis (N7K:FAB2-7009)	PMFPGA	1.003
10 slot chassis (N7K:FAB2-7010)	PMFPGA	0.007
18 slot chassis (N7K:FAB2-7018)	PMFPGA	0.007
6 slot chassis (N77:FAB2-7706)	PMFPGA	1.002
10 slot chassis (N77:FAB2-7710)	PMFPGA	1.003
18 slot chassis (N77:FAB2-7718)	PMFPGA	1.002
6 slot chassis (N77:FAB3-7706)	PMFPGA	0.010
10 slot chassis (N77:FAB3-7710)	PMFPGA	0.008

Module	FPGA Type	Version
N7K:M2-10	PMFPGA	1.006
	IOFPGA	1.003
	SFPFPGA	1.003
	EARL (Forwarding Engine)	2.012
N7K:M2-40	PMFPGA	1.006
	IOFPGA	0.012
	SFPFPGA	2.008
	EARL (Forwarding Engine)	2.012
N7K:M2-100	PMFPGA	1.007
	IOFPGA	0.009
	SFPFPGA	0.004
	EARL (Forwarding Engine)	2.012
N7K:F2E-10	PMFPGA	1.009
	IOFPGA	0.016
N77:F2E-10	PMFPGA	0.006
	IOFPGA	0.005
N7K:F3-10	PMFPGA	1.000
	IOFPGA	1.005
	SFPFPGA	1.002
N7K:F3-40	PMFPGA	2.003
	IOFPGA	1.005
N7K:F3-100	PMFPGA	2.003
	IOFPGA	1.004
N77:F3-10	PMFPGA	1.007
	IOFPGA	0.035
	SFPFPGA	1.003
N77:F3-40	PMFPGA	1.005
	IOFPGA	0.031
N77:F3-100	PMFPGA	1.008
	IOFPGA	0.021
N77:F4-100	PMFPGA	0.012
	IOFPGA	2.000
	SFPFPGA	0.009

Module	FPGA Type	Version
N7K:M3-10	PMFPGA	1.001
	IOFPGA	2.001
	SFPFPGA	1.000
N7K:M3-40	PMFPGA	1.001
	IOFPGA	2.001
	SFPFPGA	1.000
N77:M3-10	PMFPGA	1.002
	IOFPGA	2.000
	SFPFPGA	1.000
N77:M3-40	PMFPGA	1.002
	IOFPGA	2.000
	DBFPGA	1.000
N77:M3-100	PMFPGA	1.000
	IOFPGA	2.000
	DBFPGA	1.001

Cisco NX-OS Release 8.4(2) includes the following Erasable Programmable Logic Device (EPLD) images:

- n7000-s2-epld.8.4.2.img
- n7700-s2-epld.8.4.2.img
- n7700-s3-epld.8.4.2.img

Table 18 shows the modules that are supported in Cisco NX-OS Release 8.4(2):

Table 18 Supported Modules with the FPGA in Cisco NX-OS Releases 8.4(2)

Module	FPGA Type	Version
Cisco Nexus 7000 Supervisor 2	PMFPGA	38.000
	IOFPGA	1.013
Cisco Nexus 7700 Supervisor 2E	PMFPGA	22.000
Cisco Nexus 7700 Switch Supervisor 3 Enhanced Module	PMFPGA	22.000
Fan-10 slot chassis (Cisco Nexus 7000 Series)	FAN	0.007
Fan-18 slot chassis (Cisco Nexus 7000 Series)	FAN	0.002
Fan-9 slot chassis (Cisco Nexus 7000 Series)	FAN	0.009

Module	FPGA Type	Version
Fan-4 slot chassis (Cisco Nexus 7000 Series)	FAN	0.005
Fan-18 slot chassis (Cisco Nexus 7700 Series)	FAN	0.006
Fan-10 slot chassis (Cisco Nexus 7700 Series)	FAN	0.006
Fan-6 slot chassis (Cisco Nexus 7700 Series)	FAN	0.006
Fan-2 slot chassis (Cisco Nexus 7700 Series)	FAN	0.016
9 slot chassis (N7K:FAB2-7009)	PMFPGA	1.003
10 slot chassis (N7K:FAB2-7010)	PMFPGA	0.007
18 slot chassis (N7K:FAB2-7018)	PMFPGA	0.007
6 slot chassis (N77:FAB2-7706)	PMFPGA	1.002
10 slot chassis (N77:FAB2-7710)	PMFPGA	1.003
18 slot chassis (N77:FAB2-7718)	PMFPGA	1.002
6 slot chassis (N77:FAB3-7706)	PMFPGA	0.010
10 slot chassis (N77:FAB3-7710)	PMFPGA	0.008
N7K:M2-10	PMFPGA	1.006
	IOFPGA	1.003
	SFPFPGA	1.003
	EARL (Forwarding Engine)	2.012
N7K:M2-40	PMFPGA	1.006
	IOFPGA	0.012
	SFPFPGA	2.008
	EARL (Forwarding Engine)	2.012
N7K:M2-100	PMFPGA	1.007
	IOFPGA	0.009
	SFPFPGA	0.004
	EARL (Forwarding Engine)	2.012

Module	FPGA Type	Version
N7K:F2E-10	PMFPGA	1.009
	IOFPGA	0.016
N77:F2E-10	PMFPGA	0.006
	IOFPGA	0.005
N7K:F3-10	PMFPGA	1.000
	IOFPGA	1.005
	SFPFPGA	1.002
N7K:F3-40	PMFPGA	2.003
	IOFPGA	1.005
N7K:F3-100	PMFPGA	2.003
	IOFPGA	1.004
N77:F3-10	PMFPGA	1.007
	IOFPGA	0.035
	SFPFPGA	1.003
N77:F3-40	PMFPGA	1.005
	IOFPGA	0.031
N77:F3-100	PMFPGA	1.008
	IOFPGA	0.021
N77:F4-100	PMFPGA	0.012
	IOFPGA	2.000
	SFPFPGA	0.009
N7K:M3-10	PMFPGA	1.001
	IOFPGA	2.000
	SFPFPGA	1.000
N7K:M3-40	PMFPGA	1.001
	IOFPGA	1.002
	SFPFPGA	1.000
N77:M3-10	PMFPGA	1.002
	IOFPGA	2.000
	SFPFPGA	1.000
N77:M3-40	PMFPGA	1.002
	IOFPGA	2.000
	DBFPGA	1.000
N77:M3-100	PMFPGA	1.000
	IOFPGA	2.000
	DBFPGA	1.001

Cisco NX-OS Release 8.4(1) includes the following Erasable Programmable Logic Device (EPLD) images:

- n7000-s2-epld.8.4.1.img
- n7700-s2-epld.8.4.1.img
- n7700-s3-epld.8.4.1.img

Table 19 shows the modules that are supported in Cisco NX-OS Release 8.4(1):

Table 19 Supported Modules with the FPGA in Cisco NX-OS Releases 8.4(1)

Module	FPGA Type	Version
Cisco Nexus 7000 Supervisor 2	PMFPGA	38.000
	IOFPGA	1.013
Cisco Nexus 7700 Supervisor 2E	PMFPGA	22.000
Cisco Nexus 7700 Switch Supervisor 3 Enhanced Module	PMFPGA	20.000
Fan-10 slot chassis (Cisco Nexus 7000 Series)	FAN	0.007
Fan-18 slot chassis (Cisco Nexus 7000 Series)	FAN	0.002
Fan-9 slot chassis (Cisco Nexus 7000 Series)	FAN	0.009
Fan-4 slot chassis (Cisco Nexus 7000 Series)	FAN	0.005
Fan-18 slot chassis (Cisco Nexus 7700 Series)	FAN	0.006
Fan-10 slot chassis (Cisco Nexus 7700 Series)	FAN	0.006
Fan-6 slot chassis (Cisco Nexus 7700 Series)	FAN	0.006
Fan-2 slot chassis (Cisco Nexus 7700 Series)	FAN	0.016
9 slot chassis (N7K:FAB2-7009)	PMFPGA	1.003
10 slot chassis (N7K:FAB2-7010)	PMFPGA	0.007
18 slot chassis (N7K:FAB2-7018)	PMFPGA	0.007
6 slot chassis (N77:FAB2-7706)	PMFPGA	1.002
10 slot chassis (N77:FAB2-7710)	PMFPGA	1.003
18 slot chassis (N77:FAB2-7718)	PMFPGA	1.002

Module	FPGA Type	Version
6 slot chassis (N77:FAB3-7706)	PMFPGA	0.008
10 slot chassis (N77:FAB3-7710)	PMFPGA	0.007
N7K:M2-10	PMFPGA	1.006
	IOFPGA	1.003
	SFPFPGA	1.003
	EARL (Forwarding Engine)	2.012
N7K:M2-40	PMFPGA	1.006
	IOFPGA	0.012
	SFPFPGA	2.008
	EARL (Forwarding Engine)	2.012
N7K:M2-100	PMFPGA	1.007
	IOFPGA	0.009
	SFPFPGA	0.004
	EARL (Forwarding Engine)	2.012
N7K:F2E-10	PMFPGA	1.009
	IOFPGA	0.016
N77:F2E-10	PMFPGA	0.006
	IOFPGA	0.005
N7K:F3-10	PMFPGA	1.000
	IOFPGA	1.003
	SFPFPGA	1.002
N7K:F3-40	PMFPGA	2.003
	IOFPGA	1.005
N7K:F3-100	PMFPGA	2.003
	IOFPGA	1.004
N77:F3-10	PMFPGA	1.007
	IOFPGA	0.031
	SFPFPGA	1.003
N77:F3-40	PMFPGA	1.005
	IOFPGA	0.031
N77:F3-100	PMFPGA	1.008
	IOFPGA	0.021

Module	FPGA Type	Version
N77:F4-100	PMFPGA	0.012
	IOFPGA	1.003
	SFPFPGA	0.009
N7K:M3-10	PMFPGA	1.001
	IOFPGA	1.003
	SFPFPGA	1.000
N7K:M3-40	PMFPGA	1.001
	IOFPGA	1.002
	SFPFPGA	1.000
N77:M3-10	PMFPGA	1.002
	IOFPGA	1.003
	SFPFPGA	1.000
N77:M3-40	PMFPGA	1.002
	IOFPGA	1.002
	DBFPGA	1.000
N77:M3-100	PMFPGA	1.000
	IOFPGA	1.002
	DBFPGA	1.001

For more information about upgrading to a new EPLD image, see the *Cisco Nexus 7000 Series FPGA/EPLD Upgrade Release Notes, Release 8.x*.

