Cisco Nexus 7000 Series NX-OS 8.x, Release Notes

First Published: December 22, 2016
Last Modified: February 16, 2024
Current Release: 8.2(11)

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 160.

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.

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
February 16, 2024	Created release notes for Cisco NX-OS Release 8.2(11).
May 26, 2023	Created release notes for Cisco NX-OS Release 8.2(10).
September 30, 2022	Created release notes for Cisco NX-OS Release 8.2(9).
December 03, 2021	Created release notes for Cisco NX-OS Release 8.2(8).
July 02, 2021	Updated the Supported Upgrade and Downgrade Paths, page 41 section to include Cisco NX-OS Release 7.3(8)D1(1).
June 25, 2021	Created release notes for Cisco NX-OS Release 8.2(7a).

Cisco Systems, Inc.
www.cisco.com

Table 1 Change History

Date	Description
January 08, 2021	Updated the Supported Upgrade and Downgrade Paths, page 41 section to include Cisco NX-OS Release 7.3(7)D1(1).
November 4, 2020	Added Bug details: for Cisco NX-OS Release 8.2(3).
July 24, 2020	Created release notes for Cisco NX-OS Release 8.2(6).
April 17, 2020	Updated the Supported Upgrade and Downgrade Paths, page 41 section to include Cisco NX-OS Release 7.3(6)D1(1).
November 15, 2019	Updated the Supported Upgrade and Downgrade Paths, page 41 section to include Cisco NX-OS Release 7.3(5)D1(1).
November 14, 2019	Created release notes for Cisco NX-OS Release 8.2(5).
June 21, 2019	Created release notes for Cisco NX-OS Release 8.2(4).
March 1, 2019	Created release notes for Cisco NX-OS Release 8.2(3).
November 2, 2018	Updated the Supported Upgrade and Downgrade Paths, page 41 section to include Cisco NX-OS Release 7.3(3)D1(1).
September 26, 2018	Updated the Supported Upgrade and Downgrade Paths, page 41 section to include Cisco NX-OS Release 7.3(2)D1(3a).
June 11, 2018	Updated the Supported Upgrade and Downgrade Paths, page 41 section to include Cisco NX-OS Release 7.3(2)D1(3).
April 12, 2018	Created release notes for Cisco NX-OS Release 8.2(2).
March 7, 2018	Created release notes for Cisco NX-OS Release 8.1(2a).
January 30, 2018	Created release notes for Cisco NX-OS Release 8.1(2).
September 28, 2017	Created release notes for Cisco NX-OS Release 8.2(1).
June 30, 2017	Updated the Cisco NX-OS Release 8.2(3) supports the following cold boot support matrix:, page 86 section to include Cisco NX-OS Release 7.3(2)D1(1).
May 3 2017	Created release notes for Cisco NX-OS Release 8.1(1).
February 21, 2017	Updated the Upgrade and Downgrade Paths and Caveats, page 41 section to include Cisco NX-OS Release 6.2(18).
December 22, 2016	Created release notes for Cisco NX-OS Release 8.0(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.

System Requirements

This section includes the following topic:

- Supported Device Hardware, page 3

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.

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)

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

Product ID	Hardware	Minimum Software Release
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)
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)

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

Product ID	Hardware	Minimum Software Release
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)
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-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-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)

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

Product ID	Hardware	Minimum Software Release
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)
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-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)

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)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	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)
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)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	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)
	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)
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)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	SFP-GE-Z	1000BASE-ZX SFP (DOM)	6.0(1)
	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	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)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	QSFP-40G-CSR4 QSFP-40G-SR4 QSFP-40G-SR4-S QSFP-40G-SR-BD	Multi-mode fiber (MMF)	7.3(0)DX(1)
	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)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	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)
	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)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	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)
	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)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	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)
	QSFP-40G-LR4	40GBASE-LR4 QSFP+ (Ethernet and OTU3 capable)	6.2(12)
	QSFP-40G-ER4	40GBASE-ER4 QSFP+ (40km)	6.2(12)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
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)
	QSFP-H40G-AOCxM	Active optical cable assembly	8.0(1)
	QSFP-4X10G-AC7M	Direct attach breakout 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-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)
	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)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	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 8.1(1), page 34
- Guidelines and Limitations—Cisco NX-OS Release 8.0(1), page 35
- Guidelines and Limitations Common for Cisco NX-OS Release 8.0(1) and Cisco NX-OS Release 8.1(1), page 36

Guidelines and Limitations - Cisco NX-OS Release 8.2(9)

N7K-SUP2

Cisco NX-OS Release 8.x utilizes more memory than earlier NX-OS releases. As a result, N7K-SUP2 (Non-enhanced) experiences low memory condition with multi-dimensional scale.

Refer to Cisco Nexus 7000 Series NX-OS Verified Scalability Guide for more information.

Starting from NX-OS Release 8.2(9) and Release 8.4(6), low memory syslog threshold alerts are set as mentioned below:

```
minor 80 severe 85 critical 91
2023 Apr 20 01:22:43 700710-1 %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : MINOR.
```

Prior to Release 8.2(9) and Release 8.4(6) in release 8.x train the thresholds must be configured through NX-OS CLI:

```
system memory-thresholds minor 80 severe 85 critical 91
```

You can use the following NX-OS commands to monitor memory usage:

```
show system internal memory-usage-per-module
show system resources
show system resources module all
```

Guidelines and Limitations—Cisco NX-OS Release 8.2(3)

This section describes the guidelines and limitations for the Cisco Nexus 7000 Series in Cisco NX-OS Release 8.2(3).

- 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 the second case. This is a known limitation.

Guidelines and Limitations—Cisco NX-OS Release 8.2(2)

This section describes the guidelines and limitations for the Cisco Nexus 7000 Series in Cisco NX-OS Release 8.2(2).

- You need to use the breakout configuration on the interface in order to use the CVR-QSFP-SFP10G converter on N77-M324FQ-25L and N77-F324FQ-25 modules.

Guidelines and Limitations—Cisco NX-OS Release 8.2(1)

This section describes the guidelines and limitations for the Cisco Nexus 7000 Series in Cisco NX-OS Release 8.2(1).

- When you run Cisco NX-OS Release 8.2(1) on a Cisco Nexus 7000 or Cisco Nexus 7700 switches having overlay technology (OTV, VXLAN or L2VPN/VPLS) configuration with M3 series modules, there is a chance that some Layer 2 tunneled multicast traffic might be mis-forwarded due to scale conditions on the M3 module or the M3 module might go into a failure state with the following error:

  ```
  FATAL interrupt with Error Description: BEM_EL3_CTL_INVLD
  %MODULE-2-MOD_SOMEPORTS_FAILED: Module 1 (Serial number: JAE202004WF) reported failure
  on ports Ethernet1/7 (Ethernet) due to fatal error in device DEV_SLF_BRI (device error
  0xce401600)
  ```

  For more information and workaround details refer to CSCvg09282.

  In order to check and confirm if you come across this issue, look for the exact failure reason using the **sh module internal exceptionlog module <***mod_num***>** command.

  This defect can affect a Cisco Nexus 7000 or Cisco Nexus 7700 chassis running M3 modules under the following condition. (This issue is specific to M3 modules and not applicable to F3 or any other modules.)

  - OTV or VXLAN with scaled configuration close to 2K VLANs/BD extended.
  - Network churn in a short period of time (multiple overlay flaps within 10 minutes) which involves bringing down the tunnels and recreating them in the system might lead to above symptoms.

  The workaround for this issue is to reload the affected M3 module. To avoid re-occurrence of this problem, reduce the number of VLANs/BD extended over DCI.

  A SMU for this fix is being tested and validated and will be published to the field.

- All Virtual Private LAN Services (VPLS) and Ethernet over MPLS (EoMPLS) functionalities, except Ethernet Flow Points (EFP), service instances, and bridge domains, are supported on M3-Series I/O modules.
- Flexible ACL TCAM bank chaining is supported on the M2 Series modules in Cisco NX-OS Release 8.2(1) along with the existing support for the M3 Series modules.
- Starting with Cisco NX-OS Release 8.2(1), FabricPath feature is supported on a VDC that has M3 and F3 Series modules.
- When you use the **storm-control unicast level** *percentage* command in a module, both the unknown and known unicast traffic gets discarded after reaching the threshold value.

VXLAN BGP EVPN and OTV inter operation feature has the following limitations on M3 modules for in Cisco NX-OS Release 8.2(1):

- This feature is supported only on the M3-only VDC.
- A secondary IP has to be configured on each BDI. Anycast IP should also be configured, it acts as a primary and continue to be used on the VXLAN side.
- To enable seamless mobility across legacy and VXLAN PODs, HSRP MAC and Anycast gateway MAC should be explicitly cross configured as gateway MAC.
- The **tunnel-stitching** command flaps the overlay interface.
- Static ARP is required for Layer 3 connectivity between vPC peers.
- Orphan port should not be connected to the vPC secondary.

- OTV Proxy ARP is not supported for OTV with BDI.
- VXLAN ARP Suppression and OTV Proxy ARP should be consistently configured.
- There is no ISSU support for VXLAN with OTV and BDI feature.
- Router-on-a-stick approach is used for overlay multicast routing.
- OTV loopback is not supported.
- Migration option 1 or option 2 should be used in Cisco NX-OS Release 8.2(1).
- Layer 3 multicast routing is not supported on border leaf with VXLAN+OTV extension.
- Two overlays on a same join interface are not supported.
- VXLAN BGP EVPN and OTV inter operation feature does not have any convergence improvements in Cisco NX-OS Release 8.2(1).
- VXLAN BGP EVPN and OTV inter operation feature supports only 3 OTV sites in Cisco NX-OS Release 8.2(1).

Guidelines and Limitations—Cisco NX-OS Release 8.1(1)

This section describes the guidelines and limitations in Cisco NX-OS Release 8.1(1) for the Cisco Nexus 7000 Series.

- vPC+ feature is supported on the M3 modules in Cisco NX-OS Release 8.1(1).
- FabricPath feature is not supported on a VDC that has M3 and F3 modules in Cisco NX-OS Release 8.1(1).
- The in-band Power On Auto Provisioning (POAP) works in any setup where connectivity to the DHCP server is present in the in-band port. You can use the in-band port in the non-FabricPath setups.
- In Cisco NX-OS Release 8.1(1) only the admin users are allowed to access/initiate the secure FTP (SFTP).
- The multi-hop BFD feature supports only the static routes in Cisco NX-OS release 8.1(1),
- When you use the **storm-control unicast level** *percentage* command in a module, both the unknown and known unicast traffic gets discarded after reaching the threshold value.

M3 FEX Support

The number of VLANs per Fabric Extender server interface is 300 for M3 modules.

M3 FEX does not support the following features in Cisco NX-OS Release 8.1(1):

- vPC+ / FabricPath
- PVLAN over FEX
- VSI / EVPN with FEX
- FEX AA (active-active mode)

Dynamic Routing over vPC

- Dynamic Routing over vPC feature (for IPv4 Unicast traffic only) is supported on F2E, F3, and M3 series modules in Cisco NX-OS. Dynamic Routing is not supported over vPC+.

Unsupported Features - VDC on M3 Module

The following features are not supported on a VDC that has an M3 module:

- MPLS L2VPN
- MPLS L2VPN QoS
- LISP
- Physical port vPC
- Storage VDC
- QoS Template: 7e/6e/4e network QOS: The QoS templates are globally applied from the default VDC and hence this would not be allowed at the system level, which means if the system has an M3 module, the QoS templates would not be supported.
- PTP Pong

Guidelines and Limitations—Cisco NX-OS Release 8.0(1)

This section describes the guidelines and limitations in Cisco NX-OS Release 8.0(1) for the Cisco Nexus 7000 Series.

Unsupported Features - VDC on M3 Module

The following features are not supported on a VDC that has an M3 module:

- FabricPath
- vPC+
- MPLS L2VPN
- MPLS L2VPN QoS
- LISP
- Physical port vPC
- FEX
- Storage VDC
- QoS Template: 7e/6e/4e network QOS: The QoS templates are globally applied from the default VDC and hence this would not be allowed at the system level, which means if the system has an M3 module, the QoS templates would not be supported.
- PTP Pong

Dynamic Routing over vPC

- Dynamic Routing over vPC feature (for IPv4 Unicast traffic only) is supported only on F2E and F3 series modules in Cisco NX-OS.

Storm-control Suppresses Unicast Traffic

- When you use the **storm-control unicast level** *percentage* command in a module, both the unknown and known unicast traffic gets discarded after reaching the threshold value.

Network Analysis Module (NAM-NX1)

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

Guidelines and Limitations Common for Cisco NX-OS Release 8.0(1) and Cisco NX-OS Release 8.1(1)

The following guidelines and limitations are applicable to both the Cisco NX-OS Release 8.0(1) and Cisco NX-OS Release 8.1(1).

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 and M3 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.

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).

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

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 8.2(11)

See Table 5 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.2(11).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 8.2(11))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 8.2(11)	8.2(10)
	8.2(9)
	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(9)D1(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)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.

Note

1. Multi-hop ISSU term refers to two successive ISSUs between major releases.
2. A major release introduces significant new software features, hardware platforms.
   The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.
   For example - Consider an upgrade from 8.1(1) TO 8.4(5).
   The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.
   The procedure for the ISSU upgrade path is as follows:

   Step 1 **ISSU from major release 8.1(1) to another major release 8.2(3).**

   Step 2 **ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.**

   Step 3 **ISSU from major release 8.2(5) to another major release 8.4(5).**

   Step 4 **Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.**

   You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch. We recommend doing a
binary reload instead of upgrading.
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.2(10)

See Table 6 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.2(10).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 8.2(10))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 8.2(10)	8.2(9)
	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(9)D1(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)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.

Note

1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.
   The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.
   For example - Consider an upgrade from 8.1(1) TO 8.4(5).
   The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.
   The procedure for the ISSU upgrade path is as follows:

   Step 1 **ISSU from major release 8.1(1) to another major release 8.2(3).**

   Step 2 **ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.**

   Step 3 **ISSU from major release 8.2(5) to another major release 8.4(5).**

   Step 4 **Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.**

   You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch. We recommend doing a
binary reload instead of upgrading.
```

```
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.2(9)

See Table 7 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.2(9).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 8.2(9))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 8.2(9)	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(9)D1(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)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.

Note

1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.
   The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.
   For example - Consider an upgrade from 8.1(1) TO 8.4(5).
   The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.
   The procedure for the ISSU upgrade path is as follows:

   Step 1 **ISSU from major release 8.1(1) to another major release 8.2(3).**

   Step 2 **ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.**

   Step 3 **ISSU from major release 8.2(5) to another major release 8.4(5).**

   Step 4 **Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.**

   You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch. We recommend doing a
binary reload instead of upgrading.
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.2(8)

See Table 8 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.2(8).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 8.2(8))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 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)

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.

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.

Note

1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.
The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.
For example - Consider an upgrade from 8.1(1) TO 8.4(5).
The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.
The procedure for the ISSU upgrade path is as follows:

Step 1 **ISSU from major release 8.1(1) to another major release 8.2(3).**

Step 2 **ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.**

Step 3 **ISSU from major release 8.2(5) to another major release 8.4(5).**

Step 4 **Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.**

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch. We recommend doing a
binary reload instead of upgrading.
```

```
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.2(7a)

See Table 9 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.2(7a).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 8.2(7a))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 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)

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

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.

Note

1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.
   The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.
   For example - Consider an upgrade from 8.1(1) TO 8.4(5).
   The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.
   The procedure for the ISSU upgrade path is as follows:

   Step 1 **ISSU from major release 8.1(1) to another major release 8.2(3).**

   Step 2 **ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.**

   Step 3 **ISSU from major release 8.2(5) to another major release 8.4(5).**

   Step 4 **Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.**

   You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch. We recommend doing a
binary reload instead of upgrading.
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.2(6)

See Table 10 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.2(6).

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 8.2(6))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 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)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.

Note

1. Multi-hop ISSU term refers to two successive ISSUs between major releases.
2. A major release introduces significant new software features, hardware platforms.
   The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.
   For example - Consider an upgrade from 8.1(1) TO 8.4(5).
   The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.
   The procedure for the ISSU upgrade path is as follows:

   Step 1 **ISSU from major release 8.1(1) to another major release 8.2(3).**

   Step 2 **ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.**

   Step 3 **ISSU from major release 8.2(5) to another major release 8.4(5).**

Step 4 **Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.**

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch. We recommend doing a
binary reload instead of upgrading.
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.2(5)

See Table 11 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.2(5).

Note Only the ISSU paths/combinations in Table 11 have been tested and are supported.

Table 11 *Supported ISSU Paths for Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switch (Cisco NX-OS Release 8.2(5))*

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 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)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.

Note

1. Multi-hop ISSU term refers to two successive ISSUs between major releases.
2. A major release introduces significant new software features, hardware platforms.
   The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.
   For example - Consider an upgrade from 8.1(1) TO 8.4(5).
   The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.
   The procedure for the ISSU upgrade path is as follows:

   Step 1 **ISSU from major release 8.1(1) to another major release 8.2(3).**

   Step 2 **ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.**

   Step 3 **ISSU from major release 8.2(5) to another major release 8.4(5).**

   Step 4 **Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.**

   You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch. We recommend doing a
binary reload instead of upgrading.
```

```
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.2(4)

See Table 12 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.2(4).

Note Only the ISSU paths/combinations in Table 12 have been tested and are supported.

Table 12 Supported ISSU Paths for Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switch (Cisco NX-OS Release 8.2(4))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 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)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.

Note

1. Multi-hop ISSU term refers to two successive ISSUs between major releases.
2. A major release introduces significant new software features, hardware platforms.
   The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.
   For example - Consider an upgrade from 8.1(1) TO 8.4(5).
   The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.
   The procedure for the ISSU upgrade path is as follows:

   Step 1 **ISSU from major release 8.1(1) to another major release 8.2(3).**

   Step 2 **ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.**

   Step 3 **ISSU from major release 8.2(5) to another major release 8.4(5).**

   Step 4 **Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.**

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
    Multiple Major ISSU has been performed on this switch. We recommend doing a
    binary reload instead of upgrading.
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.2(3)

See Table 13 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.2(3).

Note Only the ISSU paths/combinations in Table 13 have been tested and are supported.

Table 13 Supported ISSU Paths for Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switch (Cisco NX-OS Release 8.2(3))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 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)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.

