Cisco Nexus 7000 Series NX-OS Release Notes, Release 7.3

Date: September 1, 2020
Current Release:7.3(6)D1(1)

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 Related Documentation.

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
September 1, 2020	Updated the " Resolved Caveats—Cisco NX-OS Release 7.3(5)D1(1)" section to add CSCuv02817.
April 17, 2020	Created release notes for Cisco NX-OS Release 7.3(6)D1(1).
November 15, 2019	Created release notes for Cisco NX-OS Release 7.3(5)D1(1).
May 24, 2019	Created release notes for Cisco NX-OS Release 7.3(4)D1(1).
February 15, 2019	Updated the " Upgrade/Downgrade Paths and Caveats"section to include Cisco NX-OS Release 6.2(22).
November 2, 2018	Created release notes for Cisco NX-OS Release 7.3(3)D1(1).
September 26, 2018	Created release notes for Cisco NX-OS Release 7.3(2)D1(3a).
August 2, 2018	Updated the " Upgrade/Downgrade Paths and Caveats"section to include Cisco NX-OS Release 6.2(20a).
June 11, 2018	Created release notes for Cisco NX-OS Release 7.3(2)D1(3).

Table 1 Online History Change

Date	Description
December 8, 2017	Updated the " Upgrade/Downgrade Paths and Caveats"section to include Cisco NX-OS Release 6.2(20).
November 13, 2017	Created release notes for Cisco NX-OS Release 7.3(2)D1(2).
July 7, 2017	Created release notes for Cisco NX-OS Release 7.3(2)D1(1).
February 21, 2017	Updated the " Upgrade/Downgrade Paths and Caveats"section to include Cisco NX-OS Release 6.2(18).
November 14, 2016	Updated the " Open Caveats—Cisco NX-OS Release 7.x" section to add CSCvb84395.
November 8, 2016	Updated the " Resolved Caveats—Cisco NX-OS Release 7.2(0)D1(1)" section to add CSCun41202.
October 18, 2016	Updated the " Resolved Caveats—Cisco NX-OS Release 7.3(2)D1(1)" section to add CSCuy55178.
September 11, 2016	Created release notes for Cisco NX-OS Release 7.3(1)D1(1).
August 17, 2016	Updated the "Transceivers Supported by Cisco NX-OS Software Releases" table to include information for CVR-QSFP-SFP10G.
May 10, 2016	Created release notes for Cisco NX-OS Release 7.3(0)DX(1).
April 14, 2016	Updated the "Cisco Nexus 7000 and 7700 Series Hardware Supported by Cisco NX-OS Software" table and " New Hardware" section to add 3.5 KW HVAC/HVDC power supply details.
February 12, 2016	Created release notes for Cisco NX-OS Release 7.3(0)D1(1).
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.
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.
September 22, 2015	Reorganized the " New and Enhanced Software Features" section based on feature groupings.
September 7, 2015	Updated the " Resolved Caveats—Cisco NX-OS Release 7.2(0)D1(1)" section to add CSCuq28545.
June 18, 2015	Created release notes for Cisco NX-OS Release 7.2(0)D1(1).

Contents

This document includes the following sections:

Introduction

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

System Requirements

Cisco Nexus 7000 Supervisor 2 and 2E Modules are required for Cisco NX-OS 7.2.x and Cisco NX-OS 7.3.x releases.

FAB-1 modules, F1 series modules, M1 series modules (non-XL mode), and Cisco Nexus 7000 Supervisor 1 modules are not supported in Cisco NX-OS Release 7.3(0)D1(1) and later releases.

This section includes the following topics:

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 7.3(2)D1(1) 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 recommended Cisco NX-OS software releases for use with Cisco Nexus 7000 Series switches, see the document *Minimum Recommended 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)

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

Product ID	Hardware	Minimum Software Release
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)
N7K-C7010	Cisco Nexus 7010 chassis	4.0(1)
N7K-C7010-FAB-2	Fabric module, Cisco Nexus 7000 Series 10-slot	6.0(1)
N7K-C7010-FAN-F	Fabric fan tray for the Cisco Nexus 7010 chassis	4.0(1)
N7K-C7010-FAN-S	System fan tray for the Cisco Nexus 7010 chassis	4.0(1)
N7K-C7018	Cisco Nexus 7018 chassis	4.1(2)
N7K-C7018-FAB-2	Fabric module, Cisco Nexus 7000 Series 18-slot	6.0(1)
N7K-C7018-FAN	Fan tray for the Cisco Nexus 7018 chassis	4.1(2)
N7K-DC-3KW	3.0-kW DC power supply unit	6.1(2)
N7K-DC-6.0KW N7K-DC-PIU N7K-DC-CAB=	6.0-kW DC power supply unit (cable included) DC power interface unit DC 48 V, -48 V cable (spare)	5.0(2) 5.0(2) 5.0(2)
N7K-F248XP-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)

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

Product ID	Hardware	Minimum Software Release
N7K-F312FQ-25	Cisco Nexus 7000 12-port 40-Gigabit Ethernet QSFP+ I/O module (F3 Series)	6.2(6)
N7K-F348XP-25	Cisco Nexus 7000 48-port 1/10-Gigabit Ethernet SFP+ I/O module (F3 Series)	6.2(12)
N7K-HV-3.5KW	3.5KW High Voltage Power Supply Unit	7.3(0)D1(1)
N7K-M108X2-12L	8-port 10-Gigabit Ethernet I/O module XL[1]	5.0(2)
N7K-M132XP-12L	32-port 10-Gigabit Ethernet SFP+ I/O module XL[1]	5.1(1)
N7K-M148GS-11L	48-port 1-Gigabit Ethernet I/O module XL[1]	5.0(2)
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-C7706-FAN	Fan, 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)

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

Product ID	Hardware	Minimum Software Release
N77-C7718-FAN	Fan, Cisco Nexus 7718 chassis	6.2(2)
N77-DC-3KW	Cisco Nexus 7700 DC power supply	6.2(2)
N77-F248XP-23E	Cisco Nexus 7700 Enhanced 48-port 1/10 Gigabit Ethernet SFP+ I/O module (F2E Series)	6.2(2)
N77-F312CK-26	Cisco Nexus 7700 12-port 100-Gigabit Ethernet CPAK I/O module (F3 Series)	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-HV-3.5KW	3.5KW High Voltage Power Supply Unit	7.3(0)D1(1)
N77-M348XP-23L	48-port 1/10-Gigabit Ethernet SFP+ I/O module (M3 series)	7.3(0)DX(1)
N77-M324FQ-25L	24-port 40-Gigabit Ethernet QSFP+ I/O module (M3 series)	7.3(0)DX(1)
N77-SUP2E	Cisco Nexus 7700 Supervisor 2 Enhanced module	6.2(2)

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		

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

Cisco Nexus 7000 Series Module	FEX Module	Minimum Software Release
12-port 40-Gigabit Ethernet QSFP I/O F3 Series module (N7K-F312FQ-25)	N2K-C2224TP-1GE N2K-C2248TP-1GE N2K-C2232PP-10GE N2K-C2232TM N2K-C2248TP-E N2K-C2232TM-E N2K-C2248PQ N2K-B22HP[1]	6.2(12)
	N2K-C2348UPQ N2K-C2348TQ N2K-B22IBM	7.2(0)D1(1)
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)

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 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)
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		

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

Cisco Nexus 7000 Series Module	FEX Module	Minimum Software Release
24-port Cisco Nexus 7700 F3 Series 40-Gigabit Ethernet QSFP I/O module (N77-F324FQ-25)	N2K-C2224TP-1GE	6.2(8)
	N2K-C2248TP-1GE	
	N2K-C2232PP-10GE	
	N2K-C2232TM	
	N2K-C2248TP-E	
	N2K-C2232TM-E	
	N2K-C2248PQ	
	N2K-B22HP[2]	
	N2K-C2348UPQ	7.2(0)D1(1)
	N2K-C2348TQ	
	N2K-B22IBM	
48-port Cisco Nexus 7700 F3 Series 1/10-Gigabit Ethernet SFP+ I/O module (N77-F348XP-23)	N2K-C2224TP-1GE	6.2(6)
	N2K-C2248TP-1GE	
	N2K-C2232PP-10GE	
	N2K-C2232TM	
	N2K-C2248TP-E	
	N2K-C2232TM-E	
	N2K-C2248PQ	
	N2K-B22HP	
	N2K-C2348UPQ	7.2(0)D1(1)
	N2K-C2348TQ	
	N2K-B22IBM	
48-port 1/10 Gigabit Ethernet SFP+ I/O module (F2E Series) (N77-F248XP-23E)	N2K-C2224TP-1GE	6.2(2)
	N2K-C2248TP-1GE	
	N2K-C2232PP-10GE	
	N2K-C2232TM	
	N2K-C2232TM-E	
	N2K-C2248PQ	
	N2K-C2248TP-E	
	N2K-B22HP	
	N2K-C2348UPQ	7.2(0)D1(1)
	N2K-C2348TQ	
	N2K-B22IBM	

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.

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

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-SR4	Multi-mode fiber (MMF)	7.3(2)D1(1)
	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)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	QSFP-4X10G-ACxM	40GBASE-CR4 QSFP+ to 4x SFP+ Twinax Direct Attach Copper Breakout Cable Active (7 m, 10 m)	6.2(8)
	QSFP-H40G-AOCxM	40GBASE-AOC (Active Optical Cable) QSFP Cable (1 m, 2 m, 3 m, 5 m, 7 m, 10 m)	6.2(8)
	QSFP-H40G-AOC15M	40GBASE-AOC (Active Optical Cable) QSFP Cable (15m)	7.2(0)D1(1)
	QSFP-4X10G-AOCxM	40GBASE-AOC (Active Optical Cable) QSFP to 4x10G SFP+ Breakout Cable (1 m, 2 m, 3 m,5 m, 7 m, 10 m)	6.2(8)
	WSP-Q40GLR4L	40GBASE-LR4 lite (2km SMF) QSFP+	6.2(10)
	QSFP-40G-LR4	40GBASE-LR4 QSFP+ (Ethernet and OTU3 capable)	6.2(12)
	QSFP-4X10G-LR-S	Single-mode fiber (SMF)	7.3(1)D1(1)
	QSFP-40G-ER4	40GBASE-ER4 QSFP+ (40km)	6.2(12)
N77-F348XP-23	CWDM-SFP-xxxx[2]	1000BASE-CWDM	6.2(8)
	DWDM-SFP-xxxx[2]	1000BASE-DWDM	6.2(8)
	GLC-TE	1000BASE-T SFP	6.2(10)
	FET-10G	Cisco Fabric Extender Transceiver (FET)	6.2(6)
	SFP-10G-AOCxM	110GBASE-AOC (Active Optical Cable) SFP+ Cable (1 m, 2 m, 3 m, 5 m, 7 m, 10 m)	6.2(10)
	SFP-10G-BXD-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, downstream	7.2(0)D1(1)
	SFP-10G-BXU-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, upstream	7.2(0)D1(1)
	SFP-10G-SR SFP-10G-SR-S	10GBASE-SR SFP+	6.2(6)
	SFP-10G-LR SFP-10G-LR-S	10GBASE-LR SFP+	6.2(6)
	SFP-10G-ER SFP-10G-ER-S	10GBASE-ER SFP+	6.2(6)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	SFP-10G-ZR SFP-10G-ZR-S	10GBASE-ZR SFP+	6.2(6)
	DWDM-SFP10G-xx.xx	10GBASE-DWDM SFP+	6.2(6)
	SFP-10G-LRM[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)
	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)

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+	6.2(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)
	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	CPAK-100G-SR4	Multi-mode fiber (MMF)	7.3(2)D1(1)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	CVR-QSFP-SFP10G (This is supported only on F3 40G I/O modules with SFP-10G-SR or SFP-10G-SR-S optics. If the F3 I/O module is reloaded, the ports containing the CVR-QSFP-SFP10G adapter may remain down even after the F3 I/O module comes back up. If so, the CVR-QSFP-SFP10G adapter must be reseated.) (Only version V02 of the CVR-QSFP-SFP10G module is supported.)	Cisco 40G QSFP	6.2(14)
	QSFP-40G-SR-BD	Cisco 40G BiDi QSFP+	6.2(6)
	QSFP-40G-SR4 QSFP-40G-SR4-S	40GBASE-SR4 QSFP+	6.2(6)
	QSFP-40G-CSR4	40GBASE-CSR4 QSFP+	6.2(6)
	QSFP-40GE-LR4 QSFP-40G-LR4-S	40GBASE-LR4 QSFP+	6.2(6)
	FET-40G	Cisco 40G Fabric Extender Transceiver (FET)	6.2(6)
	QSFP-H40G-ACUxM	40GBASE-CR4 QSFP+ Direct Attach Copper Cable Active (7 m, 10 m)	6.2(8)
	QSFP-4X10G-ACxM	40GBASE-CR4 QSFP+ to 4x SFP+ Twinax Direct Attach Copper Breakout Cable Active (7 m, 10 m)	6.2(8)
	QSFP-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-4X10G-LR-S	Single-mode fiber (SMF)	7.3(1)D1(1)
	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)

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

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

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	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)
N77-M348XP-23L	GLC-TE	Category 5	7.3(0)DX(1)
	GLC-LH-SMD GLC-SX-MMD	Multi-mode fiber (MMF)	7.3(0)DX(1)
	CWDM-SFP-xxxx [3] DWDM-SFP-xxxx GLC-BX-U GLC-BX-D GLC-EX-SMD GLC-LH-SMD GLC-ZX-SMD	Single-mode fiber (SMF)	7.3(0)DX(1)
	SFP-10G-SR	Multi-mode fiber (MMF)	7.3(0)DX(1)
	SFP-10G-SR-S	Multi-mode fiber (MMF)	7.3(0)DX(1)
	DWDM-SFP10G-xx.xx [4] SFP-10G-BXD-I SFP-10G-BXU-I SFP-10G-ER SFP-10G-LR SFP-10G-LRM SFP-10G-ZR	Single-mode fiber (SMF)	7.3(0)DX(1)
	SFP-10G-ER-S SFP-10G-LR-S SFP-10G-ZR-S	Single-mode fiber (SMF)	7.3(0)DX(1)
	SFP-H10GB-CU1M SFP-H10GB-CU1-5M SFP-H10GB-CU2M SFP-H10GB-CU2-5M SFP-H10GB-CU3M SFP-H10GB-CU5M	Twinax cable assembly, passive	7.3(0)DX(1)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	SFP-H10GB-ACU7M SFP-H10GB-ACU10M	Twinax cable assembly, active	7.3(0)DX(1)
	SFP-10G-AOC1M SFP-10G-AOC2M SFP-10G-AOC3M SFP-10G-AOC5M SFP-10G-AOC7M SFP-10G-AOC10M	Active optical cable assembly	7.3(0)DX(1)
N77-M324FQ-25L	QSFP-40G-CSR4 QSFP-40G-SR4 QSFP-40G-SR-BD	Multi-mode fiber (MMF)	7.3(0)DX(1)
	QSFP-40G-ER4 QSFP-40G-LR4 QSFP-4X10G-LR-S WSP-Q40G-LR4L	Single-mode fiber (SMF)	7.3(0)DX(1)
	QSFP-H40G-ACU7M QSFP-H40G-ACU10M	Direct attach copper, active	7.3(0)DX(1)
	QSFP-H40G-AOC1M QSFP-H40G-AOC2M QSFP-H40G-AOC3M QSFP-H40G-AOC5M QSFP-H40G-AOC7M QSFP-H40G-AOC10M QSFP-H40G-AOC15M	Active optical cable assembly	7.3(0)DX(1)
N7K-F248XP-25	FET-10G	Cisco Fabric Extender Transceiver (FET)	6.0(1)
	SFP-10G-BXD-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, downstream	7.2(0)D1(1)
	SFP-10G-BXU-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, upstream	7.2(0)D1(1)
	SFP-10G-SR SFP-10G-SR-S	10GBASE-SR SFP+	6.0(1)
	SFP-10G-LR SFP-10G-LR-S	10GBASE-LR SFP+	6.0(1)