Cisco Nexus 7700 switches have an EPLD image that is programmed on the switches. This EPLD image is different than the EPLD image for the Cisco Nexus 7000 switches.

New and Enhanced Software Features

This section includes the following topics:

New and Enhanced Software Features - Cisco NX-OS Release 8.4(4)

OSPFv3 IPSec ESP Encryption Support

This feature provide strong authentication mechanism to OSPFv3. This feature provides IPSec ESP Encryption Support to OSPFv3. For more details, see Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide.

New and Enhanced Software Features - Cisco NX-OS Release 8.4(3)

CLI to Disable Selective VRF Download in F3 Modules

To completely disable selective VRF download in F3 modules in all VDCs, use the **no hardware forwarding selective-vrf** command in global configuration mode. You must reload the device after applying this command. For more details, see Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide.

ITD Enhancements

From Cisco NX-OS Release 8.4(3) statistics for an ITD service that has include ACL is supported. For more details, see Cisco Nexus 7000 Series NX-OS Intelligent Traffic Director Configuration Guide.

New and Enhanced Software Features - Cisco NX-OS Release 8.4(2)

Scale ACL

Scale ACL is introduced in Cisco NX-OS Release 8.4(2) and it is supported on M3 modules. This feature support is added only for RACL policies with object-group. This feature helps you to implement large scale configuration of ACL with support of object-group configuration. Both IPv4 and IPv6 RACL is supported.

MPLSoGRE

From Cisco NX-OS Release 8.4(2), the MPLS over GRE interwork support is applicable to M3 series modules.

ITD

From Cisco NX-OS Release 8.4(2), the ACLs created by ITD are not displayed in the show ip/ipv6 access-list command output. You need to use show ip/ipv6 access-list dynamic command to get the ITD ACL list. Upto 2000 ACEs are supported for multiple Include ACLs.

QSA with M3/F4

To bring up the link with CVR-QSFP-SFP10G adapter in a M3/F4 100G module, you need to perform the 10x4g breakout configuration on the interface. In older release versions with CVR-QSFP-SFP10G, the adapter link remains down. After ISSU to Cisco NX-OS Release 8.4(2) the link will still remain down. Perform OIR to bring up the link.

Smart Licensing with Satellite

Smart Software Manager satellite is a component of Smart Software Licensing and works in conjunction with the Smart Software Manager to manage software licenses. You can intelligently manage product licenses and get near real-time visibility and reports pertaining to the Cisco licenses you purchased and consumed.

ACL Name

From Cisco NX-OS Release 8.4(2), the ACL time range name has a maximum length of 256 characters.

Bloom Filter for Glean Adjacency

Bloom Filter Support for Glean Adjacencies is introduced in Cisco NX-OS Release 8.4(2). This feature is supported on M3 and F4 modules. To avoid this punting of the supervisor module, the L3 engine hashes a flow to set a bit in a leak table to indicate that the packet has been punted to the supervisor module. Subsequent frames are dropped until the software clears the leak table bit. This helps to forward the packets without any further delay.

64-way ECMP for F4

Starting from Cisco NX-OS Release 8.4(2), the BGP feature supports up to 64 paths to a destination on F4-Series I/O modules.

PIM Allow RP IPv6

IPv6 PIM Allow RP is supported from Cisco NX-OS Release 8.4(2).

New and Enhanced Software Features - Cisco NX-OS Release 8.4(1)

Dell FEX support on F4

B22 Dell FEX is supported on F3-Series and M3-Series I/O modules. Starting from Cisco NX-OS 8.4(1), B22 Dell FEX is also supported on F4-Series I/O modules. For more information refer the Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide for Cisco Nexus 7000 Series Switches.

Dynamic Routing over vPC

The dynamic routing over vPC is supported on M3 modules. Starting from Cisco NX-OS 8.4(1), this feature is supported on F4 Series modules for IPv4 and IPv6 unicast traffic. For more information refer the Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide.

Fabric Diagnostics

Starting with the Cisco NX-OS Release 8.4(1), the Internal Cyclic Redundancy Check (CRC) error detection and isolation feature is supported on the Cisco Nexus 7000 Series switches. For more information, refer Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide.

FEX Support on Breakout (40 - 4X10) (F4)

Starting from Cisco NX-OS Release 8.4(1), FEX is supported on F4-Series breakout (40G -> 4x10G) interfaces. For more information, refer Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide.

F4-100 40G Mode Breakout Support (4X10G) and F4-100 100G Mode Breakout Support (4X25G) (F4)

Starting from Cisco NX-OS Release 8.4(1), the breakout feature that enables splitting of both 40 Gigabit and 100 Gigabit ethernet ports, based on the transceiver at the interface, is supported on the Cisco Nexus 7700 F4-Series 30-port 100-Gigabit Ethernet I/O module. The 40-Gigabit Ethernet port can be split into four independent and logical 10 Gigabit Ethernet ports. The 100 Gigabit Ethernet port can be split into four independent and logical 25 Gigabit Ethernet ports. For more information, refer Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide.

Generic FEX Support (F4 in 40G mode)

Starting from Cisco NX-OS Release 8.4(1), FEXs are supported with Cisco Nexus F4-Series 30-port 100-Gigabit Ethernet I/O modules (N77-F430CQ-36) in 40G mode. For more information, refer the Cisco Nexus 7700 Series Hardware Installation Guides and the Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide for Cisco Nexus 7000 Series Switches.

GOLD Enhancements

The aggressive mode of corrective action configuration is introduced in Cisco NX-OS Release 8.4(1). The aggressive mode reduces the reaction time by lowering the consecutive failure count. When the consecutive failure count of a test matches the configured consecutive failure count, actions are taken based on the fault type and mode.

The conservative and aggressive actions are added for PCIe bus, spine control bus, and the status bus from Cisco NX-OS Release 8.4(1). For more details, refer the Cisco Nexus 7000 Series NX-OS System Management Configuration Guide.

GOLF: VRFLITE- ACI

GOLF VRF Lite ACI is supported on M3 modules. Starting from Cisco NX-OS 8.4(1), it is also supported on F4 Series modules. For more information refer the Cisco Nexus 7000 Series NX-OS VXLAN Configuration Guide.

GOLF: MPLS-VPN-ACI

GOLF MPLS VPN ACI is supported on M3 modules. Starting from Cisco NX-OS 8.4(1), it is also supported on F4 Series modules. For more information refer the Cisco Nexus 7000 Series NX-OS VXLAN Configuration Guide.

Honor Mode Licensing

Honor-based licensing is supported on Cisco Nexus 7000 Series switches for Cisco NX-OS Release 8.4(1). For more information, refer Cisco NX-OS Licensing Guide.

Inner MAC Address-based Classification

Starting from Cisco NX-OS Release 8.4(1), you can classify packets coming from a FabricPath interface using the inner MAC address. This feature is supported on M3-, F3- and F4-Series I/O modules. For more information, refer Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide.

IPv6 Static Routes with Next-Hop Support

IPv6 static routes with next-hop support is supported in Cisco NX-OS Release 8.4(1). IPv6 static routes with next-hops that are learnt over a VXLAN tunnel can be added to the Unicast Routing Information Base (URIB). For more information, refer Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide.

ITD on F4 (Bucket reassignment and distribution time delay)

From Cisco NX-OS Release 8.4(1), the ITD failaction feature is enhanced to optimally pre-fetch the failaction node per bucket. For more information refer the Cisco Nexus 7000 Series NX-OS Intelligent Traffic Director Configuration Guide.

ITD on F4 (Include ACL + Multidevice group)

This feature enables the user to configure multiple ACLs under an ITD service. This feature also provides an option to associate each ACL with its own device-group. For more information refer the Cisco Nexus 7000 Series NX-OS Intelligent Traffic Director Configuration Guide.

MoFRR

MoFRR is supported on F3 and M3 modules. Starting from Cisco NX-OS 8.4(1), it is also supported on F4 Series modules. For more information refer the Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide.

Multicast VRF

The multicast VRF is supported on M3 modules. Starting from Cisco NX-OS 8.4(1), it is also supported on F4 Series modules. For more information refer the Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide.

