Cisco Nexus 7000 Series NX-OS Release Notes, Release 7.2

Last Modified Date: May 11, 2020
Current Release: 7.2(2)D1(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 the Upgrade and Downgrade.

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 Online History Change

Date	Description
June 18, 2015	Created release notes for Cisco NX-OS Release 7.2(0)D1(1).
September 7, 2015	Updated the " Resolved Caveats—Cisco NX-OS Release 7.2(0)D1(1)" section to add CSCuq28545.
September 22, 2015	Reorganized the " New and Enhanced Software Features" section based on feature groupings.
October 29, 2015	Updated the release notes for Cisco NX-OS Release 7.2(1)D1(1). Updated the " Cisco NX-OS Release 7.2(1)D1(1) – Software Features" and " Caveats" section.
November 12, 2015	Updated the "Transceivers Supported by Cisco NX-OS Software Releases" table to add a footnote for CPAK-100G-LR4 and CPAK-100G-SR10.
July 15, 2016	Updated the release notes for Cisco NX-OS Release 7.2(2)D1(1). Updated the " Upgrade/Downgrade Paths and Caveats" and " Caveats" section.
August 5, 2016	Updated the release notes for Cisco NX-OS Release 7.2(2)D1(2). Updated the " Caveats" section.

Cisco Systems, Inc.
www.cisco.com

Table 1 Online History Change

Date	Description
August 17, 2016	Updated the "Transceivers Supported by Cisco NX-OS Software Releases" table to include information for CVR-QSFP-SFP10G.
November 8, 2016	Updated the " Resolved Caveats—Cisco NX-OS Release 7.2(0)D1(1)" section to add CSCun41202.
December 8, 2016	Updated Table 2—Cisco Nexus 7000 and 7700 Series Hardware Supported by Cisco NX-OS Software to add N7K-C7018-FAB-1 and N7K-F132XP-15.
February 21, 2017	Updated the " Upgrade/Downgrade Paths and Caveats"section to include Cisco NX-OS Release 6.2(18).
December 8, 2017	Updated the " Upgrade/Downgrade Paths and Caveats"section to include Cisco NX-OS Release 6.2(20).
August 3, 2018	Updated the " Upgrade/Downgrade Paths and Caveats"section to include Cisco NX-OS Release 6.2(20a).
February 15, 2019	Updated the " Upgrade/Downgrade Paths and Caveats"section to include Cisco NX-OS Release 6.2(22).
February 14, 2020	Updated the " Upgrade/Downgrade Paths and Caveats"section to include Cisco NX-OS Release 6.2(24).
May 11, 2020	Updated the " Upgrade/Downgrade Paths and Caveats"section to include Cisco NX-OS Release 6.2(24a).

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

Cisco Nexus 7000 Supervisor 2 and 2E Modules are required for Cisco NX-OS Release 7.2(0)D1(1).

This section includes the following topics:

- Supported Device Hardware

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.*

Table 2 shows the Cisco Nexus 7000 and 7700 Series hardware supported by Cisco NX-OS Release 7.2.x and earlier releases.

Table 3 shows the FEX modules supported by the Cisco Nexus 7000 and 7700 Series I/O modules.

Table 4 shows the Service Modules Supported by Cisco Nexus 7000 Series Switches

Table 5 shows the transceiver devices supported by each release.

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

Table 2 Cisco Nexus 7000 and 7700 Series Hardware Supported by Cisco NX-OS Software

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

Table 2 Cisco Nexus 7000 and 7700 Series Hardware Supported by Cisco NX-OS Software (continued)

Product ID	Hardware	Minimum Software Release
N7K-C7010	Cisco Nexus 7010 chassis	4.0(1)
N7K-C7010-FAB-2	Fabric module, Cisco Nexus 7000 Series 10-slot	6.0(1)
N7K-C7010-FAN-F	Fabric fan tray for the Cisco Nexus 7010 chassis	4.0(1)
N7K-C7010-FAN-S	System fan tray for the Cisco Nexus 7010 chassis	4.0(1)
N7K-C7018	Cisco Nexus 7018 chassis	4.1(2)
N7K-C7018-FAB-1	Fabric module, Cisco Nexus 7000 Series 18-slot	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-F132XP-15	32-port 1/10 Gigabit Ethernet module (F1 Series)	5.1(1)
N7K-F248XP-25	48-port 1/10 Gigabit Ethernet SFP+ I/O module (F2 Series)	6.0(1)
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-M108X2-12L	8-port 10-Gigabit Ethernet I/O module XL[1]	5.0(2)
N7K-M132XP-12	32-port 10-Gigabit Ethernet SFP+ I/O module	4.0(1)

Table 2 Cisco Nexus 7000 and 7700 Series Hardware Supported by Cisco NX-OS Software (continued)

Product ID	Hardware	Minimum Software Release
N7K-M132XP-12L	32-port 10-Gigabit Ethernet SFP+ I/O module XL[1]	5.1(1)
N7K-M148GS-11	48-port 1-Gigabit Ethernet SFP I/O module	4.1(2)
N7K-M148GS-11L	48-port 1-Gigabit Ethernet I/O module XL[1]	5.0(2)
N7K-M148GT-11	48-port 10/100/1000 Ethernet I/O module	4.0(1)
N7K-M148GT-11L	48-port 10/100/1000 Ethernet I/O module XL[1]	5.1(2)
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-SUP2	Supervisor 2 module	6.1(1)
N7K-SUP2E	Supervisor 2 Enhanced module	6.1(1)
Cisco Nexus 7700 Series Hardware		
N77-AC-3KW	Cisco Nexus 7700 AC power supply	6.2(2)
N77-C7702	Cisco Nexus 7702 chassis	7.2(0)D1(1)
N77-C7702-FAN	Fan, Cisco Nexus 7702 chassis	7.2(0)D1(1)
N77-C7706	Cisco Nexus 7706 chassis	6.2(6)
N77-C7706-FAB-2	Fabric Module, Cisco Nexus 7706 chassis	6.2(6)
N77-C7710	Cisco Nexus 7710 chassis	6.2(2)
N77-C7710-FAB-2	Fabric Module, Cisco Nexus 7710 chassis	6.2(2)
N77-C7710-FAN	Fan, Cisco Nexus 7710 chassis	6.2(2)
N77-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-DC-3KW	Cisco Nexus 7700 DC power supply	6.2(2)

Table 2 Cisco Nexus 7000 and 7700 Series Hardware Supported by Cisco NX-OS Software (continued)

Product ID	Hardware	Minimum Software Release
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)	6.2(6)
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-SUP2E	Cisco Nexus 7700 Supervisor 2 Enhanced module	6.2(2)

[1] Requires the Cisco Nexus 7010 Scalable Feature Package license (N7K-C7010-XL) or the Cisco Nexus 7018 Scalable Feature Package license (N7K-C7018-XL), depending on the chassis, to enable all XL-capable I/O modules to operate in XL mode.

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		
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)
32-port 10-Gigabit Ethernet SFP+ I/O module (N7K-M132XP-12)	N2K-C2248TP-1GE	5.2(1)
	N2K-C2348UPQ N2K-C2348TQ N2K-B22IBM	7.2(0)D1(1)

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

Cisco Nexus 7000 Series Module	FEX Module	Minimum Software Release
32-port 10-Gigabit Ethernet SFP+ I/O module (N7K-M132XP-12L)	N2K-C2224TP-1GE N2K-C2232PP-10GE	5.2(1)
	N2K-C2232TM N2K-C2248TP-E	6.1(1)
	N2K-2232TM-E N2K-C2248PQ N2K-B22HP	6.2(2)
	N2K-C2348UPQ N2K-C2348TQ N2K-B22IBM	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 F2 Series module (N7K-F248XP-25)	N2K-C2224TP-1GE N2K-C2248TP-1GE N2K-C2232PP-10GE	6.0(1)
	N2K-C2232TM N2K-C2248TP-E	6.1(1)
	N2K-2232TM-E N2K-2248PQ N2K-B22HP	6.2(2)
	N2K-C2348UPQ N2K-C2348TQ N2K-B22IBM	7.2(0)D1(1)

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

Cisco Nexus 7000 Series Module	FEX Module	Minimum Software Release
48-port 1/10 Gigabit Ethernet SFP+ I/O F3 Series module (N7K-F348XP-25)	N2K-C2224TP-1GE N2K-C2248TP-1GE N2K-C2232PP-10GE N2K-C2232TM N2K-C2248TP-E N2K-2232TM-E N2K-2248PQ N2K-B22HP	6.2(12)
	N2K-C2348UPQ N2K-C2348TQ N2K-B22IBM	7.2(0)D1(1)
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)
FEX Modules Supported by Cisco Nexus 7700 Series Modules		
24-port Cisco Nexus 7700 F3 Series 40-Gigabit Ethernet QSFP I/O module (N77-F324FQ-25)	N2K-C2224TP-1GE N2K-C2248TP-1GE N2K-C2232PP-10GE N2K-C2232TM N2K-C2248TP-E N2K-C2232TM-E N2K-C2248PQ N2K-B22HP[2]	6.2(8)
	N2K-C2348UPQ N2K-C2348TQ N2K-B22IBM	7.2(0)D1(1)

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

Cisco Nexus 7000 Series Module	FEX Module	Minimum Software Release
48-port Cisco Nexus 7700 F3 Series 1/10-Gigabit Ethernet SFP+ I/O module (N77-F348XP-23)	N2K-C2224TP-1GE N2K-C2248TP-1GE N2K-C2232PP-10GE N2K-C2232TM N2K-C2248TP-E N2K-C2232TM-E N2K-C2248PQ N2K-B22HP	6.2(6)
	N2K-C2348UPQ N2K-C2348TQ N2K-B22IBM	7.2(0)D1(1)
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)

[1] FEX server-facing interfaces should be configured in autonegotiate mode. Do not force a specific data rate. See DDTS CSCuj84520 for additional information.

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 Fabric Extenders.

Table 4 Service Modules Supported by Cisco Nexus 7000 Series Switches

Service Module	Product ID	Minimum Software Release
Cisco Nexus 7000 Series Network Analysis Module	NAM-NX1	6.2(2)

Table 5 Transceivers Supported by Cisco NX-OS Software Releases

I/O Module	Product ID	Transceiver Type	Minimum Software Version
N77-F312CK-26	CPAK-100G-ER4L	Cisco 100GBASE-ER4L CPAK	7.2(1)D1(1)
	CPAK-100G-LR4 [1]	Cisco 100GBASE-LR4 CPAK	6.2(6)
	CPAK-100G-SR10 [1]	Cisco 100GBASE-SR10 CPAK	6.2(6)
N77-F324FQ-25	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-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 5 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 [2]	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 5 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)
N7K-F306CK-25	CPAK-100G-ER4L	Cisco 100GBASE-ER4L CPAK	7.2(1)D1(1)
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)
	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 [2]	10GBASE-LRM SFP+	6.2(12)

Table 5 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	SFP-H10GB-CUxM	SFP-H10GB-CUxM Twinax Cable Passive (1 m, 3 m, 5 m)	6.2(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-F312FQ-25	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)

Table 5 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	FET-40G	Cisco 40G Fabric Extender Transceiver (FET)	6.2(6)
	QSFP-H40G-ACUxM	40GBASE-CR4 QSFP+ Direct Attach Copper Cable Active (7 m, 10 m)	6.2(8)
	QSFP-4X10G-ACxM	40GBASE-CR4 QSFP+ to 4x SFP+ Twinax Direct Attach Copper Breakout Cable Active (7 m, 10 m)	6.2(8)
	QSFP-H40G-AOCxM	40GBASE-AOC (Active Optical Cable) QSFP Cable (1 m, 2 m, 3 m, 5 m, 7 m, 10 m)	6.2(8)
	QSFP-H40G-AOC15M	40GBASE-AOC (Active Optical Cable) QSFP Cable (15m)	7.2(0)D1(1)
	QSFP-4X10G-AOCxM	40GBASE-AOC (Active Optical Cable) QSFP to 4x10G SFP+ Breakout Cable (1 m, 2 m, 3 m, 5 m, 7 m, 10 m)	6.2(8)
	WSP-Q40GLR4L	40GBASE-LR4 lite (2km SMF) QSFP+	62(10)
	QSFP-40G-LR4	40GBASE-LR4 QSFP+ (Ethernet and OTU3 capable)	6.2(12)
	QSFP-40G-ER4	40GBASE-ER4 QSFP+ (40km)	6.2(12)
N7K-F306CK-25	CPAK-100G-LR4 [1]	Cisco 100GBASE-LR4 CPAK	6.2(10)
	CPAK-100G-SR10 [1]	Cisco 100GBASE-SR10 CPAK	6.2(10)
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 5 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 [2]	10GBASE-DWDM SFP+	6.2(2)
	DWDM-SFP-xxxx [2]	1000BASE-DWDM	6.2(2)
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)