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+	6.0(1)
	SFP-10G-LRM	10GBASE-LRM SFP+	6.0(1)
	SFP-10G-ZR [2] SFP-10G-ZR-S	10GBASE-ZR SFP+	6.1(1)
	SFP-10G-AOCxM	10GBASE-AOC (Active Optical Cable) SFP+ Cable (1 m, 2 m, 3 m, 5 m, 7 m, 10 m)	6.2(2)
	SFP-H10GB-CUxM	SFP-H10GB-CUxM Twinax Cable Passive (1 m, 3 m, 5 m)	6.0(1)
	SFP-H10GB-CUxM	SFP-H10GC-CUxM Twinax Cable Passive (1.5 m, 2 m, 2.5 m)	6.2(2)
	SFP-H10GB-ACUxM	SFP-H10GB-ACUxM Twinax Cable Active (7 m, 10 m)	6.0(1)
	SFP-GE-T	1000BASE-T SFP	6.0(1)
	SFP-GE-S	1000BASE-SX SFP (DOM)	6.0(1)
	SFP-GE-L	1000BASE-LX/LH SFP (DOM)	6.0(1)
	SFP-GE-Z	1000BASE-ZX SFP (DOM)	6.0(1)
	GLC-TE	1000BASE-T SFP	6.2(10)
	GLC-LH-SM	1000BASE-LX/LH SFP	6.0(1)
	GLC-LH-SMD	1000BASE-LX/LH SFP	6.0(1)
	GLC-SX-MM	1000BASE-SX SFP	6.0(1)
	GLC-SX-MMD	1000BASE-SX SFP	6.0(1)
	GLC-ZX-SM	1000BASE-ZX SFP	6.0(1)
	GLC-ZX-SMD	1000BASE-ZX SFP	6.2(2)
	GLC-T	1000BASE-T SFP	6.0(1)
	GLC-BX-D	1000BASE-BX10-D	6.0(1)
	GLC-BX-U	1000BASE-BX10-U	6.0(1)
	GLC-EX-SMD	1000BASE-EX SFP	6.1(1)
	CWDM-SFP-xxxx [2]	1000BASE-CWDM	6.0(1)
	DWDM-SFP10G-xx.xx [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)

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+	6.1(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)
	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)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	DWDM-SFP10G-xx.xx [2]	10GBASE-DWDM SFP+	6.1(2)
	DWDM-SFP-xxxx [2]	1000BASE-DWDM	6.1(2)
N7K-M108X2-12L	SFP-10G-SR[2]	10GBASE-SR SFP+	5.2(3a)
	SFP-10G-SR-S		
	SFP-10G-LR[2]	10GBASE-LR SFP+	5.2(3a)
	SFP-10G-LR-S		
	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-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)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
N7K-M132XP-12L	FET-10G	Cisco Fabric Extender Transceiver (FET)	5.1(1)
	SFP-10G-BXD-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, downstream	7.2(0)D1(1)
	SFP-10G-BXU-I	10GBASE-BX Bidirectional (single fiber) SFP+, 10km reach, upstream	7.2(0)D1(1)
	SFP-10G-SR SFP-10G-SR-S	10GBASE-SR SFP+	5.1(1)
	SFP-10G-LR SFP-10G-LR-S	10GBASE-LR SFP+	5.1(1)
	SFP-10G-ER SFP-10G-ER-S	10GBASE-ER SFP+	5.1(1)
	SFP-10G-LRM	10GBASE-LRM SFP+	5.1(1)
	SFP-10G-ZR [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 [4]	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 [4]	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)
	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)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	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] CWDM-SFP-xxxx is supported only with 1-Gigabit Ethernet I/O modules.

[4] 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.

Cisco NX-OS Release 7.3(2)D1(2)

- F3 module does not install routes in its hardware:

  If there is resource over utilization in the FIB TCAM table, new routes cannot be installed in TCAM for the hardware forwarding.

  If the F3 module is not able to install a specific prefix into TCAM due to its over utilization, the prefix installation does not happen till all the resources are freed up.

  The only way to get the prefix installed is to clear the specific IP route by using **clear ip route** <*prefix*> command if you know exactly what prefix was not programmed due to over utilization or clear all the routes, if the exact prefix is not known.

  Sometimes this type of clearing the IP route does not help with programming prefix. If clearing the IP route does mot work, you might then need to reload the F3 module.
- 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.

Cisco NX-OS Release 7.3(2)D1(1)

- Cisco onePK is not supported in Cisco NX-OS Release 7.3(2)D1(1).
- When you use the **storm-control unicast level** *percentage* command in a module, both the unknown and known unicast traffic gets discarded after reaching the threshold value.

Cisco NX-OS Release 7.3(1)D1(1)

- Inter-VSAN routing (IVR) is not supported with FEX.
- Static ARP entry configuration with unicast IP pointing to multicast destination MAC is not supported on M3 modules.
- When you use the **storm-control unicast level** *percentage* command in a module, both the unknown and known unicast traffic gets discarded after reaching the threshold value.
- VPLS and EoMPLS are not supported in M3 modules.
- The following features are not supported on a VDC that has an M3 module:
  - FabricPath
  - vPC+
  - MPLS L2VPN
  - MPLS L2VPN QoS
  - LISP
  - Physical port vPC
  - FEX
  - 40G to 10G Breakout
  - Storage VDC
  - QoS Template: 7e/6e/4e network QOS: The QoS templates are globally applied from the default VDC and hence this would not be allowed at the system level, which means if the system has an M3 module, the QoS templates would not be supported.
  - PTP Pong

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

- Static ARP entry configuration with unicast IP pointing to multicast destination MAC is not supported on M3 modules.
- When you use the **storm-control unicast level** *percentage* command in a module, both the unknown and known unicast traffic gets discarded after reaching the threshold value.
- VPLS and EoMPLS are not supported in M3 modules.
- The following features are not supported on a VDC that has an M3 module:
  - FabricPath
  - vPC+
  - MPLS L2VPN
  - MPLS L2VPN QoS
  - LISP
  - Physical port vPC

  - FEX
  - 40G to 10G Breakout
  - Storage VDC
  - QoS Template: 7e/6e/4e network QOS: The QoS templates are globally applied from the default VDC and hence this would not be allowed at the system level, which means if the system has an M3 module, the QoS templates would not be supported.
  - PTP Pong

Unsupported Hardware - Cisco NX-OS Release 7.3(0)DX(1), Cisco NX-OS Release 7.3(1)D1(1), and Cisco NX-OS Release 7.3(2)D1(1)

The following list provides the unsupported hardware for Cisco NX-OS Release 7.3(0)DX(1), Cisco NX-OS Release 7.3(1)D1(1), Cisco NX-OS Release 7.3(2)D1(1):

- N7K-M108X2-12
- N7K-M148GT-11
- N7K-M132XP-12
- N7K-M148GS-11
- N7K-C7010-FAB-1
- N7K-C7018-FAB-1
- N7K-F132XP-15
- Cisco Nexus 7000 Supervisor 1 Module

Unsupported Hardware - Cisco NX-OS Release 7.3(0)D1(1)

The following list provides the unsupported hardware for Cisco NX-OS Release 7.3(0)D1(1):

- N7K-M148GT-11
- N7K-M132XP-12
- N7K-M148GS-11
- N7K-C7010-FAB-1
- N7K-C7018-FAB-1
- N7K-F132XP-15
- Cisco Nexus 7000 Supervisor 1 Module

Native VLAN Change Causes Link Flap

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

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

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

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

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

– N7K-M206FQ-23L

– N7K-F312FQ-25

– N77-F324FQ-25

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

MPLS over GRE

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

VLAN Translation on Fabric Extender Is Not Supported

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

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

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

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

This applies only to the Cisco Nexus 7700 Series devices.

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.

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

Role-Based Access Control

You can configure role-based access control (RBAC) in the Cisco Nexus 7000 storage VDC using Cisco NX-OS CLI commands. You cannot configure RBAC in the Cisco Nexus 7000 storage VDC using Cisco Data Center Network Manager (DCNM). Note that RBAC in the storage VDC 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

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

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.

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

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.

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 7.3(6)D1(1)

See Table 6 for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 7.3(6)D1(1).

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 7.3(6)D1(1)

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 7.3(6)D1(1)	7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2) 7.3(2)D1(1) 7.3(1)D1(1) 7.3(0)DX(1) 7.3(0)D1(1) 7.2(2)D1(2) 7.2(2)D1(1) 7.2(1)D1(1) 7.2(0)D1(1)

Multi-hop ISSU is not supported. If you are upgrading from any release other than the non-disruptive upgrade releases listed in Table 6, a reload is required.

ISSU Paths for Cisco NX-OS Release 7.3(5)D1(1)

See Table 7 for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 7.3(5)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 7.3(5)D1(1)

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 7.3(5)D1(1)	7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2) 7.3(2)D1(1) 7.3(1)D1(1) 7.3(0)DX(1) 7.3(0)D1(1) 7.2(2)D1(2) 7.2(2)D1(1) 7.2(1)D1(1) 7.2(0)D1(1)

Multi-hop ISSU is not supported. If you are upgrading from any release other than the non-disruptive upgrade releases listed in Table 7, a reload is required.

ISSU Paths for Cisco NX-OS Release 7.3(4)D1(1)

See Table 8 for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 7.3(4)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 7.3(4)D1(1)

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 7.3(4)D1(1)	7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2) 7.3(2)D1(1) 7.3(1)D1(1) 7.3(0)DX(1) 7.3(0)D1(1) 7.2(2)D1(2) 7.2(2)D1(1) 7.2(1)D1(1) 7.2(0)D1(1)

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

ISSU Paths for Cisco NX-OS Release 7.3(3)D1(1)

See Table 9 for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 7.3(3)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 7.3(3)D1(1)

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 7.3(3)D1(1)	7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2) 7.3(2)D1(1) 7.3(1)D1(1) 7.3(0)DX(1) 7.3(0)D1(1) 7.2(2)D1(2) 7.2(2)D1(1) 7.2(1)D1(1) 7.2(0)D1(1)

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

ISSU Paths for Cisco NX-OS Release 7.3(2)D1(3a)

See Table 10 for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 7.3(2)D1(3a).

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

Table 10 Supported ISSU Paths for the Cisco Nexus 7000 and 7700 Series Chassis (Cisco NX-OS Release 7.3(2)D1(3a))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 7.3(2)D1(3a)	7.3(2)D1(3) 7.3(2)D1(2) 7.3(2)D1(1) 7.3(1)D1(1) 7.3(0)DX(1) 7.3(0)D1(1) 7.2(2)D1(2) 7.2(2)D1(1) 7.2(1)D1(1) 7.2(0)D1(1)

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

ISSU Paths for Cisco NX-OS Release 7.3(2)D1(3)

See Table 11 for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 7.3(2)D1(3).

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

Table 11 Supported ISSU Paths for the Cisco Nexus 7000 and 7700 Series Chassis (Cisco NX-OS Release 7.3(2)D1(3))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 7.3(2)D1(3)	7.3(2)D1(2) 7.3(2)D1(1) 7.3(1)D1(1) 7.3(0)DX(1) 7.3(0)D1(1) 7.2(2)D1(2) 7.2(2)D1(1) 7.2(1)D1(1) 7.2(0)D1(1)

Multi-hop ISSU is not supported. If you are upgrading from any release other than the non-disruptive upgrade releases listed in Table 11, a reload is required.

ISSU Paths for Cisco NX-OS Release 7.3(2)D1(2)

See Table 12 for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 7.3(2)D1(2).

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

Table 12 Supported ISSU Paths for the Cisco Nexus 7000 and 7700 Series Chassis (Cisco NX-OS Release 7.3(2)D1(2))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 7.3(2)D1(2)	7.3(2)D1(1) 7.3(1)D1(1) 7.3(0)DX(1) 7.3(0)D1(1) 7.2(2)D1(2) 7.2(2)D1(1) 7.2(1)D1(1) 7.2(0)D1(1)

Note Multi-hop ISSU is not supported. If you are upgrading from any release other than the non-disruptive upgrade releases listed in Table 12, a reload is required.

ISSU Paths for Cisco NX-OS Release 7.3(2)D1(1)

See Table 13 for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 7.3(2)D1(1).

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

Table 13 Supported ISSU Paths for the Cisco Nexus 7000 and 7700 Series Chassis (Cisco NX-OS Release 7.3(2)D1(1))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 7.3(2)D1(1)	7.3(1)D1(1) 7.3(0)DX(1) 7.3(0)D1(1) 7.2(2)D1(2) 7.2(2)D1(1) 7.2(1)D1(1) 7.2(0)D1(1)

Note Multi-hop ISSU is not supported. If you are upgrading from any release other than the non-disruptive upgrade releases listed in Table 13, a reload is required.

ISSU Paths for Cisco NX-OS Release 7.3(1)D1(1)

See Table 14 for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 7.3(1)D1(1).

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

Table 14 Supported ISSU Paths for the Cisco Nexus 7000 and 7700 Series Chassis (Cisco NX-OS Release 7.3(1)D1(1))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 7.3(1)D1(1)	7.3(0)DX(1) 7.3(0)D1(1) 7.2(2)D1(2) 7.2(2)D1(1) 7.2(1)D1(1) 7.2(0)D1(1)

Note Multi-hop ISSU is not supported. If you are upgrading from any release other than the non-disruptive upgrade releases listed in Table 14, a reload is required.

ISSU Paths for Cisco NX-OS Release 7.3(0)DX(1)

See Table 15 for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 7.3(0)DX(1).

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

Table 15 Supported ISSU Paths for the Cisco Nexus 7000 and 7700 Series Chassis (Cisco NX-OS Release 7.3(0)DX(1))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 7.3(0)DX(1)	7.3(0)D1(1) 7.2(2)D1(2) 7.2(2)D1(1) 7.2(1)D1(1) 7.2(0)D1(1)

Note Multi-hop ISSU is not supported. If you are upgrading from any release other than the non-disruptive upgrade releases listed in Table 15, a reload is required.

ISSU Paths for Cisco NX-OS Release 7.3(0)D1(1)

See Table 16 for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 7.3(0)D1(1).

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

Table 16 Supported ISSU Paths for the Cisco Nexus 7000 and 7700 Series Chassis (Cisco NX-OS Release 7.3(0)D1(1))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 7.3(0)D1(1)	7.2(2)D1(2) 7.2(2)D1(1) 7.2(1)D1(1) 7.2(0)D1(1)

Note Multi-hop ISSU is not supported. If you are upgrading from any release other than the non-disruptive upgrade releases listed in Table 16, a reload is required.

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

See Table 17 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 17 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(22) 6.2(20a) 6.2(20) 6.2(18) 6.2(16) 6.2(14) 6.2(12) 6.2(10)

Note Multi-hop ISSU is not supported. If you are upgrading from any release other than the non-disruptive upgrade releases listed in Table 17, a reload is required.

ISSU Paths for Cisco NX-OS Release 7.2(2)D1(1)

See Table 18 for the in-service software upgrade (ISSU) path to 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 18 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(22) 6.2(20a) 6.2(20) 6.2(18) 6.2(16) 6.2(14) 6.2(12) 6.2(10)

Note Multi-hop ISSU is not supported. If you are upgrading from any release other than the non-disruptive upgrade releases listed in Table 18, a reload is required.