Multihop BFD IPv6

Starting from Cisco NX-OS Release 8.4(1), the BFD multihop feature is supported over IPv6. For more information, refer Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide.

Non-Disruptive Migration from Supervisor 2E Modules (N77-SUP2E) to Supervisor 3E Modules (N77-SUP3E)

Starting from Cisco NX-OS Release 8.4(1), Non-Disruptive Migration from Supervisor 2E Modules (N77-SUP2E) to Supervisor 3E Modules (N77-SUP3E) is supported. For more information, refer the Cisco Nexus 7706, 7710 and 7718 Hardware Installation Guides.

PIM Allow RP

PIM Allow RP enables the receiving device to use its own RP to create state and build shared trees when an incoming (*, G) Join is processed and a different RP is identified. This allows the receiving device to accept the (*, G) Join from the different RP. For more information refer the Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide.

Pong Support on M3

Starting from Cisco NX-OS 8.4(1), Pong is supported on M3 Series modules. For more information refer the Cisco Nexus 7000 Series NX-OS System Management Configuration Guide.

Proportional Multipath for VNF

Starting from Cisco NX-OS Release 8.4(1), a common loopback address can be configured for the BGP connection between the ToR switches and the VNF instance. For more information refer the Cisco Nexus 7000 Series NX-OS VXLAN Configuration Guide.

PTP with F4

PTP is supported on F2, F2e, F3, M2, and M3 modules. Starting from Cisco NX-OS 8.4(1), PTP is also supported on F4 Series modules. For more information refer the Cisco Nexus 7000 Series NX-OS System Management Configuration Guide.

PVLAN over OTV

The PVLAN over OTV feature is supported on F3 and M3 modules. Starting from Cisco NX-OS 8.4(1), this feature is supported on F4 Series modules. For more information refer the Cisco Nexus 7000 Series NX-OS OTV Configuration Guide.

Route Leaking with ACI GOLF

The Giant Overlay Fabric (GOLF) Virtual Routing and Forwarding (VRF) Leak feature enables the VRFs in the EVPN fabric to access shared services in a specific VRF. For more information, refer Centralized VRF Route-Leaking for VXLAN BGP EVPN Fabrics.

Router ACL

Starting from Cisco NX-OS Release 8.4(1), Router ACL is supported on Bridge domain interfaces. For more information, refer Cisco Nexus 7000 Series NX-OS Security Configuration Guide.

Supervisor-to-Supervisor EOBC Link Redundancy

Starting from Cisco NX-OS Release 8.4(1), the Supervisor-to-Supervisor EOBC Link Redundancy feature is introduced. This feature provides redundancy for EOBC communication between the active and standby supervisors by enabling the secondary redundant EOBC link in case the primary EOBC link fails and vice-versa. For more information, refer Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide.

Support for 4096 RSA Keys on Nexus

Starting from Cisco NX-OS Release 8.4(1), support has added for 4096 RSA key bits. For more information, refer Cisco Nexus 7000 Series NX-OS Security Configuration Guide.

VPLS and EoMPLS

The VPLS and EoMPLS features are supported on M3 modules. Starting from Cisco NX-OS 8.4(1), these features are supported on F4 Series modules. For more information refer the Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide.

Configure Replace

This feature is supported on Supervisor 3 and Fabric Module 3. Starting from Cisco NX-OS 8.4(1), Configure Replace is also supported on F4 Series modules. For more information refer the Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide.

MPLS Deaggregate Labels Reserve

For information on the MPLS deaggregate labels reserve enhancement, refer the Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide.

Scale Enhancements

Cisco NX-OS Release 8.4(1) has the following scale enhancements:

32-port LAG Support

Starting from Cisco NX-OS Release 8.4(1), you can bundle up to 32 active links into a port channel on the M3-Series and F4-Series modules. For more information, refer Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide.

64-way ECMP

Starting from Cisco NX-OS Release 8.4(1), the BGP feature supports up to 64 paths to a destination on M3- and F3-Series I/O modules. For more information, refer Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide.

PBR Scale

- Number of configured sequences per policy is enhanced to 100.
- Number of configured sequences per policy when the **hardware access-list allow deny ace** is configured) is 23.

SDA - Scale increase of EID for IPv4 and IPv6

Number of EID prefixes on xTR map cache is enhanced to 150,000.

iCAM Scale Monitoring

The following components are monitored by iCAM in Cisco NX-OS Release 8.4(1):

- FEX
- FabricPath
- Port Channel Interfaces
- vPC
- BFD
- GRE,
- Sub-interfaces
- Layer 2 Switching
- Spanning Tree Protocol
- OTV
- PVLAN
- QoS
- Security
- ACL
- DHCP
- UDP Relay
- SPAN and ERSPAN
- PTP
- NetFlow
- Unicast Routing
- ARP
- ISIS
- BGP
- VXLAN EVPN

Refer to Cisco Nexus 7000 Series NX-OS Verified Scalability Guide for other Cisco NX-OS Release scale numbers.

MIBs

No new MIBs are added for Cisco NX-OS Release 8.4(1) and for Cisco NX-OS Release 8.4(2).

Licensing

Honor-based licensing is supported on Cisco Nexus 7000 Series switches from Cisco NX-OS Release 8.4(1).

Smart Licensing with Satellite is supported on Cisco Nexus 7000 Series switches from Cisco NX-OS Release 8.4(2).

Smart Software Manager satellite is a component of Smart Software Licensing and works in conjunction with the Smart Software Manager to manage software licenses. You can intelligently manage product licenses and get near real-time visibility and reports pertaining to the Cisco licenses you purchased and consumed.

For details on licensing information, see the "Licensing Cisco NX-OS Software Features" chapter in the *Cisco NX-OS Licensing Guide.*

Caveats

The following topics provide a list of open and resolved caveats:

- Open Caveats—Cisco NX-OS Release 8.4(5)
- Open Caveats—Cisco NX-OS Release 8.4(4)
- Open Caveats—Cisco NX-OS Release 8.4(2)
- Open Caveats—Cisco NX-OS Release 8.4(1)
- Resolved Caveats—Cisco NX-OS Release 8.4(5)
- Resolved Caveats—Cisco NX-OS Release 8.4(4a)
- Resolved Caveats—Cisco NX-OS Release 8.4(4)
- Resolved Caveats—Cisco NX-OS Release 8.4(3)
- Resolved Caveats—Cisco NX-OS Release 8.4(2)
- Resolved Caveats—Cisco NX-OS Release 8.4(1)

Note Release note information is sometimes updated after the product Release Notes document is published. Use the Cisco Bug Toolkit to see the most up-to-date release note information for any caveat listed in this document.

Open Caveats—Cisco NX-OS Release 8.4(5)

Table 20 Cisco NX-OS Release 8.4(5) Open Caveats

Identifier	Description
CSCvz34580	N7K - after VDC type is changed from F3 to F3 F4 , VPC+ loops received PIM hello/general Query.

Open Caveats—Cisco NX-OS Release 8.4(4)

Table 21 Cisco NX-OS Release 8.4(4) Open Caveats

Identifier	Description
CSCvy51868	Interface not recognized after upgrading from 8.2(4) to 8.2(7).

Open Caveats—Cisco NX-OS Release 8.4(2)

Table 22 Cisco NX-OS Release 8.4(2) Open Caveats

Identifier	Description
CSCvs19141	IPv4/IPv6 FIB does not install properly
CSCvs99135	VPC peer link is getting down after flapping VPC peer-link from secondary in 8.4.2(222) build
CSCvs93006	After SSO compress stats of SACL will not show up counters
CSCvs63830	ACL: NTP access-group accepting more than 64 char ACLs. But, truncating to 64 ACL in “show run”.
CSCvr66312	Port-channels remain down with Micro BFD after LC reload and Switchover
CSCvt38687	Few fields missing in 'show lacp counters detail' CLI output when Fex is attached to N7K
CSCvv17360	ISSU support for MPLSoGRE with explicit Null feature with M3 LC

Open Caveats—Cisco NX-OS Release 8.4(1)

Table 23 Cisco NX-OS Release 8.4(1) Open Caveats

Identifier	Description
CSCvr83684	MAC throttling values are corrupted post upgrade to 8.4.1
CSCvn00010	8.4.1: VXLAN-BDI: F4: ACL on BDI in ingress dir programmed on multiple instances in VDC
CSCvn47068	8.4.1:Not able to enable ACL Capture on VXLAN Setups
CSCvo48548	F4 4x25G PO mem ints are jumbled after un-allocate and re-allocate ints to VDC
CSCvo50116	8.4.1: HSRP IPv4 vMAC being toggled between the OTV L2 join interface and Anycast HSPR GW switch-id