Table 5 Transceivers Supported by Cisco NX-OS Software Releases (continued)

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

Table 5 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	CWDM-SFP-xxxx [2]	1000BASE-CWDM	6.0(1)
	DWDM-SFP10G-xx.xx [2]	10GBASE-DWDM SFP+	6.1(1)
	DWDM-SFP-xxxx [2]	1000BASE-DWDM	6.0(1)
N7K-F248XP-25E	FET-10G	Cisco Fabric Extender Transceiver (FET)	6.1(2)
	SFP-10G-BXD-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, downstream	7.2(0)D1(1)
	SFP-10G-BXU-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, upstream	7.2(0)D1(1)
	SFP-10G-SR SFP-10G-SR-S	10GBASE-SR SFP+	6.1(2)
	SFP-10G-LR SFP-10G-LR-S	10GBASE-LR SFP+	6.1(2)
	SFP-10G-ER SFP-10G-ER-S	10GBASE-ER SFP+	6.1(2)
	SFP-10G-LRM	10GBASE-LRM SFP+	6.1(2)
	SFP-10G-ZR[2] 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)

Table 5 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	GLC-ZX-SM	1000BASE-ZX SFP	6.1(2)
	GLC-ZX-SMD	1000BASE-ZX SFP	6.1(2)
	GLC-T	1000BASE-T SFP	6.1(2)
	GLC-TE	1000BASE-T SFP	6.2(10)
	GLC-BX-D	1000BASE-BX10-D	6.1(2)
	GLC-BX-U	1000BASE-BX10-U	6.1(2)
	GLC-EX-SMD	1000BASE-EX SFP	6.1(2)
	CWDM-SFP-xxxx [2]	1000BASE-CWDM	6.1(2)
	DWDM-SFP10G-xx.xx [2]	10GBASE-DWDM SFP+	6.1(2)
	DWDM-SFP-xxxx [2]	1000BASE-DWDM	6.1(2)
N7K-F132XP-15	SFP-10G-SR SFP-10G-SR-S	10GBASE-SR SFP+	5.2(1)
	GLC-TE	1000BASE-T SFP	6.2(10)
	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[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)	5.1(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)	5.1(1)
	SFP-GE-T	1000BASE-T SFP	5.1(1)
	SFP-GE-S	1000BASE-SX SFP (DOM)	5.1(1)
	SFP-GE-L	1000BASE-LX/LH SFP (DOM)	5.1(1)
	SFP-GE-Z	1000BASE-ZX SFP (DOM)	5.1(1)
	GLC-LH-SM	1000BASE-LX/LH SFP	5.1(1)
	GLC-SX-MM	1000BASE-SX SFP	5.1(1)

Table 5 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	GLC-ZX-SM	1000BASE-ZX SFP	5.1(1)
	GLC-ZX-SMD	1000BASE-ZX SFP	6.2(2)
	GLC-T	1000BASE-T SFP	5.1(1)
	GLC-LH-SMD	1000BASE-LX/LH SFP	5.2(1)
	GLC-SX-MMD	1000BASE-SX SFP	5.2(1)
	GLC-EX-SMD	1000BASE-EX-SFP	6.1(1)
	DWDM-SFP10G-xx.xx [2]	10-GBASE-DWDM SFP+	6.1(1)
N7K-M108X2-12L	SFP-10G-SR [2] SFP-10G-SR-S	10GBASE-SR SFP+	5.2(3a)
	SFP-10G-LR [2] SFP-10G-LR-S	10GBASE-LR SFP+	5.2(3a)
	SFP-10G-LRM [2]	10GBASE-LRM SFP+	5.2(1)
	SFP-H10GB-CUxM[2]	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= [2]	10GBASE-DWDM X2	5.0(2a)
N7K-M148GS-11	SFP-GE-S	1000BASE-SX	4.1(2)
	GLC-SX-MM		4.1(2)
	SFP-GE-L	1000BASE-LX	4.1(2)
	GLC-LH-SM		4.1(2)
	SFP-GE-Z	1000BASE-ZX	4.1(2)
	GLC-ZX-SM		4.1(2)
	GLC-EX-SMD	1000BASE-EX SFP	6.2(2)
	GLC-ZX-SMD	1000BASE-ZX SFP	6.2(2)
	GLC-T	1000BASE-T	4.2(1)
	SFP-GE-T		4.2(1)

Table 5 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	GLC-BX-D	1000BASE-BX10-D	5.2(1)
	GLC-BX-U	1000BASE-BX10-U	5.2(1)
	GLC-SX-MMD	1000BASE-SX	5.2(1)
	GLC-LH-SMD	1000BASE-LX	5.2(1)
	CWDM-SFP-xxxx [2]	1000BASE-CWDM	4.2(1)
	DWDM-SFP-xxxx [2]	1000BASE-DWDM	4.2(1)
N7K-M148GS-11L	SFP-GE-S	1000BASE-SX	5.0(2a)
	GLC-SX-MM		5.0(2a)
	SFP-GE-L	1000BASE-LX	5.0(2a)
	GLC-LH-SM		5.0(2a)
	SFP-GE-Z	1000BASE-ZX	5.0(2a)
	GLC-ZX-SM		5.0(2a)
	GLC-EX-SMD	1000BASE-EX SFP	6.2(2)
	GLC-ZX-SMD	1000BASE-ZX SFP	6.2(2)
	GLC-T	1000BASE-T	5.0(2a)
	SFP-GE-T		5.0(2a)
	GLC-BX-D	1000BASE-BX10-D	5.2(1)
	GLC-BX-U	1000BASE-BX10-U	5.2(1)
	GLC-SX-MMD	1000BASE-SX	5.2(1)
	GLC-LH-SMD	1000BASE-LX	5.2(1)
	GLC-TE	1000BASE-T SFP	6.2(10)
	DWDM-SFP-xxxx [2]	1000BASE-DWDM	5.0(2a)
	CWDM-SFP-xxxx [2]	1000BASE-CWDM	5.0(2a)
N7K-M132XP-12	FET-10G	Cisco Fabric Extender Transceiver (FET)	5.1(1)
	SFP-10G-SR SFP-10G-SR-S	10GBASE-SR SFP+	4.2(6)
	SFP-10G-LR SFP-10G-LR-S	10GBASE-LR SFP+	4.0(3)
	SFP-10G-ER SFP-10G-ER-S	10GBASE-ER SFP+	4.0(1)
	SFP-H10GB-ACUxM [2]	SFP-H10GB-ACUxM Twinax Cable Active (7 m, 10 m)	5.1(2)
N7K-M132XP-12L	FET-10G	Cisco Fabric Extender Transceiver (FET)	5.1(1)

Table 5 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+	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 [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-ACUxM	SFP-H10GB-ACUxM Twinax Cable Active (7 m, 10 m)	5.1(1)
	SFP-H10GB-CUxM [2]	SFP-H10GB-CUxM Twinax Cable Passive (1 m, 3 m, 5 m)	5.1(2)
	SFP-H10GB-CUxM	SFP-H10GC-CUxM Twinax Cable Passive (1.5 m, 2 m, 2.5 m)	6.2(2)
	DWDM-SFP10G-xx.xx [3]	10GBASE-DWDM SFP+	6.1(1)
N7K-M224XP-23L	SFP-10G-BXD-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, downstream	7.2(0)D1(1)
	SFP-10G-BXU-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, upstream	7.2(0)D1(1)
	FET-10G	Cisco Fabric Extender Transceiver (FET)	6.1(1)
	SFP-10G-SR SFP-10G-SR-S	10GBASE-SR SFP+	6.1(1)
	SFP-10G-LR SFP-10G-LR-S	10GBASE-LR SFP+	6.1(1)

Table 5 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+	6.1(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 [3]	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)
N7K-M206FQ-23L	QSFP-40G-SR-BD	Cisco 40G BiDi QSFP+	6.2(6)
	FET-40G	Cisco 40G Fabric Extender Transceiver (FET)	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)

Table 5 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	QSFP-4X10G-AOCxM	40GBASE-AOC (Active Optical Cable) QSFP to 4x10G SFP+ Breakout Cable (1 m, 2 m, 3 m, 5 m, 7 m, 10 m)	6.2(8)
	WSP-Q40GLR4L	40GBASE-LR4 lite (2km SMF) QSFP+	62(10)
	QSFP-40G-LR4	40GBASE-LR4 QSFP+ (Ethernet and OTU3 capable)	6.2(12)
	QSFP-40G-ER4	40GBASE-ER4 QSFP+ (40km)	6.2(12)
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)

[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.

[2] Minimum version supported is -02.

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

Limitations

This section describes the limitations in Cisco NX-OS Release 7.2(0)D1(1) and later releases for the Cisco Nexus 7000 Series.

Unsupported Hardware

The following list provides the unsupported hardware for Cisco NX-OS Release 7.2(0)D1(1):

- Cisco Nexus 7000 Supervisor 1 Module

FabricPath Bidirectional Forwarding Detection (BFD)

Refer to CSCut89986 bug fix for the FabricPath BFD behavior.

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

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).

Note Electronic dispersion compensation (EDC) is a method for mitigating the effects of chromatic dispersion in fiber-optic communication links with electronic components in the receiver. The delay in link up event in SFP+ implementation is due to EDC that can mitigate power penalties associated with optical link budgets. On ports or receivers without EDC/non EDC (for example - SFP, where there is no delay in bringing the port up) optical signal can be recovered only if the dispersion is less than approximately one-half Unit Interval (UI) over the length of fiber.

MPLS over GRE

MPLS over GRE is not supported on F3 and M3 modules.

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

The no hardware ejector enable command cannot be a configured command in both the startup configuration and the runtime configuration. This command is a debugging command and should not be configured for long-term use.

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 devices.

Routing over VPC

Routing protocol adjacency over a FabricPath VLAN is not supported.

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, do one of the following:

- Configure one of the clients as the server.
- Complete these 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.

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

Behavior of Control Plane Packets on 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 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 the following error:

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

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

Enter Yes to the prompt “This command will reboot the system. (y/n)? [n] y.”

There is no operational impact and no configuration loss when the switch reloads.

PONG in a vPC Environment

There are two situations where **PONG** is not supported in a vPC environment:

- 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 need 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 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 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 CoPP rate limiters.

Standby Supervisor Can Reset with Feature-Set Operation

The standby supervisor might reload when a feature-set operation (install, uninstall, enable, or disable) is performed if the 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 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 it 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.

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 is RBAC for the Cisco Nexus 7000 Series switches, which is different from that for the Cisco MDS 9500 Series switches.

RBAC CLI scripts used in Cisco MDS 9500 Series switches 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, make sure to assign RBAC in Cisco MDS and the Cisco Nexus 7000 storage VDC to different Cisco Fabric Services (CFS) regions.

Level 4 Protocol Entries on the M Series Modules

There is a limitation of using 7 entries for Level 4 protocols on the M Series modules.

Proxy Limitation for the N7K-F132XP-15 Module

When the 6-port 40-Gigabit Ethernet I/O module XL (M2 Series) (N7K-M206FQ-23L) acts as a proxy for more than 90 G traffic from the 32-port 10-Gigabit Ethernet I/O module XL (N7K-F132XP-15), packet drops can occur. You might experience this issue if ports are oversubscribed on the N7K-F132XP-15 F1 Series module.