ISSU Paths for Cisco NX-OS Release 7.2(1)D1(1)

See Table 19 for the in-service software upgrade (ISSU) path to 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 19 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(22) 6.2(20a) 6.2(20) 6.2(18) 6.2(16) 6.2(14) 6.2(12) 6.2(10)

Note Multi-hop ISSU is not supported. If you are upgrading from any release other than the non-disruptive upgrade releases listed in Table 19, a reload is required.

ISSU Paths for Cisco NX-OS Release 7.2(0)D1(1)

See Table 20 for the in-service software upgrade (ISSU) path to 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 20 Supported ISSU Paths for the Cisco Nexus 7000 and 7700 Series Chassis (Cisco NX-OS Release 7.2(0)D1(1))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
Cisco NX-OS Release 7.2(0)D1(1)	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)

Note Multi-hop ISSU is not supported. If you are upgrading from any release other than the non-disruptive upgrade releases listed in Table 20, a reload is required.

In-Service Software Upgrade (ISSU)

Note For all Cisco Nexus 7000 series platforms in-service software upgrade (ISSU) is not supported in maintenance mode when you upgrade from Cisco NX-OS Release 7.2(0) or Cisco NX-OS Release 7.2(1) to Cisco NX-OS Release 7.3(0). You must perform a cold boot upgrade with maintenance mode to upgrade from Cisco NX-OS Release 7.2(0)D1(1) to Cisco NX-OS Release 7.3(0)D1(1).

To perform an ISSU upgrade to Cisco NX-OS Release 7.3(0)D1(1) and later releases from one of the ISSU supported releases listed in tables 7 to 9 mentioned 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 perform a reload ASCII and a disruptive upgrade from Cisco NX-OS Release 7.3(2)D1(2) to Cisco NX-OS Release 7.3(3)D1(1), you might face issues with dual-homed FEXes.

  To overcome this issue perform one of the following:

  – Perform ISSU to avoid problems with the dual-homed FEXes and to keep them online or

  – Shut the AA fabric port channels before the disruptive upgrade

- When you upgrade from Cisco NX-OS Release 6.2(20) to Cisco NX-OS Release 7.3(2)D1(2) or downgrade from Cisco NX-OS Release 7.3(2)D1(2) to Cisco NX-OS Release 6.2(20), the ACL policy on virtual teletype (VTY) may not get activated during quiet period. You need to reconfigure the appropriate 'block-for' and the 'quiet-mode' configurations so that the ACL on VTY works properly.

  The following example shows how to reconfigure the 'block-for' and the 'quiet-mode' configurations in Cisco NX-OS Release 7.3(2)D1(2):

  ```
  system login block-for 20 attempts 1 within 30
  system login quiet-mode access-class foo
  ```

  The following example shows how to reconfigure the 'block-for' and the 'quiet-mode' configurations in Cisco NX-OS Release 6.2(20):

  ```
  login block-for 20 attempts 1 within 30
  login quiet-mode access-class foo
  ```

- 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.
- If a switch running the Cisco NX-OS Release 7.2(0)D1(1) has M1, F1 or Fab1 modules installed, you cannot perform an ISSU from Cisco NX-OS Release 7.2(0)D1(1) to Cisco NX-OS Release 7.3(0)DX(1) as the M1, F1 and Fab1 modules are not supported in Cisco NX-OS Release 7.3(0)DX(1). To overcome this issue, remove the unsupported modules before proceeding with the ISSU. This caveat applies only if the unsupported modules are present on the switch undergoing the upgrade.
- The following list provides the PIDs of the unsupported modules in Cisco NX-OS Release 7.3(0)DX(1):

  — N7K-M108X2-12
  — N7K-M148GT-11

— N7K-M132XP-12
— N7K-M148GS-11
— N7K-C7010-FAB-1
— N7K-C7018-FAB-1
— N7K-F132XP-15

- If you install an M3 module in the system prior to upgrading to Cisco NX-OS Release 7.3(0)DX(1), you cannot proceed with the ISSU. You need to first upgrade to Cisco NX-OS Release 7.3(0)DX(1) and then install an M3 module.
- When you ISSU from Cisco NX-OS Release 7.2(1)D1(1) to Cisco NX-OS Release 7.3(0)D1(1) and have DFS (Data Frame Snooping) profiles applied, subsequent actions could cause the profiles to be un-applied and re-applied, resulting in a momentary traffic loss.

  Specifically, if the vPC peer-link were to flap or a module reload/OIR was performed (where all host interfaces are on that module), the profile would transition from Active to Holddown and then get un-applied. Subsequent host traffic would then re-apply the profile.

  Additionally, during the profile un-apply and re-apply sequence, VNI-BD Inconsistency syslogs may be observed with possible traffic loss. To resolve this issue, use the **clear fabric database host vni** *vni-id* command to clear the profile for those specific VNIs. This only applies to profiles triggered by dot1q hosts (DFS).
- If ISSU fails during a FEX module upgrade, you need to clear the flash as per the following steps and then proceed with the upgrade:
  - rlogin to the failing FEX—rlogin 192.0.2.<FEX-ID> -l root
  - umount /mnt/cfg
  - flash_eraseall /dev/mtd5
  - mount -t jffs2 -rw /dev/mtdblock5 /mnt/cfg

    The **mount** command enables you to mount a file from a source folder to a destination folder.
- FCoE FEX
  - 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 7.3(0) release should be uninstalled.
- For details on ISSU for other earlier releases refer to the following: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/7_x/nx-os/release/notes/72_nx-os_release_note.html#pgfId-1146014.
- 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-ISSU Upgrade/Cold Boot Upgrade Steps

To perform a non-ISSU upgrade to Release 7.3(x) from any prior supported releases follow these steps:

1. Change the boot variable.

   Example:

   ```
   boot kickstart bootflash:/n7000-s2-kickstart.7.3.0.D1.1.bin sup-1
   boot system bootflash:/n7000-s2-dk9.7.3.0.D1.1.bin sup-1
   boot kickstart bootflash:/n7000-s2-kickstart.7.3.0.D1.1.bin sup-2
   boot system bootflash:/n7000-s2-dk9.7.3.0.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.

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

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

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 7.3(6)D1(1) has the following cold boot support matrix:

Table 21 Supported Cold Boot Matrix in Cisco NX-OS Release 7.3(6)D1(1)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
8.4(2)	7.3(6)D1(1)
8.4(1)	7.3(6)D1(1)
8.3(2)	7.3(6)D1(1)
8.3(1)	7.3(6)D1(1)
8.2(5)	7.3(6)D1(1)
8.2(4)	7.3(6)D1(1)
8.2(3)	7.3(6)D1(1)
8.2(2)	7.3(6)D1(1)
8.2(1)	7.3(6)D1(1)
8.1(2a)	7.3(6)D1(1)
8.1(2)	7.3(6)D1(1)
8.1(1)	7.3(6)D1(1)
8.0(1)	7.3(6)D1(1)

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

Cisco NX-OS Release 7.3(5)D1(1) has the following cold boot support matrix:

Table 22 Supported Cold Boot Matrix in Cisco NX-OS Release 7.3(5)D1(1)

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

Cisco NX-OS Release 7.3(4)D1(1) has the following cold boot support matrix:

Table 23 Supported Cold Boot Matrix in Cisco NX-OS Release 7.3(4)D1(1)

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

Cisco NX-OS Release 7.3(3)D1(1) has the following cold boot support matrix:

Table 24 Supported Cold Boot Matrix in Cisco NX-OS Release 7.3(3)D1(1)

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

Cisco NX-OS Release 7.3(2)D1(3a) has the following cold boot support matrix:

Table 25 Supported Cold Boot Matrix in Cisco NX-OS Release 7.3(2)D1(3a)

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

Cisco NX-OS Release 7.3(2)D1(3) has the following cold boot support matrix:

Table 26 Supported Cold Boot Matrix in Cisco NX-OS Release 7.3(2)D1(3)

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

Cisco NX-OS Release 7.3(2)D1(2) has the following cold boot support matrix:

Table 27 Supported Cold Boot Matrix in Cisco NX-OS Release 7.3(2)D1(2)

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

Cisco NX-OS Release 7.3(2)D1(1) has the following cold boot support matrix:

Table 28 Supported Cold Boot Matrix in Cisco NX-OS Release 7.3(2)D1(1)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
7.3(2)D1(1)	7.3(1)D1(1)
	7.3(0)DX(1)
	7.3(0)D1(1)
	7.2(2)D1(2)
	7.2(2)D1(1)
	7.2(1)D1(1)
	7.2(0)D1(1)
	6.2(22)
	6.2(20a)
	6.2(20)
	6.2(18)
	6.2(16)
	6.2(14)
	6.2(12)
	6.2(10)
	6.2(8b)
	6.2(8a)
	6.1(5a)

Cisco NX-OS Release 7.3(1)D1(1) has the following cold boot support matrix:

Table 29 Supported Cold Boot Matrix in Cisco NX-OS Release 7.3(1)D1(1)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
7.3(1)D1(1)	7.3(0)DX(1)
	7.3(0)D1(1)
	7.2(2)D1(2)
	7.2(2)D1(1)
	7.2(1)D1(1)
	7.2(0)D1(1)
	6.2(22)
	6.2(20a)
	6.2(20)
	6.2(18)
	6.2(16)
	6.2(14)
	6.2(12)
	6.2(10)
	6.1(5a)

Note For the below listed combination of cold boot matrix, the switch will boot up with ASCII configuration file. If a FEX configuration exists an additional **copy running-config startup-config vdc-all** is required to bring up the FEX interfaces.

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
7.3(1)D1(1)	6.1(5a)
	6.2(10)
	6.2(12)
	6.2(14)
	6.2(16)
	6.2(18)
	6.2(20)
	6.2(20a)
	6.2(22)
	7.2(0)D1(1)
	7.2(1)D1(1)
	7.2(2)D1(1)

	7.2(2)D1(2)
	7.3(0)D1(1)
	7.3(0)DX(1)

Cisco NX-OS Release 7.3(0)DX(1) has the following cold boot support matrix:

Table 30 Supported Cold Boot Matrix in Cisco NX-OS Release 7.3(0)DX(1)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
7.3(0)DX(1)	7.3(0)D1(1)
7.3(0)DX(1)	7.2(1)D1(1)
7.3(0)DX(1)	7.2(0)D1(1)
7.3(0)DX(1)	6.2(22)
7.3(0)DX(1)	6.2(20a)
7.3(0)DX(1)	6.2(20)
7.3(0)DX(1)	6.2(18)
7.3(0)DX(1)	6.2(16)
7.3(0)DX(1)	6.2(14)
7.3(0)DX(1)	6.2(12)
7.3(0)DX(1)	6.2(10)
7.3(0)DX(1)	6.1(5a)
6.1(5a)	7.3(0)DX(1)
6.2(10)	7.3(0)DX(1)
6.2(12)	7.3(0)DX(1)
6.2(14)	7.3(0)DX(1)
6.2(16)	7.3(0)DX(1)
7.2(0)D1(1)	7.3(0)DX(1)
7.2(1)D1(1)	7.3(0)DX(1)
7.3(0)D1(1)	7.3(0)DX(1)

Cisco NX-OS Release 7.3(0)D1(1) has the following cold boot support matrix:

Table 31 Supported Cold Boot Matrix in Cisco NX-OS Release 7.3(0)D1(1)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
7.3(0)D1(1)	7.2(1)D1(1)
7.3(0)D1(1)	7.2(0)D1(1)
7.3(0)D1(1)	6.2(22)
7.3(0)D1(1)	6.2(20a)

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
7.3(0)D1(1)	6.2(20)
7.3(0)D1(1)	6.2(18)
7.3(0)D1(1)	6.2(16)
7.3(0)D1(1)	6.2(14)
7.3(0)D1(1)	6.2(12)
7.3(0)D1(1)	6.2(10)
7.3(0)D1(1)	6.1(5a)
6.1(5a)	7.3(0)D1(1)
6.2(10)	7.3(0)D1(1)
6.2(12)	7.3(0)D1(1)
6.2(14)	7.3(0)D1(1)
7.2(0)D1(1)	7.3(0)D1(1)
7.2(1)D1(1)	7.3(0)D1(1)

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

Table 32 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(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)

Table 32 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
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 33 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(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)
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 34 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(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(0)D1(1)	6.2(12)
7.2(0)D1(1)	6.2(10)
7.2(0)D1(1)	6.2(8b)
7.2(0)D1(1)	6.2(8a)
7.2(0)D1(1)	6.1(5a)
6.1(5a)	7.3(0)D1(1)
6.2(8a)	7.3(0)D1(1)
6.2(8b)	7.3(0)D1(1)
6.2(10)	7.3(0)D1(1)
6.2(12)	7.3(0)D1(1)
6.2(14)	7.3(0)D1(1)
7.2(0)D1(1)	7.3(0)D1(1)
7.2(1)D1(1)	7.3(0)D1(1)

Non-ISSU Upgrade/Cold Boot Upgrade Caveats

If you face any issue while performing a cold boot upgrade from Cisco NX-OS Release 7.3.2 to Cisco NX-OS Release 8.0.1, perform the cold boot using the ASCII upgrade and do not perform a binary upgrade.

ASCII Configuration Replay

Saving VLAN Configuration Information:

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

The following steps list the workaround for this limitation:

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

- Reload the switch with Cisco NX-OS Release 6.2(2) or a later release.

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

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

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

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

The following steps list the workaround for this limitation:

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

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

Non 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 7.3(2)D1(2), Cisco NX-OS Release 7.3(2)D1(1) or Cisco NX-OS Release 7.3(1)D1(1) 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 7.3(0)D1(1) includes the following new EPLD images:

- n7000-s1-epld.7.3.0.D1.1.img
- n7700-s2-epld.7.3.0.D1.1.img

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.

- 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.

For more information about upgrading to a new EPLD image for Cisco NX-OS 7.3.x and Cisco NX-OS 7.2.x release, see the Cisco Nexus 7000 Series FPGA/EPLD Upgrade Release Notes, Release 7.x.

New Hardware

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

Cisco NX-OS Release 7.3(1)D1(1)

The following modules are supported for Cisco NX-OS 7.3(1)D1(1) release:

- Cisco Nexus 7000 series supports M1XL, M2XL, F2, F2E, and F3 modules.
- Cisco Nexus 7700 series supports F2E, F3, and M3 modules.

Cisco NX-OS Release 7.3(0)DX(1) - M3 Series Modules

The following M3 series modules are supported in Cisco NX-OS Release 7.3(0)DX(1):

- Cisco Nexus 7700 48-port 1/10-Gigabit Ethernet SFP+ I/O module (PID: N77-M348XP-23L)
- Cisco Nexus 7700 24-port 40-Gigabit Ethernet QSFP+ I/O module (PID: N77-M324FQ-25L).

Cisco NX-OS Release 7.3(0)D1(1) - 3.5 KW HVAC/HVDC Power Supply

The following section includes the hardware introduced in Cisco NX-OS Release 7.3(0)D1(1):

- Cisco Nexus 7000 3.5KW High Voltage Power Supply Module (N7K-HV-3.5KW)
- Cisco Nexus 7700 3.5KW High Voltage Power Supply Module (N77-HV-3.5KW)

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

Cisco NX-OS Release 7.3(1)D1(1)–Software Features

ACI WAN Interconnect

Cisco Application Centric Infrastructure (ACI) WAN Interconnect provides multi-tenancy extension from ACI to the WAN edge.

With the Cisco Nexus 7000 series switch at the WAN edge paired with ACI, virtual network context can be extended to MPLS L3VPN in an integrated and automated way.

From an infrastructure perspective, the Cisco Nexus 7000 series switch is physically connected to the ACI Spine, which act as proxy Policy Repository (PR). Through Application Policy Infrastructure Controller (APIC), Policy Element (PE) extension is driven and the Cisco Nexus 7000 series switches are configured through OpFlex policy framework. The information received through OpFlex cater to the configuration towards the ACI fabric while the WAN Edge configuration can still be maintained separately. This facilitates the segregation of duty between the data center and the WAN operations.

For more details refer to the Cisco Nexus 7000 Series NX-OS VXLAN Configuration Guide.

Campus Fabric

Campus Fabric provides the basic infrastructure for building virtual networks based on policy-based segmentation constructs. Fabric overlay provides services such as host mobility and enhanced security, which are in addition to normal switching and routing capabilities. This feature provides Virtual Network Overlay capabilities by using a VXLAN-based encapsulation with a LISP control-plane for reachability. This feature is supported only on the M3 module.

The Cisco Nexus 7000 Series Switches with M3 Modules are providing the Fabric Border functionality that connects traditional Layer 3 networks and interconnects multiple Campus Fabrics. In this function, the Nexus 7000/7700 also provides the ability to translates reachability and policy information in between different Campus Fabrics and network domains.

For more details refer to the Cisco Nexus 7000 Series NX-OS VXLAN Configuration Guide.

ITD Scale

ITD scale enhancements for Cisco NX-OS Release 7.3(1)D1(1) are listed in the Cisco Nexus 7000 Series NX-OS Verified Scalability Guide.

Cisco NX-OS Release 7.3(0)DX(1)– Software Features

M3 series module is supported on Cisco Nexus 7700 Series Switches. The following features are supported in Cisco NX-OS Release 7.3(0)DX:

Layer 3 Unicast and Multicast

These features are supported on M3 series modules starting from Cisco NX-OS Release 7.3(0)DX(1).

Layer 2 Unicast and Multicast

These features are supported on M3 series modules starting from Cisco NX-OS Release 7.3(0)DX(1).

QoS

QoS features are supported on M3 series modules starting from Cisco NX-OS Release 7.3(0)DX(1).

vPC

vPC is supported on M3 series modules starting from Cisco NX-OS Release 7.3(0)DX(1).

SPAN

SPAN is supported on M3 series modules starting from Cisco NX-OS Release 7.3(0)DX(1).

OTV

OTV 1.0 and OTV 2.5 are supported on M3 series modules starting from Cisco NX-OS Release 7.3(0)DX(1).

NetFlow

NetFlow is supported on M3 series modules starting from Cisco NX-OS Release 7.3(0)DX(1).

GOLD

Generic online diagnostics (GOLD) is supported on M3 series modules starting from Cisco NX-OS Release 7.3(0)DX(1).

MPLS / L3VPN

These features are supported on M3 series modules starting from Cisco NX-OS Release 7.3(0)DX(1).

VXLAN (EVPN border-spine and VRF Lite hand off)

These features are supported on M3 series modules starting from Cisco NX-OS Release 7.3(0)DX(1).

IP GRE

IP GRE is supported on M3 series modules starting from Cisco NX-OS Release 7.3(0)DX(1).

mGRE

mGRE is supported on M3 series modules starting from Cisco NX-OS Release 7.3(0)DX(1).

GTP Hashing

The **port-channel load-balance** command has been enhanced with a new keyword, **gtp-teid** for configuring load-balancing using port-channels for M3 Series modules.

BFD FSA Offload Support

The **bfd hw-offload-module** command is enabled by default in M3 series modules. The BFD Fabric Services Accelerator (FSA) Offload on F3 and M3 Line Cards feature allows the offload of asynchronous BFD transmission (Tx) and reception (Rx) to the network processing unit on the F3 and M3 module. The BFD FSA Offload on F3 and M3 module 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.

MACsec (256)

The existing SAP GCM cipher suite supports 128 bit AES key generation which is being used to encrypt and decrypt the data. The new generation line card (M3) has the capability to encrypt and decrypt with 256 bit AES key with 64 bit sequence number. A new SAP GCM cipher mode (GCM 256) is introduced in Cisco NX-OS Release 7.3(0)DX(1) to leverage the 256 bit AES key capability of the hardware.

ACL

ACL is supported on M3 series modules starting from Cisco NX-OS Release 7.3(0)DX(1).

The guidelines and limitations are:

- M3 Series modules support ACL capture.
- FCoE ACLs are not supported for M3 Series modules.
- For M3 Series modules, the mac packet-classify command enables a MAC ACL for port and
- VLAN policies.
- M3 Series modules support WCCP.

Cisco NX-OS Release 7.3(0)D1(1) – Software Features

IPv6 BGP PIC Edge for IPv6

The BGP PIC for Edge feature improves BGP convergence after a network failure. This convergence is applicable to edge failures in an IP network. The BGP PIC Edge feature creates and stores a backup path in the routing information base (RIB) and forwarding information base (FIB) so that when the primary path fails, the backup path can immediately take over, enabling fast failover in the forwarding plane. In this release, BGP PIC Edge support is now extended to the IPv6 address family.

Light Weight DHCPv6 Relay Agent

The Lightweight DHCPv6 Relay Agent (LDRA) forwards DHCPv6 messages between clients and servers when they are not on the same IPv6 link. The LDRA feature allows relay agent information to be inserted by an access node that performs a link-layer bridging (non-routing) function. The relay agent information is primarily used to identify client facing interfaces.

Logging IPv6 Gap

This feature extends the capability of setting a logging source interface from 'loopback only' to support other kind of IP-configurable interfaces like Ethernet, VLAN, management and port-channel. In this release, the existing logging source-interface command is extended with options to set IP based interface as the logging source.

BFD Support for HSRPv6

BFD supports all IPv4 and IPv6 HSRP groups, if HSRP BFD ALL interfaces is configured.

Per-link BFD

The Per-link Bidirectional Forwarding (BFD) feature enables users to configure individual BFD sessions on every Link Aggregation Group (LAG) member interfaces (as defined in RFC 7130).

OSPFv3 IPSec Authentication

OSPFv3 messages can be authenticated to prevent unauthorized or invalid routing updates in the network. This feature enhances Cisco NX-OS OSPFv3 to add authentication and encryption to its packets. It uses IPSec AH header with the MD5 or SHA1 authentication. To configure IPSec, you configure a security policy, which is a combination of security policy index (SPI) and the key. You can configure OSPFv3 authentication at the following levels:

- Router / process
- Area
- Interface

Dynamic Route Leaking Using Route Targets Between Default VRF and Created VRF

This feature supports the export of IP prefixes to the global routing table (the default VRF) from any other VRF using export vrf default command. This leaks a VRF route into the default VRF BGP table, which will then be installed in the IPv4/IPv6 routing table.

MPLS Features

MPLS TE CSPF Cost Limit

Constrained shortest path first (CSPF) cost limit feature allows you to specify a maximum permitted total cost for a tunnel's path and invalidate if the cost is higher. The configured cost limit applies to metric type that is used while calculating the tunnel's path, which may be IGP or TE link metrics. By default, cost-limit is not imposed.

CSPF Enhancements

The following Constrained shortest path first (CSPF) enhancements are available:

- Hop limit
- Dynamic ABR determination
- Interface address as destination
- Strict / loose intra-area paths
- Link-load balancing

Logging LSP and FRR Events