Table 23 Cisco NX-OS Release 8.4(1) Open Caveats

Identifier	Description
CSCvo81147	8.4.1-BFD session over FP interfaces flap when netflow feature is negated
CSCvo90099	NX-SNMP: snmp-server hosts getting modified after configuration(DNSv6 case)
CSCvp10070	vxlan is up when bdi is down after reload
CSCvp35566	8.4.1: consistency-checker l2mcast for single mCast group takes ~ 20mins to complete
CSCvp78880	Standby reload after config 1000 Vlan Translation at physical interface
CSCvp88371	8.4.1: Consistency-checker fail on CTS enable l2 interface
CSCvp91503	Sometimes Fangio linecard remains in power down state if card is reloaded multiple times.
CSCvq03504	8.4.1: erbdg table programming issue when fex is online before the FP core ports are UP
CSCvq17207	ISSU from 8.2.X to 8.4.X: nve is failing to read svi-ifdb
CSCvq42066	After Leaf reload, ipv4 VNF prefix RNH update with rnh_best flag FALSE by URIB in N7K BL.
CSCvq44936	Seeing issue with “Logflash firmware upgrade failed: 5"
CSCvq32976	PTP not functioning at 32LAG PO after config lacp max/min link CLI at PO

Resolved Caveats—Cisco NX-OS Release 8.4(5)

Table 24 Cisco NX-OS Release 8.4(5) Resolved Caveats

Identifier	Description
CSCvj50674	N77-M348XP-23L card may reboot due SLF inband link issue(LINK_GOOD_TO_FAULT_12)
CSCvq89022	Continuous logging of Invalid arguments in rpm_eval_policy_match
CSCvu64601	High memory usage after streaming high volume of telemetry data for more than 6 days
CSCvu69869	Configuring "vpc role preempt" will cause vPCs with port-type network to go into BKN state
CSCvx07840	N7K - pktmgr loops packets when tunnel interface has next-hop via itself.
CSCvx08319	Ethpm was reloaded by sysmgr during bootup after upgrade from 6.2(10) to 7.3(2)D1(2).
CSCvx13177	N77 F3 40G port become hardware failure due to PS_PPC_EG_LC_HDR_UNKNOWN_ERR
CSCvx13871	N7K PTP BC DSCP priority markings on egress
CSCvx18137	Need a recovery mechanism for power supplies showing fail/shut due to shorted out bus
CSCvx38812	STP Dispute: STP root election is impacted on presence of dual homed FEX HIF in a port-channel
CSCvx48078	Cisco NX-OS Software MPLS OAM Denial of Service Vulnerability
CSCvx50786	N7K Sup3E CPU-Mac Inband Events Not Showing High/Low Water Marks
CSCvx54653	SMU request to back out CSCvv62656
CSCvx67356	Post ISSU/reload Service "snmpd" (PID xxxx) hasn't caught signal 11 (core will be saved)
CSCvx71150	DOM value monitoring for CPAK-100G-LR4 lanes is erroneous when pulled over SNMP
CSCvx75284	DFA :: host mobility not working between DCs if leaves are VPC
CSCvx77868	SNMP walk doesn't return value of eth 1/1 interface of LLDP neighbors.
CSCvx79358	ED_SCH_UC_QTYPE_HANG, ED_SCH_MC_QTYPE_HANG, VAL_KEI_CP_IRQ__0_FLD_RBRX_IDLE caused cpu tx pause
CSCvx79932	N7K ITD does't update route-map correctly, upon node failure at the same time (sub-sec) across VDCs
CSCvx84613	Nexus 7k 8.4 PKI Authentication Failure
CSCvx87204	ICMP Packet Too Big not sent by N7K MPLS P-router
CSCvx87308	N77-M3 - ARP reply drop when arrive on N7K CTS port
CSCvx90337	Nexus 7000 pause frame loop after upgrade to 8.4.4.
CSCvx93145	Topology information is not propagated from ISIS to MPLS TE when authentication configured for ISIS
CSCvy00853	aclmgr crash after executing show startup config
CSCvy04296	Nexus7710 M3 Linecard crash in IPFIB process

Table 24 Cisco NX-OS Release 8.4(5) Resolved Caveats

Identifier	Description
CSCvy04379	When configuring RACL on SVI with L2VPN/Psuedowire getting cryptic error message
CSCvy16417	N7k IP Overlap Detection Fails for HSRP VIPs
CSCvy22967	N7K- load interval I/O rates are missing from SVI show interface command
CSCvy26850	MET table exhaustion without any mcast groups with M3 modules
CSCvy28073	PIM crashes after configuring - ip pim rp-candidate
CSCvy33368	M3-Interfaces in intFailErrDis after multiple ports are brought up
CSCvy34214	'port-channel bfd destination x.x.x.x' is accepted but not shown in running-config
CSCvy56436	OTV allows 65 vlan ranges to be extended and causing 0 Vlans to be extended after reload.
CSCvy78382	Transit packet dropped instead of punting to CPU when there is no ARP entry for next hop
CSCvy84652	N7K Doesn't flush locally generated default route after default route changes from bgp to ospf
CSCvz01927	N7K ARP process crash
CSCvz03090	M3 module reloading due to fatal interrupt BEM_EL3_CTL_INVLD [SLF_BIB_INT_BEM_EL3_CTL_INVLD]
CSCvz05712	CTS MAC table reaches 64K after multiple remove/add of cts role-based sgt cli under vlan
CSCvz05986	N9K/N7K - OSPF does not report syslog like EIGRP/BGP for Deadtimer Expired condition
CSCvz17681	Snapshot creation permission denied
CSCvz27481	Iftmc - interface w/ LTL 0 incorrectly bound to VLAN SDB active ports list
CSCvz31168	SNMP MIB CISCO-EIGRP-MIB table cEigrpInterfaceTable does not return the correct ifIndex

Resolved Caveats—Cisco NX-OS Release 8.4(4a)

Table 25 Cisco NX-OS Release 8.4(4a) Resolved Caveats

Identifier	Description
CSCvx54653	SMU request to back out CSCvv62656
CSCvy51868	Interface not recognized after upgrading from 8.2(4) to 8.2(7).

Resolved Caveats—Cisco NX-OS Release 8.4(4)

Table 26 Cisco NX-OS Release 8.4(4) Resolved Caveats

Identifier	Description
CSCvr33431	Unable to add interfaces to a port-channel
CSCvs09223	After code upgrade, XL license is enable by default in honor mode
CSCvs45159	N9K VXLAN/VTEP with arp suppression enabled will not flood arp with sender IP 0.0.0.0
CSCvu39910	IPv6 routes redistributed from BGP missing after changing to MT
CSCvu70729	After PIM restart, multicast routes stuck in pending, stale operations in MRIB txlist
CSCvu87859	OSPF LSAs are not refreshed after failed ISSU
CSCvv24436	Fabricpath - Additional HSRP Anycast group config causes MCM MTS Buffer Buildup
CSCvv33208	N7K netflow flows are reported with a negative flow duration time
CSCvv49494	Nexus 7000/7700 supervisor switchover when F4 line cards is removed and reinserted multiple times
CSCvv53024	Daylight time is not considered when we use plus option with one-shot start time configuration
CSCvv62656	OTV Multicast Transport: RARP broadcast encapsulated with non-standard multicast DMAC (01:00:00...)
CSCvv73708	FX2/MLD: IGMP/MLD crash on secondary VPC peer due to missing null check for group header
CSCvv81470	Terminal monitor not showing any output eventhough terminal monitor is enabled
CSCvv87092	F3 interfaces goes to “faulty” or LC reset during recovery due to fatal interrupts
CSCvv93565	show hardware internal errors is splitting counter names
CSCvv93710	TRM-MS Sanity Failure: Remove/Add EVPN Multisite Global Config on BGW
CSCvv97176	HSRPv6 packets leaking instead of having ACL causing HSRP flaps for v6 groups
CSCvw05878	Multiple interfaces in “hardware failure” state after running L3 inconsistency checker
CSCvw15198	N5K Service “__inst_001__rip” (PID 4884) hasn't caught signal 11 (core will be saved)
CSCvw15473	MPLS LDP IGP SYNC is not working properly on N7K/8.4.3/M3 with ISIS.
CSCvw18496	“cisco id is --” in show interface transceiver | Nexus 5672UP
CSCvw24386	Memory leak in N7K device due to malformed WCCP packets
CSCvw32747	Static routes not in (vrf) uRIB
CSCvw42838	private-vlan trunk not forwarding new vlans on Nexus 7000
CSCvw43266	`show hardware flow utilization module x` does not give the correct number of flows.
CSCvw45465	Nexus TACACS crash due to SHA1 memory leak
CSCvw47475	after adding secondary IP, Route is inconsistent in FIB Hardware

Table 26 Cisco NX-OS Release 8.4(4) Resolved Caveats

Identifier	Description
CSCvw48927	Memory leak on acllog “acllog_net_l2_pkt_handle”
CSCvw52454	N77-SUP3E // 8.4(3) // M3 linecard // Nexus 7706 config session is timing out after importing ACL
CSCvw57079	Steady CPU load increase once the number of SNMP TCP sessions exceeds 30
CSCvw60214	EEM script blocks certain PTS and after 32 blocked terminal logging stops working
CSCvw64171	HSRP Version 2 vmac will be remained in mac table after changing HSRP from Version 2 to Version 1
CSCvw64290	TrustSec Packets programming to Drop Index On N7k 8.2.6 code
CSCvw71878	Scale ACL mis programmed with prefix as source and object-group as destination in same ACL entry
CSCvw71912	Improper error message printing causing RPM crash
CSCvw73389	N77-SUP3E // 8.4(3) // M3 linecard // Nexus 7706 config session is timing out after importing ACL
CSCvw76585	Port fix for CSCvb18053 to NX-OS to 7.3, 8.2, 8.4 for Nexus 7k
CSCvw77879	N7k- Config from SVI to BDI breaking ipv6
CSCvw78496	N7K returns SNMP queries from different vrf contexts on release 8.2(5)
CSCvw85776	N7k crash: %SYSMGR-3-HEARTBEAT_FAILURE: Service “igmp” sent SIGABRT for not setting heartbeat
CSCvw93857	lit process crashed on module DS-X9448-768K9
CSCvx02142	ISIS does not propagate topology information to MPLS-TE depending on TLV order
CSCvx07840	N7K - pktmgr loops packets when tunnel interface has next-hop via itself.
CSCvx08319	Ethpm was reloaded by sysmgr during bootup after upgrade from 6.2(10) to 7.3(2)D1(2).
CSCvx13177	N77 F3 40G port become hardware failure due to PS_PPC_EG_LC_HDR_UNKNOWN_ERR
CSCvx13871	N7K PTP BC DSCP priority markings on egress
CSCvx14567	N7K: Host (/32) VRF route leak remains stale after removing config

