Cisco Nexus 7000 Series NX-OS 8.3, Release Notes

Modified Date: July 02, 2021
Current Release: 8.3(2)

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 68.

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
December 02, 2021	Added Cisco NX-OS Release 8.2(8) to the " Upgrade and Downgrade Paths and Caveats" section.
July 02, 2021	Added Cisco NX-OS Release 7.3(8)D1(1) to the " Upgrade and Downgrade Paths and Caveats" section.
June 25, 2021	Added Cisco NX-OS Release 8.2(7a) to the " Upgrade and Downgrade Paths and Caveats" section.
January 08, 2021	Added Cisco NX-OS Release 7.3(7)D1(1) to the " Upgrade and Downgrade Paths and Caveats" section.

Cisco Systems, Inc.
www.cisco.com

Table 1 Change History (continued)

Date	Description
October 06, 2020	Added N77-F312CK-26 to the "Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switches Hardware Support" table.
July 24, 2020	Added Cisco NX-OS Release 8.2(6) to the " Upgrade and Downgrade Paths and Caveats" section.
April 17, 2020	Added Cisco NX-OS Release 7.3(6)D1(1) to the " Upgrade and Downgrade Paths and Caveats" section.
November 15, 2019	Updated the " Upgrade and Downgrade Paths and Caveats" section to include Cisco NX-OS Release 8.2(5) and Cisco NX-OS Release 7.3(5)D1(3).
March 28, 2019	Updated the " Supported Device Hardware" section to include F4 Series Module details.
December 17, 2018	Created release notes for Cisco NX-OS Release 8.3(2).
November 2, 2018	Updated the " Upgrade and Downgrade Paths and Caveats" section to include Cisco NX-OS Release 7.3(3)D1(3).
September 26, 2018	Updated the " Upgrade and Downgrade Paths and Caveats" section to include Cisco NX-OS Release 7.3(2)D1(3a).
July 5, 2018	Created release notes for Cisco NX-OS Release 8.3(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

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)
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)

Table 2 Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switches Hardware Support (continued)

Product ID	Hardware	Minimum Software Release
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)
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)

Table 2 Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switches Hardware Support (continued)

Product ID	Hardware	Minimum Software Release
N7K-SUP2E	Supervisor 2 Enhanced module	6.1(1)
Cisco Nexus 7700 Series Hardware		
N77-AC-3KW	Cisco Nexus 7700 AC power supply	6.2(2)
N77-C7702	Cisco Nexus 7702 chassis	7.2(0)D1(1)
N77-C7702-FAN	Fan, Cisco Nexus 7702 chassis	7.2(0)D1(1)
N77-C7706	Cisco Nexus 7706 chassis	6.2(6)
N77-C7706-FAB-2	Fabric Module, Cisco Nexus 7706 chassis	6.2(6)
N77-C7706-FAB-3	Fabric Module, Cisco Nexus 7706 chassis	8.3(1)
N77-C7706-FAN	Fan, Cisco Nexus 7706 chassis	6.2(6)
N77-C7706-FAN-2	Generation 2 Fan Tray, Cisco Nexus 7706 Chassis	8.1(1)
N77-C7710	Cisco Nexus 7710 chassis	6.2(2)
N77-C7710-FAB-2	Fabric Module, Cisco Nexus 7710 chassis	6.2(2)
N77-C7710-FAB-3	Fabric Module, Cisco Nexus 7710 chassis	8.3(1)
N77-C7710-FAN	Fan, Cisco Nexus 7710 chassis	6.2(2)
N77-C7710-FAN-2	Fan, Cisco Nexus 7710 chassis	8.1(1)
N77-C7718	Cisco Nexus 7718 chassis	6.2(2)
N77-C7718-FAB-2	Fabric Module, Cisco Nexus 7718 chassis	6.2(2)
N77-C7718-FAN	Fan, Cisco Nexus 7718 chassis	6.2(2)
N77-C7718-FAN-2	Fan, Cisco Nexus 7718 chassis	8.1(1)
N77-DC-3KW	Cisco Nexus 7700 DC power supply	6.2(2)
N77-F248XP-23E	Cisco Nexus 7700 Enhanced 48-port 1/10 Gigabit Ethernet SFP+ I/O module (F2E Series)	6.2(2)
N77-F312CK-26	Cisco Nexus 7700 12-port 100-Gigabit Ethernet CPAK I/O module (F3 Series)	7.3(2)D1(1)
N77-F324FQ-25	Cisco Nexus 7700 24-port 40-Gigabit Ethernet QSFP+ I/O module (F3 Series)	6.2(6)
N77-F348XP-23	Cisco Nexus 7700 48-port 1/10-Gigabit Ethernet SFP+ I/O module (F3 Series)	6.2(6)
N77-F430CQ-36	Cisco Nexus 7700 F4-Series 30-port 100-Gigabit Ethernet I/O module	8.3(1)
N77-HV-3.5KW	3.5KW High Voltage Power Supply Unit	7.3(0)D1(1)
N77-M312CQ-26L	12-Port 100-Gigabit Ethernet (M3 Series)	8.0(1)
N77-M348XP-23L	48-port 1/10-Gigabit Ethernet SFP+ I/O module (M3 series)	7.3(0)DX(1)

Table 2 Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switches Hardware Support (continued)

Product ID	Hardware	Minimum Software Release
N77-M324FQ-25L	24-port 40-Gigabit Ethernet QSFP+ I/O module (M3 series)	7.3(0)DX(1)
N77-SUP2E	Cisco Nexus 7700 Supervisor 2 Enhanced module	6.2(2)
N77-SUP3E	Cisco Nexus 7700 Supervisor 3 Enhanced module	8.3(1)

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

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

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

Cisco Nexus 7000 Series Module	FEX Module	Minimum Software Release
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)
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)

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

Cisco Nexus 7000 Series Module	FEX Module	Minimum Software Release
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		
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)