Logs are extensively used to monitor networks. This feature enables you to generate system logs for the events related to tunnels, label switched paths (LSPs) and fast reroute (FRR).

GIR Enhancement

Starting with Cisco NX-OS Release 7.3(0)D1(1), the default mode for GIR is “isolate”. Use the **system mode maintenance** command to put all the enabled protocols in maintenance-mode. The switch will use the **isolate** command to isolate the protocols from the network. The switch will then be isolated from the network but is not shut down.

Hitless STP for vPC Role Change

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

Asynchronous Link Debounce

The Debounce link up feature enables you to set separate values for debounce up and debounce down links.

PVLAN (isolated) on FEX

The isolated PVLAN support on FEX HIF feature enables users to configure PVLAN isolated host and secondary trunk ports on Fabric Extenders (FEX) ports, where the parent switch must be a Cisco Nexus 7000 series switch.

Port Channel (Random Load Balancing)

Random load balancing on port channels is a software solution that enables better port link bandwidth utilization for GPRS Tunneling Protocol (GTP) over IP-UDP packets. The line card hardware does not have the capability to perform random load balancing and hence, this software solution helps in load balancing and optimizing the port channels bandwidth.

Link OAM

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

Ethernet OAM is supported on the following modules from Cisco Nexus Release 7.3(0)D1(1):

- M2-Series 10-Gigabit Ethernet Series Module for Cisco Nexus 7000 Series Switches.
- F3-Series 10-Gigabit Ethernet Series Module for Cisco Nexus 7000 Series Switches and Cisco Nexus 7700 Switches.

Ethernet OAM is not supported on the F2 series modules.

Fabric OAM

Ethernet operations, administration, and maintenance (OAM) is a protocol for installing, monitoring, and troubleshooting Ethernet networks to enhance management in VXLAN based overlay networks.

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 leaf switch (L2/L3 Gateway with Distributed Anycast Gateway and vPC) border-leaf switch (L2/L3 Gateway, MPLS, and Classic Ethernet Layer2 with and without vPC) and spine switch with and without route-reflector. For VXLAN multi-destination traffic, PIM ASM and Bidirectional PIM are required.

VXLAN Leaf Switching/Routing

These features describe the functioning of the VXLAN fabric which comprises of ToR (leaf) switches at the access layer and spine switches at the aggregation layer. The leaf switches perform the role of Virtual Tunnel End Points (VTEPs) in the VXLAN fabric, thereby encapsulating or decapsulating VXLAN packets from/to the end hosts. VTEPS also perform Integrated Route/Bridge (IRB), deciding whether to route or bridge packets in the VXLAN overlay network. Designated spine switches perform the role of route reflector (RR) in the control plane.

VXLAN Border Leaf / Border Spine Switching/Routing

These features describe the Data Centre Interconnect (DCI) functionality on the border-leaf/spine switches, with virtual port channels (vPCs). The VXLAN DCI hand-off scenarios include classical Ethernet hand-off for layer 2, and hand-off to MPLS L3VPN and LISP enabled networks.

Auto Configuration

Virtual Machine Tracker auto configuration is a feature that automatically configures a tenant for provisioning. The Virtual Machine Tracker auto configuration feature retrieves information about a tenant from the database (LDAP) and issues the necessary configuration commands for the provisioning.

Support for Chef and Puppet Agents

Support for open agents, such as Chef and Puppet has been added to Cisco Nexus 7000 and Cisco Nexus 7700 Series switches. However, open agents cannot be directly installed on these platforms. Instead, they run in a special environment--a decoupled execution space within a Linux Container (LXC)—called the Open Agent Container (OAC). Decoupling the execution space from the native host system allows customization of the Linux environment to suit the needs of the applications without impacting the host system or applications running in other Linux Containers.

FCoE Features

FCoE FEX over F3 and FCoE Access Features

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.

FCoE over FEX is now supported on F3 modules along with the existing support on F2 and F2e modules. F3 is available in 40G and 10G variants on both Cisco Nexus 7000 and Cisco Nexus 7700 series switches.

The following FCoE features are supported for Cisco NX-OS 7.3(0)D(1)1:

- FCoE over FEX with F3 and F2 (N2K-C2348UPQ-10GE , B22HP, N2K-C2232PP-10GE)
- F3 FCoE support with physical port vPC and vPC+
- F3 FCoE support for FEX with physical port vPC and vPC+

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 F3

In addition to the existing F3 cards support, the following card is also supported on FCoE:

- N7K-F348XP-25 (48 ports 10G card for Cisco Nexus 7000 series switches)

F3 card support in Cisco NX-OS Release 7.2(0)D1(1) is listed in the FCoE on F3 section.

FCoE Scale

FCoE scale enhancements for Cisco NX-OS Release 7.3(0)D1(1) are listed in the Cisco Nexus 7000 Series NX-OS Verified Scalability Guide.

iSCSI TLV

This feature lowers the cost solution of deployment of iSCSI over loss-less Ethernet over FCoE. No hardware or gateways are needed that coverts iSCSI to FC traffic. Now, iSCSI targets are present which can do end-to-end iSCSI with initiators. iSCSI TLV supports both Cisco Nexus 7000 series and Cisco Nexus 7700 series switches. Refer to Configuring iSCSI TLV chapter in Cisco Nexus 7000 Series NX-OS SAN Switching Configuration Guide for iSCSI TLV configuration details.

Cisco TrustSec Features

Subnet to SGT Mapping

Subnet to security group tag (SGT) mapping binds an SGT to all the host addresses of a specified subnet. After the implementation of this mapping, Cisco TrustSec imposes the SGT on any incoming packet that has a source IP address which belongs to the specified subnet. This enables the user to enforce CTS policy on traffic flowing through data center hosts.

SGT Exchange Protocol Version 3

The SGT Exchange Protocol Version 3 (SXPv3) feature provides the support to transport IPv4 Subnet to SGT bindings.

SGACL Monitor Mode

In the pre deployment phase of Cisco TrustSec, an administrator would use the monitor mode to test security policies without enforcing them to make sure the policies are what were originally intended. The monitor mode provides a convenient way to roll back before enforcing the security policy if the security policy contains errors. This feature enables administrators to have increased visibility to the outcome of the policy actions before enforcement and confirmation that the subject policy meets the security need. It denies access to resources if the individuals are not authorized. This feature also reduces the eventual deployment time for a Cisco TrustSec system.

SGACL ACLLOG

SGACL ACLLOG feature enables the user to observe the effects of the SGACL policies after the enforcement at the egress point. The user can check the following:

- Whether the flow was permitted or denied.
- Whether the flow is monitored or enforced by the SGACL.

Flexible TCAM Bank Chaining

The user can configure flexible ACL TCAM bank chaining feature to chain two banks within a TCAM enabling two lookups with two results per packet per direction. This helps the user to handle larger ACLs that can be spread across multiple TCAM banks, and also allows the configuration of up to two ACL features per destination. This feature is only supported for F3 modules.

ITD Features

ACL Allowed Traffic to be Load-balanced

This feature is used to simultaneously filter traffic with an ACL and to load-balance the traffic. An user-defined ACL can be configured in the Include ACL feature. For each ACE that has permit method in the ACL, the feature filters the unwanted traffic and generates IP access lists and route-maps to load-balance the permitted traffic.

Optimized Node Insertion/Removal

This feature enables users to dynamically add or remove nodes with minimal disruption to the existing traffic, irrespective of whether the ITD service is shutdown or not. This feature maintains an intermittent state of nodes when the nodes are deleted or added in a service that is active. The feature provides a CLI trigger to re-program the buckets after the user add or delete the node.

Audio Video Bridging (AVB)

Audio Video Bridging (AVB) is a set of standards that enable time-synchronized low latency streaming services on Ethernet networks, including wireline Ethernet networks shared with other data traffic and wireless LANs. AVB implements the set of standards developed by the IEEE Audio Video Bridging Task Group. AVB functions by reserving a fraction of the Ethernet bandwidth that is available for AVB traffic. AVB consists of the following specifications that are defined under the standard IEEE 802.1BA: Audio/Video Bridging (AVB) Systems:

- IEEE 802.1AS – gPTP: Generalized Precision Time Protocol (gPTP)
- IEEE 802.1Qat: Multiple Stream Reservation Protocol (MSRP) that defines an end-to-end bandwidth reservation protocol within a bridged LAN.
- IEEE 802.1Qav: Forwarding and Queuing for Time-Sensitive Streams (FQTSS), which is AV traffic scheduling capability for a mainstream Ethernet and other network switches.

4K VLANs per SPAN or ERSPAN

The 4K VLANs per SPAN or ERSPAN feature enables addition of a new source type, source interface all, to the monitor session in the Ethernet VDC. This feature enables the session to monitor all ports and VLANs in the VDC.

NetFlow on CoPP Interface

The NetFlow on CoPP Interface feature uses traffic flows to provide statistics for network traffic accounting, network monitoring, and network planning on the CoPP interface.

OpenFlow on F3

Cisco Plug-in for OpenFlow provides better control over networks making them more open, programmable, and application-aware and supports the following specifications defined by the Open Networking Foundation (ONF) standards organization:

- OpenFlow Switch Specification Version 1.0.1 (Wire Protocol 0x01) (referred to as OpenFlow 1.0)
- OpenFlow Switch Specification Version 1.3.0 (Wire Protocol 0x04) (referred to as OpenFlow 1.3)

Netconf Enhancements

Network Configuration Protocol (NETCONF) (RFC 4741) is an IETF network management protocol that provides mechanisms to install, manipulate and delete the configuration of network devices. The Cisco NX-OS Release 7.3(0)D1(1) supports the following Netconf capabilities:

- get-config
- copy-config
- validate
- enhancements in edit-config to support Default-Operation and Operations (Actions)
- enhancements in edit-config to support Rollback on Error, Stop on Error, and Continue on Error
- enhancement in edit-config to support candidate configuration
- commit and discard-changes
- lock
- unlock
- logging of all the Netconf operations and its status in syslog
- extending hello capabilities for all of the above

Update to Hostname

The character limit for a switch name and a host name is increased from 32 to 63 alphanumeric characters.

Login Block Per User

The Login Block Per User feature helps detect suspected Denial of Service (DoS) attacks and slow down dictionary attacks. You can configure login parameters to block logins per user. This feature is applicable only for local users.

EXEC Banner

The EXEC banner is displayed after a user logs in to a switch. This banner can be used to post reminders to your network administrators.

NTP Authentication Key Length Enhancement

Beginning with Cisco NX-OS Release 7.3(0)D1(1), you can use up to 32 alphanumeric characters for the MD5 string.

UDP Relay

UDP relay feature is used to relay broadcasts destined to UDP ports except DHCPv4 port numbers 67 and 68. This feature is supported only for M1 and M2 line cards.

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

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 Fabric Path on F3

Cisco TrustSec MACSec is supported over Fabric Path via native VLAN tagging on trunk and Fabric Path 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)

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, M2, and M3 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 Fabric Path 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 Fabric Path 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). Dynamic Routing is not supported over vPC+.

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 Fabric Path Core Ports

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

L3 BFD Sessions over Fabric Path Links

When switches are connected through Fabric Path and core port is configured for L3 services over SVI, BFD over Fabric path 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 FP network, BFD resolves adjacency for the given L3 peer address over FP link and exchanges BFD packets with Fabric Path 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.

Fabric Path OAM

Fabric Path OAM facilitates operators to monitor, isolate and verify data plane faults on Fabric Path networks. Fabric Path 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 (BIDIR) 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

Beginning with Cisco NX-OS Release 7.3(0)D1(1), FCoE is supported on the following F3 Series module:

- N7K-FCOE-F348XP-25

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:

- 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(2)D1(2)
- 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.x

Table 35 Open Caveats for Cisco NX-OS Release 7.3(4)D1(1)

Identifier	Description
CSCvp41853	STP flush is not sent from the upcoming AED - Convergence Issue
CSCvp87136	RSTP bpdu are not sent/received on VSI interfaces

Table 36 Open Caveats for Cisco NX-OS Release 7.3(2)D1(3)

Identifier	Description
CSCva16707	F3 - static MAC programmed for TCAM Bucket0
CSCvb74706	N7K: F3 2s convergence time on module OIR
CSCvb93995	Cisco NX-OS Software removes ACL from VTY interface
CSCvc55528	WCCP crashed due to memory leak - WCCP_MEM_msg_control_packet
CSCvd10140	Dynamic Mac address has wrong DI (Destination index) on M2
CSCve07101	N7k/6.2(16) BGP not prepending as-path for certain prefixes in a prefix-list
CSCve10859	NXOS Default prefix LSA handling change
CSCve40271	N7K crashes while opening startup-config
CSCve46211	ethpcm crash when trying to allocate memory
CSCve54480	ARP ACL not working on M3 card
CSCvf87011	M3 - Ncpinfraclnt Crash
CSCvg10842	Input discards after issu to 7.3 or 8.x code, egress throughput reduction for F3-100gig/40gig ports.
CSCvg38672	vpc self-isolation:vpc legs are up on local after all modules up when MCT down
CSCuc35049	Need syslog to match error state of fabric modules

Table 37 Open Caveats for releases prior to Cisco NX-OS Release 7.3(2)D1(3)

Identifier	Description
CSCuy90706	adbm hap reset in sQuery->server_info
CSCve70445	Bfd is not coming up with cts on M3
CSCvf04693	Orphan ports enabled with “vpc orphan-port suspend” remains down after auto recovery.
CSCvc19961	aclqos ddb crash during ISSU from 7.3.1 to 8.3.0
CSCve83414	pltfm_config_core when cold boot from 7.3.2 to 8.0.1
CSCve72891	[732] N77-F324FQ-25 module failure happened after ISSU from 7.2.1 to 7.3.2
CSCve56073	The IPFIB crashes during ISSU from 7.3(2)D1(1) to 8.1(1)b with MPLS TE configurations.
CSCve51455	Issue with the F3 module ipfib core for two modules after ISSU to upgrade the image, FLN_FIB_LSMET_EXHAUSTED.
CSCve51455	ECMP Path Table Entries Exhaustion causes Route Programming Failures on F3 Module
CSCvc72202	CVR-QSFP-SFP10G goes down after the F3 module reload
CSCvb84395	CTS: M3 module failure with log enabled deny policies.
CSCva38063	BFD sessions are flapping on removing the bfd auth ipv6 command
CSCva84959	F2 1G port fails to recover after remote end comes back up
CSCvb02263	Interface MTU gets rewritten to 9216 after Ascii Reload
CSCva95215	PORT_CMD_VLAN not being programmed for FEX ports for LLDP native hosts
CSCva62428	7.3(1)DX(0.92) : Failed to verify ospf neighbor aftr enable bfd
CSCva72699	Extended S-N traffic loss during ISSU from 7.3.1.DX.0.96.bin to upg
CSCvb12045	ipfib core after vdc reload with 731(D1)1. S2
CSCva12806	64+1 ports missing cieIfStatusListTable in ciscoIfExtensionMIB