Note

1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.
   The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.
   For example - Consider an upgrade from 8.1(1) TO 8.4(5).
   The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.
   The procedure for the ISSU upgrade path is as follows:

   Step 1 **ISSU from major release 8.1(1) to another major release 8.2(3).**

   Step 2 **ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.**

   Step 3 **ISSU from major release 8.2(5) to another major release 8.4(5).**

   Step 4 **Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.**

   You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

   ```
   Multiple Major ISSU has been performed on this switch. We recommend doing a
   binary reload instead of upgrading.
   ```

```
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.2(2)

See Table 14 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.2(2).

Note Only the ISSU paths/combinations in Table 14 have been tested and are supported.

Table 14 Supported ISSU Paths for Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switch (Cisco NX-OS Release 8.2(2))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 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)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.

Note

1. Multi-hop ISSU term refers to two successive ISSUs between major releases.
2. A major release introduces significant new software features, hardware platforms.
   The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.
   For example - Consider an upgrade from 8.1(1) TO 8.4(5).
   The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.
   The procedure for the ISSU upgrade path is as follows:

   Step 1 ISSU from major release 8.1(1) to another major release 8.2(3).

   Step 2 ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.

   Step 3 ISSU from major release 8.2(5) to another major release 8.4(5).

   Step 4 Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

   You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
   Multiple Major ISSU has been performed on this switch. We recommend doing a
   binary reload instead of upgrading.
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.1(2a)

See Table 15 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.1(2a).

Note Only the ISSU paths/combinations in Table 15 have been tested and are supported.

Table 15 Supported ISSU Paths for Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switch (Cisco NX-OS Release 8.1(2a))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 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)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.

Note

1. Multi-hop ISSU term refers to two successive ISSUs between major releases.
2. A major release introduces significant new software features, hardware platforms.
   The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).
The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.
The procedure for the ISSU upgrade path is as follows:

Step 1 **ISSU from major release 8.1(1) to another major release 8.2(3).**

Step 2 **ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.**

Step 3 **ISSU from major release 8.2(5) to another major release 8.4(5).**

Step 4 **Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.**

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
    Multiple Major ISSU has been performed on this switch. We recommend doing a
    binary reload instead of upgrading.
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.1(2)

See Table 16 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.1(2).

Note Only the ISSU paths/combinations in Table 16 have been tested and are supported.

Table 16 Supported ISSU Paths for Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switch (Cisco NX-OS Release 8.1(2))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 8.1(2)	8.1(1)
	8.0(1)
	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)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.

Note

1. Multi-hop ISSU term refers to two successive ISSUs between major releases.
2. A major release introduces significant new software features, hardware platforms.
   The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).
The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.
The procedure for the ISSU upgrade path is as follows:

Step 1 **ISSU from major release 8.1(1) to another major release 8.2(3).**

Step 2 **ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.**

Step 3 **ISSU from major release 8.2(5) to another major release 8.4(5).**

Step 4 **Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.**

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
    Multiple Major ISSU has been performed on this switch. We recommend doing a
    binary reload instead of upgrading.
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.2(1)

See Table 17 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.2(1).

Note Only the ISSU paths/combinations in Table 17 have been tested and are supported.

Table 17 Supported ISSU Paths for Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switch (Cisco NX-OS Release 8.2(1))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 8.2(1)	8.1(1)
	8.0(1)
	7.3(2)D1(1)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.

Note

1. Multi-hop ISSU term refers to two successive ISSUs between major releases.
2. A major release introduces significant new software features, hardware platforms.
   The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.
   For example - Consider an upgrade from 8.1(1) TO 8.4(5).
   The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.
   The procedure for the ISSU upgrade path is as follows:

Step 1 **ISSU from major release 8.1(1) to another major release 8.2(3).**

Step 2 **ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.**

Step 3 **ISSU from major release 8.2(5) to another major release 8.4(5).**

Step 4 **Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.**

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
    Multiple Major ISSU has been performed on this switch. We recommend doing a
    binary reload instead of upgrading.
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.1(1)

See Table 18 for the in-service software upgrade (ISSU) path for Cisco NX-OS Release 8.1(1).

Note Only the ISSU combinations in the following table, Table 18 have been tested and are supported.

Table 18 Supported ISSU Paths for the Cisco Nexus 7000 and Cisco Nexus 7700 Series Chassis (Cisco NX-OS Release 8.1(1)

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release

Cisco NX-OS Release 8.1(1)	8.0(1)
	7.3(1)D1(1)
	7.3(0)DX(1)
	7.3(0)D1(1)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.

Note

1. Multi-hop ISSU term refers to two successive ISSUs between major releases.
2. A major release introduces significant new software features, hardware platforms.
   The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.
   For example - Consider an upgrade from 8.1(1) TO 8.4(5).
   The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.
   The procedure for the ISSU upgrade path is as follows:

Step 1 **ISSU from major release 8.1(1) to another major release 8.2(3).**

Step 2 **ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.**

Step 3 **ISSU from major release 8.2(5) to another major release 8.4(5).**

Step 4 **Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.**

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch. We recommend doing a
binary reload instead of upgrading.
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.0(1)

See Table 19 for the in-service software upgrade (ISSU) path for Cisco NX-OS Release 8.0(1).

Note Only the ISSU combinations in the following table, Table 19 have been tested and are supported.

Table 19 Supported ISSU Paths for the Cisco Nexus 7000 and 7700 Series Chassis (Cisco NX-OS Release 8.0(1)

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release

Cisco NX-OS Release 8.0(1)	7.3(1)D1(1)
	7.3(0)DX(1)
	7.3(0)D1(1)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.

Note

1. Multi-hop ISSU term refers to two successive ISSUs between major releases.
2. A major release introduces significant new software features, hardware platforms.
   The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.
   For example - Consider an upgrade from 8.1(1) TO 8.4(5).
   The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.
   The procedure for the ISSU upgrade path is as follows:

Step 1 **ISSU from major release 8.1(1) to another major release 8.2(3).**

Step 2 **ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.**

Step 3 **ISSU from major release 8.2(5) to another major release 8.4(5).**

Step 4 **Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.**

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
   Multiple Major ISSU has been performed on this switch. We recommend doing a
   binary reload instead of upgrading.
Do you want to continue with the installation (y/n)? [n]
```

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

- When you perform ISSU from Cisco NX-OS Release 8.1(1) to Cisco NX-OS Release 8.2(1) or to Cisco NX-OS Release 8.1(2) HSRP VIP is not reachable from the standby device. ARP for VIP shows resolved or complete on the standby Cisco Nexus 7000 device but it is shown as a static entry. When you face this symptom flap the HSRP state from standby to active. You can configure preempt on both the peers and then bump the priority on the HSRP standby so that it takes an active role.
- Before performing ISSU to Cisco NX-OS Release 8.2(1) from earlier releases, with the given bridge domain configurations, make sure NVE interface is brought up (by using the **no shut** command). If the NVE interface is not brought up, bridge domains may not come up after performing ISSU and when you run the **no shut** command. The issue occurs because the NVE interface is in “shut” state with bridge domain configurations during the ISSU. If you perform ISSU to Cisco NX-OS Release 8.2(1) from earlier releases with NVE interface in “no shut” state, upgrade will happen successfully.
- When you configure **ip directed-broadcast <acl-name>** command with the **acl-name** as **hw-assist**, you cannot delete this configuration post ISSU. This is applicable to releases prior to Cisco NX-OS Release 8.2(1).
- The CoPP statistics accumulated before ISSU to Cisco NX-OS Release 8.1(1) are not retained after the ISSU. If you want to retain the CoPP statistics from earlier releases, back it up before you perform the ISSU to Cisco NX-OS Release 8.1(1).
- When you perform ISSU in a set up where the Routing Information Protocol (RIP) has dependency on other protocols for redistribution, you should adjust the RIP timers because RIP does not support stateful restart. Use the **timers basic** *update invalid holddown flush* command in the address-family-mode under the router configuration mode to adjust the timer values.
- **ISSU upgrade from Cisco NX-OS 7.3.x releases to Cisco NX-OS Release 8.0(1) with RISE configuration:**
  - RISE configuration must be removed prior to starting your upgrade to Cisco NX-OS Release 8.0(1). 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) 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) 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 8.2(11) supports the following cold boot support matrix:

Table 20 Supported Cold Boot Matrix in Cisco NX-OS Release 8.2(11)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
8.2(11)	8.2(10)
	8.2(9)
	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(9)D1(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 8.2(10) supports the following cold boot support matrix:

Table 21 Supported Cold Boot Matrix in Cisco NX-OS Release 8.2(10)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
8.2(10)	8.2(9)
	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(9)D1(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 8.2(9) supports the following cold boot support matrix:

Table 22 Supported Cold Boot Matrix in Cisco NX-OS Release 8.2(9)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
8.2(9)	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(9)D1(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 8.2(8) supports the following cold boot support matrix:

Table 23 Supported Cold Boot Matrix in Cisco NX-OS Release 8.2(8)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
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 8.2(7a) supports the following cold boot support matrix:

Table 24 Supported Cold Boot Matrix in Cisco NX-OS Release 8.2(7a)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
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)

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

Cisco NX-OS Release 8.2(6) supports the following cold boot support matrix:

Table 25 Supported Cold Boot Matrix in Cisco NX-OS Release 8.2(6)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
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 8.2(5) supports the following cold boot support matrix:

Table 26 Supported Cold Boot Matrix in Cisco NX-OS Release 8.2(5)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
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 8.2(4) supports the following cold boot support matrix:

Table 27 Supported Cold Boot Matrix in Cisco NX-OS Release 8.2(4)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
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)

Cisco NX-OS Release 8.2(3) supports the following cold boot support matrix:

Table 28 Supported Cold Boot Matrix in Cisco NX-OS Release 8.2(3)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
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)

Cisco NX-OS Release 8.2(2) supports the following cold boot support matrix:

Table 29 Supported Cold Boot Matrix in Cisco NX-OS Release 8.2(2)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
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(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)

Cisco NX-OS Release 8.1(2a) supports the following cold boot support matrix

Table 30 Supported Cold Boot Matrix in Cisco NX-OS Release 8.1(2a)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
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(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)

Cisco NX-OS Release 8.1(2) supports the following cold boot support matrix:

Table 31 Supported Cold Boot Matrix in Cisco NX-OS Release 8.1(2)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
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(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(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)

Cisco NX-OS Release 8.2(1) supports the following cold boot support matrix:

Table 32 Supported Cold Boot Matrix in Cisco NX-OS Release 8.2(1)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
8.2(1)	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(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)

Cisco NX-OS Release 8.1(1) has the following cold boot support matrix:

Table 33 Supported Cold Boot Matrix in Cisco NX-OS Release 8.1(1)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
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(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)

Cisco NX-OS Release 8.0(1) has the following cold boot support matrix:

Table 34 Supported Cold Boot Matrix in Cisco NX-OS Release 8.0(1)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
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(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)
	6.1(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 34 follow these steps:

1. Change the boot variable, as shown here:

   Example for Cisco NX-OS Release 8.2(1)

```
boot kickstart bootflash:/n7000-s2-kickstart.8.2.1.bin sup-1
boot system bootflash:/n7000-s2-dk9.8.2.1.bin sup-1
boot kickstart bootflash:/n7000-s2-kickstart.8.2.1.bin sup-2
boot system bootflash:/n7000-s2-dk9.8.2.1.bin sup-2
```

Example for Cisco NX-OS Release 8.1(1)

```
boot kickstart bootflash:/n7000-s2-kickstart.8.1.1.bin sup-1
boot system bootflash:/n7000-s2-dk9.8.1.1.bin sup-1
boot kickstart bootflash:/n7000-s2-kickstart.8.1.1.bin sup-2
boot system bootflash:/n7000-s2-dk9.8.1.1.bin sup-2
```

Example for Cisco NX-OS Release 8.0(1)

```
boot kickstart bootflash:/n7000-s2-kickstart.8.0.1.bin sup-1
boot system bootflash:/n7000-s2-dk9.8.0.1.bin sup-1
boot kickstart bootflash:/n7000-s2-kickstart.8.0.1.bin sup-2
boot system bootflash:/n7000-s2-dk9.8.0.1.bin sup-2
```

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 Cisco NX-OS Release 8.1(1) 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). 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)/Cisco NX-OS Release 8.1(1). After upgrading to Cisco NX-OS Release 8.0(1)/Cisco NX-OS Release 8.1(1), 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)/Cisco NX-OS Release 8.1(1) 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 8.2(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 8.2(1) includes the following Erasable Programmable Logic Device (EPLD) images:

- n7000-s2-epld.8.2.1.img
- n7700-s2-epld.8.2.1.img

Cisco NX-OS Release 8.1(1) includes the following Erasable Programmable Logic Device (EPLD) images:

- n7000-s2-epld.8.1.1.img
- n7700-s2-epld.8.1.1.img

Cisco NX-OS Release 8.0(1) includes the following Erasable Programmable Logic Device (EPLD) images:

- n7000-s2-epld.8.0.1.img
- n7700-s2-epld.8.0.1.img

Table 35 shows the modules that are supported in Cisco NX-OS Release 8.0(1), Cisco NX-OS Release 8.1(1), and Cisco NX-OS Release 8.2(1) and later releases:

Table 35 Supported Modules with the FPGA

Module	FPGA Type	Version
Cisco Nexus 7000 Supervisor 2	PMFPGA	37.000
	IOFPGA	1.013
Cisco Nexus 7700 Supervisor 2E	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

Module	FPGA Type	Version
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	0.001
10 slot chassis (N77:FAB3-7710)	PMFPGA	0.001
18 slot chassis (N77:FAB3-7718)	PMFPGA	9.008
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
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

Module	FPGA Type	Version
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
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 Hardware

This section briefly describes the new hardware and hardware enhancements introduced in Cisco NX-OS Release 8.2(1), Cisco NX-OS Release 8.1(1) and in Cisco NX-OS Release 8.0(1). For detailed information about the new hardware, see the *Cisco Nexus 7000 Series Hardware Installation and Reference Guide*.

Cisco NX-OS Release 8.2(1)

Cisco Nexus Fabric Extender Modules

From Cisco NX-OS Release 8.2(1), the Cisco Nexus B22 Fabric Extender (N2K-B22DELL-P) and the Cisco Nexus Fabric Extender, N2k-C2348TQ-E are supported on the F3 Series and M3 Series I/O modules.

Cisco NX-OS Release 8.1(1)

New Fan Tray for N7700

The 38mm fans do not meet NEBS compliance when the Cisco Nexus 7700 12-port 100-Gigabit Ethernet I/O Module (N77-M312CQ-26L) is used in a Nexus 7700 6-slot, 10-slot, or 18-slot chassis. The new 76mm fans are required to meet NEBS compliance when the M3 12-port 100 Gigabit I/O Module (N77-M312CQ-26L) is used in a Nexus 7700 6-slot, 10-slot, or 18-slot chassis.

- Cisco Nexus 7706 Fan (PID: N77-C7706-FAN-2)
- Cisco Nexus 7710 Fan (PID: N77-C7710-FAN-2)
- Cisco Nexus 7718 Fan (PID: N77-C7718-FAN-2)

N7004 Support for M3 modules

Starting from Cisco NX-OS Release 8.1(1), the following M3-Series I/O modules are supported on the Cisco Nexus 7004 switch:

- 48-port 1-/10-Gigabit Ethernet SFP+ I/O module (N7K-M348XP-25L)
- 24-port 40-Gigabit Ethernet QSFP+ I/O module (N7K-M324FQ-25L)

Cisco NX-OS Release 8.0(1)

The following modules are supported in Cisco NX-OS Release 8.0(1):

- Cisco Nexus 7000 series supports M2XL, F2E, F3, and M3 modules.
- Cisco Nexus 7700 series supports F2E, F3, and M3 modules.

The following M3-Series I/O modules have been introduced:

- M3-Series 12-Port 100-Gigabit Ethernet (N77-M312CQ-26L)
- M3-Series 48-Port 1-/10-Gigabit Ethernet (N7K-M348XP-25L)
- M3-Series 24-Port 10-/40-Gigabit Ethernet (N7K-M324FQ-25L)

PSM4 Support on 100G M3

The QSFP-100G-PSM4-S transceiver is supported with the M3-Series 12-Port 100-Gigabit Ethernet (N77-M312-CQ-26L) I/O module.

Breakout Cable for M3-Series 40-Gigabit Ethernet I/O modules

Starting with Cisco NX-OS Release 8.0(1), the QSFP-4X10G-AOC transceiver with the 40GBASE-AOC QSFP+ to four SFP+ breakout cable type is supported on the M3-Series 24-Port 10-/40-Gigabit Ethernet I/O modules.

M3 Laser on Support

Starting with Cisco NX-OS Release 8.0(1), Laser-On support is available on the M3-Series modules.

New and Enhanced Software Features

This section includes the following topics:

Cisco NX-OS Release 8.2(8) Software Features

Secure Erase

The Secure Erase feature is introduced to erase all customer information for Nexus 7000 series switches from Cisco NX-OS Release 8.2(8).

From this release, you can use factory reset command to erase customer information.

Secure Erase is an operation to remove all the identifiable customer information on Cisco NX-OS devices in conditions of product removal due to Return Merchandise Authorization (RMA), or upgrade or replacement, or system end-of-life.

Cisco NX-OS Release 8.2(6) Software Features

CoPP Enhancements

A CoPP class to match all uRPF exception packets and police them as per the policy is introduced from Cisco NX-OS Release 8.2(6).

Bloom Filter for Glean Adjacency

Bloom Filter Support for Glean Adjacencies is also supported in Cisco NX-OS Release 8.2(6). 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.

Cisco NX-OS Release 8.2(4) Software Features

IPv6 Static Route

Starting from Cisco NX-OS Release 8.2(4), static IPv6 route with VxLAN route as the next-hop is supported.

Honor Mode Licensing

Starting from Cisco NX-OS Release 8.2(4), Honor Mode Licensing is supported on Cisco Nexus 7000 Series switches. Honor mode licensing allows you to enable or continue using a feature without having a valid license for that feature. In such a scenario, a syslog is generated once every 7 days until you acquire the required license.

LACP Fast Timers Scale Qualification

The number of interfaces validated with LACP Fast Timers in Cisco NX-OS Release 8.2(4) are:

- 250 physical member ports with port-channel in Layer 3 mode.
- 100 physical member ports with port-channel in Layer 2 mode with 1000 RSTP instances active on the system.

Cisco NX-OS Release 8.2(3) Software Features

MACSEC Enhancements

Cisco NX-OS Release 8.2(3) has the following MACSEC enhancements:

- The **should-secure** security policy support is added.
- Pre-shared keys (PSK) are supported on break out interfaces.
- Syslog messages are displayed when the MACSEC session goes up or down.
- MACsec supports the Security entity MIB, IEEE8021-SECY-MIB.
- Unrecoverable Secure Association Key (SAK) is supported.

MAC-Move Enhancements

The following methods/commands are introduced to protect the supervisor from excessive mac move:

- Software throttle: Using **mac address loop-detect flow-control-fe** command.
- Hardware throttle: Using **mac address loop-detect disable-learn-vlan** command.

Ethernet OAM Enhancements

Cisco NX-OS Release 8.2(3) has the following Ethernet OAM enhancements:

- Frame error threshold values can be configured on the Ethernet link to measure the quality of the link.
- The dying-gasp and the discovery-timeout options are supported under the **errdisable recovery cause** command to recover the Ethernet link OAM.

DHCP Enhancement

This enhancement enables you to configure a different interface as the source interface by using the **ip dhcp relay source-interface** *interface-name* command.

Cisco NX-OS Release 8.1(2) Software Features

Cisco NX-OS Release 8.1(2) has the following scale enhancement:

250,000 OSPF LSA is supported only with specific below listed parameters:

Platform	N77-M3
LSA type	Type 5 Type 3
Interface type	SVI
OSPF Neighours	150
Number of Areas	2
Number of VDCs	1
OSPF timers	Default timers
Number of ECMP	2
OSPF type	OSPF v2

Cisco NX-OS Release 8.2(1) Software Features

iCAM Monitoring

From Cisco NX-OS Release 8.2(1), you can configure the Intelligent CAM (iCAM) analytics and machine-learning monitor interval and obtain the following traffic analytics on TCAM entries and resources:

- Current, Historical, and Predictive Analytics for traffic per hardware table entry. For example, per TCAM-entry traffic.
- Current, Historical and Predictive Analytics for hardware table utilization per feature.
- Top/Bottom X% hitters, sorting, filtering, based on traffic.
- Historical analytics provide history of traffic for a past date/time.
- Predictive traffic analytics provides traffic for a future date/time.

iCAM provides the above listed analytics for the following features:

- ACL, QoS, PBR, CoPP, WCCP, VACL, PACL, NAT, and so on about 32 features and combinations of these features.
- Forwarding tables.
- Multicast tables.

GUI for iCAM is available in DCNM as an experimental feature (click on **Monitor** --> **iCAM**).

MKA

MACsec is a standard, which can be set up using Cisco security association (SA) protocol or MACsec Key Agreement (MKA). The SA protocol was used to set up the MACsec standard prior to Cisco NX-OS Release 8.2(1). MACsec can also use the MKA protocol in Cisco NX-OS Release 8.2(1) to exchange session keys and manage encryption keys. MKA is supported only on physical ports and port channels.

MKA supports the following point-to-point use cases:

- Securing Data Center Interconnect (DCI)
- Securing Provider Edge (PE)-to-Customer Edge (CE) links in Multiprotocol Label Switching (MPLS) network
- Securing PE-to-PE using dark fiber
- Securing CE-to-CE using an MPLS or Virtual Private LAN Services (VPLS) network
- MACSec on port channels

Using MKA, you can also secure a CE to multiple CEs using an MPLS or VPLS network, which is a point-to-multi point deployment.