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

Cisco Nexus 7000 Series Module	FEX Module	Minimum Software Release
24-port Cisco Nexus 7700 F3 Series 40-Gigabit Ethernet QSFP I/O module (N77-F324FQ-25)	N2K-C2224TP-1GE	6.2(8)
	N2K-C2248TP-1GE	
	N2K-C2232PP-10GE	
	N2K-C2232TM	
	N2K-C2248TP-E	
	N2K-C2232TM-E	
	N2K-C2248PQ	
	N2K-B22HP[2]	
	N2K-C2348UPQ	7.2(0)D1(1)
	N2K-C2348TQ	
	N2K-B22IBM	
	N2K-C2332TQ	8.1(1)
	N2k-C2348TQ-E	8.2(1)
	N2K-B22DELL-P	
48-port Cisco Nexus 7700 F3 Series 1/10-Gigabit Ethernet SFP+ I/O module (N77-F348XP-23)	N2K-C2224TP-1GE	6.2(6)
	N2K-C2248TP-1GE	
	N2K-C2232PP-10GE	
	N2K-C2232TM	
	N2K-C2248TP-E	
	N2K-C2232TM-E	
	N2K-C2248PQ	
	N2K-B22HP	
	N2K-C2348UPQ	7.2(0)D1(1)
	N2K-C2348TQ	
	N2K-B22IBM	
	N2K-C2332TQ	8.1(1)
	N2k-C2348TQ-E	8.2(1)
	N2K-B22DELL-P	

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 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)

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

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

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
N77-F324FQ-25	CVR-QSFP-SFP10G (Only version V02 of the CVR-QSFP-SFP10G module is supported.)	QSFP 40G to SFP+ 10G Adapter Module	8.2(1)
	CVR-QSFP-SFP10G (This is supported only on F3 40G I/O modules with SFP-10G-SR or SFP-10G-SR-S optics. If the F3 I/O module is reloaded, the ports containing the CVR-QSFP-SFP10G adapter may remain down even after the F3 I/O module comes back up. If so, the CVR-QSFP-SFP10G adapter must be reseated.) (Only version V02 of the CVR-QSFP-SFP10G module is supported.)	Cisco 40G QSFP	6.2(14)
	QSFP-40G-SR-BD	Cisco 40G BiDi QSFP+	6.2(6)
	QSFP-40G-SR4 QSFP-40G-SR4-S	40GBASE-SR4 QSFP+	6.2(6)
	QSFP-40G-CSR4	40GBASE-CSR4 QSFP+	6.2(6)
	QSFP-40GE-LR4 QSFP-40G-LR4-S	40GBASE-LR4 QSFP+	6.2(6)
	FET-40G	Cisco 40G Fabric Extender Transceiver (FET)	6.2(8)
	QSFP-H40G-ACUxM	40GBASE-CR4 QSFP+ Direct Attach Copper Cable Active (7 m, 10 m)	6.2(8)
	QSFP-4X10G-ACxM	40GBASE-CR4 QSFP+ to 4x SFP+ Twinax Direct Attach Copper Breakout Cable Active (7 m, 10 m)	6.2(8)
	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)

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

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

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	GLC-LH-SMD	1000BASE-LX/LH SFP	6.2(8)
	GLC-SX-MM	1000BASE-SX SFP	6.2(8)
	GLC-SX-MMD	1000BASE-SX SFP	6.2(8)
	GLC-ZX-SM	1000BASE-ZX SFP	6.2(8)
	GLC-ZX-SMD	1000BASE-ZX SFP	6.2(8)
	GLC-T	1000BASE-T SFP	6.2(8)
	GLC-BX-D	1000BASE-BX10-D	6.2(8)
	GLC-BX-U	1000BASE-BX10-U	6.2(8)
	GLC-EX-SMD	1000BASE-EX SFP	6.2(8)
	FET-10G	Cisco Fabric Extender Transceiver (FET)	6.2(8)
N77-F430CQ-36	QSFP-100G-SR4-S	Multi-mode fiber (MMF)	8.3(1)
	QSFP-40G-CSR4 QSFP-40G-SR4 QSFP-40G-SR4-S QSFP-40G-SR-BD QSFP-40G-BD-RX QSFP-40/100-SRBD	Multi-mode fiber (MMF)	8.3(2)
	QSFP-100G-CWDM4-S QSFP-100G-PSM4-S QSFP-100G-LR4-S	Single-mode fiber (SMF)	8.3(1)
	QSFP-40G-ER4 QSFP-40G-LR4	Single-mode fiber (SMF)	8.3(2)
	QSFP-100G-AOC1M QSFP-100G-AOC2M QSFP-100G-AOC3M QSFP-100G-AOC5M QSFP-100G-AOC7M QSFP-100G-AOC10M QSFP-100G-AOC15M QSFP-100G-AOC20M QSFP-100G-AOC25M QSFP-100G-AOC30M	Active optical cable assembly	8.3(1)

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

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

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)
N7K-F348XP-25	CWDM-SFP-xxxx[2]	1000BASE-CWDM	6.2(12)
	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)

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(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)
	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)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	SFP-10G-LR SFP-10G-LR-S	10GBASE-LR SFP+	6.0(1)
	SFP-10G-ER SFP-10G-ER-S	10GBASE-ER SFP+	6.0(1)
	SFP-10G-LRM	10GBASE-LRM SFP+	6.0(1)
	SFP-10G-ZR [2] SFP-10G-ZR-S	10GBASE-ZR SFP+	6.1(1)
	SFP-10G-AOCxM	10GBASE-AOC (Active Optical Cable) SFP+ Cable (1 m, 2 m, 3 m, 5 m, 7 m, 10 m)	6.2(2)
	SFP-H10GB-CUxM	SFP-H10GB-CUxM Twinax Cable Passive (1 m, 3 m, 5 m)	6.0(1)
	SFP-H10GB-CUxM	SFP-H10GC-CUxM Twinax Cable Passive (1.5 m, 2 m, 2.5 m)	6.2(2)
	SFP-H10GB-ACUxM	SFP-H10GB-ACUxM Twinax Cable Active (7 m, 10 m)	6.0(1)
	SFP-GE-T	1000BASE-T SFP	6.0(1)
	SFP-GE-S	1000BASE-SX SFP (DOM)	6.0(1)
	SFP-GE-L	1000BASE-LX/LH SFP (DOM)	6.0(1)
	SFP-GE-Z	1000BASE-ZX SFP (DOM)	6.0(1)
	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)

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

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

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

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

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

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

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

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

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	QSFP-H40G-ACU7M QSFP-H40G-ACU10M	Direct attach copper, active	8.0(1)
	QSFP-100G-AOC1M QSFP-100G-AOC2M QSFP-100G-AOC3M QSFP-100G-AOC5M QSFP-100G-AOC7M QSFP-100G-AOC10M QSFP-100G-AOC15M QSFP-100G-AOC20M QSFP-100G-AOC25M QSFP-100G-AOC30M QSFP-H40G-AOC1M QSFP-H40G-AOC2M QSFP-H40G-AOC3M QSFP-H40G-AOC5M QSFP-H40G-AOC7M QSFP-H40G-AOC10M QSFP-H40G-AOC15M	Active optical cable assembly	8.0(1)
	WSP-Q40G-LR4L	40GBASE-LR4 QSFP40G (for Single-mode Fiber (SMF))	8.0(1)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[1]Minimum version supported is -02.