Resolved Caveats—Cisco NX-OS Release 8.4(3)

Table 27 Cisco NX-OS Release 8.4(3) Resolved Caveats

Identifier	Description
CSCvg19850	Npacl leaks 152 bytes of memory with ntp/snmp acl add removal
CSCvj50674	N77-M348XP-23L card may reboot due SLF inband link issue(LINK_GOOD_TO_FAULT_12)
CSCvm26068	N7K - Service "pim" crash
CSCvn30912	Mem leak snmpd during longevity with F4 LC reload usm_malloc_usmStateReference and snmpv3_pss
CSCvn78885	tacacs_crypt_service or radius_crypt_service filling up nxos/tmp
CSCvq34690	Change how ports are displayed during CTS logging
CSCvr27377	ITD /RPM service timeout during bring up with ADJ /ARP changes

Table 27 Cisco NX-OS Release 8.4(3) Resolved Caveats

Identifier	Description
CSCvr40843	port-channel switching time was longer than expected with N7K-M348XP-25L
CSCvr58649	BGP service crash at rpm_acquire_bgp_shmem_lock
CSCvs21686	Need to log arbiter interrupts to OBFL
CSCvs37194	Need “match exception ip/ipv6 unicast rpf-failure” added to default copp policy
CSCvs54611	need to add a syslog or any form of notification when the interface chip failure
CSCvs62687	F3 - MAC hardware entry point to wrong interface instead of peer-link
CSCvs67823	[Trustsec] Nexus 7700 Downloading SGACLs for dgts not on the database when doing CoA push from ISE.
CSCvs84593	eem_syslog_regex_ev_spec_handler is output when eem is created
CSCvs88208	"copy run start" fails with port-profile signal 11 crash
CSCvs93402	BGP hellos seen after peer admin shut
CSCvt13462	NX-OS: BGP memory leak within 'BGP BF slab' when more than 30 neighbors configured
CSCvt17690	AS number isn't displayed in BGP-5-ADJCHANGE up/down log
CSCvt19467	BFD ACL programming issue after downgrading from 8.3(1) to 8.2(4) using boot variables methd.
CSCvt19773	VDC failed to come up post VDC reload
CSCvt33067	Traffic Black-holing with VPC SFC failure(L2LU Drops, VSL Check)
CSCvt38574	Changing prefix-list in route-map doesn't change number of prefixes received in BGP summary
CSCvt44562	rttMonCtrlAdminTag = (null) notification is generated along with the sla notification.
CSCvt46409	N7k OSPF area range not advertising cost
CSCvt49191	Cisco Nexus 9000 URIB process crash
CSCvt60639	client link-layer address option only showing 32-bit from the client RFC6939
CSCvt64262	VPC+ VPC-BPDU redirection/tunneling not working
CSCvt64493	N7K-SUP2/E: Unable to Save Configuration system not ready
CSCvt66012	STP process crashes while writing updates to PSS/SDB
CSCvt68098	BFD discriminator change for an active session is not acknowledged
CSCvt70010	IP-SGTs not installed in RBM DB for one VRF: "CTS fails to add prefix to PT since it already exists"
CSCvt74784	(S,G) not expiring when ip pim sg-expiry-timer infinity sg-list is configured
CSCvt77249	fc4-types:fc4_features missing from fcns database and fcoe traffic interrupted
CSCvt83262	Switch reload due to sys-mgr process.
CSCvt84013	N7K: interface-vlan process crash or stale ifindex entries in queue when SNMP used to shut down SVIs

Table 27 Cisco NX-OS Release 8.4(3) Resolved Caveats

Identifier	Description
CSCvt87450	snmpwalk GETNEXT for mpls sub-layer ifIndex returns object from the IfDescr section
CSCvt88871	N7K/F3: CLI to Disable Selective VRF in FIB on Flanker linecard
CSCvt93544	Match exception ip unicast rpf-fail on M3 matches all traffic in CoPP
CSCvt93631	entPhysicalMfgName always defaults to Cisco Systems for transceivers
CSCvt94979	M3: HIF-vPc ports going Internal-Fail errDisable when trying bring them up
CSCvt97613	undebug all does not stop debug snmp req-latency-time x
CSCvt97628	Deleting the snmp_log file from log: when you do debug snmp req-latency-time does not free the space
CSCvu00553	With Route summarization OSPF Sets FA on the route Type-5 LSA
CSCvu00825	N7K - M2 - LACP PDUs classified in default queue when received on L3 port-channel
CSCvu01732	N7K HSRP Secondary with mismatched physical/virtual subnets uses physical IP when sourcing ARP
CSCvu05247	StandbyFabricLoopback Diag Test on Nexus7k-Sup2E | Unexpected Behavior
CSCvu12601	N7K proxy-routing multicast Num_replicators >16, Mcast OIL missing in MFDM but present in Mrib.
CSCvu18593	CTS and IPv6 ACL applied to an egress interface may impact traffic
CSCvu20245	PIM crash when freeing memory
CSCvu23201	NX-OS BGP: rare BGP updates corruption
CSCvu30191	Glean traffic from HSRP standby generates syslog %ARP-4-OWN_SRCMAC: on HSRP active
CSCvu39195	Heartbeat failure on process VNTAGC may cause a linecard crash
CSCvu44271	"show tech aclqos" encapsulates show commands in single-quotes, not grave accents.
CSCvu47702	ISSU failed while M3 LC upgrade in progress
CSCvu51632	eobc logging enhancement on M2 LC for HB Loss debugging
CSCvu53710	M3/F4 HAP reset seen in SLF_BRIDGE process.
CSCvu55134	"SFP security check: MD5 failed" error message output when insert SFP to N77-F430CQ-36
CSCvu60044	Pings to SVI HSRP VIP might see intermittent loss when LISP is enabled
CSCvu61173	MDS 9396T show interface [interface-range] txwait-history not working
CSCvu66701	N7K: OSPF will not generate type 3 summary LSA
CSCvu77230	service ipp will crash when 'no opflex-peer' is entered
CSCvu79185	cts role-based policy not updated when deploying policy matrix from ISE
CSCvu85408	Supervisor xbar sync failed exceptionlogs and syslogs do not identify the failing serial link
CSCvu87085	OSPF is querying BGP AS number with incorrect VRF ID

Table 27 Cisco NX-OS Release 8.4(3) Resolved Caveats

Identifier	Description
CSCvu92822	N77-M3: Traffic to breakout ports drops when breakout command is set to same LC's other port
CSCvu93555	Nexus7700 N77-SUP2E running 7.3(2)D1(1) experiences aclmgr crash causing vdc restart and failvoer
CSCvu94685	2 receivers deleted from igmp snooping table when only one wants to leave a group
CSCvu98502	Post LDP crash due to Abort/HB timeout LDP might be unable to bind to the socket and fails recover
CSCvu99685	"ip pim passive" causes loss of interface DF status after reload
CSCvv01546	GIR stuck in unplanned maintenance mode
CSCvv04761	FEX 2248 dropping multicast during IGMP update from client on a different FEX
CSCvv06752	Route-Map applied through Peer-Policy under VPNv4 neighbor NOT performing actions specified
CSCvv08021	N7k netflow output interface is not updated when traffic is rerouted on new interface
CSCvv10509	Forwarding not correctly programmed for host network when we stop advertising prefix and SGT exists
CSCvv12387	Improve VNTAG_MGR IFTMC programming failure syslog and documentation
CSCvv17360	ISSU support for MPLSoGRE with explicit Null feature with M3 LC
CSCvv18307	N7K wrong LIF value got displayed for the route - after config play around
CSCvv22452	Cisco NX-OS HSRP stuck in "Initial" state after reload with static HSRP MAC configured
CSCvv27689	Default route metric changes after SUP switchover
CSCvv38244	Netflow Manager (nfm) unresponsive, manual process restart doesn't recover
CSCvv44858	N7K large number of vlan ranges configured, show run vlan shows only subset of the overall number
CSCvv48130	F3 interfaces goes to "faulty" state because of few new fatal interrupts
CSCvv51221	aclqos crash while modifying ACL
CSCvv52514	EIGRP subnet goes SIA if link failover occurs with mix of wide/narrow metric and offset-list
CSCvv69592	M3 LC fatal error in device DEV_SLF_BRI (device error 0xce400600)
CSCvu42699	Writing log to linecard bootflash until file system is full
CSCvq69766	eobc logging enhancement on F3 LC for HB Loss debugging
CSCvu99115	circuit-id in the packet with 'dhcp-relay information option 82' not carrying the vlan information
CSCvv49316	IPv6 floating (static) route is chosen while routes with lesser AD value are still available