Flexible ACL TCAM Bank Chaining

From Cisco NX-OS Release 8.2(1), the Flexible ACL TCAM Bank Chaining feature is supported on the M2 Series modules.

DHCP Response Redirect

From Cisco NX-OS Release 8.2(1), you can use the **ip dhcp redirect-response** command on the DHCP server-facing interface to redirect the packets to the correct switch. When you enable this command, the relay agent on a border node includes source locater and VNI ID of the client segment as remote ID option in request packets, and relays it to the DHCP server. When the DHCP server sends the OFFER packets, the border node uses the information from the same remote ID option to create a VXLAN header. This header includes the source locater set as the outer destination address and the VNI ID of the client segment. This helps the border node to send the OFFER packet to the correct switch.

Slow Drain Enhancements for FCoE

The congestion drop timeout and pause frame timeout commands are modified for FCoE to align with the commands used in Fibre Channel.

The following commands are modified:

- Congestion drop timeout command has changed from **system default interface congestion timeout** *milliseconds* **mode {core | edge}** to **system timeout fcoe congestion-drop {***milliseconds* **| default} mode {core | edge}**.
- Pause frame timeout command has changed from **system default interface pause timeout** *milliseconds* **mode {core | edge}** to **system timeout fcoe pause-drop {***milliseconds* **| default} mode {core | edge}**.

Connecting Data Center Fabrics with VXLAN BGP EVPN and OTV

This feature enables you to configure VXLAN and OTV on the same device (a single-box solution). The VXLAN and OTV overlays are stitched together in the device, ensuring that the Layer-2 traffic between the tunnels is within the bridge domain.

MPLS L3VPN DCI

VXLAN fabric supports external connectivity. Data centers in different sites can be connected using the Data Center Interconnect (DCI) functionality. In the MPLS hand off scenario, the VXLAN encapped packet is terminated and reoriginated to MPLS.

Configuring ACI WAN Interconnect

ACI WAN Interconnect feature is supported on M3 modules in Cisco NX-OS Release 8.2(1).

PBR support for the VXLAN BGP EVPN Fabric

Policy-based routing (PBR) support is provided for the VXLAN BGP EVPN fabric. PBR allows you to configure a defined policy for IPv4 and IPv6 traffic flows, lessening the reliance on routes derived from the routing protocols. All the packets received on an interface with policy-based routing enabled are passed through enhanced packet filters or route maps. The route maps dictate the policy, determining the destination to forward packets. PBR configurations have to be enabled on relevant ToR or leaf switches, and spine switches in the VXLAN BGP EVPN fabric.

Plug and Play

Network plug and play (PnP) is a software application that runs on a Cisco Nexus 7000 switch. The PnP feature provides a simple, secure, unified, and integrated offering to ease new branch or campus roll-outs, and for provisioning updates to an existing network. This feature provides a unified approach to provision networks that comprise different devices with a near zero-touch deployment experience.

Consistency Checker Enhancements

Consistency checker compares the software state with the hardware state in a module and if there is any inconsistency, it flags the issue immediately. This helps to reduce troubleshooting time at a later period. The consistency checker enables users to perform basic troubleshooting and identify issues before reaching out to support teams for resolution thereby reducing the mean time to resolve issues.

Except for Persistent Storage Service (PSS) consistency checker all other features are supported since Cisco NX-OS Release 8.0(1) and are enhanced in Cisco NX-OS Release 8.2(1). Consistency checker is supported on M3 and F3 modules. Users can execute the **show consistency-checker all** command to perform consistency check for all components/features.

The following consistency checker components are supported in Cisco NX-OS Release 8.2(1):

- FabricPath
- Interface-properties
- Layer 2 Unicast and Multicast Tables
- L3-Interface Tables
- Link-State
- Proxy Forwarding
- Spanning-Tree
- Persistent Storage Service (PSS)

Distributed Packet Tracer

Distributed Packet Tracer (DPT) enables users to find and track specific traffic flow across all network devices from a single-point server or network controller or network management system (NMS).

The DPT framework uses a central controller device (CCD) to communicate with an on-switch software module called On-Switch-DPT. The CCD gets the input from the network administrator to trace a given packet in a network. CCD then communicates this information to each of the switches in the network. The On-Switch-DPT traces the packet and passes the information to CCD.

The CCD then collates all the information from various switches and analyzes them before presenting the result to users.

Configure Replace

The Configure Replace (CR) feature enables a Nexus 7000 Series switch to replace the running configuration with a user provided configuration without reloading. Device reload may be required only when a configuration itself requires a reload. A user provided configuration is running configuration taken from a Cisco NXOS switch. CR replaces the entire running configuration with new configuration provided by a user. In case of failure in CR the original configuration is restored in the switch.

Hardware Forwarding of IP Directed Broadcast Packets

From Cisco NX-OS Release 8.2(1), all Cisco Nexus 7000 Series I/O modules support hardware forwarding of IP-directed broadcast packets. This feature is limited to the virtual device contexts (VDC) on which this feature is applied. You cannot configure both software and hardware forwarding of IP-directed broadcast packets on the same interface.

Layer 3 Routing over vPC

From Cisco NX-OS Release 8.2(1), Layer 3 routing over vPC is supported in the M3 Series I/O modules for IPv6 unicast traffic.

IP TCP Maximum Segment Size

The IP TCP Maximum Segment Size (MSS) feature enables the configuration of a maximum segment size for all TCP connections that originate from or are terminated in a Cisco Nexus 7000 Series switch.

Precision Time Protocol

From Cisco NX-OS Release 8.2(1), Precision Time Protocol (PTP) can be enabled in the M3 Series I/O modules.

Catena

Catena works in transparent, routed, and mixed modes, which means each Catena instance can forward traffic through a mix of Layer 2 and Layer 3 devices. Failover using probing is supported for traffic redirection. Catena solution supports hash-based load balancing across appliances in the transparent mode.

Data flow through these appliances is based on traffic type which is qualified by access control lists. Each Catena service contains many chains of appliances, and each chain of appliance contains many sequences of access-lists based on vlan-group, port-group, and device-group identifiers.

Subscription-based Licensing

From Cisco NX-OS Release 8.2(1), subscription-based licensing is available on Cisco Nexus 7000 Series switches. This enables the user to purchase licenses for any period of time.

From Cisco NX-OS Release 8.2(1), the Intelligent CAM Analytics and Machine-learning (iCAM) feature is available under the ENHANCED_LAYER2_PKG license.

Virtual Private LAN Service

From Cisco NX-OS Release 8.2(1), all Virtual Private LAN Service (VPLS) functionalities, except Ethernet Flow Points, (EFP), service instances and bridge domains, are supported in the M3 Series I/O modules.

Ethernet over Multiprotocol Label Switching

From Cisco NX-OS Release 8.2(1), all Ethernet over Multiprotocol Label Switching (EoMPLS) functionalities, except EFPs, service instances and bridge domains, are supported in the M3 Series I/O modules.

Private VLAN over OTV

From Cisco NX-OS Release 8.2(1), Cisco Nexus 7000 Series switches support Private VLAN (PVLAN) that is extended over the Overlay Transport Virtualization (OTV) overlay. This allows a device to extend Layer 2 VLANs across Layer 3 IP networks. Transmission occurs in a Layer2 frame attached to a Layer 3 header. In an OTV overlay, this feature allows two VLANs to communicate, based on the PVLAN association.

Multicast only Fast Re-Route

From Cisco NX-OS Release 8.2(1), Cisco Nexus 7000 Series switches aim to achieve sub-sec convergence delay for 16K (S, G) running on F3 and M3 Modules, using the Multicast only Fast Re-Route (MoFRR) feature. This feature allows faster programming and improved convergence.

Web Cache Communication Protocol Support

From Cisco NX-OS Release 8.2(1) Web Cache Communication Protocol (WCCP) version 2 feature is supported on bridge domain interfaces (BDIs) as an ingress feature.

Intelligent Traffic Director HTTP Probe

HTTP probes are supported to probe each node periodically to monitor their health.

Multicast VRF Route Leaking

With multicast extranet, the RPF lookup for multicast route in the receiver VRF can be carried out in a source VRF, thereby allowing the return of a valid RPF interface. This forms a source or RP tree from the receiver VRF to the source VRF, thus enabling the traffic originating from the source VRF to be forwarded to the OIFs in the receiver VRF.

IPv6 Support

From Cisco NX-OS Release 8.2(1), you can configure peer-keepalive link using an IPv4 or IPv6 address.

ITD on M3

From Cisco NX-OS Release 8.2(1), Intelligent Traffic Director (ITD) is supported on M3 modules.

M3 support for LISP

From Cisco NX-OS Release 8.2(1), Locator/ID Separation Protocol (LISP) is supported on M3 modules.

ITD VIP Knob for Static Route

From Cisco NX-OS Release 8.2(1), the ITD VIP knob for static route feature allows you to configure a Virtual IP Address (VIP) for ITD device group, with route creation based on the health of a device group node. With a VIP knob, creation and deletion of routes is automatic and is triggered based on the health of the ITD device group.

Cisco NX-OS Release 8.1(1) Software Features

M3 FEX

From Cisco NX-OS Release 8.1(1), M3 Series modules are supported for FEX.

Disjoint Routing Locator (RLOC)

The Disjoint Routing Locator (RLOC) feature facilitates inter-fabric LISP traffic support by ensuring that the LISP mapping system is aware of multiple fabrics. Each fabric is defined by a locator scope that groups a range of RLOC (or fabric underlay) addresses that routers within the fabric are associated with.

L3 Over VPC for M3

From Cisco NX-OS release 8.1(1), routing over vPC for IPv4 unicast traffic is supported on the M3 Series modules.

M3 FabricPath

From Cisco NX-OS Release 8.1(1), FabricPath is supported on the M3 Series modules.

SGT Tagging Exemption for Layer 2 Protocols

From Cisco NX-OS release 8.1(1), you can exempt the Layer 2 (L2) control plane protocols from SGT tagging when interlinking with ports.

This is to ensure that the packets from L2 control protocols are transmitted untagged from Ethernet peers to ports.

Multi-hop BFD Support

The Bidirectional Forwarding Detection (BFD) Multi-hop feature enables detection of IPv4 network failure between paths that are not directly connected. This feature also enables users to configure IPv4 BFD sessions over multi-hop routes.

If a BFD session is up (that is, the next-hop destination is reachable), IPv4 static routes that are associated with IPv4 static BFD configuration are added to a routing table. If the BFD session is down, the routing table removes all associated static routes from the routing table.

BFD notifies BGP when the path goes down. The path to reach the destination (BGP neighbor) is through a static route only (with no IGP support).

The multi-hop BFD feature supports only the static routes in Cisco NX-OS release 8.1(1),

Cisco NX-OS Release 8.0(1) Software Features

VXLAN Fabric

MPLS L3VPN Hand Off Scenario in a VXLAN BGP EVPN Fabric

VXLAN BGP EVPN fabrics with a Cisco Nexus 7000 Series border leaf switch having an M3 module can use the MPLS L3VPN network for WAN connectivity or for Layer-3 Data Center Interconnect.

VXLAN OAM – Ping

The VXLAN OAM – Ping functionality is used to detect errors and path failures for traffic from a leaf/ToR switch VTEP to an attached end host, to another leaf/ToR switch VTEP, or to an end host attached to a VTEP.

VXLAN OAM – Traceroute/Pathtrace

VXLAN OAM – Traceroute/Pathtrace functionality is used for fault isolation in the VXLAN overlay. Traceroute is an ICMP based solution that provides more information regarding the ingress and egress interface paths. The **traceroute** command uses ICMP packets (channel-1) to trace the path the packet traverses in the VXLAN BGP EVPN fabric overlay, and the **pathtrace** command traces the path the packet traverses in the VXLAN overlay using the NVO3 channel (channel-2).

VXLAN OAM – Interface and Error Verification Statistics

This feature provides a provision to view interface and error verification statistics, when the pathtrace function is used.

Pervasive Load Balancing (PLB)

Pervasive Load Balancing (PLB) is a fabric feature that provides Layer-3 and Layer-4 load balancing at terabits speed without the need for any virtual or physical external load balancer equipment. Servers, VMs and containers (specific to a given service) attached to different ToR/leaf switches might be distributed across the fabric and this feature enables the switching fabric to load balance client-specific service requests to these servers.

In this feature, the same virtual IP (VIP) is assigned to the group of servers that might be distributed across the fabric. When different clients (local to the fabric or from a remote location) send requests for a given service, these requests are destined to the VIP of these servers.

In the fabric, ToR/leaf switches matches these clients' IP address bits/mask, the VIP and relevant Layer3/Layer4 fields to load balance these requests among the servers.

VXLAN Support on the M3 Module

VXLAN support on the M3 module is added for the following features:

- IPv4/v6 unicast Layer-3 gateway

- Layer-2 Multicast
- M3 module as the Border Leaf switch
- OTV hand off on the M3 module (two box solution)
- Layer-2 CE hand off

Intelligent CAM Analytics and Machine-learning (iCAM)

Beginning with Cisco NX-OS Release 8.0.1, on the Cisco Nexus 7000/7700 Series Switches the Intelligent CAM Analytics and Machine-learning (iCAM) feature is supported. The iCAM feature enables you to view the traffic analytics per feature, Ternary Content-Addressable Memory (TCAM) resources and entries. Prior to the introduction of iCAM feature, it was difficult to get an overall view of how many TCAM/SRAM resource entries were used/free with various features and how much traffic was flowing through the various subnets/applications.

iCAM can be used to view historical TCAM data. iCAM analyses this historical data using machine learning algorithms to predict TCAM usage and traffic stats at a future date and time.

Catena

This feature helps in chaining of devices so that packets are redirected through multiple devices. These devices can be appliances like firewall, IPS, IDS and Load balancer, and so on. The devices are inserted in the data path in such a way that there are no topological changes, or changes to existing configuration. This feature can support scalability with many number of appliances in the data path.

Data flow through these appliances is based on traffic type which is qualified by access control lists. Each Catena service contains many chains of appliances, and each chain of appliance contains many sequences of access-lists based on **vlan-group** and **port-group** identifiers.

VPNv4 Multipath

The VPN Multipath Support for Inter-AS VPNs feature enables the switch to pick one path as the best path and mark the other legitimate paths between Autonomous System Boundary Routers (ASBRs) as multi path. This feature enables load sharing of traffic among the different multi paths and the best path to reach the destination.

GIR Enhancements

A delay has been added before the after_maintenance snapshot is taken. A visible CLI indicator has been added to display when the system is in the maintenance mode. Support for SNMP traps has been added when the device moves from the maintenance mode to the normal mode and vice-versa through CLI reload, or system reset.

X.509v3 Certificate-Based SSH Authentication

You can configure SSH authentication using X.509v3 certificates (RFC 6187). X.509v3 certificate-based SSH authentication uses certificates combined with a smart card to enable two-factor authentication for Cisco device access.

Flexible ACL TCAM bank chaining feature for M3

M3 Series modules support Flexible ACL TCAM bank chaining feature.

SGACL Policy Enforcement Per Interface

This feature provides support to enable or disable SGACL policy enforcement on L3 interfaces and L3 port-channels.

System Security Monitoring

System security monitoring functionality monitors and provides visibilities to the following system related security technologies:

- XSPACE
- Address Space Layout Randomization (ASLR)
- Object Size Checking (OSC)
- SafeC

Integrity Measurement Architecture (IMA)/Runtime Integrity

The Integrity Measurement Architecture (IMA)/Runtime Integrity feature provides assurance about authenticity of Cisco NX-OS system and its components. This feature ensures that the system has not been exposed to tampered code by measuring the Cisco NX-OS system and its components. You can verify authenticity by comparing the measured value against a known standard value.

IPv6 First-Hop Security Features

IPv6 RA Guard

The IPv6 RA Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue router advertisement (RA) guard messages that arrive at the network device platform.

DHCPv6 Guard

The DHCPv6 Guard feature blocks reply and advertisement messages that come from unauthorized DHCP servers and relay agents.

IPv6 Snooping

The IPv6 Snooping feature bundles several Layer 2 IPv6 first-hop security features, including IPv6 neighbor discovery inspection, IPv6 device tracking, IPv6 address glean, and IPv6 binding table recovery, to provide security and scalability. IPv6 ND inspection operates at Layer 2, or between Layer 2 and Layer 3, to provide IPv6 functions with security and scalability.

SXPv4

Cisco TrustSec SXP version 4 (SXPv4) enhances the functionality of SXP by adding a loop detection and prevention mechanism to prevent stale binding in the network. In addition, Cisco TrustSec with SXPv4 supports SGT inline tagging, which allows propagation of SGT embedded in clear-text (unencrypted) Ethernet packets.

SGACL Egress Policy Overwrite

The SGACLs downloaded by using Integrated Services Engine (ISE) and configured by using CLI can co-exist. You can prioritize whether to use SGACLs downloaded from ISE or configured SGACLs by using CLI. By default, the SGACLs configured by using CLI have higher priority in Cisco NX-OS.

Smart Licensing

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure – you control what users can access. With Smart Licensing you get:

- **Easy Activation**: Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- **Unified Management**: My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- **License Flexibility**: Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central (software.cisco.com).

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

vPC enhancements for Hitless vPC role change

The vPC hitless role change feature provides a framework to switch vPC roles between vPC peers without impacting traffic flows. The vPC role swapping is done based on the role priority value of the device under the vPC domain. A vPC peer device with lower role priority is selected as the primary vPC device when the **vpc role preempt** command is executed.

BGP PIC Edge for IPv6

The BGP PIC Edge feature creates and stores a backup path in the routing information base (RIB) and forwarding information base (FIB) so that when a failure on an eBGP link to SP is detected (the primary path fails), the backup path can immediately take over, enabling fast fail over in the forwarding plane. BGP PIC Edge feature supports both IPv4 and IPv6 address families.

BGP Enhancements

Modified the soft-reconfiguration inbound command, which was used to configure a soft reconfiguration for inbound policy changes. The modified command is soft-reconfiguration inbound always. The always option was added in this release and must be used for complete soft-reconfiguration inbound functionality.

Show Tech Binary Support

Binary tech support is a log-collecting framework that collects logs internally from all Cisco NX-OS processes that are running on the device. Enter the **show tech-support all binary <uri>** command to collect logs from across the entire device, including virtual device contexts (VDCs), and modules. Binary tech support can either be parsed within the device or moved to an external log server where it can be parsed off line. If a module fails during the log collection, binary tech support continues to collect logs from all remaining modules and VDCs.

MTS Serviceability

The message and transaction service (MTS) is a high-performance interprocess communications (IPC) message broker that specializes in high-availability semantics. MTS handles message routing and queuing between services on and across modules and between supervisors. MTS facilitates the exchange of messages such as event notification, synchronization, and message persistency between system services and system components. MTS can maintain persistent messages and logged messages in queues for access even after a service restart.

MTS provides extensive serviceability features. For instance, MTS provides notifications to inform an application when its queue has reached a predefined limitation. Corresponding to each notification, a default callback action is defined in MTS. From Cisco NX-OS Release 8.0(1), the System Message Logging contains new logs that indicates the highest MTS memory users. These logs are set to severity level 4. In addition, detailed memory usage stats with timestamps are collected per application. You can use the command **show sys int mts sup sap APP_SAP_NUM queue_stats** to collect the technical support, if an application contains an issue.

IPSLA IPv6

IPv6 support has been added for the ICMP Echo operations.

Link OAM

Link OAM is supported only on F2+M3 modules. This feature allows service providers to monitor and troubleshoot a single physical point-to-point Ethernet link. Service providers can monitor specific events, take actions on events, and troubleshoot. Ethernet link OAM operates on a single, physical link and it can be configured to monitor either side or both sides of that link.

Consistency Checker

Consistency checker is a tool that checks for system consistency, helps in root cause analysis and fault isolation, checks for software versus hardware programming, and includes on demand trigger through CLI.