CSCvb05732	%VNTAG_MGR-2-VNTAG_SEQ_ERROR: Error ("sequence timeout")
CSCva60579	traffic duplication seen for BIDIRv6 with SSO for less than sec
CSCva45161	Mcast traffic loss for few secs with SSO in 7.3.1.DX.0.78 img
CSCva90756	N-S mcast traffic black hole for 8 secs after core link no shut
CSCva84822	Excessive updates between mfib and iftmc in EVPN VXLAN
CSCva63951	731(DX)87: rsvp gets disabled on interfaces upon rsvp process restart
CSCva42140	Packet to tail end of MPLS TE could be more than 1460 bytes
CSCva76338	7.3.1.DX.0.91 - mpls allocating label for loopback interface
CSCva92716	F3: NetFlow timeouts are not configured properly
CSCvb17860	M3: NetFlow timeouts are not retained on default vdc after LC reload
CSCva60666	Duplicate traffic when remote S,G decap route is installed
CSCva96911	vrf configs remain for failed add vrf case
CSCva67416	Cos of FIP packet changed from 3 to 6 on egress in FP spine

Table 37 Open Caveats for releases prior to Cisco NX-OS Release 7.3(2)D1(3)

Identifier	Description
CSCva53102	crash observed @ aclqos_starlifter_pl_policer_alloc_old_aggr
CSCva98223	BGP Traceback %BGP-2-SLAB_ELEM_ERR Seen on NXOS 7.3(0)DX(1).
CSCvb14897	Map-caches resolution may be delayed or not resolved in some cases
CSCvb14596	RLOC probes delayed after clearing the map-cache entries
CSCvb09924	SF: Negative map-cache missing on PxTR for static map-cache cli
CSCvb05915	Underlay (vrf core) - VRF Shut takes more that 60 seconds
CSCuz55153	Console Hang while connecting to OAC with hsk2 after first activation
CSCva24748	transceivers in FEX use math instead of transceiver alarm flag
CSCuv72625	N7K - SNMP get one for 4 objects “No Such Instance” CISCO-SYSLOG-EXT-MIB
CSCva45358	vPC scaling: LC is unable to powered up in time.
CSCva69911	host delete should be sent to hmm on removing port-channel members
CSCvb04007	FEX A/A: Convergence takes 5-6 secs on FPC secondary "no shut"
CSCva88233	interface config missing while copy saved config into runn-conf
CSCva75647	IP Phone is unable to register with CUCM when fabric border is N7k
CSCva16746	LISP: VNI state and BDI VRF membership out-of-sync
CSCvb15403	Post ISSU: Port Flap on hif port of fex id > 164 removes the Flogi on Cisco Nexus 7000.
CSCuz55153	Console Hang while connecting to OAC with hsk2 after first activation
CSCuz33057	ACLQOS failure: ELTMC COMMIT ERROR 0x42650010, when VDC is suspended
CSCuz24669	ACL config failed due to TCAM Spanlogic
CSCuz18973	aclqos crash with many match keywords in single ACE
CSCuz18992	wrong ACL matching for IPv6 packets with Authentication ext hdr
CSCuz19882	non initial frag pkt does not match tcp/udp any any entry
CSCuz40601	Longevity - MTS Buffer Leaks - HSRP/BFD
CSCuz15957	bfd ipv6 authentication command doesnot have any affect on bfd sess
CSCuz19909	CTS :On switch reload, CTS-dot1x links goes to INIT
CSCuz33853	CTS rol-based enforcement is not effective for one specfic scenario.
CSCuz22357	Packet drops on F2e LC on vdc reload trigger wtih CTS configuration
CSCuz05917	eltm crashed on enabling 3966 vlan translation
CSCuy79367	IFTMC_INTERFACE_INTERNAL_ERROR: Invalid intf state provided to IFTMC
CSCuy97188	seeing eobc drop on the scale testbed
CSCuy69373	dropped mac are not learnt after increasing port-sec max
CSCuz35151	ASCII replay with Booting modules can be unpredicatable
CSCuy88114	PFC gets disabled on non-Macsec CTS ports on F-series linecards

Table 37 Open Caveats for releases prior to Cisco NX-OS Release 7.3(2)D1(3)

Identifier	Description
CSCuy78035	Ability of modify failure count as part of CSCuu47125 not allowing 10+
CSCuz13193	BootupPortLoopback UNTESTED when first inserting to the switch.
CSCuy31282	XMLization support for HSRP MGO and HSRP Anycast features
CSCuw34945	Expected output is not seen for snmp query
CSCuy82339	Few BFD sessions down with subinterface optimization on sh/no sh
CSCuy17686	With BFD optimize sub interface multiple BFD clients are not allowed
CSCuz24167	N77/N7K - SNMP cshcModRxTotalDroppedPackets - all zeros
CSCuy68449	seeing vsh cores on Active & standby SUP while collecting show tech det
CSCuy02073	TE: F3 line card crash
CSCuy58448	Cb10: link flaps if the speed on the interface is mismatch on 1G
CSCuy86259	43% frame loss after changing PC load balance to ip-l4port
CSCuz29940	MFIB fail to install route with Tunnel after LC reload
CSCuz46248	sup1/m1-non-xl cards are seen under "show module supported"
CSCuy02338	After enable/disable mvrp, vlan not programmed on member ports
CSCuy72928	After SSO, Observed traffic drop for 0.5-1 sec.
CSCuz12435	Admin vdc migration to new vdc with FEX is giving error
CSCuy96171	Few BFD sessions flapping after vdc suspend/resume, reload, lc reload
CSCuy14744	N77 - C7702 not populated for cshcNetflowResourceUsageTable
CSCuz04721	vsh crash observed while executing show running | xml
CSCuz23469	Port profile crash in N7K DCI (Opflex setup) on doing "no feature ipp"
CSCux46318	Unable to modify the config profile template after no feature ipp
CSCuv14693	Out of band programming occuring, please try Service-policy again later.
CSCuz25546	SSTE: LISP Process crash during continuous process restart
CSCuy56270	STP timedout after removing all vlans on vPC Primary on Full MST Scale
CSCux35453	L2 BFD sessions taking L3 bfd variables
CSCuq12660	netboot NPE image gets a non-NPE image
CSCuz46473	N7K - tar core during ISSU from 7.2(1)D1(1) to 7.3(0)DX(1)
CSCuy45648	GRE: Service not responding when changed the "tunnel destin" to DNS
CSCuz19597	GRE: Tunnel Path MTU ignored tunnel port MTU
CSCuy83217	Tunnel intf is down(Hardware prog failed) with M3-F3 GRE Tunnel scenario
CSCuz44784	FIB Consistency checker fail for NVE loopback
CSCuy35651	Removing IPSG config from one Client int, clears other entries from H/W
CSCuz15332	SSTE: ipfib crash on F3 during longevity - 7.3.0.DX.0.141.S1
CSCuy12229	Traffic does not reconverge after primary vpc or LC reload
CSCuz38530	PeerKeepAlive vrf is not migrated: tatus: Suspended (UNUSABLE VRF)
CSCuz39212	FP & VPC ports has Vlan membership in ELTM although no config present

Table 37 Open Caveats for releases prior to Cisco NX-OS Release 7.3(2)D1(3)

Identifier	Description
CSCuz13758	Removing interface config throws Error ("fu hashtable key not present")
CSCuy91444	Enabling vtp in Fabricpath enabled setup should throw error
CSCuy81855	SGACL with > 1 ACE is not installed when policy caching is enabled
CSCuy18682	Cisco Nexus 7000 Series 10G: VSH crashed in 4 F3 LC when collecting sh logg onboard
CSCuw72856	FCOE-scale:"aclqos" service crash on activating 1k IVR zones
CSCux28164	DOM not supported and cisco id empty for QSFP-40G-SR-BD SFP on MDS
CSCux48530	40Gb LC LED does not flash on running IO
CSCuy00151	Crash in feature-mgr when we use show feature cli on standby RP
CSCus52139	post L3, l2 flood traffic not going out on peer-link
CSCuy00282	Traffic to FEXAAHIF gets dropped when FEX not online on a vpc peer
CSCuw13014	MTS buffer exhaustion in mcecm/vpc
CSCux96194	After ISSU from 7.2(1) to 7.3(0) when we flap vpc leg seei dup packets
CSCux67642	FEX ports unavailable after FPC mod off, Switchover and FPC mod powered on
CSCux34166	NXAPI on sys switchover, the configured ports are resetting to default
CSCux59918	Profile conflict after vdc reload
CSCuy17010	VPC PVLAN with PO Trunk Secondary is not Supported
CSCux44590	Python script errors on 'detail' command
CSCuh23173	SH crashed on software over running UTE script
CSCuy12229	Traffic does not re-converge after primary vpc or LC reload
CSCux11960	ADBM: Frequent bind/unbind issue.
CSCuy17372	PVLAN trunk secondary association removal causing traffic drop.
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

Table 37 Open Caveats for releases prior to Cisco NX-OS Release 7.3(2)D1(3)

Identifier	Description
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
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

Table 37 Open Caveats for releases prior to Cisco NX-OS Release 7.3(2)D1(3)

Identifier	Description
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 Fabric Path 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
CSCuw34008	F1 Fabric path. 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
CSCux49719	pam_aaa_motd:cannot open motd file : /vdc_4/etc/motd - dcos_sshd

Resolved Caveats—Cisco NX-OS Release 7.3(6)D1(1)

Table 38 Cisco NX-OS Release 7.3(6)D1(1) Resolved Caveats

Identifier	Description
CSCux65385	NXOS DATACORRUPTION-DATAINCONSISTENCY error in PIM process
CSCuz30263	After upgrade, eigrp failed to come up due to K value mismatch
CSCvb23106	unexpected eigrp metric calculation in aci
CSCvd38589	Empty field is seen and Mac's are not secured in Avalon image
CSCvj05813	ARP Does Not Respond For VRRPv3 VIP After Module Reload "Destination address is not local"
CSCvj63137	Copy command can't overwrite world-writable files
CSCvo11853	Service rsvp crashes twice in quick succession, first with signal 11, then with signal 6
CSCvo90099	NX-SNMP: snmp-server hosts getting modified after configuration(DNSv6 case)
CSCvp36080	Nexus doesn't send Register-Stop when Register is denied by PIM Register Policy
CSCvq05447	N9K NX-OS 9.2(3) SNMPd Crash / MTS Queue Congestion When Doing GETBULK on entPhysicalEntry
CSCvq48447	N9K snmpd signal 8 crash
CSCvr08197	N7k PIXM/PIXMc should attempt to recover if they get out of sync
CSCvr10766	N7k netflow input and output interface does not map to IOD database for M3 LC for Version 5 template
CSCvr19809	cosmetic: native 40G port (non-breakout) report incorrect Quesize for F3. breakout 4x10G unaffected.
CSCvr30525	IGMPv3/MLD Snoop - Mcast Traffic Loss To All Receivers After One Receiver Sends Multiple Leafs
CSCvr39538	N7K may report false memory utilization values
CSCvr57551	Cisco Nexus 9000 reloads with Kernel panic - unable to handle kernel paging request
CSCvr62671	SSH quietly fails - aaa reports failed to remove the access list configured : sl_def_acl
CSCvr62735	BGP attribute-map for aggre address sets the last attribute without matching the prefix list.
CSCvr63838	SNMP walk using OID 1.3.6.1.2.1.1 returns NULL [Expert Info (Note/Response): endOfMibView]
CSCvr63916	Module id incorrectly formatted in CPUHOG messages
CSCvr85588	VTP crashed after multiple trunking interfaces flapped
CSCvr96953	Users cannot authenticate against RADIUS/TACACS+ if custom role offered was recently modified
CSCvs00187	vsh.bin process crash

Table 38 Cisco NX-OS Release 7.3(6)D1(1) Resolved Caveats

Identifier	Description
CSCvs11098	Rollback fails to update OTV extend-vlan list on Nexus 7000 switch platforms
CSCvs16170	corrupted/incorrect router ID sent in update packet for external routes.
CSCvs20377	RPF nbr pointing to Assert Loser on RP in MVPN environment
CSCvs23562	MALLOC_FAILED: mcastfwd [27776] m_copyin failed in mfwd_ip_main()
CSCvs26685	%NETSTACK-3-URIB_ASSERT_ERROR on u6rib_process_notify
CSCvs29433	EIGRP learned routes flapping when associated prefix-list is modified
CSCvs43451	fcoe n7k with 2232pp fex after sup switchover hif ports change from pfc to link level pause
CSCvs49787	MAC Address learning failed due to unexpected "port-security" function remaining enabled
CSCvs54854	Crash while executing - show logging onboard error-stats - in show tech
CSCvs57779	N7K: Port-Profiles disappear after shut fex-fabric ports & no feature-set fex
CSCvs58870	Collect dmesg during SLF inband failure on M3
CSCvs59985	Netlow StartTime and EndTime being reported in the future by almost 2 minutes.
CSCvs69194	N7K only listens one ip for tcp 64999 when cts sxp source ip is configured
CSCvs84593	eem_syslog_regex_ev_spec_handler is output when eem is created
CSCvs97090	ITD reverse policies are not programmed properly.
CSCvt19467	BFD ACL programming issue after downgrading from 8.3(1) to 8.2(4) using boot variables methd.
CSCvt33067	Traffic Black-holing with VPC SFC failure(L2LU Drops, VSL Check)
CSCvt35882	n7k Service "statsclient" crash
CSCvt46409	N7k OSPF area range not advertising cost
CSCvn54508	vsh core triggered by CLI
CSCvs56900	U2RIB 452 MTS buffer stuck with memorey leak and crash in the MCM/U2RIB
CSCvt17690	AS number isn't displayed in BGP-5-ADJCHANGE up/down log
CSCvs71659	RIT changes to support Local, GLEAN punt path for MPLS ADJACENCIES
CSCvo82792	VTP core seen doing ISSU from bin to .upg
CSCvm69150	l2vpn process crash while bringing up VPLS between ASR9K and Nexus 7K
CSCvo18982	OSPF Configuration removed after Supervisor Switchover
CSCvs83567	NX-OS 8.x IP redirect source check not working

Resolved Caveats—Cisco NX-OS Release 7.3(5)D1(1)

Table 39 Cisco NX-OS Release 7.3(5)D1(1) Resolved Caveats

Identifier	Description
CSCuv02817	Default-information-originate behavior change for OSPFv2 and v3
CSCut88214	Nexus 3172 forwards both copies of IP redirect frames
CSCuw39988	N5672 - NXAPI sandbox browser will not work over HTTPS port 443
CSCva90832	TACACS non blocking connect failed with error code 98
CSCvb49085	n7k M3: Shaping policy causes interfaces to go to suspended state and IntPortloopback to fail
CSCvc91280	incomplete error output during duplicate IP address entry
CSCvd17852	PIM BIDir DF election issue
CSCvd48792	Lamira processes should clear /var/tmp logs periodically
CSCvf24911	ARP memory leak @ LIBBL_MEM_bitfield_malloc_t & LIBSLAB_MEM_create_slab
CSCvf79399	2232PP FEX module(with N5/6/7/9K parents) Crash when inserting 4 GLC-TE transceivers into HIF port
CSCvg07239	VxLAN PBR : Ipfib core post ISSU to upg
CSCvg77231	BGP stuck into Shut (NoMem) and neighbourship not formed
CSCvh63779	F3: Disable flexible TCAM bank-chaining "ERROR: Entry not found in copp database"
CSCvi05048	Netflow sends packet with Invalid payload size causing fln_l3 core
CSCvj24868	MTS buffers' leak while constantly polling objects in BRIDGE-MIB
CSCvj63877	Cisco NX-OS Software Command Injection Vulnerability (CVE-2019-1735)
CSCvj65666	Cisco FXOS and NX-OS Software CLI Command Injection Vulnerability (CVE-2019-1611)
CSCvj78681	Tacacs crash with nginx authentication and CLI command authorization
CSCvk05550	N7k - SPAN Destination traffic leaves untagged in setup with bridge-domain
CSCvk51138	N7K Fabricpath :: MAC address not re-learned on broadcast ARP
CSCvk68792	NXOS: Netstack crash observed with active timer library in heap_extract_min
CSCvk76030	Cisco NX-OS Software Virtualization Manager Command Injection Vulnerability
CSCvm52059	CPU Traffic Not Sent out on L3 VRF Interface
CSCvm65141	cannot rewrite vlan at dual-active exclude interface-vlan-bridge-domain
CSCvn01886	Nexus SW - Route missing in RIB while track object is up upon reload
CSCvn09912	N7k/F2E: 'Disabling PFC on port x since macsec is disabled' logs filling syslog
CSCvn10484	Tacacs: Under stress condition, few tacacs authentication/authorization transactions has failed

Table 39 Cisco NX-OS Release 7.3(5)D1(1) Resolved Caveats

Identifier	Description
CSCvn36429	Service "AAA Daemon" failed to store its configuration (error-id 0x80480018)
CSCvn37301	With passive TWINAX cable N2K-C2348TQ-10G-E reports the Fan Failure
CSCvn51301	ARP crashed on BL while other BL comes online // ARP mbuf leak
CSCvn57953	NVE failed to learn remote VTEP RMAC after ISSU aborted or canceled
CSCvn62162	no vn-segment failed to run
CSCvn63538	N7K: Entries in new created SVI mismatch between UFIB and URIB and communication fail using those
CSCvn78166	N3000 generates IGMP report with source 0.0.0.0 preventing the mcast group from timeout
CSCvn99435	API snmp_get_mgmt_conf_last_change_time return ERROR
CSCvo07343	VXLAN IPv6 packets loop due to NVE invalid source-intf state while peerlink is down or unconfigured.
CSCvo14963	N7K-PPM: Issues seen under interface when port-profile is inherited.
CSCvo15505	Egress packet loss from CPU when dest is recursive through EVPN
CSCvo15674	crash because of memory leak in bfd process
CSCvo29957	Output of "show mpls ldp igp sync" inconsistent with configuration
CSCvo61537	HTTP GET sent too late in python shell
CSCvo68452	Pending mroute entries persists after VRF is deleted
CSCvo73682	sac_usd hap reset when standby supervisor becomes active
CSCvo80379	BGP route may stuck at dampened state
CSCvo80677	Linecard CPU utilization is displayed incorrectly for some processes
CSCvo90639	N7K/N77 // TOS bits from IP header not being copied to MPLS EXP Bits in MPLS Header
CSCvo93018	Malformed ISIS Hello packet due to extra GRE header