Table 27 Cisco NX-OS Release 8.4(3) Resolved Caveats

Identifier	Description
CSCvu88985	PBR Convergence Improvement: V6 Nexthops are not programmed properly in HW
CSCvv23045	aclmgr passing wrong size while fetching priv data
CSCvv63531	F4 remains downs in slot 5 due to module purge failure
CSCvm61055	Packets drop at vxlan encap due to LIF prog failure after LC reload
CSCvv49120	PIM: auto-rp config without auto-rp listen keyword may loop packet indefinitely

Resolved Caveats—Cisco NX-OS Release 8.4(2)

Table 28 Cisco NX-OS Release 8.4(2) Resolved Caveats

Identifier	Description
CSCuy44133	N77-M312CQ-26L: crash due to fatal error [SLF_PUM2_INT_LINK_GOOD_TO_FAULT_12]
CSCur85599	Output Discards on F3 "show int"
CSCuw82759	Nexus 5600/6000: No LAN_BASE should disable FHRP CLI or throw error
CSCux36018	NX-OS Flexera Arbitrary Remote Code Execution Vulnerability
CSCuz30263	After upgrade, eigrp failed to come up due to K value mismatch
CSCvj06473	System hap reset with sla_sender process crash
CSCvj50674	N77-M348XP-23L card may reboot due SLF inband link issue(LINK_GOOD_TO_FAULT_12)
CSCvk05550	N7k - SPAN Destination traffic leaves untagged in setup with bridge-domain
CSCvn34448	ITD stops responding after servers are shutdown
CSCvn58682	IP SLA tcp connect probe is not taking the configured source-ip address
CSCvn77141	Cisco Secure Boot Hardware Tampering Vulnerability
CSCvo15674	crash because of memory leak in bfd process
CSCvo72473	show tech forwarding takes too much time to run on large scale MPLS deployments with M2/M3
CSCvo80677	Linecard CPU utilization is displayed incorrectly for some processes
CSCvo90099	NX-SNMP: snmp-server hosts getting modified after configuration(DNSv6 case)
CSCvp32585	CTS repeatedly crashed on cts_sxp_axn & cts_sgt_map
CSCvp35682	Target Address on IP SLA (udp) probes is getting changed to a new IP other than the configured one
CSCvp36080	Nexus doesn't send Register-Stop when Register is denied by PIM Register Policy

Table 28 Cisco NX-OS Release 8.4(2) Resolved Caveats

Identifier	Description
CSCvp57934	Optimization of internal NXOS parameters
CSCvp58845	After remove/add VRF, remote host routes not installed to URIB and report 'remote nh not installed'
CSCvp75032	VRF missing after upgrade to 7.3(5)N1(1)
CSCvq04585	Mcast trafffic loss seen sometimes with module reload and other triggers
CSCvq05743	MPLS LDP over GRE Tunnel is flapping when "mpls ldp explicit-null" is configured in N7K.
CSCvq09112	Incorrect parsing when using " " in loopback configuration
CSCvq14721	Error of 'system bridge-domain add' CLI due to existing vlan deletes all existing bridge-domains
CSCvq16130	Ignore comma and later for ip sla group schedule add
CSCvq17890	The port-channel cannot be controlled by this input policy after removed the port-channel members.
CSCvq18379	Netflow Start Time Drift Issue
CSCvq18837	Python Security Regression Unicode Encoding Vulnerability
CSCvq21920	Nexus 56K console loop on username/password prompt
CSCvq24098	N7K: show run diff breaks after enabling CTS
CSCvq26431	N7K 8.2(3) PIM process crashed
CSCvq26767	Supervisor hang and redundancy switchover failure
CSCvq32044	BGP process crash with aggregate-address config without summary-only option under VRF
CSCvq40508	n7k/FP - LPOE index reused for 2 different GPC on same SOC
CSCvq42668	nexus7k heartbeat failure IGMP crash
CSCvq42730	Standby SUP reset due to Service "adjmgr" hasn't caught signal 11
CSCvq48220	Cisco NX-OS Software Anycast Gateway Invalid ARP Vulnerability
CSCvq51543	MPLS-TE tunnel not forwarding traffic as "IP is disabled"
CSCvq53154	mrib crash when collecting mcast show tech with N7K in SDA border role.
CSCvq56953	Need standby Sup to detect a hung active Sup and reload it to trigger a switchover.
CSCvq57865	Memory leak is seen in DHCP process when show run is executed on a VLAN
CSCvq60859	Traffic loss on F3 linecard after module reload due to delay in VPN_INST_BITMAP
CSCvq65248	Traffic across GRE Tunnel configured with MPLS fails in N7K
CSCvq65959	80% packets loss in route leaking environment after changing SVI IP address
CSCvq70392	Reverted breakout interface on N77-M324FQ-25L fails to come up.
CSCvq71294	LR transceiver stops transmitting laser when port unshut after a long shut
CSCvq95046	Nexus 7000 EIGRP does not advitise routes to peer after several resyncs and neighbor flap

Table 28 Cisco NX-OS Release 8.4(2) Resolved Caveats

Identifier	Description
CSCvr01927	End to End Vrf ping with MPLSoGRE + MPLS stitching doesnt work with explicit Null.
CSCvr02232	"show logging onboard internal kernel" logging many EOBCM: HB_RX_INVAL_FRAME_NUMBER errors on 8.4(1)
CSCvr04377	ISIS Default route advertised to N7K won't be installed to RIB.
CSCvr05966	Race in Flanker/MTM/L2FM can lead to learning gateway mac out local interface while SVI Up
CSCvr06297	[MultiHop] Upgrade 7.3(2)D1(3a) to 8.2.2 on N7K, show tech/show tech det is not getting complete.
CSCvr08197	N7k PIXM/PIXMc should attempt to recover if they get out of sync
CSCvr09812	F3 can learn its own GMAC from IPv6 ingress SMAC if v6 not configured
CSCvr10766	N7k netflow input and output interface does not map to IOD database for M3 LC for Version 5 template
CSCvr12510	%MTM-SLOT2-2-INVALID_SLOT: Received invalid slot value 9999 in mts message from vdc
CSCvr19809	cosmetic: native 40G port (non-breakout) report incorrect Quesize for F3. breakout 4x10G unaffected.
CSCvr31356	GARP not updating ARP table on remote VTEPs
CSCvr31478	DATACORRUPTION Tracebacks when adding N7K to SNMP Management
CSCvr34577	OSPF is not Generating type 3 summary LSA 0.0.0.0
CSCvr35592	N77/F3 8.2(1) & (2) // Slow drain EB egress_timeout drops
CSCvr37274	DHCP Relay in VXLAN BGP EVPN- missing suboptions
CSCvr39538	N7K may report false memory utilization values
CSCvr62671	SSH quietly fails - aaa reports failed to remove the access list configured : sl_def_acl
CSCvr63916	Module id incorrectly formatted in CPUHOG messages
CSCvr73481	"show ip pim vrf <> internal" status:down evpn PIM&VRF are up status
CSCvr74305	Nexus pim hap reset
CSCvr83684	MAC throttling values are corrupted post upgrade to 8.4.1
CSCvr85588	VTP crashed after multiple trunking interfaces flapped
CSCvs15237	BGP memory leak when 'soft-reconfiguration inbound always' configured
CSCvs20377	RPF nbr pointing to Assert Loser on RP in MVPN environment
CSCvs43451	fcoe n7k with 2232pp fex after sup switchover hif ports change from pfc to link level pause
CSCvs49787	MAC Address learning failed due to unexpected "port-security" function remaining enabled
CSCvs50843	IP mobility not updating route on source leaf
CSCvs54854	Crash while executing - show logging onboard error-stats - in show tech
CSCvs57779	N7K: Port-Profiles disappear after shut fex-fabric ports & no feature-set fex

Table 28 Cisco NX-OS Release 8.4(2) Resolved Caveats

Identifier	Description
CSCvs58870	Collect dmesg during SLF inband failure on M3
CSCvs59985	Netlow StartTime and EndTime being reported in the future by almost 2 minutes.
CSCvs61482	Incorrect annotations of XBAR internal errors in show hardware internal errors
CSCvs69194	N7K only listens one ip for tcp 64999 when cts sxp source ip is configured
CSCvs76901	cli function returns cmd_exec_error when collecting show tech-support via python
CSCvs97090	ITD reverse policies are not programmed properly.
CSCvt00423	N7K linecard "fwd_stats_client" process crash
CSCvs90047	ipv4 routes with ipv6 NH BGP routes redistributed into OSPF as Type-5 expires in 30 min
CSCvr18425	8.2.4.47:: vsh core on obfl_cli_show_log
CSCvr21201	N7K: cryptographic-algorithm HMAC-SHA-xxx keys show up as unknown
CSCvk63501	N7K Hw rate-limiter statistics per fwding engine required
CSCvs71659	RIT changes to support Local, GLEAN punt path for MPLS ADJACENCIES
CSCvg71883	Speed auto negotiate can not be disabled on FEX 1G SFP port.
CSCvs26756	Wrong VPC limit error "ERROR: Operation failed: [Reached the max vPC limit]"
CSCvr42578	N7K M2 mac address missing on vpc peer when port-channel member port flap
CSCvs83567	NX-OS 8.x IP redirect source check not working
CSCvc46006	vrrp ipv4 is incorrect state after multiple reload