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/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 a L3 sub-interface to force the dot1q over the L3 interconnection.

Fabric Module Removal on the Cisco Nexus 7700 Series

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

Fabric Utilization on the Cisco Nexus 7700 Series

When traffic ingresses from a module on the Cisco Nexus 7700 Series 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 Series 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.

Clearing FEX Queuing Statistics Is Not Supported

Cisco NX-OS Release 7.2(0)D1.1 does not support clearing queuing statistics for FEX host interfaces.

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 part of the bridge domain (BD). This issue occurs when multicast traffic is sent to OMF LTL, which happens if an unknown unicast and flood occur when OMF is enabled.

FEX interfaces can support multicast routers, but OMF on those VLANs must be disabled. 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 a FEX

If an ASCII configuration has incompatible ports, such as when the configuration is created with ports that are added to the FEX from different line cards or VDC type, 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 replayed.

DSCP Queuing with FEX and M1 Series Modules

Differentiated services code point (DSCP) based queuing does not work for FEX uplinks to the 32-port 10-Gigabit Ethernet SFP+ I/O module (N7K-M132XP-12) or the 32-port 10-Gigabit Ethernet SFP+ I/O module XL (N7K-M132XP-12L). All FEX data traffic will be in the default queue.

This limitation applies only when a FEX is attached to ports on a N7K-M132XP-12 or N7K-M132XP-12L module. It does not affect COS based queuing.

DHCP Snooping with vPC+ FEX

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

Storm-control Suppresses Unicast Traffic

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

Upgrade/Downgrade Paths and Caveats

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

- Supported Upgrade and Downgrade Paths
- In-Service Software Upgrade (ISSU)
- Non In-Service Software Upgrade (ISSU) Steps
- In-Service Software Upgrade (ISSU) Caveats
- Non In-Service Software Downgrade (non-ISSU)/Cold Boot Downgrade Steps

Supported Upgrade and Downgrade Paths

Note 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.

Do not change any configuration settings or network settings during a software upgrade. Any changes in the network settings might cause a disruptive upgrade.

See Table 7 for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 7.2(2)D1(1). Releases that are not listed for a particular release train do not support a direct ISSU.

See Table 8 for the ISSU path to Cisco NX-OS Release 7.2(1)D1(1). Releases that are not listed for a particular release train do not support a direct ISSU.

See Table 9 for the ISSU path to Cisco NX-OS Release 7.2(0)D1(1). 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 7.2(0)D1(1) and later releases.

SMUs are dependent on the version of Cisco NX-OS software release installed. You need to install SMUs compatible with your release. Moving to another Cisco NX-OS software release using reload or ISSU will inactivate the SMUs installed for the previously installed Cisco NX-OS software release. For example, if you have SMUs for Cisco NX-OS Release 7.2.0 in your Supervisor 2 setup, moving to an image of another release, say Cisco NX-OS Release 7.2.2 will cause the SMU to become inactive.

However, once the upgraded system is running the new target code, the fix from SMU will no longer be activated. If your new upgraded version does not have the fix from the SMU, you can obtain and install the SMU corresponding to your new release. See the Guidelines and Limitation of SMU for details on installing SMU.

Note For a non-disruptive upgrade dual supervisor modules are required.

ISSU Paths for Cisco NX-OS Release 7.2(2)D1(2)

See Table 6 for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 7.2(2)D1(2).

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

Table 6 Supported ISSU Paths for the Cisco Nexus 7000 and 7700 Series Chassis (Cisco NX-OS Release 7.2(2)D1(2)

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release

Cisco NX-OS Release 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)

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 7.2(2)D1(1)

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

Table 7 Supported ISSU Paths for the Cisco Nexus 7000 and 7700 Series Chassis (Cisco NX-OS Release 7.2(2)D1(1))

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

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 7.2(1)D1(1)

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

Table 8 Supported ISSU Paths for the Cisco Nexus 7000 and 7700 Series Chassis (Cisco NX-OS Release 7.2(1)D1(1))

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

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 7.2(0)D1(1)

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

Table 9 Supported ISSU Paths for the Cisco Nexus 7000 and 7700 Series Chassis (Cisco NX-OS Release 7.2(0)D1(1))