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

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

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

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

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

Guidelines and Limitations

This section includes the following topics:

Guidelines and Limitations—Cisco NX-OS Release 8.3(2)

This section describes the guidelines and limitations for the Cisco Nexus 7000 Series in Cisco NX-OS Release 8.3(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 8.3(1)

This section describes the guidelines and limitations for the Cisco Nexus 7000 Series in Cisco NX-OS Release 8.3(1).

- The new hardware introduced in Cisco NX-OS Release 8.3(1) as mentioned in the New Hardware - Cisco NX-OS Release 8.3(1) section will have feature parity in general with Cisco NX-OS Release 8.1(2).
- The new hardware will also support the following features which was introduced in Cisco NX-OS Release 8.2(1):
  - vPC Peer Keep Alive IPv6 Support
  - iCAM Enhancements
  - OTV Scale Enhancements - F4 parity with F3 (Refer to Cisco Nexus 7000 Series NX-OS Verified Scalability Guide)
- FEX and Breakout will not be supported in the new hardware, F4-Series 30-port 100-Gigabit Ethernet I/O module (N77-F430CQ-36).

Note For EPLDs available for Cisco NX-OS Release 8.3(1), see EPLDs Available for Release 8.x section in the Cisco Nexus 7000 Series FPGA/EPLD Upgrade Release Notes, Release 8.x.

- There are no updates in Nexus 7000 Sup2 EPLD images. Hence n7000-s2-epld.8.3.1.img is not posted to https://www.cisco.com.

- If you decide to upgrade EPLD anyway, or it is determined necessary in your environment, then the following guidelines should be followed.

- For Cisco NX-OS Release 6.2(10) and later releases it is recommended to perform EPLD upgrade with the current image before upgrading to Cisco NX-OS Release 8.3(1).

- For releases prior to Cisco NX-OS Release 6.2(10), you need to first upgrade to Cisco NX-OS Release

6.2(10) or later releases and perform EPLD upgrade with the current image before upgrading to Cisco NX-OS Release 8.3(1).

- The above guidelines and limitations do not apply to the Nexus 7700 series switches, and their EPLD can be upgraded through the standard process if needed.

Please see CSCvk35999 under the Open Caveats—Cisco NX-OS Release 8.3(1), page 57 for more details.

- Beginning with Cisco NX-OS Release 8.3(1), the default value for the SNMP cache expiry timeout is changed from 50 seconds to 140 seconds.
- If a Supervisor 3 module continuously receive FCoE packets at a high rate (for example, 64K pps); it might result in cpuhog/kernel-panic/reload. This is applicable to Cisco Nexus 77xx Series in Cisco NX-OS Release 8.3(1) and later releases.

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

- 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.

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

- 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 Common for Cisco NX-OS Release 8.x

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

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

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

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

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

VXLAN BGP EVPN in VDCs having M3 modules

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

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

EVPN Border Leaf Hand Off Limitation in M3 Module

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

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

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

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

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

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

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

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

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

Native VLAN Change Causes Link Flap

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

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

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

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

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

– N7K-M206FQ-23L

– N7K-F312FQ-25

– N77-F324FQ-25

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

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

– N7K-M324FQ-25L

– N77-M324FQ-25L

– N77-M312CQ-26L

MPLS over GRE

MPLS over GRE is not supported on F3 modules.

VLAN Translation on Fabric Extender Is Not Supported

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

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

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

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

This applies only to the Cisco Nexus 7700 Series switches.

Saving VLAN Configuration Information

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

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

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

3. Reload the switch.

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

Behavior of Control Plane Packets in an F2e Series Module

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

Error Appears When Copying a File to the Running Configuration

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

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

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

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

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

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

PONG in a vPC Environment

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

- In a vPC environment, a PONG to an access switch or from an access switch might fail. To work around this issue, use the interface option while executing a PONG from an access switch to a vPC peer. The interface can be one that does not have to go over the peer link, such as an interface that is directly connected to the primary switch.
- When FabricPath is enabled and there are two parallel links on an F2 Series module, PONG might fail. To work around this issue, form a port channel with the two links as members.

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

LISP Traffic

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

Standby Supervisor Might Reset with a Feature-Set Operation

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

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

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

Unfair Traffic Distribution for Flood Traffic

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

BFD Not Supported on the MTI Interface

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

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

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

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

Role-Based Access Control

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

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

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

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

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

Network Analysis Module (NAM-NX1)

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

SVI Statistics on an F2 Series Module

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

TrustSec SGT on the F3 Series Modules

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

Fabric Module Removal on the Cisco Nexus 7700 Switches

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

Fabric Utilization on the Cisco Nexus 7700 Switches

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

MTU Changes do not Take Effect on FEX Queues

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

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

Multicast Traffic is Forwarded to FEX Ports

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

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

F2 Connectivity Restrictions on Connecting Ports to an FEX

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

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

DHCP Snooping and vPC+ FEX

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

Upgrade and Downgrade Paths and Caveats

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

Supported Upgrade and Downgrade Paths

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

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

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

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

Note For a nondisruptive upgrade dual supervisor modules are required.

ISSU Paths for Cisco NX-OS Release 8.3(2)

See Table 5 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.3(2).

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

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 8.3(1)

See Table 6 for the In-Service Software Upgrade (ISSU) paths for Cisco NX-OS Release 8.3(1).

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

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 Upgrade

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

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

In-Service Software Upgrade (ISSU) Caveats

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

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

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

Checking dynamic incompatibilities for vdc 'switch':
```

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

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

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

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

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

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

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

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

Non-ISSU Upgrade/Cold Boot Upgrade

Table 7 Supported Cold Boot Matrix in Cisco NX-OS Release 8.3(2)

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

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 6 and Table 7 follow these steps:

1. Change the boot variable, as shown here:

   Example for Cisco NX-OS Release 8.3(1)