Resolved Caveats—Cisco NX-OS Release 8.4(1)

Table 29 Cisco NX-OS Release 8.4(1) Resolved Caveats

Identifier	Description
CSCue83764	NXOS/VQI:counter per CCOS/class needed in show hardware queueing drops
CSCuh31678	Allow L4 port number with span filter (F3 Only)
CSCut67978	Multiple Vulnerabilities in libxml2
CSCux36018	NX-OS Flexera Arbitrary Remote Code Execution Vulnerability
CSCuy77045	configuring "mpls ldp sync" removes "mpls traffic-eng router-id" command
CSCuz67595	Incorect IGP metric calculation for ISIS
CSCva83447	BGP stuck at 90% after redistributing OSPF routes to BGP with EVPN VXLAN
CSCva92054	Route-leak (inter-vrf) - hmm route not flushed on host vMotion

Table 29 Cisco NX-OS Release 8.4(1) Resolved Caveats

Identifier	Description
CSCvc73543	N7K adding ip address into object group stuck
CSCvc91280	incomplete error output during duplicate IP address entry
CSCvc92277	NFP crash after associating netflow-orignal flow record to active flow monitor
CSCve21405	Inconsistent formatting for 'show interface' outputs collected through NXAPI using JSON
CSCvf24911	ARP memory leak @ LIBBL_MEM_bitfield_malloc_t & LIBSLAB_MEM_create_slab
CSCvi05048	Netflow sends packet with Invalid payload size causing fln_l3 core
CSCvi15800	N7k - OTV Fast Convergence is delayed during AED switchover
CSCvi45642	MDS 97xx: Incorrect state and no data for reason code/return code for svi enabled snmpd error logs
CSCvi78416	N7K Consistency Checker: URIB/AM to UFIB CC
CSCvj09711	N7K - Service "acllog" crash with PBR
CSCvj12608	provide drop counter when packets are dropped due to incorrect ltl to vdc mapping in KLM vdc
CSCvj23813	Remove stale LTL entries from IM as a part of CSCvj10306
CSCvj33348	N77-M348XP-23L/N77-SUP2E Linecard crash for IPFIB process followed by IFTMC crash
CSCvj36340	FCoE pause drop threshold reached when VL is paused/resumed quickly
CSCvj55192	Kernel memory commands not working
CSCvj58687	Intermittent 51 second frame timeout drops without congestion
CSCvj61790	MSDP CORE on N9k due to RPM
CSCvj63798	Cisco FXOS and NX-OS Software CLI Command Injection Vulnerability (CVE-2019-1611)
CSCvj70748	Output of "show mpls ldp igp sync" inconsistent with configuration
CSCvj77201	user logged out from ssh session in user VDC when admin VDC is configured with exec-timeout
CSCvj84775	PIM6 Anycast-RP failling to send Register-Stop
CSCvk01435	M3- PTP Multicast-224.0.1.129 packet drop
CSCvk03597	PTP GM clock sync loss after system reload, process restart
CSCvk10690	Additional debugability for SLF LINK_GOOD_TO_FAULT_12 on N77-M348XP-23L
CSCvk10930	N7K Interface stuck in LACP suspend after link flap with ethernet oam
CSCvk16641	ipv6 static route with next-hop as ipv6 address across the vxlan fabric does not get into URIB
CSCvk22288	n7k/GOLD: conservative mode improvements
CSCvk24064	Flanker (F3) diag failures on multiple modules in 8.2(x)
CSCvk28290	Fabricpath DCE mode of port-channel member inconsistent

Table 29 Cisco NX-OS Release 8.4(1) Resolved Caveats

Identifier	Description
CSCvk28894	Nexus 8.x - MPLS can blackhole traffic if you have multiple VDCs on the same instance of M2 linecard
CSCvk31556	invalid source ip for inter vrf ping for /32 destination
CSCvk35035	logging server vrf name in startup-config changed after reload
CSCvk35999	Nexus 7000 Series EPLD upgrade fails on 8.3(1)
CSCvk38405	N7k M3/F3/F4:Fragmented PIM BSR packets are CPU punted and dropped
CSCvk38474	Suppress the bcast check on /31 VIP or pass mask from VIP to API if mask < 31
CSCvk44309	N7K iftmc crashed when tried to bring up gre tunnel
CSCvk45949	When a private-vlan is the first extended vlan more than 64 ranges can be configured in OTV
CSCvk51138	N7K Fabricpath :: MAC address not re-learned on broadcast ARP
CSCvk51388	Cisco NX-OS Software CLI Command Injection Vulnerability (CVE-2019-1609)
CSCvk51420	Cisco NX-OS Software NX-API Command Injection Vulnerability
CSCvk53943	HSRP active replies arp request with physical mac address after preempt
CSCvk54735	FCoE "uSecs VL3 is in internal pause rx state" increments when eth port is not currently paused
CSCvk55799	STP BPDUS for pruned VLANs are reaching the cpu.
CSCvk56857	MPLS BGP to OSPF redistribution DN bit not set
CSCvk58123	In maintenance mode profile, a route-map in BGP is only applied on either inbound or outbound.
CSCvk58529	N7k - Various NTP features not working on 8.3(1)
CSCvk60178	M3 CB100: Remove 40G and insert of 100g in one port impact the traffic in adj port
CSCvk68623	IPv6 recursive nexthop is not working in VRF leaking setup
CSCvk68792	NXOS: Netstack crash observed with active timer library in heap_extract_min
CSCvk74490	LDP flushes static label bindings after graceful restart completes
CSCvk75372	N7K - self-originated LSAs subjected to MinLSArrival check
CSCvm01077	LISP - SVI responds and allows ssh for non-existing hosts in the subnet
CSCvm02470	POAP acl config is added to running-config after system bootup
CSCvm05636	IP redirects disabled in configuration but enabled in ELTM
CSCvm09089	Command 'show hardware flow' results into a crash when it creates a temporary file
CSCvm09452	N77-F348XP-23 kernel panic
CSCvm11792	ISIS IPv6 multi-topology - fixing MT attached bit
CSCvm14482	Switch reload due to kernel panic
CSCvm16677	PSS memory leak in igmp_snoop for key type 0x04 and 0x0d

Table 29 Cisco NX-OS Release 8.4(1) Resolved Caveats

Identifier	Description
CSCvm19090	DDB sanity check and client notification changes
CSCvm21746	ospfIfIpAddress not working for specific index
CSCvm28899	GARP/ARP does not trigger EID detection
CSCvm29785	N7k BGP L2VPN VPLS Auto Discovery route not imported after route flaps
CSCvm32486	PSS memory leak Type-0x0d on large burst of join/leave
CSCvm35215	Cisco NX-OS Software Privilege Escalation Vulnerability
CSCvm43644	NXOS BGP is not advertising some of the BGP prefixes to the Neighbors
CSCvm46017	Netflow active timeout is not working as expected
CSCvm50765	Default route (track added) not getting advertised after box reload
CSCvm52059	CPU Traffic Not Sent out on L3 VRF Interface
CSCvm55640	FEX not process NIF down when parent's ports shutdown or power off
CSCvm56314	OTV VDC ignores dst IP in port-channel hash
CSCvm63999	Issue with the BGP "pre-bestpath" point of insertion (POI) on Nexus7k
CSCvm65141	cannot rewrite vlan at dual-active exclude interface-vlan-bridge-domain
CSCvm67806	FabricPath - use PURGE instead of DELETE when LSA expire
CSCvm69204	N77 who is HSRP active can not reply ARP if NIF is down
CSCvm74036	N7k MPLS LDP Advertise Label Prefix-List not properly applied
CSCvm74044	PBR feature disabled after cold-boot upgrade to 8.3(1)
CSCvm84486	Tracked IPv4 local HMM stays UP while route is learned as remote
CSCvm93582	N7K/NTP: ensure monolithic time sync between active and standby
CSCvm99009	Port Info missing in level 2 L2FM log messsage when MAC moves continuously at a high rate
CSCvm99288	pktmgr process memory leak @ libnve.so
CSCvn01886	Nexus SW - Route missing in RIB while track object is up upon reload
CSCvn03958	Drop OAM packets in KLM VDC
CSCvn08550	N7K - 'ip routing multicast holddown' not working as expected
CSCvn09912	N7k/F2E: 'Disabling PFC on port x since macsec is disabled' logs filling syslog
CSCvn13028	"nfp" crash on module when configuring netflow
CSCvn14579	F3 Egress buffer lockup handling
CSCvn20899	BGP next-hop-self behavior changed back for reflected routes
CSCvn22059	N7K - aclqos crash
CSCvn24277	M3: EOBC heartbeat failure in device DEV_EOBC_MAC
CSCvn25428	Line card on Nexus7K will start forwarding traffic before routes are programmed
CSCvn25706	bfd is down before it times out, which causes bgp down.
CSCvn27072	N77:status in "show pc cli status" output shows "Commit in progress"