Fault Management (Trigger Based Auto Capture of Logs and MTS Statistics Collection)

The Fault-Management System is used to enhance the Cisco NX-OS serviceability by providing an efficient means to capture data relevant and adequate to debug issues being reported at the earliest possible time, without any manual intervention.

EtherChannel Symmetric Hash for Ipv6

This feature enables fair distribution of traffic across all members of a port channel. This feature is applicable to Cisco Nexus 7000 48-Port 1 and 10 Gigabit Ethernet F2-Series Modules and Cisco Nexus 7000 Enhanced F2-Series 48-Port Fiber 1 and 10 Gigabit Ethernet Modules only.

Enhancements to NX-API

Cisco NX-API allows HTTP-based programmatic access to the Cisco Nexus platform. NX-API extends the capability of running CLIs for configuration management using HTTP/HTTPS. NX-API embeds the commands into the body of XML, JSON or JSONRPC requests and executes them by spawning VSH sessions.

The following enhancements have been made to NX-API:

- Configuration Validation—Allows you to validate the commands before applying them on the switch. This feature will enable you to verify the consistency of a configuration.
  - Validate-Only—Validates the configuration only; will not set the configuration.
  - Validate-and-Set—Validates the configuration, if successful it applies the configuration on the switch.
- Configuration Lock—Allows you to set an exclusive lock on the configuration; no other management or programming agent will be able to modify the configuration if this lock is held.
- Checkpoint-Rollback—In case a CLI from a batch of configuration performed through NX-API fails, you can ask for stop-on-error, continue-on-error or rollback-on-error while configuring.
  - Stop-on-error—Stops on the first CLI that fails.
  - Continue-on-error—Ignores and continues with other CLIs.
  - Rollback-on-error—Rolls back to the previous state the system had before executing the commands
- Command Live Reference—Displays the schema (i.e. the description of the keywords) for the CLIs on NX-API Web Interface.
- Generation of Java and JavaScript—Generates the Java code/JavaScript for each of the request posted through the sandbox.

OTV Loopback Join Interface

The OTV Loopback Join Interface feature allows the overlay to use a loopback interface as the Join Interface. This feature adds multicast based OTV control plane into the multicast core by using a loopback as join interface. This also allows to have multiple physical uplinks into the provider multicast core. This feature has the following enhancements:

- The existing **otv join-interface** configuration is expanded to allow for **loopback x** under overlay mode.
- This feature is supported on M1, M2, M3, and F3 modules.

- This feature is supported on OTV GRE encapsulation (OTV 1.0) and UDP encapsulation (OTV 2.5).
- This feature supports multiple overlays on the same Loopback Interface (Multicast-based OTV control-plane only).

The OTV Loopback Join Interface feature has the following limitations:

- There is no physical interface support as a join-interface when using Multicast-based OTV control-plane.
- A OTV edge-device can not mix loopback and physical join-interface.
- Adjacency server configuration is not supported with the loopback join-interface.
- Only PIM ASM is supported for OTV Control-Group when using the Loopback Join Interface.
- Only PIM SMM is supported for OTV Control-Group when using the Loopback Join Interface.
- Bidirectional PIM is NOT supported when using the Loopback Join Interface.
- IP address of the loopback join-interface can not be set to the same IP as the AnyCast-Rp IP address.

ITD Enhancements

- The **fail action bucket distribute** and **fail action mode least-bucket** commands have been introduced to specify how traffic is reassigned after a node failure.
- Added optimized addition or deletion of ACEs in include or exclude ACLs.

Scale Enhancements

MPLS Inter AS option B

- Cisco NX-OS Release 7.3(0)DX(1) and 7.3(1)D1(1) have support for Inter AS option B on M3 modules with 150,000 labels.
- When M2 and M3 are used in the same VDC, the supported scale in the VDC is 150,000.
- From Cisco NX-OS Release 8.0(1) onwards up to 500,000 routing entries are supported on the M3 modules for Inter AS Option B.
- Number of VRFs for hand off (MP-BGP) in a M3 module is 4000.

HSRP Multiple Group Optimization (MGO)

- On Cisco Nexus 7000 Series Switches with M3 modules, you can scale HSRP Multiple Group Optimization (MGO) up to 8000 HSRP groups.

Note: You must create a custom control plane policing (CoPP) policy to change the Committed Information Rate (CIR) to allow more control plane packets.

Change the **u6route-mem** command value for VDC from 64 to the default value of 24.

Refer to Cisco Nexus 7000 Series NX-OS Verified Scalability Guide for other Cisco NX-OS Release 8.0(1) scale enhancements.

MIBs

No new MIBs are added for Cisco NXOS Release 8.0(1) and for Cisco NXOS Release 8.1(1).

Licensing

Smart Licensing feature is introduced in Cisco NX-OS Release 8.0(1).

Refer to the “Smart Licensing Chapter” in the *Cisco NX-OS Licensing Guide.* for more details on the Smart Licensing feature.

For details on licensing information for earlier releases, see the “Licensing Cisco NX-OS Software Features” chapter in the *Cisco NX-OS Licensing Guide.*

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

Caveats

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

- Open Caveats—Cisco NX-OS Release 8.2(7a)
- Open Caveats—Cisco NX-OS Release 8.2(5)
- Open Caveats—Cisco NX-OS Release 8.2(4)
- Open Caveats—Cisco NX-OS Release 8.2(3)
- Open Caveats—Cisco NX-OS Release 8.2(2)
- Open Caveats—Cisco NX-OS Release 8.1(2)
- Open Caveats—Cisco NX-OS Release 8.2(1)
- Open Caveats—Cisco NX-OS Release 8.1(1)
- Open Caveats—Cisco NX-OS Release 8.0(1)
- Resolved Caveats-Cisco NX-OS Release 8.2(11)
- Resolved Caveats-Cisco NX-OS Release 8.2(10)
- Resolved Caveats—Cisco NX-OS Release 8.2(8)
- Resolved Caveats—Cisco NX-OS Release 8.2(7a)
- Resolved Caveats—Cisco NX-OS Release 8.2(6)
- Resolved Caveats—Cisco NX-OS Release 8.2(5)
- Resolved Caveats—Cisco NX-OS Release 8.2(4)
- Resolved Caveats—Cisco NX-OS Release 8.2(3)
- Resolved Caveats—Cisco NX-OS Release 8.2(2)
- Resolved Caveats—Cisco NX-OS Release 8.1(2a)
- Resolved Caveats—Cisco NX-OS Release 8.1(2)
- Resolved Caveats—Cisco NX-OS Release 8.2(1)
- Resolved Caveats—Cisco NX-OS Release 8.1(1)
- Resolved Caveats—Cisco NX-OS Release 8.0(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 8.2(7a)

Table 36 Cisco NX-OS Release 8.2(7a) Open Caveats

Caveat ID Number	Description
CSCvo90653	Graceful SPT switch-over
CSCvu90705	ISIS IPv6 routes are shown as pending ((nil), 0) for MT-IPV6-UNICAST topology
CSCvw71912	Improper error message printing causing RPM crash
CSCvx93145	Topology information is not propagated from ISIS to MPLS TE when authentication configured for ISIS

Open Caveats—Cisco NX-OS Release 8.2(5)

Table 37 Cisco NX-OS Release 8.2(5) Open Caveats

Caveat ID Number	Description
CSCvn34448	ITD stops responding after servers are shutdown
CSCvr12121	Policy-map applied using port-profile loses bandwidth configuration during downgrade.
CSCvr53184	Deletion logic for static mac added for fixing CSCvr09812 issue.

Open Caveats—Cisco NX-OS Release 8.2(4)

Table 38 Cisco NX-OS Release 8.2(4) Open Caveats

Identifier	Description
CSCvp70746	n7k/F2: EEM to ignore interrupt during EG recovery
CSCvn31805	MDS: CLI error through curl post "found ns syscli and copied it to blob syscli len 6"

Open Caveats—Cisco NX-OS Release 8.2(3)

Table 39 Cisco NX-OS Release 8.2(3) Open Caveats

Identifier	Description
CSCvo58120	Assigning same vpc id to a different port-channel is reflecting on the secondary in vpc config sync

Open Caveats—Cisco NX-OS Release 8.2(2)

Table 40 Cisco NX-OS Release 8.2(2) Open Caveats

Identifier	Description
CSCvi76590	Hitting cts_core at dl_iterate_phdr () from /lib/libc.so
CSCvb67954	EVPN to LISP hand off on Nexus7K does not work in NX-OS 7.3
CSCvi27159	S-N LISP traffic from ACI POD to remote WAN router is dropped on M3 GOLF module
CSCvi56044	IPFIB cores with BGP shut/no shut after ISSU from NX-OS 7.3.2 to NX-OS 8.2.2

Open Caveats—Cisco NX-OS Release 8.1(2)

Table 41 Cisco NX-OS Release 8.1(2) Open Caveats

Identifier	Description
CSCvh62554	HSRP VIP is not reachable from Standby after ISSU between 8.x releases

Open Caveats—Cisco NX-OS Release 8.2(1)

Table 42 Cisco NX-OS Release 8.2(1) Open Caveats

Identifier	Description
CSCvf85676	XML validation failed for DRAP commands on BH
CSCvf86735	xml validation failing for OAM show event-log commands
CSCvf81432	Schema validity error for 'show monitor session all' command
CSCvg07184	iCAM : icam prediction resource acl_tcam not working when enabled on multiple modules
CSCvf87719	peer-local and peer-vdc commands not being nvgen
CSCvf81406	DLC status is missing in xml schema for "show license status"
CSCvf81421	schema validation error for licensing clis
CSCvf66631	LC Reload on Bidir ends with Extra packets
CSCvg05917	N77/vPC/MFDM: 2-3 secs mcast drop 10 secs after “vpc role preempt”
CSCvf62853	aclqos crash on F3 and M3
CSCvf86826	show otv isis commands throwing an error for validate-xml
CSCvf99101	feature poap operation failed on response timeout from service which leads to delay in POAP abort
CSCvf72890	ASCII-CFG-2-ACFG_OPER_FAIL: Ascii config/replay operation failed because of Could not attach to clis

Table 42 Cisco NX-OS Release 8.2(1) Open Caveats

Identifier	Description
CSCvf85559	FP-ISIS validate-xml throwing an error for most of the option “Show fabricpath isis”
CSCvf86400	kill lisp results in traffic loss
CSCvf84382	LISP cores at lisp_rt_send during de-configuration
CSCvf84373	LISP: lisp cores on cleaning up
CSCvf93507	nve oif removed after sso from S,G entry
CSCvg01021	VxLAN OTV: *,G has NULL OIF at the Leaf
CSCvf75002	Dont refresh type-5 LSA for which route is not present in RIB
CSCvf68532	ospf core at OSPF_IPC_MTS_THREAD post multiple process restarts
CSCvf28281	OSPFv2 area summarization does not happen after config-replace
CSCvf61367	SYSTEM UI:%URIB-3-NO_L3VM_INFO_ERROR message from sal client
CSCvf85079	banner motd" cmd stucks if it has message length more than 256.
CSCvf67914	KERN-2-SYSTEM_MSG: klm_sprom: sys_srv_register_multiple FAILED (rc=-1)
CSCvg06181	Delayed VPC SVI bringup upon reload or MCT flap in scale environment (900+ SVIs)
CSCvf85702	xml validation failed for some u2rib commands
CSCvf81873	killing netstack process deleting nve peers
CSCvf89452	Vxlan Fnl UI, traffic loss after completion of ISSU from 7.3.1 to 8.2(.23)
CSCvg09282	M3: Some layer2 tunneled multicast traffic getting mis-forwarded under scaled condition
CSCvf72413	SDA::DHCP Server (shared across SDA and traditional) & Traditional DHCP shouldn't be in same instance
CSCvg13589	source background script exits if its parent session is closed causing VOAP to fail
CSCvf81747	M3: QSA (40G to 10G):SFP checksum error on inserting 40G-SR after CVR-QSFP-SFP10G.
CSCwa05551	N7700: RISE feature not available in 8.2(x)

Open Caveats—Cisco NX-OS Release 8.1(1)

Table 43 Cisco NX-OS Release 8.1(1) Open Caveats

Identifier	Description
CSCvc72202	CVR-QSFP-SFP10G goes down after the F3 module reload
CSCve98530	SYSTEM UI: xbar core during ISSU from 732 to 811
CSCve98991	Packet drop during ISSU from release 7.3(x) release to 8.1(1)
CSCve18373	"show accounting log last-index " returns the incorrect value

Table 43 Cisco NX-OS Release 8.1(1) Open Caveats

Identifier	Description
CSCve18413	"show accounting log start-seqnum <seq num>" seems to be broken in 8.1(1)
CSCve06320	Netflow - msg stuck in MTS Buffer after ISSU
CSCve13677	N7K: M3 module crash in ncpinfraclnt service on IPv6 FIB update
CSCve07736	N7K Fabricpath - MAC address not re learnt on GARP
CSCvd48720	FCoE-ST: Tail drop seen on 10G F2E N77 FPC with 2348UPQ
CSCve16857	OSPF will change its router-id live without the process restarting in 7.3(1)D1(1)
CSCve19058	HMM does not restore hosts on cold boot from 7.2.2 to 8.1.1
CSCve15020	HMM SOO mode was not set right
CSCvc66384	MHBFD-ES: MH BFD sessions remain down on m2-m3 vdc if the sessions on hosted on m3 lc
CSCvd41537	N7K - SNMP ciscoSwitchStatsMIB not populated
CSCve03125	Seeing duplicate packets after converting from vpc to vpc+
CSCvd81058	N77/PIM: Mcast duplication for local groups upon restoring peer-link
CSCve15198	multicast traffic failing after remove/add feature lisp
CSCve13327	MVPN Mcast block-hole after Core router reload (ASR9K)
CSCvd94102	Add of F3 as a SITE facing i/f triggers broadcast/Selective flood mac traffic drop
CSCvd52055	N77/MVPN: Mcast duplication upon P SSO
CSCvc91124	Issue with post migration of peer-link from M1 to M2
CSCvc50850	On a full scale EIGRP setup, nbrs flap with hold timer expiry
CSCvd98154	ACL is removed from SVI but remains programmed
CSCvc03136	BGP PIC convergence delays when a large number of interfaces are brought down
CSCve01811	vpc-config-sync fails with error message
CSCve05847	VRRPv3 crash in looped topology
CSCvd97431	stats not shown for violate class when run with per-inst option
CSCve22833	Increase memory usage running EEM+Python script and hang those with high CPU usage after a few days.
CSCve02818	All multicast traffic dropped after vdc suspend/switchover/vdc resume.

Open Caveats—Cisco NX-OS Release 8.0(1)

Table 44 Cisco NX-OS Release 8.0(1) Open Caveats

Identifier	Description
CSCvc72202	CVR-QSFP-SFP10G goes down after the F3 module reload
CSCvc34234	Large delay in getting new TLVs after ISSU in vPC causing BDs to go down.
CSCvc59235	ARP Request packet reaching via VXLAN tunnel on a VPC leg is not being forwarded to the VPC leg.

Table 44 Cisco NX-OS Release 8.0(1) Open Caveats

Identifier	Description
CSCvb86018	ACL: netflow PACL mac classify combo , traffic drop observed
CSCvc56810	Observing EPLD upgrade failed on N7718 Chassis during installation of FANs.
CSCvb93439	Host key verification failed,
CSCva65433	L2 FP BFD sessions not coming on M3 LC
CSCtx63124	bfd core in bfd_disc_node_comp_func
CSCvc34248	Memory leak in RTD monitor when getting ASLR info
CSCvc25628	Error after cold boot from 7.3.0.Dx to .8.0.
CSCvc37897	Per-if SGACL bypass feature does not work with Any-Any DENY rbacl
CSCvc32868	Switch not coming up with fabricpath license after licensing mode switch
CSCvb30907	static-host encap value displayed zero
CSCvc41428	icam does not account 2 entries for ipv6 for F3 and M3 modules
CSCvc13112	l2vpn traffic drop for EFP interfaces post ISSU from 730DX -> 8.0.0.26.S3
CSCvc42877	MPLS Scale testbed ISSU from 8.0.0.71.bin.S4 to upgrade of a module failed
CSCvb95831	Loopback OTV Overlay: OTV ISIS Adj flap on switchover
CSCvb66956	ipv6 mroute oif shows ? instead of interface
CSCvb52410	OTV loopback ASM to BiDir mode change causes Flood traffic loop
CSCvc38109	startup route for SG on reloading module
CSCvc23468	Evaluation of N9k/N7k/N5k/N3k/MDS for NTP November 2016
CSCvc43192	"show tech-support services" unavailable in RISE only VDC
CSCvc32767	xbar_client process restart and switchover results in sup to lc traffic drop
CSCvc25599	F3: port_client Crash
CSCvc49851	MST instance configurations delayd to get synced or failed
CSCvc29233	validate-xml of sh ipv6 snoop policy and counters fail with some special sub-options set
CSCvc28523	Configuration update aborted with invalid ip address configured
CSCvc42685	M3-F3 SGT (CMD Tag) Exemption For L2 Control Protocol

Resolved Caveats-Cisco NX-OS Release 8.2(11)

Table 45 Cisco NX-OS Release 8.2(11) Resolved Caveats

Identifier	Description
CSCvy03206	SYSMGR-2-SERVICE_CRASHED: Service “snmpd”
CSCwf38091	EIGRP distribution-list out allows route that should be denied after SSO
CSCwf44325	CLI function returns cmd_exec_error when collecting show commands via python
CSCwf57099	Device crash with backup VDC failing after reload
CSCwf66528	Nexus 7000/NXOS: corrupted logflash might prevent system to boot
CSCwf98986	Nexus 7000 - mfdm crashes - Memory leak
CSCwh40306	Nexus 7000/M3: incorrect index allocated to fwd adjacency can cause packet drop
CSCwh59416	MFDM crashes while modifying virtual interfaces
CSCwh83075	Nexus 7000 - DHCPv6 Relay Breaks When RAguard Is Attached To VLAN
CSCwi25484	Layer 3 sub-interface MTU is not configured properly in ELTM

Resolved Caveats-Cisco NX-OS Release 8.2(10)

Table 46 Cisco NX-OS Release 8.2(10) Resolved Caveats

Identifier	Description
CSCwe36235	PTP Mgmt packet loop when enable ptp on vpc PL with parallel link.
CSCwe29418	Multiple ipv4 BFD redirect ACL for Vlan
CSCwe94284	OSPF Process is increasing memory utilization
CSCwe10965	N7k TACACS authentication with type6 encryption fails after VDC reload
CSCwd17629	Nexus 7K M3 card reloads with log message SLF_VOQ_CPM_MSTR_INT_ADDRNE_ERR
CSCwd68297	SNMPd Crashes when Configuring 'event snmp-notification' EEM Script
CSCwf08346	BGP traceback when update received with both connector and extended community (VRI) attributes
CSCwb60501	Nexus routing unicast packets destined to broadcast link layer address
CSCwd42069	Native vlan exclude control removed after ISSU or cold boot
CSCwe02602	PIM-Process Crash
CSCwe23797	Unexpected reload on N7702 due to %SYSMGR-2-SERVICE_CRASHED: Service “port-profile”
CSCwd78377	Bfd flap on the SVIs after the vlans are allowed on a shutdown port.
CSCwd01610	BGP AS not updated properly in Netflow flow cache
CSCwe42567	Unexpected reload vsh(non-sysmgr) crashed
CSCwd03083	Nexus 7k HAP reset due to ipqosmgr
CSCwe91401	EEM cannot disable commands on standby supervisor

Table 46 Cisco NX-OS Release 8.2(10) Resolved Caveats

CSCwd92273	N7K receiving periodical SNMP request may cause Macsec MKA peer loss
CSCwd18009	Cisco NX-OS Software CLI Command Injection Vulnerability
CSCwa95363	LIF programmed to a random value for L3 VPN prefixes, after ECMP ports/port-channels are flapped
CSCvq43264	Command ipv6 nd ra dns search-list doesn't allow '-'
CSCwb83100	Unexpected "vlan-mgr" service crash
CSCwd72862	N77K SUP2E unable to configure ip multicast multipath s-g-hash next-hop-based
CSCwe09300	Internal BGP routes are getting installed as External routes with an AD of 20 in the Routing Table
CSCwe30600	Nexus 7K - Unable to configure track under VRRP
CSCwd82039	Unexpected Supervisor failover due to sys-mgr process crash in NXOS