```
boot kickstart bootflash:/n7000-s2-kickstart.8.3.1.bin sup-2
boot system bootflash:/n7000-s2-dk9.8.3.1.bin sup-2
boot kickstart bootflash:/n7000-s2-kickstart.8.3.1.bin sup-2e
boot system bootflash:/n7000-s2-dk9.8.3.1.bin sup-2e
```

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

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

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

Feature Support:

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

Unsupported Modules:

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

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

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

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

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

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

ASCII Configuration Replay

Saving VLAN Configuration Information:

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

The following steps list the workaround for this limitation:

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

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

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

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

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

The following steps list the workaround for this limitation:

- Manually enter the **rebind interfaces** command wherever needed to the ASCII configuration file for replay.

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

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

Non-ISSU/Cold Boot Downgrade

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

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

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

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

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

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

Erasable Programmable Logic Device Images

Cisco NX-OS Release 8.3(2) includes the following Erasable Programmable Logic Device (EPLD) images:

- n7700-s2-epld.8.3.2.img
- n7700-s3-epld.8.3.2.img

Table 9 Supported Modules with the FPGA in Cisco NX-OS Releases 8.3(2)

Module	FPGA Type	Version
Cisco Nexus 7000 Supervisor 2	PMFPGA	37.000
	IOFPGA	1.013
Cisco Nexus 7700 Supervisor 2E	PMFPGA	20.000
Cisco Nexus 7700 Switch Supervisor 3 Enhanced Module	PMFPGA	0.14
Fan-10 slot chassis (Cisco Nexus 7000 Series)	FAN	0.007
Fan-18 slot chassis (Cisco Nexus 7000 Series)	FAN	0.002
Fan-9 slot chassis (Cisco Nexus 7000 Series)	FAN	0.009
Fan-4 slot chassis (Cisco Nexus 7000 Series)	FAN	0.005
Fan-18 slot chassis (Cisco Nexus 7700 Series)	FAN	0.006
Fan-10 slot chassis (Cisco Nexus 7700 Series)	FAN	0.006
Fan-6 slot chassis (Cisco Nexus 7700 Series)	FAN	0.006
Fan-2 slot chassis (Cisco Nexus 7700 Series)	FAN	0.016
9 slot chassis (N7K:FAB2-7009)	PMFPGA	1.003
10 slot chassis (N7K:FAB2-7010)	PMFPGA	0.007
18 slot chassis (N7K:FAB2-7018)	PMFPGA	0.007
6 slot chassis (N77:FAB2-7706)	PMFPGA	1.002
10 slot chassis (N77:FAB2-7710)	PMFPGA	1.003
18 slot chassis (N77:FAB2-7718)	PMFPGA	1.002
6 slot chassis (N77:FAB3-7706)	PMFPGA	0.008
10 slot chassis (N77:FAB3-7710)	PMFPGA	0.007
N7K:M2-10	PMFPGA	1.006
	IOFPGA	1.003
	SFPFPGA	1.003
	EARL (Forwarding Engine)	2.012
N7K:M2-40	PMFPGA	1.006
	IOFPGA	0.012
	SFPFPGA	2.008
	EARL (Forwarding Engine)	2.012
N7K:M2-100	PMFPGA	1.007
	IOFPGA	0.009
	SFPFPGA	0.004
	EARL (Forwarding Engine)	2.012

Table 9 Supported Modules with the FPGA in Cisco NX-OS Releases 8.3(2) (continued)

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

Cisco NX-OS Release 8.3(1) includes the following Erasable Programmable Logic Device (EPLD) images:

- n7700-s2-epld.8.3.1.img
- n7700-s3-epld.8.3.1.img

Table 9 shows the modules that are supported in Cisco NX-OS Release 8.3(1):

Table 10 Supported Modules with the FPGA in Cisco NX-OS Releases 8.3(1)

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
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	0.008
10 slot chassis (N77:FAB3-7710)	PMFPGA	0.007
N7K:M2-10	PMFPGA	1.006
	IOFPGA	1.003
	SFPFPGA	1.003
	EARL (Forwarding Engine)	2.012
N7K:M2-40	PMFPGA	1.006
	IOFPGA	0.012
	SFPFPGA	2.008
	EARL (Forwarding Engine)	2.012
N7K:M2-100	PMFPGA	1.007
	IOFPGA	0.009
	SFPFPGA	0.004
	EARL (Forwarding Engine)	2.012

Table 10 Supported Modules with the FPGA in Cisco NX-OS Releases 8.3(1) (continued)

Module	FPGA Type	Version
N7K:F2E-10	PMFPGA	1.009
	IOFPGA	0.016
N77:F2E-10	PMFPGA	0.006
	IOFPGA	0.005
N7K:F3-10	PMFPGA	1.000
	IOFPGA	1.003
	SFPFPGA	1.002
N7K:F3-40	PMFPGA	2.003
	IOFPGA	1.005
N7K:F3-100	PMFPGA	2.003
	IOFPGA	1.004
N77:F3-10	PMFPGA	1.007
	IOFPGA	0.031
	SFPFPGA	1.003
N77:F3-40	PMFPGA	1.005
	IOFPGA	0.031
N77:F3-100	PMFPGA	1.008
	IOFPGA	0.021
N77:F4-100	PMFPGA	0.012
	IOFPGA	1.003
	SFPFPGA	0.006
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 - Cisco NX-OS Release 8.3(2)

Starting from Cisco NX-OS Release 8.3(2), the Cisco Nexus 7700 F4-Series 30-port 100-Gigabit Ethernet I/O module (N77-F430CQ-36) supports 40-Gigabit Ethernet link also. For detailed information about the hardware, see the *Cisco Nexus 7000 Series Hardware Installation and Reference Guide*.

New Hardware - Cisco NX-OS Release 8.3(1)

This section briefly describes the new hardware and hardware enhancements introduced in Cisco NX-OS Release 8.3(1). For detailed information about the new hardware, see the *Cisco Nexus 7000 Series Hardware Installation and Reference Guide*.

- Cisco Nexus 7700 F4-Series 30-port 100-Gigabit Ethernet I/O module (N77-F430CQ-36)
- Cisco Nexus 7706 Fabric Module-3 (N77-C7706-FAB-3)
- Cisco Nexus 7710 Fabric Module-3 (N77-C7710-FAB-3)
- Cisco Nexus 7700 Series Supervisor Module (N77-SUP3E)

New and Enhanced Software Features - Cisco NX-OS Release 8.3(1)

Proportional Multipath for VNF

The Proportional Multipath for VNF feature enables advertising of all the available next hops to a given destination network. This feature enables the switch to consider all paths to a given route as equal cost multipath (ECMP) allowing the traffic to be forwarded using all the available links stretched across multiple ToRs.

MPLS over GRE