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

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]
```

In-Service Software Upgrade (ISSU)

To perform an ISSU upgrade to Cisco NX-OS Release 7.2(x) from one of the ISSU supported releases listed in the tables in the preceding section, follow these steps:

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

In-Service Software Upgrade (ISSU) Caveats

- When you upgrade to Cisco NX-OS Release 7.x and if you are using a non-default native VLAN (other than vlan 1), ensure you have the VLAN created on the switch, otherwise spanning tree BPDUs will be dropped.
- When you perform ISSU in a set up where the Routing Information Protocol (RIP) has dependency on other protocols for redistribution, you should adjust the RIP timers because RIP does not support stateful restart. Use the **timers basic** *update invalid holddown flush* command in the address-family-mode under the router configuration mode to adjust the timer values.
- SMU on the F3 module bound process is not supported in Cisco NX-OS Release 7.2(1)D1(1). After you install, activate, commit, and reload the switch, SMU on an F3 module will not be active. SMU on the F3 module bound process is supported from Cisco NX-OS Release 7.2(2)D1(1) onwards.
- When you upgrade to either Cisco NX-OS Release 7.2(0) or Cisco NX-OS Release 7.2(1) you need to remove any existing FabricPath BFD configuration. FabricPath BFD is not supported in Cisco NX-OS Release 7.2(0) and Cisco NX-OS Release 7.2(1). FabricPath BFD is supported from Cisco NX-OS Release 7.2(2) onwards.
- FCoE FEX
  - Post ISSU you need to change port-channel load-balance for FEX, 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 default load-balance after changing the load-balance for FEX.
- Before downgrading to unsupported release, F3 FCoE License installed in the 7.2(0) release should be uninstalled.
- For the ISSU support details for VXLAN flood and learn deployment, refer to the following: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/vxlan/configuration/guide/b_NX-OS_VXLAN_Configuration_Guide/configuring_vxlan_flood_and_learn.html#concept_A7EB2DCC739E4E24AF24E20E7A6BF4F8.
- ISSU from 6.2.X to 7.2(0) with MPLS L2VPN configuration:

  - After upgrading ISSU to 7.2(0)D1(1) MPLS L2VPN/L3VPN service updates are not processed in F3 modules.This happens when F3 module is a part of a VDC that already has MPLS configured in it. To resolve this issue, reload the F3 module after ISSU and before you do any further updates on MPLS L2VPN/L3VPN.
- 6.2.X to 7.2(0) ISSU support for OTV/GRE/ERSPAN on F3 series modules:
  - ISSU is blocked and it requires cold boot from 6.2.X to 7.2(0) when OTV/GRE/ERSPAN is enabled on F3.
- ISSU from releases prior to Cisco NX-OS Release 7.2(0)D1(1) is not supported when OTV, GRE or ERSPAN are configured on the F3 series modules:
  - The tunneling architecture for the F3 series module has been changed in the Cisco NX-OS Release 7.2(0)D1(1) in such a way that upgrading from 5.x or 6.x to 7.2.(0) is a disruptive process. Therefore ISSU is not supported from releases prior to the Cisco NX-OS Release 7.2(0)D1(1) release if OTV, GRE or ERSPAN have been enabled in VDCs where F3 series module interfaces have been allocated.
  - There are two approaches to re-enabling ISSU support:

    i) Completely remove the OTV, GRE, and/or ERSPAN configurations from VDCs where F3 series module interfaces are allocated.

    ii) Removing the F3 series module interfaces from VDCs where OTV, GRE, and/or EERSPAN have been deployed on non-F3 series modules.
  - ISSU is still fully supported if these features (OTV/GRE/ERSPAN) are enabled in VDCs with non-F3 series modules.
- For multi-hop 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 In-Service Software Upgrade (ISSU) Steps

To perform a non-ISSU upgrade to Release 7.2(x) from any supported Cisco NX-OS release prior to Release 7.2(0), follow these steps:

1. Change the boot variable.

   Example:

   ```
   boot kickstart bootflash:/n7000-s2-kickstart.7.2.0.D1.1.bin sup-1
   boot system bootflash:/n7000-s2-dk9.7.2.0.D1.1.bin sup-1
   boot kickstart bootflash:/n7000-s2-kickstart.7.2.0.D1.1.bin sup-2
   boot system bootflash:/n7000-s2-dk9.7.2.0.D1.1.bin sup-2
   ```

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

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

To perform a non-ISSU upgrade from any supported Cisco NX-OS release PRIOR to Release 6.2(2) or 6.2(2a), 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. Change the boot variable to boot Release 7.2(0)D1(1).
4. Enter the **copy running-config startup-config vdc-all** command.
5. Enter the **reload** command to reload the switch.

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

6. Once all modules come up, enter the **show running-config aclmgr** command in all VDCs.
7. Enter the **clear inactive-config acl** command for all VDCs.
8. Enter the **copy bootflash:/vdc_x/aclmgr-inactive-config.cfg running-config** command for all VDCs.

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

Note Non-ISSU upgrades/downgrades are also referred to as cold boot. During a cold boot, the network administrator changes the boot variables for the system image and the kickstart image followed by a switch reload.

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, NXOS 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.

Cisco NX-OS Release 7.2(2)D1(2) has the following cold boot support matrix:

Table 10 Supported Cold Boot Matrix in Cisco NX-OS Release 7.2(2)D1(2)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
7.2(2)D1(2)	7.2(2)D1(1)
7.2(2)D1(2)	7.2(1)D1(1)
7.2(2)D1(2)	7.2(0)D1(1)
7.2(2)D1(2)	6.2(24a)
7.2(2)D1(2)	6.2(24)
7.2(2)D1(2)	6.2(22)
7.2(2)D1(2)	6.2(20a)
7.2(2)D1(2)	6.2(20)
7.2(2)D1(2)	6.2(18)
7.2(2)D1(2)	6.2(16)
7.2(2)D1(2)	6.2(14)
7.2(2)D1(2)	6.2(12)
7.2(2)D1(2)	6.2(10)
7.2(2)D1(2)	6.2(8b)
7.2(2)D1(2)	6.2(8a)
7.2(2)D1(2)	6.1(5a)
6.1(5a)	7.2(2)D1(2)
6.2(8a)	7.2(2)D1(2)
6.2(8b)	7.2(2)D1(2)
6.2(10)	7.2(2)D1(2)
6.2(12)	7.2(2)D1(2)
6.2(14)	7.2(2)D1(2)
6.2(16)	7.2(2)D1(2)
7.2(0)D1(1)	7.2(2)D1(2)
7.2(1)D1(1)	7.2(2)D1(2)
7.2(2)D1(1)	7.2(2)D1(2)

Cisco NX-OS Release 7.2(2)D1(1) has the following cold boot support matrix:

Table 11 Supported Cold Boot Matrix in Cisco NX-OS Release 7.2(2)D1(1)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
7.2(2)D1(1)	7.2(1)D1(1)
7.2(2)D1(1)	7.2(0)D1(1)
7.2(2)D1(1)	6.2(24a)
7.2(2)D1(1)	6.2(24)
7.2(2)D1(1)	6.2(22)
7.2(2)D1(1)	6.2(20a)
7.2(2)D1(1)	6.2(20)
7.2(2)D1(1)	6.2(18)
7.2(2)D1(1)	6.2(16)

Table 11 Supported Cold Boot Matrix in Cisco NX-OS Release 7.2(2)D1(1)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
7.2(2)D1(1)	6.2(14)
7.2(2)D1(1)	6.2(12)
7.2(2)D1(1)	6.2(10)
7.2(2)D1(1)	6.2(8b)
7.2(2)D1(1)	6.2(8a)
7.2(2)D1(1)	6.1(5a)
6.1(5a)	7.2(2)D1(1)
6.2(8a)	7.2(2)D1(1)
6.2(8b)	7.2(2)D1(1)
6.2(10)	7.2(2)D1(1)
6.2(12)	7.2(2)D1(1)
6.2(14)	7.2(2)D1(1)
6.2(16)	7.2(2)D1(1)
7.2(0)D1(1)	7.2(2)D1(1)
7.2(1)D1(1)	7.2(2)D1(1)

Cisco NX-OS Release 7.2(1)D1(1) has the following cold boot support matrix:

Table 12 Supported Cold Boot Matrix in Cisco NX-OS Release 7.2(1)D1(1)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
7.2(1)D1(1)	7.2(0)D1(1)
7.2(1)D1(1)	6.2(24a)
7.2(1)D1(1)	6.2(24)
7.2(1)D1(1)	6.2(22)
7.2(1)D1(1)	6.2(20a)
7.2(1)D1(1)	6.2(20)
7.2(1)D1(1)	6.2(18)
7.2(1)D1(1)	6.2(16)
7.2(1)D1(1)	6.2(14)
7.2(1)D1(1)	6.2(12)
7.2(1)D1(1)	6.2(10)
7.2(1)D1(1)	6.2(8b)
7.2(1)D1(1)	6.2(8a)
7.2(1)D1(1)	6.1(5a)
6.1(5a)	7.2(1)D1(1)
6.2(8a)	7.2(1)D1(1)
6.2(8b)	7.2(1)D1(1)
6.2(10)	7.2(1)D1(1)
6.2(12)	7.2(1)D1(1)
6.2(14)	7.2(1)D1(1)
7.2(0)D1(1)	7.2(1)D1(1)

Non In-Service Software Downgrade (non-ISSU)/Cold Boot Downgrade Steps

Instructions provided below list the steps for the cold boot (non-ISSU) downgrade. This is an example of a cold boot downgrade of a switch that is running Cisco NX-OS Release 7.2(x) and needs to reload with Cisco NX-OS Release 6.2 (12).

- 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.

EPLD Images

Cisco NX-OS Release 7.2(0)D1(1) includes new EPLD images for the supervisor 2E module, N77-C7702-FAN, and the F3 series modules as listed below. For more information about upgrading to a new EPLD image, see the Cisco Nexus 7000 Series FPGA/EPLD Upgrade Release Notes, Release 7.2.

- Supervisor 2E module (N77-SUP2E) (from 19.000 to 20.000)
- N77-C7702-FAN (Version 0.016)
- F3 Series 48-port, 1- and 10-Gigabit Ethernet I/O module (N77-F348XP-23) (from 1.007 to 1.008)
- F3 Series 12-port, 100-Gigabit Ethernet I/O module (N77-F312CK-26) (Version 0.019)
- F3 Series 48-port, 1- and 10-Gigabit Ethernet I/O module (N77-F348XP-23) (from 1.004 to 1.007)
- F3 Series 48-port, 1- and 10-Gigabit Ethernet I/O module (N77-F348XP-23) (from 0.026 to 0.031)
- F3 Series 48-port, 1- and 10-Gigabit Ethernet I/O module (N77-F348XP-23) (from 1.002 to 1.003)

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.

The Cisco Nexus 7000 Series Network Analysis Module (Cisco NAM-NX1) also includes an EPLD image that is programmed on the device.

New Hardware

This section briefly describes the new hardware introduced in Cisco NX-OS Release 7.2(0)D1(1). For detailed information about the new hardware, see the *Cisco Nexus 7000 Series Hardware Installation and Reference Guide.*

This section includes the following topics:

Cisco Nexus 7702 Switch

The Cisco Nexus 7702 switch is a 2-slot switch with 1 slot for a supervisor module and 1 slot for an I/O module. It supports Supervisor 2E modules and F3 series I/O modules. It does not support F2E series I/O modules. The Cisco Nexus 7702 switch supports NX-OS patching, Graceful Insertion and Removal, and disruptive upgrade with installer. The Cisco Nexus 7702 switch has two power supply module slots and supports all power supply redundancy modes.

The Cisco Nexus 7702 switch has one fan-tray which has 3 variable speed fans.

  - If one fan fails, the remaining two fans run at full speed to keep the switch operational. An alert will also be displayed every 10 seconds.
  - If two or more fans fail, the switch will shut down in 120 seconds.
  - If the fan-tray is removed, the switch will shut down in 120 seconds.

- All Supervisor 2E modules shipped with the Nexus 7702 switch will be shipped with FPGA version 1.4.
  - If you install a spare Supervisor 2E module on the Nexus 7702 switch you must upgrade the FPGA version to 1.4.
  - In such a situation you will be notified with alert: "<<%PLATFORM-1-PFM_ALERT>> Incompatible Sup FPGA(12), upgrade FPGA >= 0x14 ".

Note I/O Module cannot be used till the Sup2E upgrade is completed.

New and Enhanced Software Features

This section briefly describes the new and enhanced features introduced in Cisco NX-OS Release 7.2(0)D1(1) and Cisco NX-OS Release 7.2(1)D1(1) software. For detailed information about the features listed, see the documents listed in the "Related Documentation" section. The "New and Changed Information" section in each of these books provides a detailed list of all new features and includes links to the feature description or new command.

This section includes the following topics:

- Cisco NX-OS Release 7.2(2)D1(1)
- Cisco NX-OS Release 7.2(1)D1(1) – Software Features
- Cisco NX-OS Release 7.2(0)D1(1) – Software Features

Cisco NX-OS Release 7.2(2)D1(1)

Cisco NX-OS Release 7.2(2)D1(1) does not have any new feature and this is a bug fix only release.

Cisco NX-OS Release 7.2(1)D1(1) – Software Features

Cisco NX-OS Release 7.2(1)D1(1) includes the following features:

- BFD FSA Offload on F3
- Cisco TrustSec MACSec over FabricPath on F3
- ITD Destination NAT
- Multiple Device-Groups within an ITD Service
- Scale Limit Monitoring

BFD FSA Offload on F3

The BFD Fabric Services Accelerator (FSA) Offload on F3 Line Card feature allows the offload of asynchronous BFD transmission (Tx) and reception (Rx) to the network processing unit on the F3 line card. The BFD FSA Offload on F3 Line Card feature improves scale and reduces the overall network convergence time by sending rapid failure detection packets (messages) to the routing protocols for recalculating the routing table.

Cisco TrustSec MACSec over FabricPath on F3

Cisco TrustSec MACSec is supported over FabricPath via native VLAN tagging on trunk and FabricPath ports feature. Native VLAN tagging can be configured either globally or on an interface for control packets and data packets.

Starting from Cisco NX-OS Release 7.2(1)D1(1), Cisco TrustSec MACsec support on FabricPath is available on F3 modules.

ITD Destination NAT

Network Address Translation (NAT) is a commonly deployed feature in load balancing, firewall, and service appliances. Destination NAT is one of the types of NAT that is used in load balancing because of the following advantages it provides:

- The traffic from source or client to the virtual IP address is rewritten and redirected to server.