CSCvp01676	T2 EOR: Traffic drop due to null NH in forwarding table
CSCvp04544	M3 LSMET fib exhaustion message shows wrong VDC number
CSCvp11726	NX-SNMP: Random Auth failure when performing snmp-walk (via TCP) using SNMPv3 users.
CSCvp16978	IGMP v2/v3 mix: shutdown igmpv2 receivers and igmpv3 receivers are also removed from mrib oifl
CSCvp25704	Cli show top command does not have an exit option
CSCvp35682	Target Address on IP SLA (udp) probes is getting changed to a new IP other than the configured one
CSCvp37275	Nexus 7000 Automated tech-support on hap reset Supervisor Switchover not Functioning
CSCvp37970	N7k MPLS LDP label allocate prefix-list needs to be re-applied when changes are made to prefix-list

Table 39 Cisco NX-OS Release 7.3(5)D1(1) Resolved Caveats

Identifier	Description
CSCvp40959	N9k do not age out Snooping entry against vPC Peer link port after receipt of GSQ
CSCvp41187	N7K replaces the default mpls-vpn route with the type-7 default route
CSCvp45929	N7K Supervisor Switchover due to TACACS+ hap reset - bad file descriptor
CSCvp47670	"no ip redirects" configurable on L3 port-channel member port
CSCvp58845	After remove/add VRF, remote host routes not installed to URIB and report 'remote nh not installed'
CSCvp69490	vsh core seen in steady state with traffic running [without any triggers]
CSCvp70746	n7k/F2: EEM to ignore interrupt during EG recovery (CSCux90737/CSCug39011/CSCux08154/CSCud43503)
CSCvp75032	VRF missing after upgrade to 7.3(5)N1(1)
CSCvp83475	SDA: Invalid src ip address in VXLAN header on n7k border
CSCvp93465	n9k generates LSA even when the interface fails to come up
CSCvp98039	N7K MPLS FIB programming issues after reload w/ M3 module
CSCvq03952	Procjob process does not check NULL payload of MTS messages
CSCvq07407	N9k: diff option needs to be done at parameter level
CSCvq09112	Incorrect parsing when using " " in loopback configuration
CSCvq14721	Error of 'system bridge-domain add' CLI due to existing vlan deletes all existing bridge-domains
CSCvq17890	The port-channel cannot be controlled by this input policy after removed the port-channel members.
CSCvq18837	Python Security Regression Unicode Encoding Vulnerability
CSCvq20196	leak-route doesn't happen leading to leak-route installation failure
CSCvq21920	Nexus 56K console loop on username/password prompt
CSCvq24098	N7K: show run diff breaks after enabling CTS
CSCvq26431	N7K 8.2(3) PIM process crashed
CSCvq40508	n7k/FP - LPOE index reused for 2 different GPC on same SOC
CSCvq42668	nexus7k heartbeat failure IGMP crash
CSCvq53154	mrib crash when collecting mcast show tech with N7K in SDA border role.
CSCvq57865	Memory leak is seen in DHCP process when show run is executed on a VLAN
CSCvq71294	LR transceiver stops transmitting laser when port unshut after a long shut
CSCvq95046	Nexus 7000 EIGRP does not advitise routes to peer after several resyncs and neighbor flap
CSCvr04377	ISIS Default route advertised to N7K won't be installed to RIB.
CSCvr05966	Race in Flanker/MTM/L2FM can lead to learning gateway mac out local interface while SVI Up
CSCvr06297	After upgrade from 7.3(2)D1(3a) to 8.2.2 on N7K, show tech/show tech det is not getting complete.

Table 39 Cisco NX-OS Release 7.3(5)D1(1) Resolved Caveats

Identifier	Description
CSCvr09812	F3 can learn its own GMAC from IPv6 ingress SMAC if v6 not configured
CSCvr12510	%MTM-SLOT2-2-INVALID_SLOT: Received invalid slot value 9999 in mts message from vdc
CSCvr31478	DATACORRUPTION Tracebacks when adding N7K to SNMP Management
CSCvr34577	OSPF is not Generating type 3 summary LSA 0.0.0.0
CSCvr35592	N77/F3 8.2(1) & (2) // Slow drain EB egress_timeout drops
CSCvr52113	f4/M3 bridge. Reset due to USD Failure.
CSCvr62038	Unable to save configs - service ipqosmgr failed to store its configuration
CSCvr74305	Nexus pim hap reset
CSCvn53847	ELOAM: Syslog to show more info. Auto-recover error disabled interface due to dying gasp
CSCvf77249	Max age LSA issue, OSPF can not remove the LSAs
CSCvq07837	VXLAN decap fails SLF_L3RI_CP_SW_ERR_CTR on M3 if UDP src port is 2268 AMT Tunnel is mis-identified
CSCvb73844	8.3(0)CV(0.694)S0 : N77k - vsh core @ plog_hwlog_show_file_type
CSCvn55678	N7K-M224XP-23L EOBC heartbeat failure after ISSU from 7.3(3)D1(1) to 8.3(2) followed by SSO
CSCvo13769	“Failed to analyze memory” while collecting "show tech-support module all"
CSCvh07348	zic error 0x256 with user as priv-15 role
CSCun37968	PBR : confcheck_parse_add_cap_reply() - failed in rpm_process_ctrl_msg()
CSCuy96670	ITD NAT destination CLI is not working properly
CSCvr42578	N7K M2 mac address missing on vpc peer when port-channel member port flap
CSCvn05569	N3K-C3264C 9.2(1) - Port-Channel remains suspended after reload
CSCvo06359	Race condition when "no-reload" option is specified as part "install all" command
CSCud04830	hsrp ip subnet mismatch when vrf is not present
CSCve38413	Few prefixes are not advertised to neighbor - EIGRP V6

Resolved Caveats—Cisco NX-OS Release 7.3(4)D1(1)

Table 40 Cisco NX-OS Release 7.3(4)D1(1) Resolved Caveats

Identifier	Description
CSCug85015	PORT-PROFILE-3-TSP_INVALID_LOCK_INDEX Traceback Seen After Config Change
CSCui56136	sed input handling error
CSCum83842	Detailed ip acl logging shows incorrect matching ACE number
CSCup85616	SNMP Leaks configured VLAN IDs to unauthenticated users
CSCuq77105	Receiving malformed BGP UPDATEs causes urib crash
CSCut84645	Cisco NX-OS Software SNMP Packet Denial of Service Vulnerability
CSCuu08976	Evaluation of N9k/N7k/N5k/N3k/MDS for CVE-2015-2808
CSCuu75466	Cisco Nexus 7000 Message of the Day (MOTD) Telnet Login Vulnerability
CSCuu82356	Evaluation of n7k-infra for OpenSSL June 2015
CSCuu99291	Cisco Nexus 7000 VDC Authenticated Privilege Escalation Vulnerability
CSCva92054	Route-leak (inter-vrf) - hmm route not flushed on host vMotion
CSCvc08097	Distributed reflective denial-of-service vulnerability on NTP server
CSCvc49591	Missing IGMP Entries after N7K joining vPC domain
CSCvd36108	Cisco NX-OS Software Role-Based Access Arbitrary Command Execution Vulnerability
CSCvd69962	Cisco FXOS and NX-OS Software Cisco Fabric Services Arbitrary Code Execution Vulnerability
CSCve88742	sh tech-support vpc on scale setup causes vpc crash in svi api svi_mcec_type2_get_param_info
CSCve91659	Cisco NX-OS Software CLI Arbitrary Command Execution Vulnerability
CSCvf30935	Eigrp routes flap if OSPF is removed from the switch
CSCvf53413	ENT0 : parse error on executing show command
CSCvf62912	Stale entries present in v6 route table on unconfiguring ipv6 static route
CSCvf99101	feature poap operation failed on response timeout from service which leads to delay in POAP abort
CSCvi76485	Duplicate Pkts observed due to PIM Assert not triggered
CSCvj06726	N77XX/M3: Mac sync issue
CSCvj10178	Cisco NX-OS Software Cisco Fabric Services Denial of Service Vulnerability
CSCvj23813	Remove stale LTL entries from IM as a part of CSCvj10306
CSCvj36340	FCoE pause drop threshold reached when VL is paused/resumed quickly
CSCvj63807	Cisco NX-OS Software CLI Command Injection Vulnerability (CVE-2019-1613)
CSCvj77201	user logged out from ssh session in user VDC when admin VDC is configured with exec-timeout
CSCvk28290	Fabricpath DCE mode of port-channel member inconsistent

Table 40 Cisco NX-OS Release 7.3(4)D1(1) Resolved Caveats

Identifier	Description
CSCvk38474	Suppress the bcast check on /31 VIP or pass mask from VIP to API if mask < 31
CSCvk44309	N7K iftmc crashed when tried to bring up gre tunnel
CSCvk53943	HSRP active replies arp request with physical mac address after preempt
CSCvk54735	FCoE "uSecs VL3 is in internal pause rx state" increments when eth port is not currently paused
CSCvk56857	MPLS BGP to OSPF redistribution DN bit not set
CSCvk72354	stale nexthop entry for ipv6 route in VRF leaking
CSCvk74490	LDP flushes static label bindings after graceful restart completes
CSCvm02470	POAP acl config is added to running-config after system bootup
CSCvm11792	ISIS IPv6 multi-topology - fixing MT attached bit
CSCvm21746	ospfIfIpAddress not working for specific index
CSCvm26068	N7K - Service "pim" crash
CSCvm46017	Netflow active timeout is not working as expected
CSCvm50765	Default route (track added) not getting advertised after box reload
CSCvm55640	FEX not process NIF down when parent's ports shutdown or power off
CSCvm56314	OTV VDC ignores dst IP in port-channel hash
CSCvm64931	N77:tcam utilization with QoS policy not increase
CSCvm74036	N7k MPLS LDP Advertise Label Prefix-List not properly applied
CSCvm84893	boot.log file cause /mnt/pss 94 % After cold boot from 8.1.1 to 8.3.1.72
CSCvm91348	N7K/L2FM: MTS build up during higher MAC move between LC
CSCvm93582	N7K/NTP: ensure monolithic time sync between active and standby
CSCvm99009	Port Info missing in level 2 L2FM log messsage when MAC moves continously at a high rate
CSCvn08550	N7K - 'ip routing multicast holddown' not working as expected
CSCvn13028	"nfp" crash on module when configuring netflow
CSCvn14579	F3 Egress buffer lockup handling
CSCvn27072	N77:status in "show pc cli status" output shows "Commit in progress"
CSCvn28540	Multicast packets with TTL=1 are routed and forwarded when OIF is not null
CSCvn28629	MAC move/add/delete not detected on fabricpath after l2fm process restart
CSCvn32302	M3 reload with SLF_VOQ_CPM_MSTR_INT_ADDRNE_ERR need more info
CSCvn36425	N9K - aclmgr crash @ddb functions
CSCvn38330	New mac learn triggers mac move with 2nd packet from host in fabricpath
CSCvn39414	NXOS: Local VRF leaking failed after ip clear of specific route in dest VRF
CSCvn40407	Port-channel running configuration does not show FEC mode when port-channel has no members

Table 40 Cisco NX-OS Release 7.3(4)D1(1) Resolved Caveats

Identifier	Description
CSCvn44369	NXOS advertises the pseudonode inconsistently in multitopology mode
CSCvn50809	sac_usd hap reset when standby supervisor becomes active on N7K 6.2(18)
CSCvn59937	ISCM crash/core due to NAT enable under ITD configuration
CSCvn61247	N7K M3 Span destination port accepts by default incoming traffic.
CSCvn63102	NVE failed to learn remote vtep RMAC after config change from DCNM/MW mode
CSCvn67179	IPFIB process crash after NXOS upgrade.
CSCvn70922	Static-oif functionality doesn't work on Nexus when group-range option is used
CSCvn80406	N7k setting VDC routing resource limits to max causes VDC to go in failed state
CSCvn97534	Interrupt "FLN_QUE_INTR_EB_P2_ERR_U_PLEN_MP_ZRO_N_EOS" should be added for Egress buffer recovery.
CSCvn97666	Cannot use filter options when sending nxos commands over nxapi
CSCvn99156	Incorrect number of prefixes sent if Candidate-RP list packet length greater than configured PIM MTU
CSCvn99680	PTP - GM OFFSET 37 Seconds and Nexus 7K SR 685369201
CSCvo09373	N7700- N77-M348XP-23L- Vlan tagging uncorrect in local span
CSCvo09511	CLI hangs for several minutes when applying certain interface-level commands
CSCvo10122	N7k: eem config cannot be removed when standby sup is powered down
CSCvo13456	ISIS LSP flooding broken
CSCvo13683	MPLS config lost after traditional upgrade from 6.2.16/6.2.18 to 7.3.3
CSCvo18971	Instance bit map getting mis-programmed causing fib miss.
CSCvo22236	Nexus 7k netstack crash
CSCvo28782	Crash during Free of Filter Links
CSCvo29766	Nexus / NX-OS / Multicast PIM Join not sent when IPv4 unicast route has IPv6 next-hop (RFC 5549)
CSCvo34762	IPv6 static routes may get missed in RIB on PKL/PL shut/unshut
CSCvo36285	N9K BGP sessions unstable when TCP packets received from same source to multiple local addresses.
CSCvo44343	N7K: Supervisor DIMM failure does not trigger Sup Failover.
CSCvo49272	Only one static route is installed in RIB if ECMP paths are learnt via same next-hop
CSCvo51463	N7K: VSH crash
CSCvo56362	Nexus 5k crashed due to fabric_mcast hap reset
CSCvo70466	L2MCAST crash due to null pointer dereference when searching AVL tree
CSCvo78276	LIF programmed to 0x0 for L3 VPN prefixes, after ECMP ports/port-channels are flapped

Table 40 Cisco NX-OS Release 7.3(4)D1(1) Resolved Caveats

Identifier	Description
CSCvo88678	Extraneous line in show ip bgp output
CSCvp02900	VPC: Type2 EVPN route advertised with primary IP of Loopback as next-hop
CSCvp08694	Stale arp entry/route after VM move from one VPC domain to other due to HMM update failure
CSCvp19180	N7K BFD - netstack crash
CSCvp25875	F3 card: show hardware flow ip command may cause process NFP to crash.
CSCvp30746	MAC deleted from other PO member port where MAC has aged out, when non-aged port goes down.
CSCvp33458	LISP: Forward-native cache persists after refreshed with more specific route.
CSCvp37629	N7K-F3 module reload due to FLN_QUE_INTR_EB_P6_HL_ERR interrupt and EB lockup.
CSCvp45874	N7K M3 PBR load-share does not redirect traffic as expected
CSCvp51579	Nexus 7000 / M3 / not accepting filter acces-group command in erspan config

Resolved Caveats—Cisco NX-OS Release 7.3(3)D1(1)

Table 41 Cisco NX-OS Release 7.3(3)D1(1) Resolved Caveats

Identifier	Description
CSCuj33023	MTM-SLOT1-2-MULTICAST_SOURCE_MAC_LEARNT
CSCul20456	%USER-3-SYSTEM_MSG: npacl app filter failed, err = [1106051080] - ntpd
CSCul25498	remove-private AS does not remove 4-byte private ASN's
CSCup79623	EEM:S5: show eem history events: not over writing after 50 applets
CSCur22683	NXOS - VRF aware telnet with "#" in VRF name fails
CSCut94652	Adding basic show commands to feature show techs (N7K)
CSCuv79620	Cisco NX-OS IGMP Snooping Remote Code Execution and Denial of Service Vulnerability
CSCuw91064	'show ip access-list' output does not update/display statistics
CSCuw99630	Cisco NX-OS Authenticated SNMP Denial of Service Vulnerability
CSCux53999	difference between "show run | grep ntp" and "show run ntp"
CSCux87740	N7K uses wrong MAC address for BFD when peer switches mac address
CSCuy04686	Changing user password results in clear text sent to TACACS server logs
CSCuy87697	Missing debug information for IP SLA select thread
CSCva11756	vPC+: Wrong ESDB info due to changing port-channels having VPC's
CSCva16707	F3 - static MAC programmed for TCAM Bucket0
CSCva76080	mmode crash when modifying maintenance profile
CSCva95344	F3 Line card reload
CSCvb17413	Unable to access NXAPI Sandbox(Non-default VDC) as VDC-Admin

Table 41 Cisco NX-OS Release 7.3(3)D1(1) Resolved Caveats

Identifier	Description
CSCvb24457	T2:123: %LIBOSC-2-OSC_ERR: DATACORRUPTION-DATAINCONSISTENCY EIGRP
CSCvb48317	N7K: Some static routes set BFD remain after disabled I/O module though BFD states have been down.
CSCvb52506	BGP incoming route-map not working as expected
CSCvb55686	NX-OS FSCK/format-bootflash there is a missing "space" in line 100
CSCvb65414	logging server vrf goes unknown after switchover
CSCvb74706	N7K: F3 2s convergence time on module OIR
CSCvb75651	Multicast failure when traffic ingressing on M3 port after addition and removal of igmp reciever
CSCvb81836	Service "iftmc" crash
CSCvb93553	Avoid CMD (SGT) tags in Pktmgr for L2 control packets
CSCvb93995	Cisco NX-OS Software removes ACL from VTY interface
CSCvc09777	%SYSMGR-2-VOLATILE_DB_FULL: System volatile database usage is unexpectedly high at 81%.
CSCvc18092	Traffic impact when adding VLAN under port-profile
CSCvc42886	N56xx - No SSH possible to device when root directory is full due to nxapi request
CSCvc55528	WCCP crashed due to memory leak - WCCP_MEM_msg_control_packet
CSCvc57098	Syslog MTS recv_q buffer filling up when "logging source-interface" configured
CSCvc66360	show port-channel load-balance forwarding-path is not correct
CSCvc67913	Error: AAA authorization failed for command:show version, AAA_AUTHOR_STATUS_METHOD=16(0x10)
CSCvc71792	implement a knob to allow weak ciphers aes128-cbc,aes192-cbc,aes256-cbc
CSCvc73543	N7K adding ip address into object group stuck
CSCvc91548	Incorrect forwarding address is set to OSPF type-5 LSA of summarized route
CSCvc96383	Scheduler does not work when AAA is enabled on N9K.
CSCvd10140	Dynamic Mac address has wrong DI (Destination index) on M2
CSCvd19871	Terminal monitor not showing any output
CSCvd36242	ISIS crashes in isis_srm_stop_timer_next
CSCvd69246	Incomplete error message is seen for VIP overlaps in HSRP
CSCvd72172	Evaluation of N9k/N7k/N5k/N3k/MDS for NTP March 2017
CSCvd78353	Nexus 7000 Series VDC user privilege escalation