The MPLS over GRE feature provides a mechanism for tunneling Multiprotocol Label Switching (MPLS) packets over a non-MPLS network. Starting from Cisco NX-OS Release 8.3(1), MPLS over GRE is supported on M3-Series I/O modules.

ITD Fail Action Feature Enhancement

Starting from Cisco NX-OS Release 8.3(1), the ITD fail action feature is enhanced to optimally pre-fetch the status of the service nodes before reassigning the failed node's buckets to the next available active nodes. When a node is down, instead of assigning it to the next available active node, the pre-fetch optimization internally fetches the status of all the available nodes and then reassigns the failed node to an active node. Similarly, in a least bucket node fail reassignment, the pre-fetch optimization fetches the status of all the nodes before reassigning the failed node buckets to the least bucketed node.

Prior to Cisco NX-OS Release 8.3(1), when the node is down, the bucket associated with the node is reassigned to the first active node found in the configured set of nodes. If the newly reassigned node also fails, the traffic bucket is reassigned to the next available active node. The reassignment is done in a round robin fashion across nodes. The delay in reassigning the failed node bucket to an active node impacts the network performance.

Currently, the pre-fetch optimization is enabled for failaction node least-bucket and failaction node per-bucket features.

Non-standard Ethernet Type and DMAC Support for MACsec

Starting from Cisco NX-OS Release 8.3(1), Cisco enables networks with WAN MACsec to change the EAPoL destination address, and Ethernet type values to non-standard values. The EAPoL destination Ethernet type can be changed to an alternate value from the default Ethernet type of 0x88E5, or the EAPoL destination MAC address can be changed to an alternate value from the default DMAC of 01:80:C2:00:00:03, to avoid being consumed by a provider bridge.

Redistribution of RIB Routes into LISP

Starting with Cisco NX-OS 8.3(1), the Locator ID Separation Protocol (LISP) supports the redistribution of RIB routes into the LISP feature. This feature allows LISP to import Layer 3 RIB routes in use for internal applications. Importing information from the RIBs allows for proactive learning of LISP prefixes in the control plane. This eliminates the need to statically specify prefixes to be used for map-caches or databases in LISP.

LISP Extranets

With the LISP Extranets feature, users can specify policies that allow host and resources residing in one VRF (IID) domain to communicate with hosts in a separate VRF (IID) domain.

With LISP Extranets, policies are specified in the Mapping System and the xTRs (Ingress Tunnel Router + Egress Tunnel Router) discover the leaked routes on demand, as part of the regular route discovery process.

The implementation of LISP Extranets on LISP includes the following features:

- A Map Server (MS) device running Cisco IOS XE Everest 16.9.1 release or later, where the user can establish LISP Extranet policies.
- A VRF with valid LISP instance-ID configuration that can be configured to handle leaked map-caches in LISP. This support is automatically provided on LISP from Cisco NX-OS Release 8.3(1) and later.

TWAMP Responder

The TWAMP responder feature enables you to configure the TWAMP server and the session-reflector on a Cisco device for measuring the round-trip performance between an IP SLAs TWAMP responder and a non-Cisco TWAMP control device in your network.

Streaming Telemetry

Telemetry enables a push model for continuously streaming data from the show commands that are XMLized.

40G Breakout Support on N77-M312CQ-26L

N77-M312CQ-26L supports 100G and 40G. 4x10G breakout port is supported in 40G mode, similar to breakout feature in N77-F324FQ-25 / N77-M324FQ-25L.

DPT Parity with F4 Series Modules

Starting from Cisco NX-OS Release 8.3(1), the Distributed Packet Tracer (DPT) feature is supported on the F4 series modules.

Scale Enhancements

Cisco NX-OS Release 8.3(1) has the following scale enhancements:

ARP PPS Scale Upliftment

- Number of ARP packets per second - 3000 PPS
- Number of ARP glean packets for second - 2500 PPS

The default COPP limit for ARP is unchanged. To achieve 3000 ARP PPS with a single module, ARP COPP needs to be changed accordingly. As the COPP is applied at the module, this 3000 PPS can be achieved with multiple modules with the default COPP limits. 3000 ARP PPS is system-level supported PPS.

M3 ACL Label scale for M3 module

- For Non L4OP ACL - 4000 labels
- For L4OP ACL /IPV6 ACL - 2000 labels

FIB Scale on M3

Total number of FIB entries supported in a M3 module is 1.7 million IPv4 routes or 500k IPv6 routes or 1.1 million IPv4 Routes along with 300K IPv6 Routes.

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

MIBs

No new MIBs are added for Cisco NXOS Release 8.3(1).

Licensing

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

Caveats

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

- Open Caveats—Cisco NX-OS Release 8.3(2)
- Open Caveats—Cisco NX-OS Release 8.3(1)
- Resolved Caveats—Cisco NX-OS Release 8.3(2)
- Resolved Caveats—Cisco NX-OS Release 8.3(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 8.3(2)

Table 11 Cisco NX-OS Release 8.3(2) Open Caveats

Identifier	Description
CSCvn61562	SUP3: observing QCR4 & QCR6 ECC bit errors on loading 8.3.2.S20

Open Caveats—Cisco NX-OS Release 8.3(1)

Table 12 Cisco NX-OS Release 8.3(1) Open Caveats

Identifier	Description
CSCvc49851	MST instance configurations delayed to get synced or failed
CSCvd54174	8.2/8.3:-Error message after reloading non default vdc Error ("STP PIXM setport state timedout")
CSCvh92979	~2.5 seconds delay in failover for ECMP routes
CSCvi62571	[8.3.1] - F4 card goes to offline state when ACL scale is applied
CSCvi93007	M3/F4:lou operand(gt,lt,neq etc) with src port,dst port and tcp flags don't work with ipv6 ext header
CSCvi55312	M3/F4: Clear interface snmp counters not working
CSCus69949	M3-10: OTV/GRE unicast TX counters are not working
CSCvi97122	show tech-suport fex all shows syntax errors on few clis in non-default vdc