- The traffic from the source or client to the destination or server, which is the forward path, is handled as follows: the traffic from the source or client to virtual IP address is translated and redirected as the traffic from source to the destination or server.
- The traffic from the destination to the source or client, which is the reverse path, is re-translated with the virtual IP address as the source IP address. That is, the traffic from the server or source to the client or destination is translated as client or source to client or destination.

Multiple Device-Groups within an ITD Service

The feature, by enabling the existence of multiple device-groups per service on the same interface, allows the ITD to scale. The traffic from one ingress interface is distributed based on both VIPs and device-groups.

An ITD service generates a single route-map that has next hops point to nodes from different device-groups.

Scale Limit Monitoring

Cisco NX-OS Release 7.2(1)D1(1) introduced support for scale limit monitoring on Cisco Nexus 7000 Supervisor 2 and Supervisor 2E and on Cisco Nexus 7700 switches. The Scale Limit Monitoring feature enables you to monitor the scale limit both at the system level and the VDC level. This feature monitors the scale limits for various features across different VDCs on the device and alerts you if the system crosses the permissible scale limit.

Cisco NX-OS Release 7.2(0)D1(1) – Software Features

Cisco NX-OS Release 7.2(0)D1(1) includes the following features:

- Dynamic Fabric Automation (DFA)
- Enhancements on the F3 Module
- FCoE Enhancements
- Platform Enhancements

Dynamic Fabric Automation (DFA)

This software release is the first release to support Cisco's Evolutionary Data Center Fabric solution called Dynamic Fabric Automation (DFA). DFA is evolutionary and is based on the industry leading Unified Fabric solution.

DFA focuses on simplifying, optimizing and automating data center fabric environments by offering an architecture based on four major pillars namely Fabric Management, Workload Automation, Optimized Networking and Virtual Fabrics. Each of these pillars provide a set of modular functions which can be used together or independently for easiness of adoption of new technologies in the data center environment.

Complete details on the DFA architecture can be found at: http://www.cisco.com/go/dfa.

DFA allows optimization of data centers through integration of Fabric Management, Workload Automation, Optimized Networking using enhanced forwarding and Anycast distributed gateway functionality and Virtual Fabrics. For more information on DFA configuration refer Cisco Dynamic Fabric Automation Configuration Guide.

Multi-tenancy

Multi-tenancy is a concept that refers to the logical isolation of shared virtual compute, storage, and network resources. In multi-tenant data center, tenants subscribe to virtual data center (VDC), and based on the services hosted by the tenants within the virtual data center, each virtual data center can have multiple VN-Segments.

Multi-tenant data center handles the traffic segregation between different tenants, and also within tenant traffic, for security and privacy.

Conversational Learning

You can enable conversational learning on all leaf nodes by using the **fabric forwarding conversational-learning all** command. For this command to work, the subnet needs to be instantiated on the leaf. But in case of a border leaf, this is not true as the border leaf might not have any hosts connected to it. So, the routes will always get installed in forwarding information base (FIB). But border leaf is the point of heavy load in the network and needs to conserve precious forwarding space. In this regard, we can add configuration at the border leaf for each subnet using the **fabric forwarding aggregate-subnet-prefix** command.

To enable Layer-3 conversational learning-based route download into the forwarding information base (FIB), use the **fabric forwarding conversational-learning all** command. And to configure the conversational aging timeout value, use the **fabric forwarding conversational-aging timeout** command.

Auto Configuration

Auto Configuration simplifies the management of the VRF and VLAN/BD configurations. Auto configuration can be triggered by:

- Any data frame Frame snooping
- VDP signaling from the server

Single Point of Management (SPOM)

Single Point of Management (SPOM) feature provides a single point of access from any switch to any other switches in the fabric.

SPOM utilizes XMPP as a communication protocol. SPOM feature allows customers to use XMPP chat clients running on laptops, mobile devices to talk to SPOM feature enabled switches in the network and execute the CLI commands remotely from XMPP clients.

Extensible Messaging and Presence Protocol (XMPP)

Extensible Messaging and Presence Protocol (XMPP) is a communication protocol. XMPP clients set up TCP based XMPP connection to XMPP server. XMPP server forwards the messages from one client to another client or a group of clients based on the configuration and request.

This XMPP protocol is adopted by DFA, so the administrator can manage (by issuing CLI commands) a device or group of devices in the network from the administrator’s XMPP connection with a single point of management with no separate login required for each device. Each device is a XMPP client that can be configured to connect to XMPP server. The administrator issues the CLI command and the device receives the CLI commands. Device processes the CLI commands and sends CLI output back to the administrator XMPP client.

XMPP client support is added to the Cisco NX-OS operating system with DFA from 7.2(0)D1(1) for Cisco Nexus 7000 Series Switches.

Cable Management

In a highly meshed network such as Clos topology based network fabric, miscabling can be a pragmatic problem leading to painful troubleshooting without sufficient support. The cable management feature calls out for two mechanisms to address the miscabling issues caused due to human errors. The first mechanism is based on the tier-based checks and the second mechanism is based on a user-defined cabling plan.

Enhancements on the F3 Module

VXLAN (L2/L3 gateway and BGP EVPN)

VXLAN is MAC in IP (IP/UDP) encapsulation technique with a 24-bit segment identifier in the form of a VNID (VXLAN Network Identifier). The larger VNID allows LAN segments to scale to 16 million in a cloud network. In addition, the IP/UDP encapsulation allows each LAN segment to be extended across existing Layer 3 network making use of L3 ECMP.

This feature set includes; Flood and Learn using outer multicast group for Broadcast, unknown unicast and multicast traffic, and L2/L3 VXLAN Gateway.

VXLAN with the MP-BGP/EVPN control plane is supported with the Cisco Nexus 7000 series switch acting as border-leaf with no L2 gateway functionality, vPC or ingress replication support.

MPLS on F3

Support for the following MPLS features has been added to F3 modules- MPLS L2VPN, MPLS L3VPN, MPLS TE, MPLS TE-CBTS, MPLS QoS, 6PE/6VPE and MVPN. The forwarding scale for these features is limited to the size of hardware tables (TCAM and adjacencies - 64K) on F3 modules. Control plane scale-like number of VRFs remains same as M Series modules.

EVC infrastructure has also been added for F3 modules.

MPLS Inter AS option B

With inter AS option A solution, back-to-back VRF between ASBR needs to be configured for routing exchange for each VRF. With Inter AS option B, there will be single eBGP VPNV4 connection between ASBRs and they can exchange routes associated with all VRFs.

This feature is supported on F3, M1, and M2 modules.

LISP support on F3

The following features are supported:

- ITR, ETR, and Host Mobility support on F3 modules.
- Hand off between VXLAN and LISP encapsulations is supported on F3 modules.
- Selective VRF is also supported for LISP.

Physical Port vPC for F3

Enables physical port virtual port channel for F3 modules.

F3 ERSPAN Termination

This feature supports termination of ERSPAN traffic entering F3 interfaces. It is supported for both ERSPAN type II and type III.

FCoE Enhancements

FCoE on F3

This feature brings support for T11's FC-BB_E standard FCoE over lossless Ethernet on F3-series module variants to Cisco Nexus 7000 series and Cisco Nexus 7700 series platforms in storage VDC.

The following F3 cards are supported on FCoE:

- N77-F348XP-23 (48 port 10G card for Cisco Nexus 7700 Series)
- N77-F324FQ-25 (24 port 40G card for Cisco Nexus 7700 Series)
- N7K-F312FQ-25 (12 port 40G card for Cisco Nexus 7000 Series)

Refer to Table 3 for more details on the FEX modules supported by the Cisco Nexus 7000 Series I/O modules.

FCoE FEX

The FCoE over Fabric Extenders (FEX) feature allows Fibre Channel traffic to be carried on a FEX port. To enable this feature, the FEX port is shared with the storage Virtual Device Context (VDC). The FEX is connected to the Cisco Nexus 7000/7700 device through a Fabric Port Channel (FPC). FCoE over FEX enables provision of FCoE on host connections.

The following FCoE FEX models are supported:

- N2K-C2232PP-10GE
- N2K-B22HP-P

Refer to Table 3 for more details on the FEX modules supported by the Cisco Nexus 7000 Series I/O modules. Refer to Cisco NX-OS FCoE Configuration Guide for FCoE FEX configuration details.

FCoE on FabricPath over Spine

Fibre Channel over Ethernet (FCoE) enables I/O consolidation. It permits both LAN and SAN traffic to coexist on the same switch and the same wire. This feature enables you to consolidate multiple separate networks into a single converged infrastructure.

Beginning with Cisco NX-OS Release 7.2(0)D1(1), you can use a Cisco Nexus 7000/7700 device as a spine in an FCoE over FabricPath network. Quality of Service (QoS) settings are enabled on the spine. Refer to Cisco NX-OS FCoE Configuration Guide for more details on FCoE on FabricPath over Spine.

FCoE Scale

Refer to Cisco Nexus 7000 Series NX-OS Verified Scalability Guide for FCoE over FEX scale numbers for Cisco NX-OS Release 7.2(0)D1(1).

Platform Enhancements

Graceful Insertion and Removal (GIR)

You can use GIR to isolate a switch from the network in order to perform debugging or an upgrade. When switch maintenance is complete, you can return the switch to normal mode. When you place the switch in GIR/maintenance mode, all protocols are gracefully brought down and all physical ports are shut down. When normal mode is restored, all the protocols and ports are brought back up.

The following protocols are supported:

- Border Gateway Protocol (BGP)
- BGPv6
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- EIGRPv6
- Intermediate System-to-Intermediate System (ISIS)
- Open Shortest Path First (OSPF)
- OSPFv3

The following features are also supported:

- Virtual port channel (vPC)
- Interfaces
- FabricPath

You can create a GIR/maintenance mode profile file before you put the switch in maintenance mode or you can allow the system to create a maintenance mode profile file when you enter the [**no**] **system mode maintenance** command.

You can create maintenance-mode or normal-mode profile files by using the **config profile maintenance-mode type admin** and **config profile normal-mode type admin** commands respectively.

NXOS Patching

This feature provides the following:

- Allows customer to deploy patch for point fixes.
- Unlike engineering specials, ISSU is maintained. Customer can install patches and then do ISSU to next release.
- Both binaries and libraries can be patched.
- Both module and SUP services can be patched.
- Software patching using process-restart/reload or ISSU

Actual deployment of patches might vary based on platform. For example, on some platform, if process to be patched cannot be restarted, patch will be deployed either by reload or ISSU and on other hand software can be patched simply by restarting the process for process-restart patch.

FEX AA features

Fabric Extender (FEX) is a pass-through/mux device designed to provide top of rack or end of line connectivity for servers/hosts. Currently FEX can be connected to only one Cisco Nexus 7000 series switch. If the switch goes down, FEX loses connectivity to the network. Hence all the singly connected hosts via the FEX also lose connectivity to the network. To solve this problem, FEX can be connected to two Cisco Nexus 7000 series switches in Active-Standby mode or Active-Active mode (vPC). We choose the Active-Active solution because vPC provides seamless switchover and faster convergence in case of switch failure. Moreover, traffic is also sprayed across both switches providing full utilization of bandwidth.

vPC Configuration Synchronization