Table 29 Cisco NX-OS Release 8.4(1) Resolved Caveats

Identifier	Description
CSCvn28540	Multicast packets with TTL=1 are routed and forwarded when OIF is not null
CSCvn28629	MAC move/add/delete not detected on fabricpath after l2fm process restart
CSCvn32302	M3 reload with SLF_VOQ_CPM_MSTR_INT_ADDRNE_ERR need more info
CSCvn36425	N9K - aclmgr crash @ddb functions
CSCvn39414	NXOS: Local VRF leaking failed after ip clear of specific route in dest VRF
CSCvn40407	Port-channel running configuration does not show FEC mode when port-channel has no members
CSCvn40533	BGP specific routes not advertized to labeled-unicast neighbor after aggregate removal
CSCvn42389	ACLQOS Core with FEX on N77K
CSCvn44369	NXOS advertises the pseudonode inconsistently in multitopology mode
CSCvn45757	Incorrect credit programmed for N7K-F306CK-25 after cold boot 6.x/7.x to 8.x
CSCvn49527	URIB missing Type-2 host route after host (mac-ip) move from local to remote VTEP
CSCvn50809	sac_usd hap reset when standby supervisor becomes active on N7K 6.2(18)
CSCvn51301	ARP crashed on BL while other BL comes online // ARP mbuf leak
CSCvn57717	Improve EOBC resiliency
CSCvn59162	GOLF VxLAN Type5 next-hop unchanged
CSCvn59937	ISCM crash/core due to NAT enable under ITD configuration
CSCvn61247	N7K M3 Span destination port accepts by default incoming traffic.
CSCvn61562	SUP3: observing QCR4 & QCR6 ECC bit errors on loading 8.3.2.S20
CSCvn63538	N7K: Entries in new created SVI mismatch between UFIB and URIB and communication fail using those
CSCvn65211	Timeout on "add vlan" for large port-profile
CSCvn67179	IPFIB process crash after NXOS upgrade.
CSCvn69198	N7K Netflow need First_switched and Last_switched timestamps be exported in Big endian format
CSCvn70922	Static-oif functionality doesn't work on Nexus when group-range option is used
CSCvn79001	BGP: md5 is missing on listening TCP socket after quick interface delete / re-add
CSCvn80406	N7k setting VDC routing resource limits to max causes VDC to go in failed state
CSCvn82773	N7K - ILM index for existing port allocated incorrectly to a different port after ISSU
CSCvn95608	bgp nxos: RR status not cleared after neighbor is un-configured via "no neighbor X.X.X.X"

Table 29 Cisco NX-OS Release 8.4(1) Resolved Caveats

Identifier	Description
CSCvn97534	Interrupt "FLN_QUE_INTR_EB_P2_ERR_U_PLEN_MP_ZRO_N_EOS" should be added for Egress buffer recovery.
CSCvn99156	Incorrect number of prefixes sent if Candidate-RP list packet length greater than configured PIM MTU
CSCvn99435	API snmp_get_mgmt_conf_last_change_time return ERROR
CSCvn99680	PTP - GM OFFSET 37 Seconds and Nexus 7K SR 685369201
CSCvo07343	VXLAN IPv6 packets loop due to NVE invalid source-intf state while peerlink is down or unconfigured.
CSCvo08309	LISP: Away entries take 90 seconds to be downloaded to uRIB in when RIB based mobility is enabled
CSCvo09373	N7700- N77-M348XP-23L- Vlan tagging uncorrect in local span
CSCvo09511	CLI hangs for several minutes when applying certain interface-level commands
CSCvo10122	N7k: eem config cannot be removed when standby sup is powered down
CSCvo13456	ISIS LSP flooding broken
CSCvo14963	N7K-PPM: Issues seen under interface when port-profile is inherited.
CSCvo18971	Instance bit map getting mis-programmed causing fib miss.
CSCvo22236	Nexus 7k netstack crash
CSCvo23988	'show system internal iftmc info global' command include invalid character.
CSCvo28782	Crash during Free of Filter Links
CSCvo29766	Nexus / NX-OS / Multicast PIM Join not sent when IPv4 unicast route has IPv6 next-hop (RFC 5549)
CSCvo29957	Output of "show mpls ldp igp sync" inconsistent with configuration
CSCvo34762	IPv6 static routes may get missed in RIB on PKL/PL shut/unshut
CSCvo44343	N7K: Supervisor DIMM failure does not trigger Sup Failover.
CSCvo49272	Only one static route is installed in RIB if ECMP paths are learnt via same next-hop
CSCvo51463	N7K: VSH crash
CSCvo56362	Nexus 5k crashed due to fabric_mcast hap reset
CSCvo68452	Pending mroute entries persists after VRF is deleted
CSCvo70466	L2MCAST crash due to null pointer dereference when searching AVL tree
CSCvo70810	N9k bgp outbound route-map not working properly in L3VPN implementation
CSCvo73682	sac_usd hap reset when standby supervisor becomes active
CSCvo78276	LIF programmed to 0x0 for L3 VPN prefixes, after ECMP ports/port-channels are flapped
CSCvo90639	N7K/N77 // TOS bits from IP header not being copied to MPLS EXP Bits in MPLS Header
CSCvo93018	Malformed ISIS Hello packet due to extra GRE header
CSCvo98267	N77-SUP3E:link LED of mgmt port behaves in reverse way

Table 29 Cisco NX-OS Release 8.4(1) Resolved Caveats

Identifier	Description
CSCvp02900	VPC: Type2 EVPN route advertised with primary IP of Loopback as next-hop
CSCvp08694	Stale arp entry/route after VM move from one VPC domain to other due to HMM update failure
CSCvp14470	OSPF crash due to invalid entry in interfaces array.
CSCvp19180	N7K BFD - netstack crash
CSCvp25704	Cli show top command does not have an exit option
CSCvp25875	F3 card: show hardware flow ip command may cause process NFP to crash.
CSCvp30746	MAC deleted from other PO member port where MAC has aged out, when non-aged port goes down.
CSCvp33458	LISP: Forward-native cache persists after refreshed with more specific route.
CSCvp35682	Target Address on IP SLA (udp) probes is getting changed to a new IP other than the configured one
CSCvp37275	Nexus 7000 Automated tech-support on hap reset Supervisor Switchover not Functioning
CSCvp37629	N7K-F3 module reload due to FLN_QUE_INTR_EB_P6_HL_ERR interrupt and EB lockup.
CSCvp37970	N7k MPLS LDP label allocate prefix-list needs to be re-applied when changes are made to prefix-list
CSCvp38452	MDS 32G module XBAR SYNC exceptionlog entries are missing meaningful information
CSCvp41187	N7K replaces the default mpls-vpn route with the type-7 default route
CSCvp45874	N7K M3 PBR load-share does not redirect traffic as expected
CSCvp45929	N7K Supervisor Switchover due to TACACS+ hap reset - bad file descriptor
CSCvp47670	"no ip redirects" configurable on L3 port-channel member port
CSCvp50779	N77-C7710-FAB-3 EPLD upgrade fail from 0.007 to 0.008
CSCvp51579	Nexus 7000 / M3 / not accepting filter acces-group command in erspan config
CSCvp57692	BFD session goes down upon changing IP address of unrelated interface
CSCvp58845	After remove/add VRF, remote host routes not installed to URIB and report 'remote nh not installed'
CSCvp70746	n7k/F2: EEM to ignore interrupt during EG recovery (CSCux90737/CSCug39011/CSCux08154/CSCud43503)
CSCvp83475	SDA: Invalid src ip address in VXLAN header on n7k border
CSCvp98039	N7K MPLS FIB programming issues after reload w/ M3 module
CSCvq09112	Incorrect parsing when using " " in loopback configuration
CSCvq32044	BGP process crash with aggregate-address config without summary-only option under VRF
CSCvn73615	vsh core on F4 40G/Fex
CSCvq07837	VXLAN decap fails SLF_L3RI_CP_SW_ERR_CTR on M3 if UDP src port is 2268 AMT Tunnel is mis-identified

Table 29 Cisco NX-OS Release 8.4(1) Resolved Caveats

Identifier	Description
CSCvo44103	MDS: Handling ISSD gracefully when sup2sup eobc ha backup link in use
CSCvp57934	Optimization of internal NXOS parameters
CSCvi89033	N7K Consistency Checker: L3 Mcast MRIB to MFIB CC
CSCvn60645	N7K Consistency Checker: URIB/AM to UFIB CC
CSCvk33710	sending admin dce mode in MTS_OPC_IM_PORT_LAYER_PARAM_CHANGE while port default is done
CSCvk72654	ISIS missing support for route tags
CSCvo04672	Improve convergence performance of VTEP ECMP
CSCvq20196	leak-route doesn't happen leading to leak-route installation failure
CSCud04830	hsrp ip subnet mismatch when vrf is not present

Related Documentation

Cisco Nexus 7000 documentation is available at the following URL:

http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/tsd-products-support-series-home.html

The Release Notes for upgrading the FPGA/EPLD is available at the following URL:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/epld/cisco_nexus7000_epld_rn_8x.html

Cisco NX-OS documents include the following:

Cisco NX-OS Configuration Guides

Cisco Nexus 7000 series configuration guides are available at the following URL:

http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-installation-and-configuration-guides-list.html

Cisco NX-OS Command References

Cisco Nexus 7000 series command references are available at the following URL:

http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-command-reference-list.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, 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

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.