CSCvh82008	F4-100: LC shutdown because of temperature-sensor policy trigger if adjacent slots are empty
CSCvj69689	LISP: RLOC probe failing in both V4 and V6
CSCvj75597	LISP: Extranet static map-cache not programmed after shut/no-shut source vrf
CSCvk05725	LISP: map cache for IOS device showed 4010 signal map-reply
CSCvj68156	OTV Adjs show Down for Loopback Overlays after ISSU from 8.3.1 - > UPG

Table 12 Cisco NX-OS Release 8.3(1) Open Caveats (continued)

Identifier	Description
CSCvj99830	F4-100: \"Module < > failed to power up due to IDPROM read error\" Module in Unknown Module state
CSCvg17818	N77/vPC: \"vpc role preempt\" is not \"non-disruptive\" for mcast traffic
CSCvk08905	RISE: After switch reload, APBR route map configs not reapplied/replayed to SVIs
CSCvi34278	8.3.1 - BFD flapping after changing the peer link shut/no shut or module reboot.
CSCvi76485	F4100G duplicate pkts on mcast stream while doing vdc suspend/resume on FP Root node 8.3.1
CSCvj74569	8.3.1 - ARP packets punt and flood CPU in M3/SUP3/FAB3 setup when sent in higher rates.
CSCvf88069	Xmlization of show consistency-checker all cli
CSCvi97066	8.3.1: iftmc core and M3 in failure state with fabricpath mode transit configured
CSCvi98778	VDC reload:Unicast traffic from orphan port to access is dropped on forcing through vpc+ peer-link
CSCvj72406	[8.3.1] iftmc process cored with \"default interface po< num >\" and reconfigure po< num > back
CSCvj85320	VDC MIGRATION:F3:Bfd session on FP topology flaps on moving few ports across vdcs
CSCvf93428	8.0(1) / 8.1(1) to 8.2(1),8.3(1) upgrade, ITD & RISE features get disabled & configs deleted
CSCvi78076	MDT move cause packet drop in unicast packets
CSCvj41374	8.3.1 L2VPN over GRE M3 CE to CE ping does not work
CSCvi41036	MPLSoGRE(M3-LC): loopback in PE to PE over GRE tunnel not pingable
CSCvi50050	Anycast HSRP is broken after moving vlans from non-default to default topology
CSCvi95116	BFD sessions not coming up with tunnel interfaces
CSCvk08597	8.3.1 - 1.7M Scale: bgp routes not advertised to ebgp neighbour after SSO for sometime
CSCvj82363	Getting "ACL QOS failure: ELTMC COMMIT ERROR " after reload.
CSCvk12870	LISP VRF LEAKING (NXOS XTR) - lisp mapcache show no-route after vrf restored after its deletion.
CSCvk13841	8.3(1): F3 interface goes to hardware failure after configuring port as erspan destination
CSCvh26404	8.3.1: 1.7M Scale 'no shut' on interface takes more than 1 min, instead of immediately, to go up-up
CSCvk08871	MVPN traffic taking more than 6 minutes to converge after inserting a new FAB.

Table 12 Cisco NX-OS Release 8.3(1) Open Caveats (continued)

Identifier	Description
CSCvk13988	8.3.1: CBTS Configs UnSupported on M3 Modules.
CSCvk35999	Nexus 7000 Series EPLD upgrade fails on 8.3(1).

Resolved Caveats—Cisco NX-OS Release 8.3(2)

Table 13 Cisco NX-OS Release 8.3(2) Resolved Caveats

Identifier	Description
CSCul20456	%USER-3-SYSTEM_MSG: npacl app filter failed, err = [1106051080] - ntpd
CSCuq77481	ipfib crash at lfib_pi_get_cnh_adj_with_vpn_label after noshut core int
CSCuw99630	Cisco NX-OS Authenticated SNMP Denial of Service Vulnerability
CSCvg77643	Nexus 7000 VDC not load start-up config about passphrase
CSCvg92762	N7k with SUP1/6.2.12 continuously rebooting with aclmgr crash
CSCvh19090	CVR-QSFP-SFP10G interface showing not connected after chassis cold boot
CSCvh32390	Evaluation of n7k-platform for CPU Side-Channel Information Disclosure Vulnerability.
CSCvi18966	N77XX/M3:CBL forwarding on down port
CSCvj06726	N77XX/M3: Mac sync issue
CSCvj08912	BFD is not coming up when authentication and hardware offload is used between N7K and ASR1k
CSCvj09711	N7K - Service "acllog" crash with PBR
CSCvj12608	provide drop counter when packets are dropped due to incorrect ltl to vdc mapping in KLM vdc
CSCvj14441	PTP GM clock sync loss after switchover
CSCvj36340	FCoE pause drop threshold reached when VL is paused/resumed quickly
CSCvj55192	Kernel memory commands not working
CSCvj58887	Partner fails to set collecting bit in LACP PDU causes sequence timeout
CSCvj63743	Nexus System Software Internal Network Restriction Bypass Vulnerability
CSCvj70748	Output of "show mpls ldp igp sync" inconsistent with configuration
CSCvj77201	user logged out from ssh session in user VDC when admin VDC is configured with exec-timeout
CSCvj87367	MST regions out of sync after ISSU to 8.1(2a)
CSCvk00701	Incorrect FIB programming during ISSU
CSCvk01435	M3- PTP Multicast-224.0.1.129 packet drop
CSCvk03597	PTP GM clock sync loss after system reload, process restart
CSCvk10930	N7K Interface stuck in LACP suspend after link flap with ethernet oam
CSCvk22156	n7k/GOLD: temperature sensor message improvement
CSCvk28290	Fabricpath DCE mode of port-channel member inconsistent

Table 13 Cisco NX-OS Release 8.3(2) Resolved Caveats (continued)

Identifier	Description
CSCvk31556	invalid source ip for inter vrf ping for /32 destination
CSCvk35035	logging server vrf name in startup-config changed after reload
CSCvk35999	Nexus 7000 Series EPLD upgrade fails on 8.3(1)
CSCvk38405	N7k M3/F3/F4:Fragmented PIM BSR packets are CPU punted and dropped
CSCvk38474	Suppress the bcast check on /31 VIP or pass mask from VIP to API if mask < 31
CSCvk44309	N7K iftmc crashed when tried to bring up gre tunnel
CSCvk45949	When a private-vlan is the first extended vlan more than 64 ranges can be configured in OTV
CSCvk51138	N7K Fabricpath :: MAC address not re-learned on broadcast ARP
CSCvk53943	HSRP active replies arp request with physical mac address after preempt
CSCvk54735	FCoE "uSecs VL3 is in internal pause rx state" increments when eth port is not currently paused
CSCvk55799	STP BPDUS for pruned VLANs are reaching the cpu.
CSCvk56857	MPLS BGP to OSPF redistribution DN bit not set
CSCvk58123	In maintenance mode profile, a route-map in BGP is only applied on either inbound or outbound.
CSCvk58529	N7k - Various NTP features not working on 8.3(1)
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
CSCvk68928	Non-default VDC uses the SSH hostkey of the default-VDC
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
CSCvm05636	IP redirects disabled in configuration but enabled in ELTM
CSCvm09089	Command 'show hardware flow' results into a crash when it creates a temporary file