In a vPC topology, Type-1 configuration mismatch between the peer switches can bring down the vPC leg. Administrator has to manually give the same configuration on each vPC peer switch. The vPC configuration synchronization feature provides a mechanism to keep the Type-1 configuration same on both the switches. With this feature enabled, user needs to modify the Type-1 configuration only on one switch and the vpc-config-sync will synchronize the configuration to the peer switch. The vpc-config-sync will support syncing of all global Type-1 configurations and the Type-1 configuration of vPC port-channel/Physical-Port/FEX Active-Active Ports. The vpc-config-sync will also automatically merge the Type-1 configuration when the switch boots up with start-up configuration.

Dynamic Routing over vPC

Dynamic Routing over vPC feature is supported only on F2E and F3 series modules (for IPv4 Unicast traffic only). This feature enables L3 routing protocols such as OPSF to form adjacency with the two vPC peer chassis. The equal routing cost matrices must be configured on applicable interface on each of the vPC peers, failure to do so can result in blocking the traffic. Asymmetric routing feature has to be implemented to address this issue and to configure Dynamic Routing over vPC. Additionally, when Dynamic Routing over vPC is enabled a warning log message is printed.

VIP HSRP Enhancement

Starting with Cisco NX-OS Release 7.2(0)D1(1), the Virtual IP (VIP) Hot Standby Router Protocol (HSRP) enhancement feature provides support for an HSRP Virtual IP configuration to be in a different subnet than that of the interface subnet. This feature is supported only for IPv4 address and not for IPv6. The following are the enhancements:

- Enhance ARP to source with VIP from Supervisor Engine (SUP) for hosts, when the hosts in VIP subnet are referenced by static route to VLAN configuration.
- Support periodic ARP synchronization to VPC peer if VIP HSRP feature is enabled.
- Allow VIP address as the Layer 3 source address and gateway address for all communications with a Dynamic Host Configuration Protocol (DHCP) server.
- Enhance DHCP relay agent to relay DHCP packets with source as VIP address instead of SVI IP when the feature is enabled.

Note HSRP subnet VIP should be configured in the virtual port channel topology.

For more information, see Cisco Nexus 7000 Series Unicast Configuration Guide.

NX-API

NX-API provides programmatic access to the switches by allowing application developers to remotely issue CLI commands over HTTP/HTTPS. It supports requests and responses in JSON-RPC, JSON, and XML formats.

BFD over IP Unnumbered Interfaces

In the leaf-spine architecture to reduce complexity of IP address management, interfaces could be unnumbered (which means configured with no IP addresses) but designated to derive IP address from other numbered interface. BFD is supported over such unnumbered IP interfaces for fast failure detection.

L2 BFD over FabricPath Core Ports

This feature support is added to detect forwarding failures between two directly connected switches in a fabric, which are connected through FabricPath Link. The BFD session exchanges BFD packets with classical Ethernet encapsulation over FabricPath core ports.

L3 BFD Sessions over FabricPath Links

When switches are connected through FabricPath and core port is configured for L3 services over SVI, BFD over FabricPath is required for L3 routing clients for faster convergence. If there are SVIs configured in spine and leaf node with IP addresses and if the neighbor is reachable through FabricPath network, BFD resolves adjacency for the given L3 peer address over FabricPath link and exchanges BFD packets with FabricPath Encapsulation.

VTP v3

VTP3 supports configuration propagation of all 4k VLANs (including private VLANs); an increase from the 1K VLANs in VTPv1/ VTPv2 to 4K in VTP v3.

The introduction of primary VTP server mode eliminates the VTP bombing issue, so a newly inserted VTP switch will not erase other VTP databases in the network.

It supports the propagation of MST configuration, when the switch is configured as MST primary server.

MVPN QoS Enhancement

This feature copies the inner TOS to outer TOS for MVPN.

OTV UDP Encapsulation

OTV UDP encapsulation header support is added on F3 modules. The OTV UDP encapsulation is supported in a F3 only VDC.

LISP Host Route Notification Registration for Host Mobility

Registration of Host Route Notification into LISP Mobility is supported to provide automated interoperability with domains using IGPs, BGP-VPNv4, and BGP-EVPN (VXLAN). Tag-based filtering is supported as part of the Route Notification Registration feature.

FabricPath OAM

FabricPath OAM facilitates operators to monitor, isolate and verify data plane faults on FabricPath networks. FabricPath Ping, Trace route and Multicast Trace route are the 3 main tools. These tools can be invoked on demand. This feature implementation also allows to include flow entropy to validate specific path taken by data in multi path environment.

MAC Security

The MAC Security (MACSec) feature is used for data encryption and decryption. MACSec support is available on F3 Series modules in Cisco NX-OS Release 7.2.0D1(1) with the following caveats:

- F3 Series modules with fiber interfaces—The last eight ports (41 to 48) support MACSec (N7K-F348XP-25 and N77-F348XP-23).

Note On the F3 Series, only the 10-Gigabit I/O module offers MACSec capabilities for classic Ethernet. The 40-Gigabit and 100-Gigabit F3 Series modules do not support MACSec.

TrustSec SGT Enhancement

This feature extends the TrustSec functionality to vPC/vPC+ environments. Specifically, this includes SGT tagging, SGT propagation, IP-SGT mapping, Port-SGT mapping, VLAN-SGT mapping, SGACL enforcement, SGName download, AAA policy download, SXP, MACSec and SGT caching. It is required to ensure consistent TrustSec configuration between vPC/vPC+ peers and no configuration compatibility checks (neither type-1 nor type-2) will be enforced.

SGT classification is a feature that is configurable under “cts manual” and “cts dot1x” modes. The “SGT classification via port-profiles” feature entails the changes to support port-profiles for the SGT configuration.

SGT in conjunction with Anycast HSRP or Active/Standby HSRP

CTS over vPC/vPC+ feature ensures dynamically learnt IP-SGT on both the peers are consistent. The vPC peers could also be HSRP routers.

200K IP-SGT mapping support on the M-Series module with large buffer support

IP-SGT scale is enhanced to support 200K entries subject to LC module’s TCAM capacity. M-series module (XL) supporting large TCAM sizes can easily hold 200K IP-SGT bindings.

Environment data CoA

The environment data changes can be updated using **ISE push** command.

SGACL update method/Per policy CoA

The SGACL policy changes can be updated using **ISE push** command.

CTS Port-channel compatibility check

CTS interface commands are supported under port-channels also with the necessary compatibility checks.

NetFlow

The following NetFlow features are supported beginning with Cisco NX-OS Release 7.2(0)D1(1):

Fabric Services Accelerator (FSA)

FSA is enabled for NetFlow on F3 series module. FSA increases the packet processing up to 50 thousand packets per second.

Egress NetFlow Support on F3 modules

From Cisco NX-OS Release 7.2(0)D1(1) onwards egress NetFlow is also supported on F3 modules. Egress NetFlow is accomplished by the command **ip flow monitor monitor-name output sampler sampler-name**. In earlier software version only ingress NetFlow was supported on F3 modules. Egress NetFlow is not supported on F2 and F2e line cards.

Exposure of 1:128 Sampling on F3 cards

F3 interface allows sampler as m:n for 1<=m<=31 and 1<=n<=131071.

NetFlow Support on F2, F2e, F3 Sub-interfaces

NetFlow is now supported for L3 sub-interfaces on F-series modules. Refer to Cisco Nexus 7000 Series NX-OS System Management Configuration Guide for NetFlow configuration details.

SPAN features

Following SPAN features are introduced:

- Enhanced SPAN filtering capability; by supporting combination of multiple filter rules into filter lists and allowing negative rules. This feature is applicable to extended SPAN sessions only and subject to filter resource availability.

Multiple SPAN sessions are allowed to share same destination interface, as long as rate-limit auto is not configured for these sessions.

ITD Enhancements

Following new ITD features are introduced:

- ITD node-level probes
- ITD node-level standby devices
- ITD IPv4 control plane probes to monitor IPv6 data nodes
- ITD exclude feature

RISE RHI and AutoSPAN

Cisco RISE has been enhanced to support Route Health Injection (RHI) with the Citrix NetScaler products and AutoSPAN with the Cisco Prime NAM appliance. RHI support allows VIP advertisement without the need for running routing instances on the Citrix NetScaler. AutoSPAN enables Cisco Prime NAM users to logically move data ports across VDCs within the Nexus 7000 and automatically setup SPAN sessions directly from the Cisco Prime NAM GUI.

PIM BIDIR Support on F2E

Product Independent Multicast (PIM) Bidirectional (BIDR) is supported in a F2E only Virtual Device Context (VDC), F2E /M VDC (with F2E proxying to M1/M2) and F2E/F3 VDC.

WCCP Configurable Heartbeat/Fast Timers

The WCCP—Fast Timers feature enables WCCP to establish redirection using a configurable message interval when a WCCP client is added to a service group or when a WCCP client fails. WCCP routers and WCCP clients exchange keepalive messages at a fixed interval. Prior to the introduction of the

WCCP—Fast Timers feature, the WCCP message interval was fixed at 10 seconds. The WCCP—Fast Timers feature enables use of message intervals ranging from 0.5 seconds to 60 seconds and a timeout value scaling factor of 1 to 5. The default is 10 seconds. The timer interval is driven by the WCCP client which is being redirected to. The WCCP clients must support variable message interval timers in order for the WCCP—Fast Timers feature to function correctly.

The WCCP message interval capability introduced by the WCCP—Fast Timers feature defines the transmission interval that WCCP clients and WCCP routers use when sending keepalive messages and defines a scaling factor used when calculating the timeout value. The WCCP router uses the timeout value to determine if a WCCP client is no longer available and to redirect traffic as a result. The WCCP router enforces a single message interval per service group. WCCP clients with incompatible message intervals are prevented from joining a service group. If a default message interval that is smaller than the default 10 seconds is used, CPU usage will increase.

Network Interface (NIF) Monitoring

Starting from Cisco NX-OS Release 7.2(0)D1(1), the SNMP trap clogMessageGenerated will carry the syslog payloads as SNMP trap contents. If a feature does not have a trap implemented but the syslog is logged, then the syslog will be carried by the SNMP trap mentioned above.

MIBs

Support for the following MIBs is added in 7.2(0)D1(1):

- CISCO-ENTITY-VENDORTYPE-OID-MIB.my

The following objects are added in this MIB:

MIB Object	Description
cevChassisN77c7702 OBJECT IDENTIFIER ::= {cevChassis 1648}	Cisco NX-OS 7700 2-slot chassis
cevBackplaneN77c7702 OBJECT IDENTIFIER ::= {cevBackplane 70}	Cisco NX-OS 7700 2-slot backplane
cevContainerN77c7702PowerSupplyBay OBJECT IDENTIFIER ::= {cevContainer 336}	Container for Cisco NX-OS 7700 2-slot power supply
cevContainerN77c7702FanBay OBJECT IDENTIFIER ::= {cevContainer 337}	Container for Cisco NX-OS 7700 2-slot fan
cevFanN77c7702Fan OBJECT IDENTIFIER ::= {cevFan 255}	Fan for Cisco NX-OS 7700 2-slot chassis

Licensing

Cisco NX-OS Release7.2(0)D1(1) includes the following changes to Cisco NX-OS software licenses:

- The MPLS feature license (N77-MPLS1k9) includes support for all MPLS features on Cisco Nexus 7700 chassis.

Beginning with Cisco NX-OS Release 7.2(0)D1(1), FCoE is supported on the following F3 Series modules:

- PID: N77-F348XP-23

- PID: N77-F324FQ-25
- PID: N7K-F312FQ-25

The following licenses are available for the Cisco Nexus 7702 switch:

- N77-7702-SBUN-P1
- N77-7702-5LSB-P1
- N77-7706-SBUN-P1
- N77-7718-SBUN-P1
- N77-7710-SBUN-P1

For additional information, see the *Cisco NX-OS Licensing Guide*.

Caveats

VDC Migration:

As part of virtual device context (VDC) migration, the following happens:

- FEX module gets removed in the default VDC
- ASCII configuration replay in the newly created VDC creates the FEX module again.The removal of FEX module from the default VDC triggers a deleted configuration to be sent.

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

- Open Caveats—Cisco NX-OS Release 7.2
- Resolved Caveats—Cisco NX-OS Release 7.2(2)D1(2)
- Resolved Caveats—Cisco NX-OS Release 7.2(2)D1(1)
- Resolved Caveats—Cisco NX-OS Release 7.2(1)D1(1)
- Resolved Caveats—Cisco NX-OS Release 7.2(0)D1(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 7.2

Table 13 Cisco NX-OS Release 7.2(0)D1(1) and Later Releases' Open Caveats

Record Number	Open Caveat Headline
CSCvc72202	CVR-QSFP-SFP10G goes down after the F3 module reload
CSCva36025	ISSU 7.2.1 to 7.2.2: ipfib crashed with ISSU on VPC Multicast scale