Resolved Caveats—Cisco NX-OS Release 8.2(9)

Table 47 Cisco NX-OS Release 8.2(9) Resolved Caveats

Identifier	Description
CSCvz76633	Nexus7009 F2 Module May Crash While Applying Ip Flow Monitor With Sampler
CSCwa98080	SSH source-ip option does not work on N7K
CSCwb46172	N3K/N7K/N9K ARP statistics do not increment counter for ip proxy-arp and received arp requests.
CSCwc96529	Nexus 7000 series generates syslog recurringly after upgrade to 8.4(6)
CSCwb65019	BGP crashes due to heartbeat failure if route-target imports in one vrf exceed supported scale of 1K
CSCwa70954	VDC on Nexus 7k crashes due to HAP Reset when clearing the configuration
CSCvz66984	Need to log debugging info when parition has unexpectedly high usage
CSCwa04023	Nexus // IPv4 /32 host route not in target VRF with route leaking
CSCwa64058	%NTP-6-NTP_SYSLOG_WARN: : Failed to send MTS message to destination every 90 secs
CSCwa42217	URIB/FIB inconsistency for host route when we shut the attached subnet and SGT exists
CSCwa76446	Local-pt missing entries for direct routes under certain Conditions
CSCwa43114	"nfp" and "aclqos" crash
CSCwb14542	Unexpected HSRP MAC refresh interval
CSCwa43223	SNMP MIB CISCO-EIGRP-MIB table cEigrpInterfaceTable does not return the correct ifIndex
CSCwa35108	stale nexthop entry stuck in route table if VRF leaking
CSCwa76922	MAC acl used as port acl does not take effect even if the hardware programming is correct
CSCwa34646	Nexus OSPF process crash in N5k
CSCvz38944	N9k DHCPv6 Relay breaks after IPv6 snooping is removed
CSCwa55731	EEM starting from Track object is working in duplicate.
CSCvq74899	CLI history should not show registration idtoken
CSCwc09671	SSH login might be failed on some VDCs because of connection refused after switchover
CSCwc14617	SNMP Query for ARP/IPv6 ND results in missing entries
CSCwa67594	Scheduler slow leak under libaaa.so in N7K
CSCvx94820	OSPF memory leak causes OSPF process to crash
CSCwc77419	N7K: BD configuration lost when reload ascii or downgrade
CSCwa01435	MPLS traffic engineering tunnels not coming up
CSCwb78133	SNMP Process crash and core seen on a N7k
CSCvv82637	Longevity: ipqosmgr core on a N3K-C34200YC running 9.3(4) CCO for ~130 days
CSCvy13677	No persistent logs when switchover fails with 'Switchover timeout: [0x0/0x0] Service not found'

Table 47 Cisco NX-OS Release 8.2(9) Resolved Caveats

Identifier	Description
CSCwc55730	PIM-Process Crash
CSCvw34566	NXOS rfc1583compatibility not consistent with IOS/XE implementation
CSCvu57001	Doesn't start new line of show file md5 when using ter len 0
CSCvy32777	Not enough information logged when process killed by signal 9
CSCvz25893	Remove "LBD_300_TCAM_PAR_ERR " as fatal interrupt
CSCwa69483	drops of ingress OTV GRE traffic after adding member link to OTV Join PC
CSCvh60039	N77-M348XP-23L - IFE_ACC_STATS_UNCORR_ERR continuously increase
CSCwa41729	N7k- generates syslog recurringly ->%USER-3-SYSTEM_MSG: user delete failed for userid:userdel:
CSCwc08109	N7k :: OSPFv3 packets with specific IPv6 flow labels dropped.
CSCwa61442	N7K: OSPF Process Crash due to Heartbeat Failure
CSCwa35709	Nexus 7k: PBR on a BDI interface does not work and is ignored.
CSCwa15348	N77K: Sup2E / Sup3E logflash diagnostic tests needs updating
CSCwc52051	BGP neighbor is down after Upgrade to version 8.2(7a) due to No AF configured for peer
CSCvy32406	Unnecessary TCP 'Ack' messages logged to kernel log
CSCwa09450	SNMP memory allocation failure leads to a crash
CSCwb53392	N7K fan speed below minimum
CSCwa64965	Ethertype 0xF000 seen in packet capture when using ACL Capture type SPAN
CSCwb47981	NVE peer stuck in "peer-init" after adjacency flap
CSCvz38543	N9k Type-7 to Type-5 LSA translation is not happening when Link-ID is in host IP range
CSCwc30665	IGMPv3 Leave from one receiver affects receivers on other ports briefly
CSCwc08583	vpc "peer is alive for" counter does not increase
CSCwb95798	Fabricpath vlan learning mode mismatch between L2FM and MTM
CSCwa90942	%LIBDCDI-2-DCDI_ERR: DATACORRUPTION-DATAINCONSISTENCY when printing action-log for a system policy

Resolved Caveats—Cisco NX-OS Release 8.2(8)

Table 48 Cisco NX-OS Release 8.2(8) Resolved Caveats

Identifier	Description
CSCvo90653	Graceful SPT switch-over
CSCvo91184	I:474:VPNV4/EVPN handoff path is invalid(invalid vni), no labeled nexthop
CSCvp33690	Add support for sh bgp l2vpn evpn <vrf name> for evpn
CSCvr05966	Race in Flanker/MTM/L2FM can lead to learning gateway mac out local interface while SVI Up
CSCvr09812	F3 can learn its own GMAC from IPv6 ingress SMAC if v6 not configured
CSCvs90151	Multiple Vulnerabilities in ntp
CSCvv51221	aclqos crash while modifying ACL
CSCvw71912	Improper error message printing causing RPM crash
CSCvx67356	Post ISSU/reload Service "snmpd" (PID xxxx) hasn't caught signal 11 (core will be saved)
CSCvx71883	Feature 'spt-switch-graceful' not working as expected.
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.
CSCvx87204	ICMP Packet Too Big not sent by N7K MPLS P-router
CSCvx91633	show logging commands result in not enough memory
CSCvx93145	Topology information is not propagated from ISIS to MPLS TE when authentication configured for ISIS
CSCvy04296	Nexus7710 M3 Linecard crash in IPFIB process
CSCvy04379	When configuring RACL on SVI with L2VPN/Psuedowire getting cryptic error message
CSCvy13677	No persistent logs when switchover fails with 'Switchover timeout: [0x0/0x0] Service not found'
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
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
CSCvz00628	Servicability: Add "show tech-support stp" to "show tech-support details"
CSCvz01927	N7K ARP process crash
CSCvz03090	M3 module reloading due to fatal interrupt BEM_EL3_CTL_INVLD [SLF_BIB_INT_BEM_EL3_CTL_INVLD]

Table 48 Cisco NX-OS Release 8.2(8) Resolved Caveats

Identifier	Description
CSCvz03591	N7K F3: "returned error:Invalid VLAN" when allocate interface to vdc
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
CSCvz28924	ARP Probe packets are not flooded in vlan when otv suppress-arp-nd is enabled on Overlay interface.
CSCvz34580	N7K - after VDC type is changed from F3 to F3 F4 , VPC+ loops received PIM hello/general Query.
CSCvz58844	Packets to HSRP VIP sent to CPU when SVI is shutdown with VPC+ setup
CSCwa09253	VPC member port Initializing down after N7K reload or upgrade

Resolved Caveats—Cisco NX-OS Release 8.2(7a)

Table 49 Cisco NX-OS Release 8.2(7a) Resolved Caveats

Identifier	Description
CSCva83447	BGP stuck at 90% after redistributing OSPF routes to BGP with EVPN VXLAN
CSCvh64876	sh ip mroute summary displays bogus values for pps and bit-rate
CSCvj50674	N77-M348XP-23L card may reboot due SLF inband link issue(LINK_GOOD_TO_FAULT_12)
CSCvp33690	Add support for sh bgp l2vpn evpn <vrf name> for evpn
CSCvp61064	NX-SNMP: SNMP Auth protocol changing from SHA to MD5(SNMPv3 Informs)
CSCvq89022	Continuous logging of Invalid arguments in rpm_eval_policy_match
CSCvr12510	%MTM-SLOT2-2-INVALID_SLOT: Received invalid slot value 9999 in mts message from vdc
CSCvs17183	m9396s: not able to read show logging onboard kernel-trace
CSCvs45159	N9K VXLAN/VTEP with arp suppression enabled will not flood arp with sender IP 0.0.0.0
CSCvs74209	NGINX HTTP Request Smuggling Vulnerability
CSCvs88208	"copy run start" fails with port-profile signal 11 crash
CSCvt88871	N7K/F3: CLI to Disable Selective VRF in FIB on Flanker linecard
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
CSCvu39910	IPv6 routes redistributed from BGP missing after changing to MT
CSCvu66701	N7K: OSPF will not generate type 3 summary LSA
CSCvu69869	Configuring "vpc role preempt" will cause vPCs with port-type network to go into BKN state
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
CSCvu87859	OSPF LSAs are not refreshed after failed ISSU
CSCvu90705	ISIS IPv6 routes are shown as pending ((nil), 0) for MT-IPV6-UNICAST topology
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
CSCvu99685	"ip pim passive" causes loss of interface DF status after reload
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

Table 49 Cisco NX-OS Release 8.2(7a) Resolved Caveats

Identifier	Description
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
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
CSCvv23045	aclmgr passing wrong size while fetching priv data causing aclmgr crash
CSCvv24436	Fabricpath - Additional HSRP Anycast group config causes MCM MTS Buffer Buildup
CSCvv24541	Cisco NX-OS Software ICMP Version 6 Memory Leak Denial of Service Vulnerability
CSCvv27689	Default route metric changes after SUP switchover
CSCvv33208	N7K netflow flows are reported with a negative flow duration time
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
CSCvv49316	IPv6 floating (static) route is chosen while routes with lesser AD value are still available
CSCvv52514	EIGRP subnet goes SIA if link failover occurs with mix of wide/narrow metric and offset-list
CSCvv63531	F4 remains downs in slot 5 due to module purge failure
CSCvv69592	M3 LC fatal error in device DEV_SLF_BRI (device error 0xce400600)
CSCvv73708	FX2/MLD: IGMP/MLD crash on secondary VPC peer due to missing null check for group header
CSCvv81470	No syslogs displayed in session with 'terminal monitor' enabled
CSCvv87092	F3 interfaces goes to "faulty" or LC reset during recovery due to fatal interrupts
CSCvv93710	TRM-MS Sanity Failure: Remove/Add EVPN Multisite Global Config on BGW
CSCvw03395	M3 MACSEC Output and Input Errors
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.
CSCvw24386	Memory leak in N7K device due to malformed WCCP packets
CSCvw32747	Static routes not in (vrf) uRIB
CSCvw38981	Cisco FXOS and NX-OS Software UDLD DoS and Arbitrary Code Execution Vulnerability
CSCvw42838	private-vlan trunk not forwarding new vlans on Nexus 7000

Table 49 Cisco NX-OS Release 8.2(7a) Resolved Caveats

Identifier	Description
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
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
CSCvw73389	N77-SUP3E // 8.4(3) // M3 linecard // Nexus 7706 config session is timing out after importing ACL
CSCvw75003	n7k: show hardware queueing show incorrect output inteface values
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).
CSCvx13871	N7K PTP BC DSCP priority markings on egress
CSCvx14567	N7K: Host (/32) VRF route leak remains stale after removing config
CSCvx18137	Need a recovery mechanism for power supplies showing fail/shut due to shorted out bus
CSCvx18709	Sudo Privilege Escalation Vulnerability Affecting Cisco Products: January 2021
CSCvx38812	STP Dispute: STP root election is impacted on presence of dual homed FEX HIF in a port-channel
CSCvx44280	Packet looks to be not forwarded over N7K switches within Isolated VLAN over FP.
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

Table 49 Cisco NX-OS Release 8.2(7a) Resolved Caveats

Identifier	Description
CSCvx79358	ED_SCH_UC_QTYPE_HANG, ED_SCH_MC_QTYPE_HANG, VAL_KEI_CP_IRQ__0_FLD_RBRX_IDLE caused cpu tx pause
CSCvx87308	N77-M3 - ARP reply drop when arrive on N7K CTS port
CSCvy00853	aclmgr crash after executing show startup config
CSCvy16417	N7k IP Overlap Detection Fails for HSRP VIPs

Resolved Caveats—Cisco NX-OS Release 8.2(6)

Table 50 Cisco NX-OS Release 8.2(6) Resolved Caveats

Identifier	Description
CSCup42901	"no power resource" in the output of show environment fex command
CSCux65385	NXOS DATACORRUPTION-DATAINCONSISTENCY error in PIM process
CSCuz30263	After upgrade, eigrp failed to come up due to K value mismatch
CSCvb23106	unexpected eigrp metric calculation in aci
CSCvd29708	Multiple FEX reload due to Watchdog Timeout
CSCvf79399	2232PP FEX module(with N5/6/7/9K parents) Crash when inserting 4 GLC-TE transceivers into HIF port
CSCvg13002	N3500 igmp ssm-translate not working after reload
CSCvg19850	Npacl leaks 152 bytes of memory with ntp/snmp acl add removal
CSCvh63779	F3: Disable flexible TCAM bank-chaining "ERROR: Entry not found in copp database"
CSCvj05813	ARP Does Not Respond For VRRPv3 VIP After Module Reload "Destination address is not local"
CSCvj50674	N77-M348XP-23L card may reboot due SLF inband link issue(LINK_GOOD_TO_FAULT_12)
CSCvj63137	Copy command can't overwrite world-writable files
CSCvm43644	NXOS BGP is not advertising some of the BGP prefixes to the Neighbors
CSCvm69150	l2vpn process crash while bringing up VPLS between ASR9K and Nexus 7K
CSCvn30912	Mem leak snmpd during longevity with F4 LC reload usm_malloc_usmStateReference and snmpv3_pss
CSCvn54508	vsh core triggered by CLI
CSCvn78885	tacacs_crypt_service or radius_crypt_service filling up nxos/tmp
CSCvo11853	Service rsvp crashes twice in quick succession, first with signal 11, then with signal 6
CSCvo29485	[D-192] VRRPV3 Stuck in Master Master
CSCvo82705	ACL QOS core seen when checking Spanslogic TCAM on non-existent instance

Table 50 Cisco NX-OS Release 8.2(6) Resolved Caveats

Identifier	Description
CSCvo90099	NX-SNMP: snmp-server hosts getting modified after configuration(DNSv6 case)
CSCvp59096	OSPF route was excluded from SPF after short link flap.
CSCvp64129	skywalker: run bash command works even if bash-shell feature is disabled
CSCvp74544	Mac address is getting removed for PIP learned nve peer after uncofig/config of PIP
CSCvp92934	ARP Not resolved for LISP Hosts and Incorrect host Detection
CSCvq05447	N9K NX-OS 9.2(3) SNMPd Crash / MTS Queue Congestion When Doing GETBULK on entPhysicalEntry
CSCvq05743	MPLS LDP over GRE Tunnel is flapping when "mpls ldp explicit-null" is configured in N7K.
CSCvq10954	Nexus N9K-C9236C reboots with a 'urib' core
CSCvq18837	Python Security Regression Unicode Encoding Vulnerability
CSCvq26767	Supervisor hang and redundancy switchover failure
CSCvq34690	Change how ports are displayed during CTS logging
CSCvq48447	N9K snmpd signal 8 crash
CSCvq56953	Need standby Sup to detect a hung active Sup and reload it to trigger a switchover.
CSCvq65507	OSPF summary address not advertised after reload
CSCvq90763	Static routes pointing to Null0 in a vrf wont be installed after reload
CSCvr08197	N7k PIXM/PIXMc should attempt to recover if they get out of sync
CSCvr10766	N7k netflow input and output interface does not map to IOD database for M3 LC for Version 5 template
CSCvr15081	N7k - RADIUS stops working due to DNS not resolved
CSCvr19809	cosmetic: native 40G port (non-breakout) report incorrect Quesize for F3. breakout 4x10G unaffected.
CSCvr30525	IGMPv3/MLD Snoop - Mcast Traffic Loss To All Receivers After One Receiver Sends Multiple Leafs
CSCvr31356	GARP not updating ARP table on remote VTEPs
CSCvr39538	N7K may report false memory utilization values
CSCvr40843	port-channel switching time was longer than expected with N7K-M348XP-25L
CSCvr57551	Cisco Nexus 9000 reloads with Kernel panic - unable to handle kernel paging request
CSCvr58649	BGP service crash at rpm_acquire_bgp_shmem_lock
CSCvr62038	Unable to save configs - service ipqosmgr failed to store its configuration
CSCvr62671	SSH quietly fails - aaa reports failed to remove the access list configured : sl_def_acl

Table 50 Cisco NX-OS Release 8.2(6) Resolved Caveats

Identifier	Description
CSCvr62735	BGP attribute-map for aggre address sets the last attribute without matching the prefix list.
CSCvr63838	SNMP walk using OID 1.3.6.1.2.1.1 returns NULL [Expert Info (Note/Response): endOfMibView]
CSCvr63916	Module id incorrectly formatted in CPUHOG messages
CSCvr80704	Configure replace fails when 'switchport trunk allowed vlan' list is too large
CSCvr85588	VTP crashed after multiple trunking interfaces flapped
CSCvr96953	Users cannot authenticate against RADIUS/TACACS+ if custom role offered was recently modified
CSCvr98425	Cisco Nexus 3500 BGP-3-ASSERT syslog in IPv4 Multicast AF with Ext. Communities
CSCvs00187	vsh.bin process crash
CSCvs11098	Rollback fails to update OTV extend-vlan list on Nexus 7000 switch platforms
CSCvs16170	corrupted/incorrect router ID sent in update packet for external routes.
CSCvs20377	RPF nbr pointing to Assert Loser on RP in MVPN environment
CSCvs23562	MALLOC_FAILED: mcastfwd [27776] m_copyin failed in mfwd_ip_main()
CSCvs24635	The temparature error logs are shown continuously when FEX is connected to N77-F324FQ-25.
CSCvs26685	%NETSTACK-3-URIB_ASSERT_ERROR on u6rib_process_notify
CSCvs29433	EIGRP learned routes flapping when associated prefix-list is modified
CSCvs37194	Need "match exception ip/ipv6 unicast rpf-failure" added to default copp policy
CSCvs43451	fcoe n7k with 2232pp fex after sup switchover hif ports change from pfc to link level pause
CSCvs49208	BGP - peer with md5 authentication fails after upgrade from i7(4) to 9.3(1)
CSCvs49787	MAC Address learning failed due to unexpected "port-security" function remaining enabled
CSCvs50843	IP mobility not updating route on source leaf
CSCvs53167	N7k EVPN F4/M3 8.2(5) Delay in convergence of vtep ecmp routes after peer flap
CSCvs54611	need to add a syslog or any form of notification when the interface chip failure
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
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
CSCvs62687	F3 - MAC hardware entry point to wrong interface instead of peer-link