CSCvm09452	N77-F348XP-23 kernel panic
CSCvm11792	ISIS IPv6 multi-topology - fixing MT attached bit
CSCvm13449	Stale Entries present in cli_acl_ifdb PSS on Standby Sup after Purge
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
CSCvm27147	N7K/F3 interfaces goes to Hardware Failure after creating SVI
CSCvm29785	N7k BGP L2VPN VPLS Auto Discovery route not imported after route flaps

Table 13 Cisco NX-OS Release 8.3(2) Resolved Caveats (continued)

Identifier	Description
CSCvm32486	PSS memory leak Type-0x0d on large burst of join/leave
CSCvm43644	N7K is not advertising some of the BGP prefixes to the Neighbors
CSCvm44595	N7K Aclmgr memory leak on show ip access-list expanded cmd
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
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
CSCvm99009	Port Info missing in level 2 L2FM log messsage when MAC moves continuously 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
CSCvn08550	N7K - 'ip routing multicast holddown' not working as expected
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"
CSCvn31931	N7K adding ip address into object group stuck
CSCvn36425	aclmgr crash @ddb functions
CSCvn39414	NXOS: Local VRF leaking failed after ip clear of specific route in dest VRF
CSCvn42012	Broadcast HB sup->lc is flooded on all eobcsw ports
CSCvn45757	Incorrect credit programmed for N7K-F306CK-25 after cold boot 6.x/7.x to 8.x
CSCvi76485	Duplicate Pkts observed due to PIM Assert not triggered.

Resolved Caveats—Cisco NX-OS Release 8.3(1)

Table 14 Cisco NX-OS Release 8.3(1) Resolved Caveats

Identifier	Description
CSCud46876	N7K / MSDP session does not reestablish after 'restart msdp'
CSCuq54506	RARP not flooded from OTV AED
CSCus91983	diagnostic PortLoopback test needs warning since the test is disruptive

Table 14 Cisco NX-OS Release 8.3(1) Resolved Caveats (continued)

Identifier	Description
CSCut94652	Adding basic show commands to feature show techs (N7K)
CSCuw86555	N7K Silent/Unknown supervisor switchover
CSCuw91064	'show ip access-list' output does not update/display statistics
CSCux87740	N7K uses wrong MAC address for BFD when peer switches mac address
CSCux95916	Fex crashing on bootup, generating core.
CSCuy29923	Event manager configuration is out of order in start-up configuration
CSCuy89690	"show accounting log" shows the community string on plain text
CSCva95344	F3 Line card reload
CSCvb02212	M1: Delay in Link down may result in vPC suspension
CSCvb28656	Puts sends output to syslog, not the controlling terminal
CSCvb74706	N7K: F3 2s convergence time on module OIR
CSCvb86787	Cisco Nexus 5K/6K/7K/9K/9500-R/MDS CLI Command Injection Vulnerability
CSCvc06471	eem_policy_dir hap reset in steady state without any triggers
CSCvc23468	Evaluation of N9k/N7k/N5k/N3k/MDS for NTP November 2016
CSCvc42886	No SSH possible to device when root directory is full due to nxapi request
CSCvc53473	Implement version check for post ISSU IM breakout syslog requiring copy r s
CSCvc56655	Nexus 7k itd NAT destination issue
CSCvc69075	MAC address mismatch between SUP and LC after a VPLS failover.
CSCvc69751	Unexpected reload of the Supervisor due to LDP service crashed
CSCvc78278	NXOS/ETHPM: Traffic not forwarded after port change from Channeling to Individual
CSCvc91548	Incorrect forwarding address is set to OSPF type-5 LSA of summarized route
CSCvd04835	Old connected route not removed from EIGRP topology table
CSCvd08898	Hash-algorithm HMAC-SHA-1 can't be configured on F3 linecards, after upgrading to 7.3.x
CSCvd10140	Dynamic Mac address has wrong DI (Destination index) on M2
CSCvd11125	GOLD PwrMgmtBus failure on both Active and Standby SUP with reason Non zero value for Tx status
CSCvd13580	Fatal interrupt does not get logged into OBFL logs
CSCvd25258	Bogus DHCP GIADDR being used for DHCP Smart Relay post ISSU
CSCvd69943	Cisco FXOS and NX-OS Software Cisco Fabric Services Arbitrary Code Execution Vulnerability
CSCvd69951	Cisco FXOS and NX-OS Software Cisco Fabric Services Arbitrary Code Execution Vulnerability
CSCvd72172	Evaluation of N9k/N7k/N5k/N3k/MDS for NTP March 2017
CSCvd86332	EIGRP routers stopped propagating default route.
CSCvd86490	Cisco NX-OS Python Parser Escape Vulnerability

Table 14 Cisco NX-OS Release 8.3(1) Resolved Caveats (continued)

Identifier	Description
CSCvd88316	Return value is incorrect for object-tracking configuration - VTS config push will fail
CSCvd95927	EEM script times out at 100s mark in 7.2/7.3
CSCve06320	Netflow - netflow/nfm not responding msg stuck in MTS Buffer
CSCve12380	CTS commands unavailable if medium p2p configured on a port channel
CSCve21405	Inconsistent formatting for 'show interface' outputs collected through NXAPI using JSON
CSCve34578	Nexus 7000: cts hap reset on 7.3(1)D1(1) triggered when ASA failover happens
CSCve37457	CBL wrongly programmed on VPC peer
CSCve40271	N7K crashes while opening startup-config
CSCve40970	Cisco FXOS, NX-OS, and UCS Manager Software Cisco Discovery Protocol Denial of Service Vulnerability
CSCve46183	N77-F324FQ-25 interfaces goes to Hardware Failure after creating SVI
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
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
CSCve80468	N7K/F2e/F3:Post Routed L3 MCast traffic forwarded on both the FTAG
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
CSCvf27235	N7K: Improve Logging for Interrupt Fault CLP_LBD_INT_MEM_ECC_PORT_MAP_TBL_ECC_1ERR
CSCvf29432	Cisco Nexus 7000 Series Switches Privilege Escalation via sudo
CSCvf33147	F3 - xbar sync failed during module bringup after upgrade N77-F312CF-26 ver 1.1
CSCvf36683	N7K-SUP2/E: eUSB Flash Failure or Unable to Save Configuration
CSCvf58207	vPC+ Secondary does not suspend SVIs when Primary reachable via Fabricpath

Table 14 Cisco NX-OS Release 8.3(1) Resolved Caveats (continued)

Identifier	Description
CSCvf59067	N7k-8.X- Eigrp SIA due to a query/update from non successor.
CSCvf60001	"show lldp neighbor details" doesn't list all neighbors
CSCvf61926	N7K // Ethanalzyer does not gather FIP or FCoE traffic on F3 line card
CSCvf66024	PBR programming wrong adj index when N7K up with multiple PBR configured ports