CSCuz94088	sftp to n7k works when sftpserver is disabled on n7k

Table 13 Cisco NX-OS Release 7.2(0)D1(1) and Later Releases' Open Caveats

Record Number	Open Caveat Headline
CSCuy81855	SGACL with > 1 ACE is not installed when policy caching is enabled.
CSCul05775	F3 has issues handling packets with SGT tag but without 1Q tag.
CSCuu62173	Reload of 2 modules causing FEX interface missing in storage VDC.
CSCuu07722	IVR zone set not supported for FCoE over FEX.
CSCuu92061	ISSU from 6.2(12) to 7.2(0) is failing in Cisco Nexus 7700 Series/F3 VPC Scale setup.
CSCuu35748	Post ISSU L2VPN pseudo wires don't come UP after reload Peer.
CSCuh57942	FEX Pre-Provisioning Feature to preserve FEX HIF configuration after upgrade
CSCut22695	"mts_drop:2265 proc(/isan/bin/acllog) errno(22)" message seen in Cisco NX-OS Release 7.2 (0)D1(1).
CSCuu33473	BD flap can cause Mac inconsistency leading to L3 traffic drop
CSCuu00448	Blank error output is shown when trying to map vlan-vsan from DM
CSCuu45553	bfd crash seen with bfd_mts_flush_all_bfdc_msgs decodes
CSCuu38313	ETHPORT-2-IF_SEQ_ERROR: Error ("sequence timeout")
CSCut72641	L2BFD: some L2BFD links are not coming up after ascii replay
CSCuo44480	"sh fabric connectivity neighbors" and subcommands are not xmlized correctly
CSCuu59408	ISSU, reload F2 -fex uplink results in DCBX ACK lost
CSCuu18785	ipqosmgr cored while performing ISSU from 7.2.0.475.S16 to upg image
CSCut74651	7.2.0.D1.0.456.S1:: MTS buffer leak at evmc
CSCuu20761	Delete MAC sync issue after LC module reload that does not have PL
CSCuu11726	LIM flush clears non VXLAN macs on the BD affected
CSCuu49461	Sup Mac address table shows VPC peer link for some PVLAN entries
CSCuu34174	UIN-1:After switch reload macs are not in sync between VPC peers
CSCut75451	F1 card clear counters interface should not clear snmp counters.
CSCus47276	f3 mac counters does not match traffic source counters
CSCuu12299	eg lif 0x0, when reload AC module after change AC port from VPWS to VPLS
CSCuu58619	IPFIB vrf dependency database doesn't cleanup on VDC reload
CSCuu04977	lfib memleak at lfib_l2vpn_vpls_pw_add
CSCut71442	"PIM Data Register" debug message missing after receiving data packets
CSCuu31393	RP protocol flags aren't updated on RP mode change
CSCuu36071	Packets encaped with wrong VNI after addition of new link to Peer-link PC
CSCur48779	XML schema for "show mpls switching" is missing ipv4_prefix and in label
CSCut89882	NXOS-MPLS-Traffic loss after SUP Failover
CSCut70347	"show mpls switching" has "(s)" that is ambiguous
CSCuu03546	ulib service crashed on VPLS VPC setup
CSCut86816	Duplicate sampler/no flow creation at device with CE<-->FP vlan toggle
CSCuu02232	L2 NF - does not get programmed with the module reload

Table 13 Cisco NX-OS Release 7.2(0)D1(1) and Later Releases' Open Caveats

Record Number	Open Caveat Headline
CSCut44076	ISSU from 628/6212 to 7.2.0:HMM-3-AUTO_CONF_PROFILE_ERROR
CSCuu00672	vMotion across DCI fails due to RARP packet drop on BL
CSCus57881	VPC PO continuously flapping when untagged frame statement exist
CSCuu22461	FPOAM:Memory leak after Async FPOAM ping
CSCun19959	Cisco Nexus 7000 Series: snmpd: cmd_path_get: invalid component index 0
CSCuu12677	ISL down from show topology after changing service policy of Eth port
CSCut75793	PL pkt drops seen in one F3 inst on allocating another F3 inst to a vdc
CSCus11280	RISE-Indirect service down after management SVI IP change
CSCur06896	Performing rollback and process restart simultaneously causes hap reet
CSCuu54461	Traffic loss seen after BGP Autodiscovery triggers
CSCuu53397	[VXLAN EVPN] clear bgp * results in assert failed messages with Traceback
CSCuu45698	[VXLAN EVPN] Client “bgp-65001”: skipping client convergence message
CSCuu32143	[VXLAN EVPN] Cisco Nexus 7000 Series sup standby is allowing to execute critical restart CLI
CSCut49295	7.2.0.D1.0.444.S3::UIN-1:Seeing BFD/EIGRP flap after doing 2nd SSO
CSCut58899	ISIS cored when add 200 vrfs
CSCut96307	AAFEX bringup delayed as it goes to module timed out after vpcid del add
CSCut40063	Fex in AA mode off lines when simultaneous sh tech from both vpc peers
CSCuu21923	rttMonCtrlAdminFrequency value range incorrect in CISCO-RTTMON-MIB
CSCuu19837	During ISSU and scale testing, some probes get reset
CSCup10237	reaction with missing cfg being triggered on reload
CSCuu11331	Cisco Nexus 7000 Series - SNMP snmpd core os_syscall_ioctl, tcp_api.c, libmts.c running UTE
CSCut39102	stp disputes are seen during vdc reload in vPC + setup
CSCut26755	L3 SVI BFD ACL remove failed on reload of F2 module
CSCuu09287	SSTE: pixm critical message on 'no feature-set fabric'
CSCut34478	unicast route for the NVE peer loopback IP is missing on some ASIC inst
CSCuu53575	sh vlan id 1 shows incorrect ports after doing ASCII replay twice
CSCuu38208	new member add to existing vpc+ PL fails for vlan 4045
CSCuu15391	vsi config is allowed on range of interface even with switchport
CSCuu17217	vntag_mgr crash on c r s + reload
CSCuu20131	During ISSU on vpc setup, VTP type 2 inconsistency has seen
CSCus79530	igmp snooping entry is pointing wrongly to peer-link instead of nve
CSCus93974	NVE peer is not learned later, if the NVE peer delete happens LC ISSU
CSCuw78785	ARP packets loop with dynamic arp inspection in FabricPath network
CSCuw60869	Elame does not work for Cisco Nexus 7700 Series line cards
CSCuw53020	GRE tunnel traffic dropped with drop index 0xcad or randomly punt to CPU

Table 13 Cisco NX-OS Release 7.2(0)D1(1) and Later Releases' Open Caveats

Record Number	Open Caveat Headline
CSCuw34008	F1 FabricPath. Mac not learned when ASA switchover happens
CSCuv93032	eVPC: dual-homed FEX goes off line when reloading one of the eVPC peers
CSCuv91507	Migrating FEX from Cisco Nexus 7000 Series to Cisco Nexus 5000/6000 Series may result in the FEX failing to boot
CSCuw74438	Cisco Nexus 7000 Series L3vm crash during ISSU

Resolved Caveats—Cisco NX-OS Release 7.2(2)D1(2)

Table 14 Cisco NX-OS Release 7.2(2)D1(2) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCuw62175	F3 - MTM FE Timer Expired after Gross Interrupt Threshold Exceeded
CSCva68421	N7K-F3 SMU does not work post reload

Resolved Caveats—Cisco NX-OS Release 7.2(2)D1(1)

The bug fixes pertaining to Cisco NX-OS Release 6.2(16) are also included in the fixed bugs for Cisco NX-OS Release 7.2(2)D1(1) release.

Table 15 Cisco NX-OS Release 7.2(2)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCuw59277	FEX 2348 A-A: Packets send to wrong FEX HIF interface.
CSCut89986	N77: module in failure state after power cycle due to BFDC hogging CPU
CSCux35827	M2 lockup due to ED HANG exceptions prior to RewriteEngine diag Failure
CSCuw95078	M2 VLAN Translation Missing after Module Reload
CSCuw71136	Static Mac address assigned on interface after default interface command
CSCuq94445	ISSU failed: maximum downtime exceeded (0x4093003B)
CSCuo05800	HIF of N2232PP 1G link can't up with 3rd device
CSCux17913	Migrating Fex from N7K to N6K/N5K may result in the FEX failing to boot
CSCuw25153	Traffic loss during HSRP Recovery
CSCuu58251	Missing HSRP VIP v6 link-local after reload of both HSRP routers
CSCuy02120	Memory leak caused by restarting OSPF process
CSCux62214	L2FM consistency checker can cause memory leak / crash
CSCuy07224	Physical VPC on FEX port stays suspended (suspended(LACP misconfig))
CSCuy15221	vPC: F3 module reload delay to unset VSL bit
CSCux60618	BGP RR doesn't send update

Table 15 Cisco NX-OS Release 7.2(2)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCus96878	Nexus7700 FEX interface link flap with FET-10G
CSCuy11493	Errors ""tlvu_table_convert_tlv_to_indv_field" when issuing startup
CSCus26870	December 2014 ntpd CVEs for Nexus 5k/6k/7k/MDS
CSCuw84708	Evaluation of n9k, n3k, mds, n7k and n5k infra for NTP
CSCuz34593	N7K: Incorrect filename when issuing 'copy run ftp'
CSCuw70817	"port-profile type <type>" should not be expected in the rollback diff.
CSCuw81067	DFA: Multicast SG join state missing in BGP
CSCuw92537	L3 DCI autoconfig: VRF stuck in Delete Hold + Improve path invalid debug
CSCux55826	NXOS/BGP: routers not redistributed after ATTR and prefix list change
CSCux09020	NSSA intern router originate default not ASBR post ISSU 6.2.8a to 6.2.12
CSCuy85875	Moved host route does not get installed in HW in LISP IGP Assist in ASM
CSCuw85884	N7K snmpd process seg fault crash
CSCuy07280	Evaluation of N3k,N5k,N7k,N9k for OpenSSL
CSCuv71201	Evaluation of n7k-infra for OpenSSL Vulnerability
CSCuy54488	Evaluation of n7k/n5k/MDS/n9k/n3k/n3500 for OpenSSL
CSCuz52394	Evaluation of N7k/N5k/N9k/N3k/MDS for OpenSSL
CSCux41326	Evaluation of NX-OS for OpenSSL vulnerabilities
CSCuz84286	SNMP crash on 6.2(10) with netsnmp_wrap_up_request
CSCuw76278	NX-OS - Netstack panic crash due to buffer lockup
CSCuz43145	DCNM, DM or SSH login to switch fails - "Unknown User or Password"
CSCux86332	N7K/N6K/N9K/N3K OpenSSH Vulnerabilities
CSCuw32251	Vlan should not aggregate ranges for rollback except for mode FabricPath
CSCuy47006	SSTE: MEv6 BGP neighbours not coming up after Admin VDC migration.
CSCuy70860	Multicast rpf failing in case next hop is HSRP Virtual IP.
CSCuu73828	ipfib crash upon ISSU from 6.2.10 to 7.2.0
CSCuy48431	PHY port VPC in F2/F2E cards does not work with F3 card in same VDC
CSCuy81855	SGACL with > 1 ACE is not installed when policy caching is enabled.
CSCui51401	HW acl entries are not correct when having IPv6 RACL with BFD enabled
CSCuw58529	repeating aclqos crashes caused N7K line card hap reset
CSCux35827	M2 lockup due to ED HANG exceptions prior to RewriteEngine diag Failure
CSCuy49752	N7K-C7700 : Unable to manually walk nexus coppoids cbQosPoliceStatsTable
CSCux03524	N7k: Multicast traffic not transmitted towards FEX on same FE as source
CSCut17599	N7K-F248XT-25E: Periodic PortLoopback Failures for Unknown Reason
CSCut67131	ACL_Deny mis-programmed on F1 when creating a new VDC
CSCuw95078	M2 VLAN Translation Missing after Module Reload
CSCuw71136	Static Mac address assigned on interface after default interface command

Table 15 Cisco NX-OS Release 7.2(2)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCuw76844	N77-F348XP-23 may reload on executing some show CLI on down-rev firmware
CSCuw25153	Traffic loss during HSRP Recovery
CSCuw61229	Bringing up new L3 interface may break BFD redirect adj with new int lif
CSCux78124	Broadcasts ingressing F3 cards is sent to Sup with no SVI for that vlans
CSCuw51522	Mac learnt on ES ID for host vpc+ port operating in individual mode
CSCuy02120	Memory leak caused by restarting OSPF process
CSCuy51650	iscm cores for vdc deletion
CSCux28796	OIL is not copied from (*,G) to (S,G)
CSCux99818	pim process crash at pim_get_rp_by_rp
CSCuy42849	Wrong PIM assert sent by the PE device in MPLS network (Nexus device)
CSCux19585	Increase the auto-recovery to 1 day (86400 secs)
CSCuw98364	F3: OTV broadcast/smac route PSSing wrong inst bitmap for tcam
CSCux48649	OTV with F3 can only support 50 data-groups after AED failover
CSCux19294	MPLS TE - RSVP BW incorrect for 40G and 100G interfaces
CSCuv42308	MST Disputes VPC peer-switch secondary peer sending cost of 250
CSCuu78360	Vlans not getting registered properly when mvrp configured with VPC
CSCus96878	Nexus7700 FEX interface link flap with FET-10G
CSCuv64056	N7K/N77 support NX-OS mechanism to upgrade firmware on eUSB flash
CSCup81570	npacl filter missing for line vty, also action logged is incorrect
CSCuo15557	VTY ACL with permit established keyword, permits all hosts to SSH in
CSCuy51803	otm cores found after switchover and power up of Lc
CSCuv95316	Pixmc core being observed after insert new sup or reload chassis
CSCux94893	N77: There is difference to detect removing linecard by slot number
CSCuw70817	"port-profile type <type>" should not be expected in the rollback diff.
CSCuw86978	F2E 6.2.(14) upgrade fail %VMM-2-VMM_SERVICE_ERR: VDC1: Service SAP
CSCuv80499	BGP flapping with same AS-PATH ACL matched in two or more route-map seqs
CSCux55826	NXOS/BGP: routers not redistributed after ATTR and prefix list change
CSCuy26997	eirgp core @ urib_rt_mod_nh_del
CSCuw57347	IS reachability TLV not suppressed while extended reachability TLV is
CSCus02840	IS-IS IPv6 MTR is not working
CSCuy30270	LISP: synch leads to frequent uRIB writes, which block route reads
CSCuv66399	Forwarding address not set in OSPF for routes w/ different prefix length
CSCux09020	NSSA intern router originate default not ASBR post ISSU 6.2.8a to 6.2.12
CSCuw27044	OSPFv3 takes 30 min to install route when using link-local addresses
CSCux59834	Limit OTV data-group configuration to /24

Table 15 Cisco NX-OS Release 7.2(2)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCux98493	Need to block ISSU to 7.3 if OTV data-group mask is </24
CSCuu01234	OTV, next hop pointing to wrong AED - OTV Part
CSCuq72316	N7K:Static route leak w/ unconfig/config SVIs cause traffic black hole
CSCuw85884	N7K snmpd process seg fault crash
CSCuw76278	NX-OS - Netstack panic crash due to buffer lockup