Table 50 Cisco NX-OS Release 8.2(6) Resolved Caveats

Identifier	Description
CSCvs67823	[Trustsec] Nexus 7700 Downloading SGACLs for dgts not on the database when doing CoA push from ISE.
CSCvs69194	N7K only listens one ip for tcp 64999 when cts sxp source ip is configured
CSCvs69425	Refresh profile CLI fails when updating the old profile with the new profile
CSCvs76901	cli function returns cmd_exec_error when collecting show tech-support via python
CSCvs81070	Cisco IOS, IOS XE, IOS XR, and NX-OS Software One Platform Kit DoS Vulnerability
CSCvs83567	NX-OS 8.x IP redirect source check not working
CSCvs84593	eem_syslog_regex_ev_spec_handler is output when eem is created
CSCvs93402	BGP hellos seen after peer admin shut
CSCvs95580	IGMP crash after "run ip igmp snooping access-group <route-map-name>"
CSCvs97090	ITD reverse policies are not programmed properly.
CSCvt00423	N7K linecard "fwd_stats_client" process crash
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.
CSCvt33067	Traffic Black-holing with VPC SFC failure(L2LU Drops, VSL Check)
CSCvt35882	n7k Service "statsclient" crash
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
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
CSCvt87450	snmpwalk GETNEXT for mpls sub-layer ifIndex returns object from the IfDescr section
CSCvt93544	Match exception ip unicast rpf-fail on M3 matches all traffic in CoPP

Table 50 Cisco NX-OS Release 8.2(6) Resolved Caveats

Identifier	Description
CSCvt93631	entPhysicalMfgName always defaults to Cisco Systems for transceivers
CSCvu00553	OSPF Sets Type-5 FA for local routes
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
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
CSCvu40129	Incorrect ISSU operation in some 6.2.x to 8.2.x upgrades
CSCvu44271	"show tech aclqos" encapsulates show commands in single-quotes, not grave accents.
CSCvu51632	eobc logging enhancement on M2 LC for HB Loss debugging
CSCvu53710	M3/F4 HAP reset seen in SLF_BRIDGE process.
CSCvu70729	After PIM restart, multicast routes stuck in pending, stale operations in MRIB txlist
CSCvu77230	service ipp will crash when 'no opflex-peer' is entered
CSCvu98502	Post LDP crash due to Abort/HB timeout LDP might be unable to bind to the socket and fails recover
CSCvs90047	ipv4 routes with ipv6 NH BGP routes redistributed into OSPF as Type-5 expires in 30 min
CSCun30427	Next-hop address field is 0.0.0.0 in exported netflow packets
CSCuy93263	N77/M3/BGP: ncpinfraclnt cored while injecting BGP routes
CSCvq69766	eobc logging enhancement on F3 LC for HB Loss debugging
CSCvs56900	U2RIB 452 MTS buffer stuck with memorey leak and crash in the MCM/U2RIB
CSCur73920	7.1.0.D1.0.237.S0: CDP buffer leak at OPCODE: MTS_OPC_CDP_SUP_REQ
CSCvr59780	M3 LC goes to failure with DEV_SLF_BRI (device error 0xce400600)
CSCvr61942	CN127 FEX N3K-C3248TP-1GE failed to online on 8.2.3
CSCvs71659	RIT changes to support Local, GLEAN punt path for MPLS ADJACENCIES
CSCvo82792	VTP core seen doing ISSU from bin to .upg
CSCvf01034	cts component code consolidation and cleanup

Table 50 Cisco NX-OS Release 8.2(6) Resolved Caveats

Identifier	Description
CSCuv28784	Syslog Enhancement Request for SYSMGR
CSCvo18982	OSPF Configuration removed after Supervisor Switchover

Resolved Caveats—Cisco NX-OS Release 8.2(5)

Table 51 Cisco NX-OS Release 8.2(5) Closed Caveats

Identifier	Description
CSCtr60095	Excessive aaa tcp session cause control-plane instability
CSCui46891	NX-OS: mts recv_q SNMP Response SAP - stp+dot1dBridge+qBridge
CSCui56136	sed input handling error
CSCup85616	SNMP Leaks configured VLAN IDs to unauthenticated users
CSCuq77105	Receiving malformed BGP UPDATEs causes urib crash
CSCuu75466	Cisco Nexus 7000 Message of the Day (MOTD) Telnet Login Vulnerability
CSCuu82356	Evaluation of n7k-infra for OpenSSL June 2015
CSCuu99291	Cisco Nexus 7000 VDC Authenticated Privilege Escalation Vulnerability
CSCux65385	NXOS DATACORRUPTION-DATAINCONSISTENCY error in PIM process
CSCva92054	Route-leak (inter-vrf) - hmm route not flushed on host vMotion
CSCvc49591	Missing IGMP Entries after N7K joining vPC domain
CSCvc91280	incomplete error output during duplicate IP address entry
CSCve91659	Cisco NX-OS Software CLI Arbitrary Command Execution Vulnerability
CSCvf24911	ARP memory leak @ LIBBL_MEM_bitfield_malloc_t & LIBSLAB_MEM_create_slab
CSCvj23813	Remove stale LTL entries from IM as a part of CSCvj10306
CSCvj24868	MTS buffers' leak while constantly polling objects in BRIDGE-MIB
CSCvj59431	Cisco NX-OS Software Bash Shell RBAC Privileged Escalation Vulnerability
CSCvj65666	Cisco FXOS and NX-OS Software CLI Command Injection Vulnerability (CVE-2019-1611)
CSCvk05550	N7k - SPAN Destination traffic leaves untagged in setup with bridge-domain
CSCvm57467	On changing the vlan -> vni mapping, vnis are in down state
CSCvm65141	cannot rewrite vlan at dual-active exclude interface-vlan-bridge-domain
CSCvm90522	N9000 prefers mBGP route over directly connected one causing mcast traffic black holing
CSCvn02785	ISIS does not advertise local or learned routes to neighbors after upgrade and coming out of mmode
CSCvn13645	can not change AD for ISIS ipv6 routes using distance command under ipv6 address family
CSCvn33000	Regarding ISIS redistribute maximum-prefix less than static route number

Table 51 Cisco NX-OS Release 8.2(5) Closed Caveats

Identifier	Description
CSCvn36429	Service "AAA Daemon" failed to store its configuration (error-id 0x80480018)
CSCvn36645	Vlan not added to flood list, when new vlans are created in FL ingress-replication VXLAN
CSCvn37301	With passive TWINAX cable N2K-C2348TQ-10G-E reports the Fan Failure
CSCvn56700	Nexus9000 Mcast pim spt-threshold infinity not honored when LHR transits from non-DR to DR
CSCvn57953	NVE failed to learn remote VTEP RMAC after ISSU aborted or canceled
CSCvn78166	N3000 generates IGMP report with source 0.0.0.0 preventing the mcast group from timeout
CSCvn99435	API snmp_get_mgmt_conf_last_change_time return ERROR
CSCvo07343	VXLAN IPv6 packets loop due to NVE invalid source-intf state while peerlink is down or unconfigured.
CSCvo10679	VXLAN:NGMVPN service crashes due to could not allocate slab for fabric mroute
CSCvo14963	N7K-PPM: Issues seen under interface when port-profile is inherited.
CSCvo15505	Egress packet loss from CPU when dest is recursive through EVPN
CSCvo15674	crash because of memory leak in bfd process
CSCvo29957	Output of "show mpls ldp igp sync" inconsistent with configuration
CSCvo49074	ISIS is calculating metric for IPv6 based on worse LSP
CSCvo61537	HTTP GET sent too late in python shell
CSCvo62526	N9k BGP - When changing export map on VRF, RT does not always update in EVPN AF
CSCvo73682	sac_usd hap reset when standby supervisor becomes active
CSCvo80379	BGP route may stuck at dampened state
CSCvo80677	Linecard CPU utilization is displayed incorrectly for some processes
CSCvp01676	T2 EOR: Traffic drop due to null NH in forwarding table
CSCvp02900	VPC: Type2 EVPN route advertised with primary IP of Loopback as next-hop
CSCvp04544	M3 LSMET fib exhaustion message shows wrong VDC number
CSCvp08694	Stale arp entry/route after VM move from one VPC domain to other due to HMM update failure
CSCvp11726	NX-SNMP: Random Auth failure when performing snmp-walk (via TCP) using SNMPv3 users.
CSCvp16978	IGMP v2/v3 mix: shutdown igmpv2 receivers and igmpv3 receivers are also removed from mrib oifl
CSCvp35682	Target Address on IP SLA (udp) probes is getting changed to a new IP other than the configured one
CSCvp40959	N9k do not age out Snooping entry against vPC Peer link port after receipt of GSQ

Table 51 Cisco NX-OS Release 8.2(5) Closed Caveats

Identifier	Description
CSCvp41187	N7K replaces the default mpls-vpn route with the type-7 default route
CSCvp47670	"no ip redirects" configurable on L3 port-channel member port
CSCvp57692	BFD session goes down upon changing IP address of unrelated interface
CSCvp69490	Irvine : vsh core seen in steady state with traffic running [without any triggers]
CSCvp70746	n7k/F2: EEM to ignore interrupt during EG recovery (CSCux90737/CSCug39011/CSCux08154/CSCud43503)
CSCvp75032	VRF missing after upgrade to 7.3(5)N1(1)
CSCvp92657	MRIB crashed with watchdog due to loop in txlist
CSCvp93465	n9k generates LSA even when the interface fails to come up
CSCvq03952	Procjob process does not check NULL payload of MTS messages
CSCvq04585	Mcast trafffic loss seen sometimes with module reload and other triggers
CSCvq07407	N9k: diff option needs to be done at parameter level
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
CSCvq20196	leak-route doesn't happen leading to leak-route installation failure
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
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
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.
CSCvq57865	Memory leak is seen in DHCP process when show run is executed on a VLAN
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
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	After upgrade from 7.3(2)D1(3a) to 8.2.2 on N7K, show tech/show tech det is not getting complete.

Table 51 Cisco NX-OS Release 8.2(5) Closed Caveats

Identifier	Description
CSCvr21201	N7K: cryptographic-algorithm HMAC-SHA-xxx keys show up as unknown
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
CSCvr52113	f4/M3 bridge. Reset due to USD Failure.
CSCvg77231	BGP stuck into Shut (NoMem) and neighbourship not formed
CSCvr08197	N7k PIXM/PIXMc should attempt to recover if they get out of sync

Resolved Caveats—Cisco NX-OS Release 8.2(4)

Table 52 Cisco NX-OS Release 8.2(4) Closed Caveats

Identifier	Description
CSCva90832	TACACS non blocking connect failed with error code 98
CSCvb55686	NX-OS FSCK/format-bootflash there is a missing "space" in line 100
CSCvc92277	NFP crash after associating netflow-orignal flow record to active flow monitor
CSCvd69246	Incomplete error message is seen for VIP overlaps in HSRP
CSCve18390	RBAC user role name length inconsistencies
CSCve21405	Inconsistent formatting for 'show interface' outputs collected through NXAPI using JSON
CSCve24672	BGP routes not advertised to peer after shut/no shut of interface connected to peer
CSCvf31178	N77/M3/VPLS/PIM: PIM-3-AVL_ERROR: AVL-tree operation ravl_insert() failed for PIM Assert FSM
CSCvf76652	N7K : STP internal event-history tree timestamps deviation
CSCvf80182	802.1x re-authentication fails with non-default timer 30secs because of failure of server lookup
CSCvg00359	N7K console hangs and not responsive
CSCvg08776	Nexus VRF Route Leaking RIB Update Problem with BGP Network Statement
CSCvg23978	N7K - nfp crash on F4/M3 module
CSCvg49084	PortChannel Config VLAN information is not passed LC while ports move into PC from Indiv.
CSCvg58990	passwordless ssh is not working as metnioned in the document for 6.x version
CSCvh18563	After upgrade 9148S from 6.2(17) to 8.1(1) "logging origin-id" command is missing
CSCvh65567	Can't delete ACL completely

Table 52 Cisco NX-OS Release 8.2(4) Closed Caveats

Identifier	Description
CSCvh68603	MDS: when running ldap test "test aaa group username password" it results system switchover
CSCvi05327	enhancements in fabric for apple cap
CSCvi45841	Cannot configure "rmon halerm" after snmp-get-next -v1
CSCvi54206	Scheduler job breaks RBAC if the username has multiple roles assigned from the AAA server
CSCvi97093	LSA type 4 not flushed in NSSA area
CSCvj07101	Copying SNMP MIB using IPV6 causes a reload
CSCvj16168	nxapi-server may send pure xml-encoded data in json-rpc reply
CSCvj33348	N77-M348XP-23L/N77-SUP2E Linecard crash for IPFIB process followed by IFTMC crash
CSCvk16641	ipv6 static route with next-hop as ipv6 address across the vxlan fabric does not get into URIB
CSCvk22156	n7k/GOLD: temperature sensor message improvement
CSCvk60178	M3 CB100: Remove 40G and insert of 100g in one port impact the traffic in adj port
CSCvm56314	OTV VDC ignores dst IP in port-channel hash
CSCvm63999	Issue with the BGP "pre-bestpath" point of insertion (POI) on Nexus7k
CSCvn09912	N7k/F2E: 'Disabling PFC on port x since macsec is disabled' logs filling syslog
CSCvn21120	"aaa bypass-user" option to bypass ACS authorization/accounting does not work
CSCvn24277	M3: EOBC heartbeat failure in device DEV_EOBC_MAC
CSCvn25428	Line card on Nexus7K will start forwarding traffic before routes are programmed
CSCvn42389	ACLQOS Core with FEX on N77K
CSCvn61247	N7K M3 Span destination port accepts by default incoming traffic.
CSCvn63538	N7K: Entries in new created SVI mismatch between UFIB and URIB and communication fail using those
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
CSCvo11968	%SYSMGR-2-SERVICE_CRASHED: Service "cdp" hasn't caught signal 6 (core will be saved).
CSCvo13456	ISIS LSP flooding broken
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

Table 52 Cisco NX-OS Release 8.2(4) Closed Caveats

Identifier	Description
CSCvo29766	Nexus / NX-OS / Multicast PIM Join not sent when IPv4 unicast route has IPv6 next-hop (RFC 5549)
CSCvo34762	IPv6 static routes may get missed in RIB on PKL/PL shut/unshut
CSCvo36285	N9K BGP sessions unstable when TCP packets received from same source to multiple local addresses.
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
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
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.
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
CSCvp38858	N7K Ethanalyzer Fails to Decode Internal Header with Ethertype 0xF003
CSCvp45874	N7K M3 PBR load-share does not redirect traffic as expected
CSCvp45929	N7K Supervisor Switchover due to TACACS+ hap reset - bad file descriptor
CSCvp51579	Nexus 7000 / M3 / not accepting filter acces-group command in erspan config
CSCvp58845	After remove/add VRF, remote host routes not installed to URIB and report 'remote nh not installed'
CSCvp83475	SDA: Invalid src ip address in VXLAN header on n7k border

Table 52 Cisco NX-OS Release 8.2(4) Closed Caveats

Identifier	Description
CSCvp98039	N7K MPLS FIB programming issues after reload w/ M3 module
CSCvg71883	Speed auto negotiate can not be disabled on FEX 1G SFP port
CSCvp57934	Optimization of internal NXOS parameters

Resolved Caveats—Cisco NX-OS Release 8.2(3)

Table 53 Cisco NX-OS Release 8.2(3) Closed Caveats

Identifier	Description
CSCup79623	EEM:S5: show eem history events: not over writing after 50 applets
CSCuw39988	N5672 - NXAPI sandbox browser will not work over HTTPS port 443
CSCuw91064	'show ip access-list' output does not update/display statistics
CSCuw99630	Cisco NX-OS Authenticated SNMP Denial of Service Vulnerability
CSCux44698	SVI's go down on VPC primary, when peer-link is down
CSCuz84018	%RIP-3-RPM_LIB_API_FAILED log in regards to CSCum05295
CSCva49561	Enhancement req : Securing NXAPI access
CSCva75937	port-profile configuration missed after reload
CSCva95344	F3 Line card reload
CSCvb17413	Unable to access NXAPI Sandbox(Non-default VDC) as VDC-Admin
CSCvb27736	IPSLA not allowing /31 point-to-point IP prefix x.x.x.0
CSCvc18092	Traffic impact when adding VLAN under port-profile
CSCvc42886	N56xx - No SSH possible to device when root directory is full due to nxapi request
CSCvc66360	show port-channel load-balance forwarding-path is not correct
CSCvc73543	N7K adding ip address into object group stuck
CSCve70445	Bfd is not coming up with cts on M3
CSCvf10136	Native vlan tagging not working after ISSU to 6.2.16 and reload
CSCvf11898	N7K/M3 Null0 route has DI of 0x0 and hits CPU
CSCvf30935	Eigrp routes flap if OSPF is removed from the switch
CSCvf36683	N7K-SUP2/E: eUSB Flash Failure or Unable to Save Configuration
CSCvf39800	FEX PS module status is incorrect
CSCvf47348	IPSLA ICMP-ECHO probes not coming up after reload
CSCvf60001	"show lldp neighbor details" doesn't list all neighbors
CSCvf61926	N7K // Ethanalzyer does not gather FIP or FCoE traffic on F3 line card
CSCvf69323	One of the ports of F2 line card is not linking up
CSCvf81891	N7000 sends PTP packets incorrectly with ttl-1
CSCvf83946	Memleak found at PIM

Table 53 Cisco NX-OS Release 8.2(3) Closed Caveats

Identifier	Description
CSCvf97669	M1 line-card ifOutUcastPkts is zero when polling with snmpwalk
CSCvf99101	feature poap operation failed on response timeout from service which leads to delay in POAP abort
CSCvg16920	BGP community list missing in config when updated after reload
CSCvg18985	ifInDiscards not matching # show interface mgmt0 counters errors on N7K
CSCvg38678	M2 LC: Internal link stability issue does not error disable port-group HW Fail
CSCvg42792	Running commands in 'routing-context vrf <x>' mode does not work on all commands
CSCvg44192	bfd based static route not getting deleted during interface shut
CSCvg57540	N7K Netflow M3: subinterface netflow sampler not working on breakout cable ports
CSCvg65330	IPSLA Probe-ICMPv4 over VPC : continuous MTS message without proper dst-sap
CSCvg65643	Connected devices are flapped though ports at N77-F324FQ-25 side are shutdown
CSCvg70139	%ETHPORT-3-IF_UNSUPPORTED_TRANSCEIVER: Transceiver on interface Ethernet9/6 is not supported
CSCvg77643	Nexus 7000 VDC not load start-up config about passphrase
CSCvg90880	Clipper port-channel L3 Sub intf not generate netflow
CSCvg92762	N7k with SUP1/6.2.12 continuously rebooting with aclmgr crash
CSCvg95207	N7004 - L2 multicast traffic is sent to all SOC's
CSCvg95301	Unable to save configs - service ipqosmgr failed to store its configuration (error-id 0x41170040)
CSCvg96060	N7K - after changing peer-link config in VXLAN BUM traffic blackholed
CSCvh03195	local prefixes not expected to be learned via SXP
CSCvh03275	Under track list boolean or can't restore to running-config after copying startup-config and reload
CSCvh13852	N7k Unable to send packet more than MTU size with cts manual configured on the port
CSCvh19090	CVR-QSFP-SFP10G interface showing not connected after chassis cold boot
CSCvh19223	ISSU failure when running 'show install all status' in separate window
CSCvh19585	8.2(0)SK(0.298) : N77-F4100 - eem_policy_dir core at fh_policy_cli_read_pattern
CSCvh21420	IPv6 Static route with Link Local Address not installed as RNH
CSCvh25999	N77K - Unable to configure input netflow monitor in Po
CSCvh30461	"show routing vrf all ipv6 internal distribution" causes crash at u6rib
CSCvh54503	After rip process restart only 8 ECMP routes are allowed
CSCvh54560	After route flap next-hop count increase
CSCvh56282	Physical VPC port which is in LACP I state is not brought down by VPC