CSCvf69323	One of the ports of F2 line card is not linking up
CSCvf73007	Access list is failing for SNMPv3 in N7k
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
CSCvf79399	FEX module Crash when inserting 4 GLC-TE transceivers into FEX HIF port
CSCvf81891	N7000 sends PTP packets incorrectly with ttl-1
CSCvf83485	Link interruption caused crash of isis_fabricpath
CSCvf87011	M3 - Ncpinfraclnt Crash
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
CSCvg16920	BGP community list missing in config when updated after reload
CSCvg17452	Nexus 7k GOLF router drops packets at VXLAN encap due to incorrect egress LIF programming
CSCvg18985	ifInDiscards not matching # show interface mgmt0 counters errors on N7K
CSCvg23522	Unable to remove the ACL from N7k, N3k and N9k
CSCvg23978	N7K - nfp crash on M3 40 module
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
CSCvg38672	vpc self-isolation:vpc legs are up on local after all modules up when MCT down
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
CSCvg44947	Dropping GTP ipv6 packet
CSCvg45324	Static mac programmed as dynamic for orphan mac

Table 14 Cisco NX-OS Release 8.3(1) Resolved Caveats (continued)

Identifier	Description
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
CSCvg53147	N7k -Multicast Register IP TTL copied to payload TTL in MVPN
CSCvg57540	N7K Netflow M3: subinterface netflow sampler not working on breakout cable ports
CSCvg60756	FHR not sending register to RP due to SGR prune
CSCvg61970	Tacacs Daemon process crashes due to AAA timeouts
CSCvg65643	Connected devices are flapped though ports at N77-F324FQ-25 side are shutdown
CSCvg68163	VxLAN VTEP remote site mac not get flushed after receiving TCN from BDI
CSCvg68573	N7K/F2 - EG recovery improvements
CSCvg70139	%ETHPORT-3-IF_UNSUPPORTED_TRANSCEIVER: Transceiver on interface Ethernet9/6 is not supported
CSCvg74176	Memory leak in acfg handler while hitting error in show running config
CSCvg90880	Clipper port-channel L3 Sub intf not generate netflow
CSCvg92062	Post ISSU from 7.3.1 to 8.1.2 image, record templates show junk values
CSCvg92363	F3:fln_em watchdog timer improvements
CSCvg95207	N7004 - L2 multicast traffic is sent to all SOC's
CSCvg96060	N7K - after changing peer-link config in VXLAN BUM traffic blackholed
CSCvh02279	M3: Ethernet interface stuck down (unknown enum:<296>)
CSCvh02948	After VDC reloaded native vlan mapping to VNI mismatch cause traffic disruptive
CSCvh02988	ISIS IPv6 Multitopology broken after process shut/no-shut
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
CSCvh04206	Nexus 7000/7700 | 8.2(1) | Unicast broken with wccp enabled
CSCvh05330	M3-Fex: VSH crash on M3 module Techsupport
CSCvh13852	N7k Unable to send packet more than MTU size with cts manual configured on the port
CSCvh23286	cmd_exec_error when executing show tech eigrp through python interpreter
CSCvh25999	N77K - Unable to configure input netflow monitor in Po
CSCvh30461	"show routing vrf all ipv6 internal distribution" causes crash at u6rib
CSCvh32898	VRF leaking in SDA: EVPN paths' parent ECMP doesn't update on RIT moves
CSCvh47211	Issuing 'show install all impact' command during ISSU may cause ISSU to fail
CSCvh54503	After rip process restart only 8 ECMP routes are allowed
CSCvh54560	After route flap next-hop count increase

Table 14 Cisco NX-OS Release 8.3(1) Resolved Caveats (continued)

Identifier	Description
CSCvh56282	Physical VPC port which is in LACP I state is not brought down by VPC
CSCvh61904	unable to remove duplicate entries in DNS group with cfs
CSCvh65347	LDI collision seen after sup switchover
CSCvh67120	NX-OS netflow configuration cannot enable under p2p port-channel
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
CSCvh87828	lisp punt route nexthop not deleted/updated for all interfaces/routes after BGP nexthop change
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"
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.
CSCvi12032	[N7k M3] GRE tunnel do not forward unicast/mcast traffic
CSCvi12277	FEX power supply, fan not populated in entPhysicalTable on N7k for version 8.2(1)
CSCvi14840	Nexus might crash after creating multiple MSDP mesh groups
CSCvi15800	N7k - OTV Fast Convergence is delayed during AED switchover
CSCvi20373	n7k ICMPv6 Packet too big Messages are not send after ISSU to 8.2(1)
CSCvi25701	VXLAN BDs are suspended on VPC peer after removing-restoring BD config
CSCvi34997	N7K - XML sub agent initialization fails: xml session creation failed. Out of memory.
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	Incorrect state and no data for reason code/return code for svi enabled snmpd error logs
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
CSCvi64957	BFD over FabricPath: SUP and LC out of sync - happens on OIR
CSCvi70543	Service SAP Qosmgr - (Operation timed out) in if_bind sequence

Table 14 Cisco NX-OS Release 8.3(1) Resolved Caveats (continued)

Identifier	Description
CSCvi73154	N7K // Adding a 16th WSA Client causes the N7K to drop all clients continuously
CSCvi78169	N7K VPC Crash
CSCvi78715	Netboot over EOBC fails if both supervisors were originally netbooted
CSCvi87540	N7K - HSRP libanycast cache does not sync to standby sup after changes to anycast bundle
CSCvi88803	N7K linecard crash with aclqos hap reset
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
CSCvj07101	Copying SNMP MIB using IPV6 causes a reload
CSCvj08973	snmpd hap reset crash when snmpwalk on OID stpxMSTInstanceVlansMapped2k
CSCvj10306	LTLs not deallocated in IM for broken out port after a no breakout is done on that port
CSCvj11685	IGMP hap reset during ND ISSU
CSCvj15110	Nexus9k KIM crash on SUP failover
CSCvj17451	Dynamic label not reassigned after static range defined and LDP shut/no-shut
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
CSCvj52372	show interface transceiver | json or xml output misaligned
CSCvj55813	'hardware ejector enable' command is not displayed in 'show run all' output
CSCvj84775	PIM6 Anycast-RP failling to send Register-Stop
CSCvc18137	MPLS TE: ipfib crash after forwarding restart
CSCwa05551	N7700: RISE feature not available in 8.2(x)

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.