CSCuq18021	SNMPset to community strings with special characters cause hap reset
CSCuu83574	Error in syslog of interface flap event after reload in remote server
CSCux93410	New vlan mapping not in running config after upgrade to 6.2(14)

Resolved Caveats—Cisco NX-OS Release 7.2(1)D1(1)

Table 16 Cisco NX-OS Release 7.2(1)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCuu75466	Cisco Nexus 7000 Message of the Day (MOTD) Telnet Login Vulnerability
CSCuu88453	Nexus 7010 show hardware access-list database policy output has error
CSCuu43851	Service "plog" cores
CSCuv10652	"bfd optimize subinterface" is lost after upgrade from 5.2(9) to 6.2(2)
CSCus72364	Cisco Nexus 7000 Series BFD brings down additional BFD peers - bfd optimize subinterface
CSCus47263	vPC suspension following reload with peer-link on F3 and PKA on M-Series
CSCur22130	IF-MIB::ifInDiscards erroneously increment for SNMP on M2
CSCut50838	M2 VLAN Translation Not Translating Non-Native VLAN BPDUs
CSCut17447	SPAN dest port load balancing doesn't work with M2 as span src
CSCuw10915	MPLS ldp sync disappears after interface flap
CSCuu89065	Activating L2 NetFlow causes mac flap on F2
CSCuw22271	F2/F2-E unexpected reload after span session config
CSCuu30447	F2/F2E port will keep up even the rx power is -26dBm due to ISP break
CSCut17599	N7K-F248XT-25E: Periodic PortLoopback Failures for Unknown Reason
CSCus32949	Cisco Nexus 7000 Series: flowcontrol configuration is not set after NX-OS downgrade.
CSCuv23184	Mac is egress learnt pointing to index in different VDC on M
CSCuw51522	Mac learnt on ES ID for host vpc+ port operating in individual mode
CSCuu81686	DNL bit cleared on Port-Security port-channel on member event

Table 16 Cisco NX-OS Release 7.2(1)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCuw51036	%ETHPORT-3-IF_UNSUPPORTED_TRANSCEIVER:" for LOROM twinax cable
CSCuv14400	FEX-fabric sfp invalid on N77-F324FQ-25
CSCuo98502	Port-channel MTU not set correctly if configured on members first
CSCuu72468	UDLD-4-UDLD_SFP_TYPE_CHANGED: User changed SFP type from fiber to copper
CSCut03392	Cisco Nexus 7000 Series: Dynamic Mac pointing to wrong DI on M module
CSCut05438	Cisco Nexus 7700 Series: F3 100G ipc-channel status always show fail
CSCuu13781	F3 - MTM FE Timer Expired after Gross Interrupt Threshold Exceeded
CSCuv40883	F3 unexpected reload after span session config
CSCuv76651	SGT registers not programmed properly for F3 LC
CSCuv20611	NetApp: Response to VLAN Request seen after vfc port was shut
CSCuu73084	HSRP Bundle in INIT state after reload
CSCuu35062	Cisco Nexus 7000 Series hsrp error with more than 255 secondary ip on an interface
CSCuw61229	Bringing up new L3 interface may break BFD redirect adj with new int lif
CSCut36425	F3 in FP transit mode - All traffic drop due to ports in CE mode
CSCuw38895	FabricPath Multicast traffic being forwarded incorrectly in vPC+
CSCuw13611	otv extended vlans suspended due to "IFTMC PD commit db search failed"
CSCug26438	Cisco Nexus 7000 Series: rate is 0 for conform/exceed/violate under type qos policy-map
CSCuv61896	show mac address-table should not fill up mtm debug logs
CSCut75457	HSRP VACL Filter Broken
CSCuv75088	Phyport vPC with Esxi does not come up thr FEX
CSCuu95778	6.2(14)FB(0.73) Nexus 7010 ipfib crash
CSCuv04114	Show system internal lim counters cores N6001 Janjuc 7.2(0)
CSCuu29773	Crash in the pim process after exceeding 32K multicast routes
CSCuw01105	DFA: multicast duplicate packets or loop on border leafs
CSCuv48908	Cisco NX-OS IGMP Malformed Packet DoS Vulnerability
CSCuu84449	IGMP snooping entries ageout in AA FEX topologies
CSCut75242	ISSU upgrade: igmp HAP reset
CSCur21785	Cisco Nexus 7000 Series- M1/M2 Egress Queuing behavior post 6.2(x) for control plane packet
CSCuv04681	"Orphan-port suspend" does not work as expected with port-channel
CSCuw08846	Cisco Nexus 7000 Series 7.2 %VPC-2-L3_VPC_UNEQUAL_WEIGHT:
CSCuu93248	IPFIB core due to SW index leak in MFIB for F3 modules
CSCut66193	MCAST MET table shows negative utilization percentage

Table 16 Cisco NX-OS Release 7.2(1)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCuv51488	N77-F348 Linecard misreports reset reason
CSCuv42308	MST Disputes VPC peer-switch secondary peer sending cost of 250
CSCut84904	Process "mtm" Cores on F3 Cards Shortly After Boot
CSCut77072	N7K-F248XP-25E 6.1(5) link flaps with no cable
CSCuv99403	match datalink mac destination-address use field id 57 for ingress flow
CSCum52148	Distributed reflective denial-of-service vulnerability on NTP server
CSCuv06177	copy run to sftp on linux server fails
CSCur00089	vdc-admin on Cisco Nexus 7000 Series can break out of vsh-"chroot" using symbolic links
CSCuu37319	F3:QoS Policer is inconsistent in policing traffic to the desired rate.
CSCuv14079	Hardware queueing configuration swapped on F2E module for queue 5 and 7
CSCut17903	QoS Policy statistics not updating correctly
CSCut54262	Cisco Nexus 7000 Series: UDP port 8001 is open after an ISSU. Feature RISE not configured
CSCuv80499	BGP flapping with same AS-PATH ACL matched in two or more route-map seqs
CSCup66750	BGP routes not advertised after "default address-family ipv4/6 unicast"
CSCuv82966	L3 DCI autoconfig: VRF stuck in Delete Holddown
CSCuu70539	N5K bgp process crash after configuring default-originate
CSCut06852	Cisco Nexus 7000 Series - BGP using set metric-type internal under RM not triggering update
CSCuv06106	Unable to config bgp vrf af after unconfigure vrf context
CSCuu78729	EIGRP can install non-successor to RIB in case of ECMP paths
CSCut51575	VPC breaks due to incorrect emulated switch-id after ISSU upgrade
CSCuv86125	IP SLA echo response causing the AM routes to add and delete
CSCuw09453	LISP: race condition in forwarding entries after clearing dynamic EIDs
CSCuw03410	Nexus 6.2.x OSPF taking long time in LSA generation
CSCuw19181	N7K %ISIS_OTV-4-LAN_DUP_SYSID: error message
CSCus99375	OTV crashes with vlan process in crash core
CSCus62502	OTV Tunnel Depolarization causes traffic loss when some tunnels are down
CSCuu34270	BGP:accept route-target community value "zero"
CSCus66235	Match Statements within route-map do not function as AND for table-map
CSCuu10841	NXOS RPM crash due to the CLI "show ip prefix-list | xml"
CSCut92734	PVLAN: PBR not programmed on a mod without Primary vlan of a PVLAN on it
CSCuu93298	IP/IPv6 AM learnt host routes missing in target vrf with route leaking
CSCut84448	Cisco Nexus 7000 Series- OSPF type problem when redistribution of static routes
CSCuu22117	Cisco Nexus 7000 Series F3 IPv4 FIB misprogramming

Table 16 Cisco NX-OS Release 7.2(1)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCuu35152	URIB service crash on Cisco Nexus 7000 Series running 5.2(9)
CSCuv05083	Vlan learnt SGT mappings not downloaded to HW after module comes online
CSCuu82356	Evaluation of Cisco Nexus 7000 Series infra for OpenSSL
CSCuu23485	MDS: OpenSSL to CISCO SSL Migration for Vulnerability Fixes
CSCuw03144	OpenSSH: Evaluation of Multiple OpenSSH CVEs for NX-OS
CSCuv29391	SNMPD crash on n5k
CSCuv29907	Cisco Nexus 7000 Series supervisor reload due to 'monitor' service crash
CSCuu99291	Cisco Nexus 7000 VDC Authenticated Privilege Escalation Vulnerability
CSCuv90027	NXOSv Interface ACL config should be blocked until supported
CSCuv11862	Leap second update triggers watchdog crash
CSCuu11338	Nexus 7706-Inconsistent power supply status via SNMP
CSCur44998	1.3.6.1.4.1.9.9.9000.1.1.1.1 ivr_enable_mib is wrong for Cisco Nexus 7000 Series
CSCur17440	945snmpwalk on cpmCPUTotalTable(1.3.6.1.4.1.9.9.109.1.1.1) failing
CSCut76429	On core file creation we must dump all thread PIDS
CSCuu40239	ARP traffic sent out on incorrect VLAN
CSCut61977	Crash after show forwarding route adjacency <interface> <ip address>
CSCut57953	Cisco Nexus 7000 Series "ipfib" process crash
CSCuv43023	Cisco Nexus 7000 Series: UPG to 7.2 causes VTP pruning to stop functioning
CSCuu38875	VTP is running on HIF ports

Resolved Caveats—Cisco NX-OS Release 7.2(0)D1(1)

Table 17 Cisco NX-OS Release 7.2(0)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCun41202	Weak CBC mode and weak ciphers should be disabled in SSH server.
CSCuq28545	HSRP support for subnet VIPs.
CSCus64947	Fabric Anchor and Anycast-GW cause ARP-3-DUP_VADDR_SRC_IP msg.
CSCuo99830	ISSU: port_client core on F2/F3 handling unsupported port command
CSCut43342	Cisco Nexus 7000 Series - IM API needs to correctly identify type(fiber/copper) for CPAK/CFP
CSCur66262	DFA Leaf should NOT allow auto-pull for core-vlan range/backbone vlan
CSCus94447	DFA-auto-config-recovery-does-not-work
CSCuq88032	HSRP standby in vPC will not program G flag if Priority is 0
CSCuo54868	CF3+brkout:PIM hellos dropped due to MFIB/UFIB failed to install routes

Table 17 Cisco NX-OS Release 7.2(0)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCuo13444	IP Packets are dropped at LC when one sub interface is deleted
CSCun69659	"m2rib_delete_my_bd_mroutes() failed" when creating FP vlans
CSCup88022	G bit is not set on SUP but set on LC after vPC peer-link flap
CSCuo93631	Cisco Nexus 7000 Series MAC address in hardware but missing from software after ISSU
CSCut06901	Traffic blackholing for around 60 secs after new RPF intf comes up
CSCup48229	vPC peer-link no active BD after switch restart of peer-link flap.
CSCuo66929	Core @ pthread_join after show mpls switching internal fec label
CSCup21372	service not responding after sending FPOAM ping to switch-id
CSCur14589	vulnerability related to cmd injection via DHCP offer options
CSCur97641	MPLS QoS:Show policy is showing Pkt count 0 where byte count is proper
CSCup90186	Queuing policy of eth interface is removed when added to port-channel
CSCuo15363	L3VPN/6VPE : Post BGP restart, BGP NOT Adv VPNv4 & VPNv6 routes to Peer
CSCut18721	gbr_422: urib core at urib_chlist_segv_handler
CSCup82769	snmpd crashes when cvacmSecurityGrpStatus (Row status) is set to 5
CSCuq18021	SNMPset to community strings with special characters cause hap reset
CSCur30073	switch table driving wrong multipath

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 7(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 includes the following documents:

NX-OS Configuration Guides

Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide

Cisco Nexus 7000 Series NX-OS Configuration Examples

Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide

Configuring Feature Set for FabricPath

Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide

Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide

Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide

Cisco Nexus 7000 Series NX-OS IP SLAs Configuration Guide

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide

Cisco Nexus 7000 Series NX-OS LISP Configuration Guide

Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide

Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide

Cisco Nexus 7000 Series NX-OS OTV Configuration Guide

Cisco Nexus 7000 Series OTV Quick Start Guide

Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide

Cisco Nexus 7000 Series NX-OS SAN Switching Configuration Guide

Cisco Nexus 7000 Series NX-OS Security Configuration Guide

Cisco Nexus 7000 Series NX-OS System Management Configuration Guide

Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide

Cisco Nexus 7000 Series NX-OS Verified Scalability Guide

Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide

Cisco Nexus 7000 Series NX-OS Virtual Device Context Quick Start

Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500

NX-OS Command References

Cisco Nexus 7000 Series NX-OS Command Reference Master Index

Cisco Nexus 7000 Series NX-OS FabricPath Command Reference

Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference

Cisco Nexus 7000 Series NX-OS High Availability Command Reference

Cisco Nexus 7000 Series NX-OS Interfaces Command Reference

Cisco Nexus 7000 Series NX-OS IP SLAs Command Reference

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference

Cisco Nexus 7000 Series NX-OS LISP Command Reference

Cisco Nexus 7000 Series NX-OS MPLS Command Reference

Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference

Cisco Nexus 7000 Series NX-OS OTV Command Reference

Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference

Cisco Nexus 7000 Series NX-OS SAN Switching Command Reference

Cisco Nexus 7000 Series NX-OS Security Command Reference

Cisco Nexus 7000 Series NX-OS System Management Command Reference

Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference

Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference

Cisco NX-OS FCoE Command Reference for Cisco Nexus 7000 and Cisco MDS 9500

Other Software Document

Cisco NX-OS Licensing Guide

Cisco Nexus 7000 Series NX-OS MIB Quick Reference

Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide

Cisco NX-OS System Messages Reference

Cisco Nexus 7000 Series NX-OS Troubleshooting Guide

Cisco NX-OS XML Interface User Guide

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.