Table 53 Cisco NX-OS Release 8.2(3) Closed Caveats

Identifier	Description
CSCvh61904	unable to remove duplicate entries in DNS group with cfs
CSCvh67120	NX-OS netflow configuration cannot enable under p2p port-channel
CSCvh68148	SSH terminal is stuck after rekey is enabled
CSCvh77171	N7K M2 - multicast traffic to CPU blackholed due to RL and CoPP dropping all packets
CSCvh92510	Multiple WCCP SG's on L3 interfaces will NOT remove TCAM entry when CE connected interface is DOWN
CSCvh95329	N7K "ipfib"crashed
CSCvh98764	NFM-2-VERIFY_FAIL: Verify failed - Client 0x82000146, Reason: Duplicate Sampler C, Interface
CSCvi08195	VSH crash due to some special commands
CSCvi08392	M3/F4 Flex Parser Cleanup and Conditional Changes for GTP
CSCvi09055	BGP neighbor flap or slow convergence with outbound route-map coupled with aggressive timers.
CSCvi09665	Unable to establish 10G link on N7K
CSCvi10474	TACACS Authentication fails with "DNS cache fail"
CSCvi12032	[N7k M3] GRE tunnel do not forward unicast/mcast traffic
CSCvi14840	Nexus might crash after creating multiple MSDP mesh groups
CSCvi15800	N7k - OTV Fast Convergence is delayed during AED switchover
CSCvi18966	N77XX/M3:CBL forwarding on down port
CSCvi20373	n7k ICMPv6 Packet too big Messages are not send after ISSU to 8.2(1)
CSCvi29201	Sync timezone between FEX and N9K
CSCvi34298	N77 routes IPv6 packets that are not destined to it
CSCvi37040	netstack crash while redirecting "show tech-support netstack detail" to bootflash:/
CSCvi38868	N7K creates two MDT Data Groups when the VRF uses PIM ASM
CSCvi40689	Fabric path isis interface shows MTU for vPC Peerlink incorrectly
CSCvi45642	MDS 97xx: Incorrect state and no data for reason code/return code for svi enabled snmpd error logs
CSCvi47337	Netstack should not process non Ethernet II encapsulated packets
CSCvi49478	Same port# on different FEX can not ping if connected through M3
CSCvi49900	Formatting bootflash does not recreate .patch folder- SUP in boot loop
CSCvi50857	N7K - BFD session for L3 protocol over fabricpath does not come up
CSCvi55885	Inband driver does not strip headers from outbound FCoE frames when attempting to capture traffic
CSCvi58404	Nexus Sup Module crash upon Netflow monitor application on the Interface
CSCvi61623	N7K/N77 F3 module egress buffer lock
CSCvi62706	N7k running VPC crash due to memory leak in VPC process

Table 53 Cisco NX-OS Release 8.2(3) Closed Caveats

Identifier	Description
CSCvi64957	BFD over FabricPath: SUP and LC out of sync - happens on OIR
CSCvi73154	N7K // Adding a 16th WSA Client causes the N7K to drop all clients continuously
CSCvi76485	Duplicate Pkts observed due to PIM Assert not triggered
CSCvi77191	N7K - adding kernel messages to OBFL for hung state
CSCvi78169	N7K VPC Crash
CSCvi78715	Netboot over EOBC fails if both supervisors were originally netbooted
CSCvi84074	When HSRP enabled, Proxy ARP enabled N7K doesn't respond to unicast arp request
CSCvi87540	N7K - HSRP libanycast cache does not sync to standby sup after changes to anycast bundle
CSCvi88803	N7K linecard crash with aclqos hap reset
CSCvi89389	Acllog crash after upgrading TAH EOR from Gplus to Hdev 531 and idle
CSCvi89817	fln_que hap reset during issu.
CSCvi90921	vPC config-sync abnormal cli is syncd
CSCvi91299	OTV process hang or crash post Overlay peer going up or down
CSCvi93529	N7K/F348: LC specific commands not included in "show tech forwarding l3 multicast"
CSCvi96878	LDB/ILM entries not present after VDL or linecard reload
CSCvj06233	F3 card DOM issue
CSCvj06473	System hap reset with sla_sender process crash
CSCvj06726	N77XX/M3: Mac sync issue
CSCvj08912	BFD is not coming up when authentication and hardware offload is used between N7K and ASR1k
CSCvj08973	snmpd hap reset crash when snmpwalk on OID stpxMSTInstanceVlansMapped2k
CSCvj09037	MPLS interface does not send ICMP type 3/code 4 (Fragmentation Needed and Don't Fragment was Set)
CSCvj09711	N7K - Service "acllog" crash with PBR
CSCvj10306	LTLs not deallocated in IM for broken out port after a no breakout is done on that port
CSCvj12608	provide drop counter when packets are dropped due to incorrect ltl to vdc mapping in KLM vdc
CSCvj12978	sup2:need mechanism to clear soft-voq once it gets stuck
CSCvj14367	Regular zone changes disrupt ivr traffic
CSCvj14441	PTP GM clock sync loss after switchover
CSCvj15110	Nexus9k KIM crash on SUP failover
CSCvj17451	Dynamic label not reassigned after static range defined and LDP shut/no-shut

Table 53 Cisco NX-OS Release 8.2(3) Closed Caveats

Identifier	Description
CSCvj18266	Unable to remove access-list with ERROR: Invalid argument on Nexus 3k/9k and n7k platforms
CSCvj19911	Incorporate new firmware for Unigen into NX-OS due to logflash mount unsuccessful
CSCvj31589	eth_port_channel crash in Nexus7K after "show port-channel internal lacp-channels <>" command
CSCvj36340	FCoE pause drop threshold reached when VL is paused/resumed quickly
CSCvj46259	FEX: Traffic lost on F2E-FEX L3 interface due to di-ltl-index programmed incorrectly
CSCvj46671	APEX2/SUP3/F4100: sysmgr process crashes at system() call.
CSCvj47506	eltm core observed upon shutting vPC port-channel with vlan translation enabled along mappings
CSCvj55192	Kernel memory commands not working
CSCvj55813	'hardware ejector enable' command is not displayed in 'show run all' output
CSCvj58687	Intermittent 51 second frame timeout drops without congestion
CSCvj58887	Partner fails to set collecting bit in LACP PDU causes sequence timeout
CSCvj63743	Nexus System Software Internal Network Restriction Bypass Vulnerability
CSCvj64036	Kernel traces in nexus core files can't be decoded for kernel 3.4 version
CSCvj70275	N7K %SYSMGR-2-VOLATILE_DB_FULL: high usage in /dev/shm
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
CSCvj87367	MST regions out of sync after ISSU to 8.1(2a)
CSCvj94409	When POAP is done, Maintenance mode profile config lost if switch reload
CSCvk01435	M3- PTP Multicast-224.0.1.129 packet drop
CSCvk03597	PTP GM clock sync loss after system reload, process restart
CSCvk04105	N7K - NXAPI request fails when xml payload is larger than 10k
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
CSCvk24889	CN12710- OEM SFP(Vendor:AVAGO) reported unsupported when this interface UP or DOWN
CSCvk28290	Fabricpath DCE mode of port-channel member inconsistent
CSCvk31556	invalid source ip for inter vrf ping for /32 destination
CSCvk35035	logging server vrf name in startup-config changed after reload
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

Table 53 Cisco NX-OS Release 8.2(3) Closed Caveats

Identifier	Description
CSCvk44722	Evaluation of N3K/N3500/N5K/N7K/N9K/MDS for OpenSSH CVE-2016-8858 and CVE-2016-10012
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
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.
CSCvk64742	EIGRP ExtCommunity lost in transit on Nexus7K
CSCvk68623	IPv6 recursive nexthop is not working in VRF leaking setup
CSCvk68792	NXOS: Netstack crash observed with active timer library in heap_extract_min
CSCvk68796	EIGRP traceback when redistributing with match ip next-hop
CSCvk72354	stale nexthop entry for ipv6 route in VRF leaking
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
CSCvm09452	N77-F348XP-23 kernel panic
CSCvm11792	ISIS IPv6 multi-topology - fixing MT attached bit
CSCvm13449	Stale Entries present in cli_acl_ifdb PSS on Standby Sup after Purge
CSCvm15461	Evaluation of n7k-platform for CVE-2018-5391 (FragmentSmack)
CSCvm16677	PSS memory leak in igmp_snoop for key type 0x04 and 0x0d
CSCvm19090	DDB sanity check and client notification changes
CSCvm21746	ospfIfIpAddress not working for specific index
CSCvm26010	BGP allocates label before registering with ULIB
CSCvm26068	N7K - Service "pim" crash
CSCvm27147	N7K/F3 interfaces goes to Hardware Failure after creating SVI
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
CSCvm44595	N7K Aclmgr memory leak on show ip access-list expanded cmd
CSCvm46017	Netflow active timeout is not working as expected

Table 53 Cisco NX-OS Release 8.2(3) Closed Caveats

Identifier	Description
CSCvm50765	Default route (track added) not getting advertised after box reload
CSCvm52059	CPU Traffic Not Sent out on L3 VRF Interface
CSCvm64931	N77:tcam utilization with QoS policy not increase
CSCvm65736	N7k: ELAM release may trigger clp_elam crash/LC reload
CSCvm67806	FabricPath - use PURGE instead of DELETE when LSA expire
CSCvm69204	N77 who is HSRP active can not reply ARP if NIF is down
CSCvm73959	N7K: ARP request from different subnet should be handled as error
CSCvm74036	N7k MPLS LDP Advertise Label Prefix-List not properly applied
CSCvm74044	PBR feature disabled after cold-boot upgrade to 8.3(1)
CSCvm84893	boot.log file cause /mnt/pss 94 % After cold boot from 8.1.1 to 8.3.1.72
CSCvm86801	N5K running 7.1(5)N1(1) Service "snmpd" crash
CSCvm91348	N7K/L2FM: MTS build up during higher MAC move between LC
CSCvm93582	N7K/NTP: ensure monolithic time sync between active and standby
CSCvm99009	Port Info missing in level 2 L2FM log messsage when MAC moves continously at a high rate
CSCvn01786	remove "show tech all binary" from "show tech fex"
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
CSCvn13028	"nfp" crash on module when configuring netflow
CSCvn14579	F3 Egress buffer lockup handling
CSCvn22059	N7K - aclqos crash
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"
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
CSCvn38330	New mac learn triggers mac move with 2nd packet from host in fabricpath
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
CSCvn44369	NXOS advertises the pseudonode inconsistently in multitopology mode

Table 53 Cisco NX-OS Release 8.2(3) Closed Caveats

Identifier	Description
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
CSCvn53847	ELOAM: Syslog to show more info. Auto-recover error disabled interface due to dying gasp.
CSCvn59162	VxLAN Type5 next-hop unchanged
CSCvn59937	ISCM crash/core due to NAT enable under ITD configuration
CSCvn62162	no vn-segment failed to run
CSCvn63102	NVE failed to learn remote vtep RMAC after config change from DCNM/MW mode
CSCvn67179	IPFIB process crash after NXOS upgrade.
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"
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
CSCvn99680	PTP - GM OFFSET 37 Seconds and Nexus 7K SR 685369201
CSCvo09373	N7700- N77-M348XP-23L- Vlan tagging uncorrect in local span
CSCvm14544	DHCP relay source-interface does not work on N7K
CSCvs54872	N7K SVI down (VLAN/BD is down) while there are active ports in vlan due to incorrect FLC counter

Resolved Caveats—Cisco NX-OS Release 8.2(2)

Table 54 Cisco NX-OS Release 8.2(2) Closed Caveats

Identifier	Description
CSCuw40711	Nexus - in.dcos-telnetd service crash
CSCuw86555	ENH - N7K Silent/Unknown supervisor switchover
CSCux87740	N7K uses wrong MAC address for BFD when peer switches mac address
CSCva20758	ISSU - TSH Gdb to upg Gdb Lead to SNMP Crash on MDS 9513
CSCvc69075	MAC address mismatch between SUP and LC after a VPLS failover.
CSCve01811	vpc-config-sync fails with error message
CSCve78301	N7k-PI: bps rate is incorrect under type qos policy-map
CSCve80468	N7K/F2e/F3:Post Routed L3 MCast traffic forwarded on both the FTAG
CSCvf27235	N7K: Improve Logging for Interrupt Fault CLP_LBD_INT_MEM_ECC_PORT_MAP_TBL_ECC_1ERR
CSCvf36683	N7K-SUP2/E: eUSB Flash Failure or Unable to Save Configuration
CSCvf58207	vPC+ Secondary does not suspend SVIs when Primary reachable via Fabricpath
CSCvf59067	N7k-8.X- Eigrp SIA due to a query/update from non successor.
CSCvf66024	PBR programming wrong adj index when N7K up with multiple PBR configured ports
CSCvf75002	Don’t refresh type-5 LSA for which route is not present in RIB
CSCvf77200	n7k/l2vpn: FLUSH not requested upon DOWN->UP change
CSCvf79160	OSPF type-5 routes blocked from RIB when table-map with permit route-map is applied
CSCvf87011	M3 - Ncpinfraclnt Crash
CSCvg03991	M3 linecard is parsing the Mobile IPv6 header incorrectly and assigning a drop interface index
CSCvg04072	Cisco NX-OS System Software Patch Installation Command Injection Vulnerability
CSCvg04455	N7K - RewriteEngineLoopback test failure does not error disable ports in non-default VDC
CSCvg10842	Input discards after issu to 7.3 or 8.x code, egress throughput reduction for F3-100gig/40gig ports.
CSCvg11502	Entering encapsulation mpls sub-menu and then exit in n7700 makes pseudowire to go down
CSCvg17452	Nexus 7k router drops packets at VXLAN encap due to incorrect egress LIF programming
CSCvg23522	Unable to remove the ACL from N7k
CSCvg24686	SNMP v3 information leaking vulnerability
CSCvg25737	URIB sends route notifications for broadcast routes when the client requests all-igp notifications

Table 54 Cisco NX-OS Release 8.2(2) Closed Caveats

Identifier	Description
CSCvg27491	F3 module goes HW faulty when using 1Gb Transceiver
CSCvg32741	HA policy URIB crash@urib_ext_comm_on_rte_nib on 8.2.1 release
CSCvg34717	Multicast CP packets are dropped by F2/F3 module
CSCvg44947	Dropping GTP ipv6 packet
CSCvg45324	Static mac programmed as dynamic for orphan mac
CSCvg46045	post ISSU from 7.2.2 to 7.3.2.D1.2, on collector, the flow record templates show junk values
CSCvg50660	Need Syslog when DHCP SAP has high MTS Queue Size
CSCvg61970	Tacacs Daemon process crashes due to AAA timeouts
CSCvg67835	IPSLA:sla responder memused reaching memlimit - memory not deallocated
CSCvg68573	N7K/F2 - EG recovery improvements
CSCvg70469	Drop MTS messages when DHCP SAP MTS Queue full.
CSCvg70868	Nexus 7k Sees "ipfib" Crash on N77-F348XP-23 Linecard
CSCvg92062	Post ISSU from 7.3.1 to 8.1.2 image, record templates show junk values
CSCvh02948	After VDC reloaded native vlan mapping to VNI mismatch cause traffic disruptive
CSCvh04206	Nexus 7000/7700 | 8.2(1) | Unicast broken with wccp enabled
CSCvh05330	M3-Fex: VSH crash on M3 module Tech support
CSCvh23286	cmd_exec_error when executing show tech eigrp through python interpreter
CSCvh30932	IP access list corruption after NX-OS upgrade
CSCvh32898	VRF leaking in SDA: EVPN paths' parent ECMP doesn't update on RIT moves
CSCvh62554	HSRP VIP is not reachable from Standby after ISSU between 8.x releases
CSCvh65347	LDI collision seen after sup switchover
CSCvh69235	N77 VRF stuck in 'Delete Holddown' after being deleted
CSCvh87165	Don’t set mpls-vpn flag in URIB for ipv4 LU to VRF leak
CSCvh87462	M3: Mipv6 packet dropping
CSCvh87828	lisp punt route nexthop not deleted/updated for all interfaces/routes after BGP nexthop change
CSCvi10829	var/tmp 100% full on M3 linecards due to mfib_log.txt
CSCvi11059	F2 linecard goes into a booting loop when more than 200 "vpc orphan-port suspend" are configured.
CSCvi12277	FEX power supply, fan not populated in entPhysicalTable on N7k for version 8.2(1)
CSCvi34997	N7K - XML sub agent initialization fails: xml session creation failed. Out of memory.
CSCuz92063	Two paths created from BGP peer even w/o add-path cap exchanged + bgp cores @ bgp_brib_destroy_path.

Table 54 Cisco NX-OS Release 8.2(2) Closed Caveats

Identifier	Description
CSCvh89092	N7K - adding kernel nvram-messages to show tech.
CSCvg38672	vpc self-isolation: vpc legs are up on local after all modules up when MCT down.

Resolved Caveats—Cisco NX-OS Release 8.1(2a)

Table 55 Cisco NX-OS Release 8.1(2a) Closed Caveats

Identifier	Description
CSCvh62554	HSRP VIP is not reachable from Standby after ISSU between 8.x releases.
CSCvh14951	IPv6 traffic flow blocked.
CSCvi23370	HSRP VIP resolved on stand-by is missing after SSO.
CSCvi28057	812a DCNM Failure: POAP Script execution failed.

Resolved Caveats—Cisco NX-OS Release 8.1(2)

Table 56 Cisco NX-OS Release 8.1(2) Closed Caveats

Identifier	Description
CSCuw40711	Nexus - in.dcos-telnetd service crash
CSCuw86555	ENH - N7K Silent/Unknown supervisor switchover
CSCvb74706	N7K: F3 2s convergence time on module OIR
CSCvb86787	Cisco Nexus 5K/6K/7K/9K/9500-R/MDS CLI Command Injection Vulnerability
CSCvb93995	Cisco NX-OS Software removes ACL from VTY interface
CSCvc44015	address-family ipv4 multicast path invalid in BGP but present in URIB
CSCvc56655	Nexus 7k itd NAT destination issue
CSCvc69555	Evaluation of N3K/N3500/N5K/N7K/N9K/MDS for OpenSSH vulnerability CVE-2016-10010
CSCvc71792	implement a knob to allow weak ciphers
CSCvd10140	Dynamic Mac address has wrong DI (Destination index) on M2
CSCvd72172	Evaluation of N9k/N7k/N5k/N3k/MDS for NTP March 2017
CSCvd74225	N7K/F3: Constant EOBC heartbeat failure
CSCve01811	vpc-config-sync fails with error message
CSCve06320	Netflow - netflow/nfm not responding msg stuck in MTS Buffer
CSCve07101	N7k/6.2(16) BGP not prepending as-path for certain prefixes in a prefix-list
CSCve12380	CTS commands unavailable if medium p2p configured on a port channel

Table 56 Cisco NX-OS Release 8.1(2) Closed Caveats

Identifier	Description
CSCve34578	Nexus 7000: cts hap reset on 7.3(1)D1(1) triggered when ASA failover happens
CSCve40271	N7K crashes while opening startup-config
CSCve46211	ethpcm crash when trying to allocate memory
CSCve47401	N3K/N9K/N7K OSPF Rogue LSA with maximum sequence number vulnerability
CSCve51700	Cisco FX-OS and NX-OS System Software CLI Command Injection Vulnerability
CSCve54480	ARP ACL not working on M3 card
CSCve54860	im_get_ifindex failure when creating some port-channel subinterfaces
CSCve61829	Unable to access startup config though copy run start succeeds
CSCve65582	config session pushing acls is causing fsm timeout and
CSCve66517	Memleak in URIB_SHMEM_TLV_PTR (show routing ip unicast internal mem-stats shared detail)
CSCve70348	MHBFD:HSRP vMAC being used by standby once during priority change so MH BFD sessions are flapping
CSCve78301	N7k-PI: bps rate is incorrect under type qos policy-map
CSCve78734	FHRP hello packet does not TX L3 interface
CSCve80218	ULIB process corrupted, producing route leakage between VRFs
CSCve87784	BGP Process Crash when receivng AS Path longer than 255
CSCve93651	Broken VRF Due to RD Change in BGP
CSCve99902	Cisco Nexus Series Switches CLI Command Injection Vulnerability
CSCve99925	Cisco NX-OS System Software CLI Command Injection Vulnerability
CSCvf18050	FEX: routed sub-interface stop forwarding post fex-fabric uplink reload
CSCvf29432	Cisco Nexus 7000 Series Switches Privilege Escalation via sudo
CSCvf31132	Cisco NX-OS System Software Management Interface Denial of Service Vulnerability
CSCvf33147	F3 - xbar sync failed during module bringup after upgrade N77-F312CF-26 ver 1.1
CSCvf58207	vPC+ Secondary does not suspend SVIs when Primary reachable via Fabricpath
CSCvf66000	static ARP might point to wrong physical interface
CSCvf66024	PBR programming wrong adj index when N7K up with multiple PBR configured ports
CSCvf73007	Access list is failing for SNMPv3 in N7k
CSCvf77200	n7k/l2vpn: FLUSH not requested upon DOWN->UP change
CSCvf77327	ARP Performance Improvement when ARP suppression is enabled
CSCvf87011	M3 - Ncpinfraclnt Crash

Table 56 Cisco NX-OS Release 8.1(2) Closed Caveats

Identifier	Description
CSCvg04072	Cisco NX-OS System Software Patch Installation Command Injection Vulnerability
CSCvg04455	N7K - RewriteEngineLoopback test failure does not error disable ports in non-default VDC
CSCvg10842	Input discards after issu to 7.3 or 8.x code, egress throughput reduction for F3-100gig/40gig ports.
CSCvg11502	Entering encapsulation mpls sub-menu and then exit in n7700 makes pseudowire to go down
CSCvg17452	Nexus 7k GOLF router drops packets at VXLAN encap due to incorrect egress LIF programming
CSCvg24686	SNMP v3 information leaking vulnerability
CSCvg27491	F3 module goes HW faulty when using 1Gb Transceiver
CSCvg34717	Multicast CP packets are dropped by F2/F3 module
CSCvg44947	Dropping GTP ipv6 packet
CSCvg45324	Static mac programmed as dynamic for orphan mac
CSCvg46045	Post ISSU from 7.2.2 to 7.3.2.D1.2, on collector, the flow record templates show junk values
CSCvg50660	Need Syslog when DHCP SAP has high MTS Queue Size
CSCvf36683	N7K-SUP2/E: eUSB Flash Failure or Unable to Save Configuration

Resolved Caveats—Cisco NX-OS Release 8.2(1)

Table 57 Cisco NX-OS Release 8.2(1) Closed Caveats

Identifier	Description
CSCvg10045	Vxlan fnL UI - ipfib core during ISSU from 8.1.1 to 8.2.1
CSCvf94693	8.2.1:- memory leak for ARP process
CSCvf81424	sh ip arp statistics | validate-xml shows "The output is invalid"
CSCvf83621	show ip arp suppression-cache <summary> | <statistics> shows "output is valid"
CSCvf51507	BFD neighborship does not come up with OTV site-vlan as bd
CSCvf35516	BFD session doesn't come up if the interface is configured with RACL in flexible bank chaining mode
CSCvf55349	m2 flexible bank chaining configs/feature is not getting removed while moving from 8.2.1 to 8.1.1
CSCvf17859	MKA interfaces may error disable on module reload with more than 48 P2P sessions
CSCvf85857	Bridge-domain L2vpn vfi context not deleting after no bridge-domain <id>
CSCvf00967	MTU on int pseudowire configured, but not effective

Table 57 Cisco NX-OS Release 8.2(1) Closed Caveats

Identifier	Description
CSCve90065	system switchover and LC reload, Xconnect session not come up
CSCvf77032	Few SH BFD sessions are flapping on ISSU with MH + SH BFD (echo disabled)
CSCvf42053	F3 Phy vPCs - Post fabric port-channel flap, it takes 3 mins for multicast traffic to converge
CSCvf85636	show ip igmp some option throwing an error for validate-xml option
CSCva19035	"match ipv6 multicast group-range" option not working
CSCvf66675	%PIM6-3-RWSEM_LOCK_FAIL traceback seen after VDC reload
CSCvf92758	8.2.1 S9 - Xml validation is failing for "show ip pim rp" cmd
CSCvf85600	cmd_path_get: invalid attribute index 1 component 119 for "show ip pim route | validate-xml"
CSCvf15194	ip pim state limit doesn't take effect with vrf leak
CSCvf16704	LHR takes 9 min to get converged with 2000 routes on 10 vrf
CSCvf85662	show ip mroute detail is throwing an error for validate-xml
CSCvg08603	show ip static-route multicast output not xmlised
CSCvf04475	N77/MVPN: 3 minutes mcast duplication upon PE-P link flap
CSCvf04251	N77/MVPN: unexpected mcast duplication upon reloading and restoring P router
CSCvf86088	validate-xml fails for "sh otv isis route"
CSCve84229	MKPDU is detected as "Unknown type" in ethanalyzer
CSCvf62523	Routes are stuck in RIB cleanup process due RD is down for some VRF's
CSCvf84063	lisp core on duplicate detection of multiple hosts
CSCve07881	configure replace Fails when trying to do no interface overlay 1000.
CSCvf92504	CR: IPSLA probes modification fails with DEL DB contents and with syntax error for vrf context
CSCux36446	SSTE: Vinci/Leaf: DAEMON-2-SYSTEM_MSG: fatal: login_init_entry
CSCvf80232	QSA (40G to 10G): Link comes up after multiple flaps on OIR of SFP
CSCvf85238	QSA optic: Link is up in remote side while Link is in not connected state in local
CSCve62904	CR failed with ERROR: 1 or more interfaces are from a module of type not supported by this vdc
CSCvg10842	Input discards after ISSU to Cisco NXOS 7.3 or 8.x release, egress throughput reduction for F3-100gig/40gig ports.

Resolved Caveats—Cisco NX-OS Release 8.1(1)

Table 58 Cisco NX-OS Release 8.1(1) Closed Caveats

Identifier	Description
CSCvb17981	CTS CoA ACK not sent via ip radius source-interface
CSCvc55250	RADIUS CoA ACK sent with incorrect authenticator
CSCvc46038	After Adjmgr stateful restart messages held
CSCur64880	bfd session flap after enabling BFD echo-interface on Loopback1 int
CSCvd85372	MHBFD: All MH BFD sessions flap once on rehosting via LC reload
CSCve12380	CTS commands unavailable if medium p2p configured on a port channel
CSCvd08898	Hash-algorithm HMAC-SHA-1 can't be configured on F3 linecards, after upgrading to 7.3.x
CSCvd48792	Processes should clear /var/tmp logs periodically
CSCvd51905	M3-M2 RFC2544 72 L2U port full-mesh throughput test - frame loss
CSCvd56803	M3-M2 10G Performance Issue with 256 Frame Size
CSCvd25258	Bogus DHCP GIADDR being used for DHCP Smart Relay post ISSU
CSCuy29923	Event manager configuration is out of order in start-up configuration
CSCvb28656	Puts sends output to syslog, not the controlling terminal
CSCvd38589	Empty field is seen and Mac's are not secured in Avalon image
CSCvd58766	N7k:Monitor port has VLAN membership although no config present
CSCvc78278	NXOS/ETHPM: Traffic not forwarded after port change from Channeling to Individual
CSCvd29188	Eb drop counter is showing stats doubled the real eb drops
CSCvd16811	M3 IntLoopback is not running on link down and XCVR not inserted ports
CSCvd53833	N7K: "IFTMC PD commit db search failed" error msg post ISSU to 7.2
CSCvd16210	Incorrect output structure for commands related to per vrf configuration.
CSCvc69075	MAC address mismatch between SUP and LC after a VPLS failover.
CSCvb64844	N7k/vPC+ - L2 loop cause FP core Port not copy CE MAC address
CSCvd40018	BFD packets leaving LC CPU have a vlan id of 0 when egress lookup on flanker
CSCvd70168	N77/MVPN: Mcast duplication upon clear ip route * on PE node
CSCvc62084	STP BA Inconsistent on port-channel interface when native vlan does not exist
CSCvc67913	Error: AAA authorization failed for command:show version, AAA_AUTHOR_STATUS_METHOD=16(0x10)
CSCvc42886	No SSH possible to device when root directory is full due to nxapi request
CSCvb84735	NTP sync issue with ntp distribute upon image upgrade due to incorrect vrf id
CSCvc90796	Sync with NTP servers lost intermittently
CSCvd88316	Return value is incorrect for object-tracking configuration - VTS config push will fail

Table 58 Cisco NX-OS Release 8.1(1) Closed Caveats

Identifier	Description
CSCvc65466	OTV fails to advertise mac after a mac move
CSCvc95126	High CPU caused by VSH after show tech-support issued
CSCvc04030	Setting terminal password breaks sftp/scp transfer operation on N7K
CSCvd37212	M3 vPC Scale: VSH cored after add/remove "feature vpc" and its related configurations
CSCvd17129	RBH mis programmed after removing interfaces from vpc and reusing the interface as standalone port
CSCvb93865	Nexus77: routing failover time increased 1sec after version up from 6.2(14) to 7.3(1)D1(1)
CSCvb10344	ISSU add "port-channel load-balance src-dst ip type invalid fex all" cfg
CSCvc32466	Autoconfig for DCI: VRF stuck on box after reload and add/remove triggers
CSCvc46743	N7k: Traffic from pvlan hosts blackholed when pinging primary SVI
CSCvc54555	F3: DTAG TTL 1 packets have to be rate-limited
CSCvc09777	%SYSMGR-2-VOLATILE_DB_FULL: System volatile database usage is unexpectedly high at 81%.
CSCvd86332	EIGRP routers stopped propagating default route.
CSCvd04835	Old connected route is not removed from EIGRP topology table
CSCvc81179	Nexus7k ISIS crash at txlist_tq_remove_node
CSCvc51500	LISP hand off on Nexus7K does not work in NX-OS 7.3
CSCve20025	LISP crash during vdc reload
CSCvc91548	Incorrect forwarding address is set to OSPF type-5 LSA of summarized route
CSCvc30847	OSPF LSA not withdrawn from Nexus when interface is down
CSCvd08029	SNMPD crash when RIPv2 authentication is enabled and RIPv2-MIB::rip2IfConfAuthType is being polled
CSCvc56655	Nexus 7k itd NAT destination issue
CSCvd78869	N7K10G: SMARTC crashed when ISSU from 7.3.0 to 8.1.1
CSCvb32808	statsprofiler crash with no space in sap STATSPROFILER SAP
CSCvd19647	FEX HIF VPC has STP port-type edge and bpduguard disabled on VPC secondary
CSCvb48317	N7K: Some static routes set BFD remain after disabled I/O module though BFD states have been down.
CSCvd40091	F3 FEX Scale: SNMP MIB WALK errored out "Reason: resourceUnavailable"
CSCvb65414	logging server vrf goes unknown after switchover
CSCvc57098	Syslog MTS recv_q buffer filling up when "logging source-interface" configured
CSCvd23076	TACACS crashes when buffer limit (>2072) is crossed for valid command arguments
CSCvd64752	Nexus Switch Booting In Fabricpath Mode Transit Needs To Send Notification
CSCvc46028	On N7k UDLD does not work interface is configured as promiscuous.

Table 58 Cisco NX-OS Release 8.1(1) Closed Caveats

Identifier	Description
CSCvd74634	UFDM does not download route to line card after ISSU SMU
CSCvd77099	Load sharing is not happening for OTV UDP encap traffic on F3 or M3 cards
CSCvc49851	MST instance configurations delayd to get synced or failed
CSCvb93352	N7K - Loops VTP v3 update on peer-link between vPC peers
CSCvc55528	WCCP crashed due to memory leak - WCCP_MEM_msg_control_packet
CSCvb46891	N7K CoPP: Require stats per forwarding engine for all module types
CSCvd44475	Multicast traffic loss during FP switch id change
CSCvd17080	Need to sym-link /usr/bin/python to /isan/bin/python
CSCvb86602	% Next-hop cannot be local address in same or different vrf
CSCvg10842	Input discards after ISSU to Cisco NXOS 7.3 or 8.x release, egress throughput reduction for F3-100gig/40gig ports.

Resolved Caveats—Cisco NX-OS Release 8.0(1)

Table 59 Cisco NX-OS Release 8.0(1) Closed Caveats

Identifier	Description
CSCvb84395	CTS: M3 module failure with log enabled deny policies
CSCvc07445	RISE ISCM CLIs changed to SC_ENGINE
CSCuz60225	Special Characters are not handled by NXAPI
CSCuz82684	aclqos crash on large acl with scale object groups
CSCuw03713	N7K: Layer 2 (L2) packet not dropped on length mismatch
CSCvb40562	N7K: F3 module crash in ncpinfraclnt service during FIB update
CSCvc10229	ISSU to 801 should be blocked if RISE feature is configured
CSCvb95725	AdjMgr crash during stress from ARP
CSCux97309	SSTE: [Longevity2] CFS MTS buffer leak
CSCva84959	F2 1G port fails to recover after remote end comes back up
CSCuy02586	vPC+ both switches learn mac address on peer-link on receiving garp
CSCuz10518	Nexus got dot1x hap reset
CSCut94161	EEM: Configuration failed with: 0x412c000d validation timed out
CSCvb14045	DNL bit cleared on Port-Security port-channel after member into initial
CSCuf47376	Trunk/FEX FPC port config removed by "system def switchport fabricpath"
CSCva16707	F3 - static MAC programmed for TCAM Bucket0
CSCva66159	debounce timer not honored for 1G/SGMII mode on 10/1 F3 module
CSCva63984	F3: Port stuck in 10G mode when QSFP w/ breakout is removed before conf
CSCuy82996	N7k F3 40gig fex fabric links flap continuously to FEX 2348UPQ
CSCvb23556	MDSNG : callhome crashed sig6 while replaying configs

Identifier	Description
CSCuu64415	hmm crash after removing vlan on peer link from suspended
CSCva94583	FP: Anycast HSRP stuck in Init state after VDC reload
CSCvb39993	n7k/hsrp anycast: incorrect active hold timer after timer config change
CSCva16041	N7K: HSRP holdtimer doesn't reset when receiving HSRP hello
CSCva24715	Nexus Anycast HSRP crashes when VLAN string is more than 1000
CSCva74462	N7K w/ Sup 2 Engine Incorrectly Punts MPLS Traffic to Control Plane
CSCvb26949	DFA auto-config profile refresh failure due to IPv6 address change
CSCvb27539	Nexus 7004 6.2.14 IPv6 connected L3 interface not showing up in RIB
CSCus83776	ITD: Can't advertise the route for VIP
CSCva11756	vPC+: Wrong ESDB info due to changing port-channels having VPC's
CSCva13788	post ISSU, bfdc crashed due session data structure corruption
CSCuz75979	N7k interface counters are not being updated.
CSCvb12189	SNMP Timeout Requesting lldpRemManAddrOID on Certain Interfaces
CSCvb30818	IGMP Snooping Mrouter port state is not synced during bootup in VPC
CSCvb61043	vPC Auto-recovery doesnt kick-in after reload with keep-alive down
CSCuz53597	N7K does not advertise implicit-null label as an Edge-LSR should do
CSCvb31890	Tracebacks on MPLS TE
CSCuy62745	Master Bug to port fix for 2348 Issues from N5k to N7k,N9k
CSCuy14606	enhance system internal mem for sysmgr @ LC level
CSCuu15632	Invalid PI error, configuring static nat without carving Tcam for NAT
CSCuy04933	Wrong timestamps in netflow data
CSCva81638	N7K Netflow F3/M3: Rate limiter default value incorrectly programmed
CSCvb17413	Unable to access NXAPI Sandbox(Non-default VDC) as VDC-Admin
CSCuz44147	Evaluation of N9k/N7k/N5k/N3k/MDS for NTP April 2016 CVEs
CSCux95101	Evaluation of N9k/N7k/N5k/N3k/MDS for NTP January 2016 CVEs
CSCuz92661	Evaluation of N9k/N7k/N5k/N3k/MDS for NTP June 2016 CVEs
CSCuw84708	Evaluation of N9k/N7k/N5k/N3k/MDS for NTP October 2015 CVEs
CSCvb02494	N7K OTV with BFD configured / BFD Session Flaps on System Switchover
CSCuh22289	N7k Enh: "terminal log-all" functionality should be default
CSCva25803	NX-OS route-map fails to parse v4-mapped IPv6 address
CSCuz98928	NX-OS: pipe not recognized as special character by 'exclude' cli filter
CSCvb31113	N7K PTP Process crash with NULL pointer mts_wrap_p
CSCva61554	aclqos crash due to port configuration default dscp one-to-one mapping
CSCvb49085	n7k M3: Shaping policy causes interfaces to go to suspended state and IntPortloopback to fail
CSCux77223	bestpath run in vrf - route gets deleted
CSCvb44776	BGP crashes due heartbeat failure after asserts
CSCvb14569	frequent no rd and rd config can get vrf stuck in down state

Identifier	Description
CSCva79760	IPV6 link local only BGP peering leads to installing wrong adjcaency
CSCuu06829	SUP switchover causes duplicate connection on switchover device
CSCuy07502	In show running, ffff is missing from the v4 mapped v6 address.
CSCuu78729	EIGRP can install non-successor to RIB in case of ECMP paths
CSCvb99376	N7K send Candidate Default bit in the EIGRP update
CSCva83066	Eigrp loop, route not flushed from topology table
CSCuy77045	configuring "mpls ldp sync" removes "mpls traffic-eng router-id" command
CSCuz67595	Incorect IGP metric calculation for ISIS
CSCuy99477	Change metrictype of redistributed routes from MPBGP-OSPF from E2 to E1
CSCuv66399	Forwarding address not set in OSPF for routes w/ different prefix length
CSCux69728	LSA stuck in DB
CSCuw03410	Nexus 6.2.x OSPF taking long time in LSA generation
CSCvb16035	NxOS ABR in OSPF totally stubby area does not originate default LSA
CSCuz18971	old/inactive area-ids are not cleared from the ospf db
CSCut11150	OSPF max-metric doesn't work when startup timer value is default
CSCuv81861	OSPF NSSA sending type 7 LSA after converted to regular area
CSCuw27044	OSPFv3 takes 30 min to install route when using link-local addresses
CSCvb06742	OTV SAP ignores MTS high water mark warnings
CSCuy89746	OTV VDC crashes after remote command "reload ascii"
CSCuz51928	icmpv6 crashes because of access to a non-readable memory region.
CSCva11364	ARP hap rest
CSCux63096	CSCuw89606 and CSCut84448
CSCuq72316	N7K:Static route leak w/ unconfig/config SVIs cause traffic black hole
CSCuz55002	BGP table with no nexthop when nexthop learnt thro LU
CSCuu35152	URIB service crash on N7K running 5.2(9)
CSCut46704	vman service may crash unexpectedly
CSCvb48568	Evaluation of N9k/N7k/N5k/N3k/MDS for OpenSSL September 2016 CVEs
CSCuy78340	IP SLA udp jitter v2 time out when no timestamp from netstack
CSCuz46882	rttMonEchoAdminTargetAddress not responding if part of address is zero
CSCuy19010	SNMPd causes boot loop after reload with unload-MIB configuration
CSCuw76278	NX-OS - Netstack panic crash due to buffer lockup
CSCva60566	conflicting features not prevented with bank mapping enabled
CSCuv70053	Mode access interface on AA FEX inactive after reload vPC primary
CSCus61633	N7000 ACLs are not case sensitive
CSCvb76929	N7k: ACL's are not programmed into tcam
CSCvb71127	N7K LC fail to boot up due to "LC insertion sequence failure"
CSCuz91706	Username limited to 28 characters causes issue for vmtracker feature

Identifier	Description
CSCvb04007	FEX A/A: Convergence takes 5-6 secs on FPC secondary "no shut"
CSCvb79120	N7k/2348UPQ: packet incorrectly forwarded out of HIF ports on port flap
CSCva90035	VRRP VIP not Programmed
CSCva72823	VTP type-2 configuration incompatible on VTPV2_VPC Regression
CSCvc18137	MPLS TE: ipfib crash after forwarding restart

Upgrade and Downgrade

To perform a software upgrade or downgrade, follow the instructions in the Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 8(x). For information about an In Service Software Upgrade (ISSU), see
https://www.cisco.com/c/dam/en/us/td/docs/dcn/tools/nexus-7k-issu-matrix/index.html

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:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/7_x/epld/epld_rn_72.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.