CSCvd91689	Egress QoS policy matching ACL do not work on CE port for tag2ip traffic
CSCvd92344	Traffic loops back to core ports when local mac is cleared
CSCve01811	vpc-config-sync fails with error message
CSCve02254	Some BGP prefixes with multiple paths are not advertised

Table 41 Cisco NX-OS Release 7.3(3)D1(1) Resolved Caveats

Identifier	Description
CSCve10859	NXOS Default prefix LSA handling change
CSCve12380	CTS commands unavailable if medium p2p configured on a port channel
CSCve13020	tftp_si_entries is read-only
CSCve18390	RBAC user role name length inconsistencies
CSCve23321	N7K-M224XP-23L > Multicast traffic is sent to inband of LC instead of Front ports i.e OIL
CSCve23600	Nexus 9k OSPFv3 MAX METRIC feature Does not work
CSCve24353	EIGRP default summary route not advertised
CSCve25225	N5K-C5672 zombie process [fh_ttyd] <defunct> increasing when trigger EEM applet
CSCve34254	monitor session breaks bridged multicast on F3
CSCve39279	MFDM Batch Delay Causing 4 to 15 seconds of Multicast Loss
CSCve40055	MDS:%SYSMGR-2-SERVICE_CRASHED: Service "lit" (PID xxx) hasn't caught signal 6 (core will be saved).
CSCve46183	N77-F324FQ-25 interfaces goes to Hardware Failure after creating SVI
CSCve46211	ethpcm crash when trying to allocate memory
CSCve51700	Cisco FX-OS and NX-OS System Software CLI Command Injection Vulnerability
CSCve51704	Cisco NX-OS Software CLI Arbitrary Command Execution Vulnerability
CSCve52872	Fabricpath port-channel will not become "CORE" status in vlan internal info
CSCve54480	ARP ACL not working on M3 card
CSCve55463	cdp process crashes with show_cdp_neighbor
CSCve56063	N5k Watchdog at pfm_norcal_driver_nmi_cb
CSCve63888	FCS-Err counter of snmp doesn't sync with Interface counters in M3 Card.
CSCve69170	FCoE - PFC broken on F2 linecard
CSCve70445	Bfd is not coming up with cts on M3
CSCve78301	N7k-PI: bps rate is incorrect under type qos policy-map
CSCve78734	FHRP hello packet does not TX L3 interface
CSCve80860	Config rollback fail w/ tri-state commands (default interface toggles passive-interface in show run)
CSCve87569	SNMPUSER CLI cannot create the user in the User database
CSCve89395	N3500 duplicates multicast packets due to delayed pruning of new *G path
CSCve91441	N7K - PBR not applied for interfaces with pvlan config post reload
CSCve93651	Broken VRF Due to RD Change in BGP
CSCve93863	Cisco FX-OS and NX-OS System Software CLI Command Injection Vulnerability
CSCve94985	Custom CFS configuration missing after Reload ASCII

Table 41 Cisco NX-OS Release 7.3(3)D1(1) Resolved Caveats

Identifier	Description
CSCve99197	N7k/PIM/8.2(0.80S2): PIM assert prevents (S,G)s to age out even in absence of mcast data traffic
CSCve99902	Cisco Nexus Series Switches CLI Command Injection Vulnerability
CSCve99925	Cisco NX-OS System Software CLI Command Injection Vulnerability
CSCvf03464	Netflow configuration change fails with error if Netflow was previously applied on Tunnel interface
CSCvf06565	EEM actions are replaced to "maxrun 0" in startup-config after NX-OS upgrade
CSCvf07980	N7k - auto_root_file_deletion_log.txt growing in size in /var/tmp
CSCvf08106	NCPINFRAClnt SigSegV crash along with HB crash causing Module to get reloaded
CSCvf09567	SXP Contributor
CSCvf10136	Native vlan tagging not working after ISSU to 6.2.16 and reload
CSCvf10867	Unable to manually delete the IPv6 static routes on the Nexus9k switches
CSCvf11898	N7K/M3 Null0 route has DI of 0x0 and hits CPU
CSCvf15025	BGP failed to restart after netstack crash.
CSCvf16494	Cisco NX-OS System Software Patch Signature Bypass Vulnerability
CSCvf18050	FEX: routed sub-interface stop forwarding post fex-fabric uplink reload
CSCvf27235	N7K: Improve Logging for Interrupt Fault CLP_LBD_INT_MEM_ECC_PORT_MAP_TBL_ECC_1ERR
CSCvf29432	Cisco Nexus 7000 Series Switches Privilege Escalation via sudo
CSCvf30982	Mtrace not working correctly
CSCvf31132	Cisco NX-OS System Software Management Interface Denial of Service Vulnerability
CSCvf31178	N77/M3/VPLS/PIM: PIM-3-AVL_ERROR: AVL-tree operation ravl_insert() failed for PIM Assert FSM
CSCvf33147	F3 - xbar sync failed during module bringup after upgrade N77-F312CF-26 ver 1.1
CSCvf36683	N7K-SUP2/E: eUSB Flash Failure or Unable to Save Configuration
CSCvf36902	N5K-C5672 eem_policy_dir memory usage increasing after long time get no response
CSCvf39226	Power usage details are blank for FEX
CSCvf39800	FEX PS module status is incorrect
CSCvf47348	IPSLA ICMP-ECHO probes not coming up after reload
CSCvf59067	N7k-8.X- Eigrp SIA due to a query/update from non successor.
CSCvf59201	IP SLA tracks are down, but IP reachability is up
CSCvf60001	"show lldp neighbor details" doesn't list all neighbors
CSCvf60035	L2 multicast traffic loss during ND ISSU
CSCvf61926	N7K // Ethanalzyer does not gather FIP or FCoE traffic on F3 line card

Table 41 Cisco NX-OS Release 7.3(3)D1(1) Resolved Caveats

Identifier	Description
CSCvf63612	Possible cause of sync Loss between Line card to Fabric in 7.3.2.D1.1 release
CSCvf66000	static ARP might point to wrong physical interface
CSCvf66024	PBR programming wrong adj index when N7K up with multiple PBR configured ports
CSCvf66491	PIM crash when freeing memory
CSCvf69323	One of the ports of F2 line card is not linking up
CSCvf70119	SPM memory leak detected on log queue after consecutive WCCP client flaps
CSCvf73656	After SSO, aclqos crash multiple times and service down
CSCvf76652	N7K : STP internal event-history tree timestamps deviation
CSCvf77200	n7k/l2vpn: FLUSH not requested upon DOWN->UP change
CSCvf77327	ARP Performance Improvement when ARP suppression is enabled
CSCvf79160	OSPF type-5 routes blocked from RIB when table-map with permit route-map is applied
CSCvf80182	802.1x re-authentication fails with non-default timer 30secs because of failure of server lookup
CSCvf81891	N7000 sends PTP packets incorrectly with ttl-1
CSCvf83485	Link interruption caused crash of isis_fabricpath
CSCvf87522	FDMI crash
CSCvf94052	NTP configs are lost after disruptive upgrade to 7.3.2
CSCvf97669	M1 line-card ifOutUcastPkts is zero when polling with snmpwalk
CSCvg04072	Cisco NX-OS System Software Patch Installation Command Injection Vulnerability
CSCvg04455	N7K - RewriteEngineLoopback test failure does not error disable ports in non-default VDC
CSCvg10842	Input discards after issu to 7.3 or 8.x code, egress throughput reduction for F3-100gig/40gig ports.
CSCvg11502	Entering encapsulation mpls sub-menu and then exit in n7700 makes pseudowire to go down
CSCvg11795	Ntp may go out of sync with dme after ntp server/peer configuration post issu
CSCvg16920	BGP community list missing in config when updated after reload
CSCvg17452	Nexus 7k GOLF router drops packets at VXLAN encap due to incorrect egress LIF programming
CSCvg18985	ifInDiscards not matching # show interface mgmt0 counters errors on N7K
CSCvg23522	Unable to remove the ACL from N7k, N3k and N9k
CSCvg23978	N7K - nfp crash on M3 40 module
CSCvg24686	SNMP v3 information leaking vulnerability
CSCvg25737	URIB sends route notifications for broadcast routes when client requests all-igp notifications
CSCvg34717	Multicast CP packets are dropped by F2/F3 module

Table 41 Cisco NX-OS Release 7.3(3)D1(1) Resolved Caveats

Identifier	Description
CSCvg38672	vpc self-isolation:vpc legs are up on local after all modules up when MCT down
CSCvg38678	M2 LC: Internal link stability issue does not error disable port-group HW Fail
CSCvg42792	Running commands in 'routing-context vrf <x>' mode does not work on all commands
CSCvg45324	Static mac programmed as dynamic for orphan mac
CSCvg49084	PortChannel Config VLAN information is not passed LC while ports move into PC from Indiv.
CSCvg49250	ARP Entries Are Flapping in vPC VXLAN Setup
CSCvg50660	Need Syslog when DHCP SAP has high MTS Queue Size
CSCvg53147	N7k -Multicast Register IP TTL copied to payload TTL in MVPN
CSCvg57540	N7K Netflow M3: subinterface netflow sampler not working on breakout cable ports
CSCvg58990	passwordless ssh is not working as metnioned in the document for 6.x version
CSCvg63685	EEM Script can not run completely after upgrade from 7.1 to 7.3
CSCvg65330	IPSLA Probe-ICMPv4 over VPC : continuous MTS message without proper dst-sap
CSCvg65643	Connected devices are flapped though ports at N77-F324FQ-25 side are shutdown
CSCvg66767	Nexus SNMP Polling causes device reboot
CSCvg67835	IPSLA:sla responder memused reaching memlimit - memory not deallocated
CSCvg68573	N7K/F2 - EG recovery improvements
CSCvg70139	%ETHPORT-3-IF_UNSUPPORTED_TRANSCEIVER: Transceiver on interface Ethernet9/6 is not supported
CSCvg70868	Nexus 7k Sees "ipfib" Crash on N77-F348XP-23 Linecard
CSCvg74176	Memory leak in acfg handler while hitting error in show running config
CSCvg78684	N9K: Type-6 encryption displays as disabled
CSCvg90880	Clipper port-channel L3 Sub intf not generate netflow
CSCvg92062	Post ISSU from 7.3.1 to 8.1.2 image, record templates show junk values
CSCvg92363	F3:fln_em watchdog timer improvements
CSCvg92762	N7k with SUP1/6.2.12 continuously rebooting with aclmgr crash
CSCvg93510	nfm core, ACLQOS failure, Error sending client status for verify session ret_val 0x801c0010
CSCvg95207	N7004 - L2 multicast traffic is sent to all SOC's
CSCvg96060	N7K - after changing peer-link config in VXLAN BUM traffic blackholed
CSCvh02279	M3: Ethernet interface stuck down (unknown enum:<296>)
CSCvh03195	local prefixes not expected to be learned via SXP
CSCvh04052	LISP: directed broadcasts cause false positive host detections

Table 41 Cisco NX-OS Release 7.3(3)D1(1) Resolved Caveats

Identifier	Description
CSCvh13852	N7k Unable to send packet more than MTU size with cts manual configured on the port
CSCvh17367	Time drift between fex N2K-C2348TQ-10GE running version 8.1(1)and the parent nexus C7710
CSCvh18563	After upgrade 9148S from 6.2(17) to 8.1(1) "logging origin-id" command is missing
CSCvh19223	ISSU failure when running 'show install all status' in separate window
CSCvh21420	IPv6 Static route with Link Local Address not installed as RNH
CSCvh21693	RBH misprogramming triggered by the command 'port-channel load-balance hash-modulo'
CSCvh25999	N77K - Unable to configure input netflow monitor in Po
CSCvh29101	MDS NXOS 7.x & 8.x:: OU name has space in LDAP rootDN, NXOS adding extra backward slash ' '
CSCvh30461	"show routing vrf all ipv6 internal distribution" causes crash at u6rib
CSCvh47211	Issuing 'show install all impact' command during ISSU may cause ISSU to fail
CSCvh54503	After rip process restart only 8 ECMP routes are allowed
CSCvh54560	After route flap next-hop count increase
CSCvh61904	unable to remove duplicate entries in DNS group with cfs
CSCvh65347	LDI collision seen after sup switchover
CSCvh65567	Can't delete ACL completely
CSCvh67120	NX-OS netflow configuration cannot enable under p2p port-channel
CSCvh68603	MDS::when running ldap test "test aaa group username password" it results system switchover
CSCvh69235	N77 VRF stuck in 'Delete Holddown' after being deleted
CSCvh87165	Dont set mpls-vpn flag in URIB for ipv4 LU to VRF leak
CSCvh87828	lisp punt route nexthop not deleted/updated for all interfaces/routes after BGP nexthop change
CSCvh89092	N7K - adding kernel nvram-messages to show tech
CSCvh94844	snmp-server host entry with DNS name cannot be removed
CSCvh98764	NFM-2-VERIFY_FAIL: Verify failed - Client 0x82000146, Reason: Duplicate Sampler C, Interface
CSCvi08392	M3/F4 Flex Parser Cleanup and Conditional Changes for GTP
CSCvi09055	BGP neighbor flap or slow convergence with outbound route-map coupled with aggressive timers.
CSCvi09328	Nexus 5600/6000: IGMP snooping mrouter ports are not VLAN aware
CSCvi09665	Unable to establish 10G link on N7K
CSCvi11059	F2 linecard goes into a booting loop when more than 200 "vpc orphan-port suspend" are configured.
CSCvi12032	[N7k M3] GRE tunnel do not forward unicast/mcast traffic

Table 41 Cisco NX-OS Release 7.3(3)D1(1) Resolved Caveats

Identifier	Description
CSCvi14840	Nexus might crash after creating multiple MSDP mesh groups
CSCvi15800	N7k - OTV Fast Convergence is delayed during AED switchover
CSCvi18966	N77XX/M3:CBL forwarding on down port
CSCvi20373	n7k ICMPv6 Packet too big Messages are not send after ISSU to 8.2(1)
CSCvi29201	Sync timezone between FEX and N9K
CSCvi33605	SNMP ColdStart Trap is sent, when the snmpd process is crashed
CSCvi34298	N77 routes IPv6 packets that are not destined to it
CSCvi37040	netstack crash while redirecting "show tech-support netstack detail" to bootflash:/
CSCvi38868	N7K creates two MDT Data Groups when the VRF uses PIM ASM
CSCvi47337	Netstack should not process non Ethernet II encapsulated packets
CSCvi49900	Formatting bootflash does not recreate .patch folder- SUP in boot loop
CSCvi50857	N7K - BFD session for L3 protocol over fabricpath does not come up
CSCvi54206	Scheduler job breaks RBAC if the username has multiple roles assigned from the AAA server
CSCvi56611	MDS 9700 ethanalyzer does not strip headers for FIP traffic
CSCvi58404	Nexus Sup Module crash upon Netflow monitor application on the Interface
CSCvi61623	N7K/N77 F3 module egress buffer lock
CSCvi62706	N7k running VPC crash due to memory leak in VPC process
CSCvi64957	BFD over FabricPath: SUP and LC out of sync - happens on OIR
CSCvi70543	Service SAP Qosmgr - (Operation timed out) in if_bind sequence
CSCvi73154	N7K // Adding a 16th WSA Client causes the N7K to drop all clients continuously
CSCvi77191	N7K - adding kernel messages to OBFL for hung state
CSCvi78169	N7K VPC Crash
CSCvi78715	Netboot over EOBC fails if both supervisors were originally netbooted
CSCvi84074	When HSRP enabled, Proxy ARP enabled N7K doesn't respond to unicast arp request
CSCvi87540	N7K - HSRP libanycast cache does not sync to standby sup after changes to anycast bundle
CSCvi88803	N7K linecard crash with aclqos hap reset
CSCvi89817	fln_que hap reset during issu.
CSCvi90921	vPC config-sync abnormal cli is syncd
CSCvi91299	OTV process hang or crash post Overlay peer going up or down
CSCvi93529	N7K/F348: LC specific commands not included in "show tech forwarding l3 multicast"
CSCvi96878	LDB/ILM entries not present after VDL or linecard reload
CSCvi97093	LSA type 4 not flushed in NSSA area

Table 41 Cisco NX-OS Release 7.3(3)D1(1) Resolved Caveats

Identifier	Description
CSCvj06233	F3 card DOM issue
CSCvj07101	Copying SNMP MIB using IPV6 causes a reload
CSCvj08912	BFD is not coming up when authentication and hardware offload is used between N7K and ASR1k
CSCvj08973	snmpd hap reset crash when snmpwalk on OID stpxMSTInstanceVlansMapped2k
CSCvj09037	MPLS interface does not send ICMP type 3/code 4 (Fragmentation Needed and Don't Fragment was Set)
CSCvj10306	LTLs not deallocated in IM for broken out port after a no breakout is done on that port
CSCvj12978	sup2:need mechanism to clear soft-voq once it gets stuck
CSCvj15110	Nexus9k KIM crash on SUP failover
CSCvj16168	nxapi-server may send pure xml-encoded data in json-rpc reply
CSCvj17451	Dynamic label not reassigned after static range defined and LDP shut/no-shut
CSCvj19911	Incorporate new firmware for Unigen into NX-OS due to logflash mount unsuccessful
CSCvj31589	eth_port_channel crash in Nexus7K after "show port-channel internal lacp-channels <>" command
CSCvj33348	N77-M348XP-23L/N77-SUP2E Linecard crash for IPFIB process followed by IFTMC crash
CSCvj55813	'hardware ejector enable' command is not displayed in 'show run all' output
CSCvj64036	Kernel traces in nexus core files can't be decoded for kernel 3.4 version
CSCvj84775	PIM6 Anycast-RP failling to send Register-Stop
CSCvj87367	MST regions out of sync after ISSU to 8.1(2a)
CSCvk04105	N7K - NXAPI request fails when xml payload is larger than 10k
CSCvk10690	Additional debugability for SLF LINK_GOOD_TO_FAULT_12 on N77-M348XP-23L
CSCvk22156	n7k/GOLD: temperature sensor message improvement
CSCvk22224	n7k/GOLD: allow syslog message for each DIAG failure
CSCvk38405	N7k M3/F3/F4:Fragmented PIM BSR packets are CPU punted and dropped
CSCvk64742	EIGRP ExtCommunity lost in transit on Nexus7K
CSCvk75372	N7K - self-originated LSAs subjected to MinLSArrival check
CSCvm05636	IP redirects disabled in configuration but enabled in ELTM
CSCvm13449	Stale Entries present in cli_acl_ifdb PSS on Standby Sup after Purge
CSCvm16677	PSS memory leak in igmp_snoop for key type 0x04 and 0x0d
CSCvm27147	N7K/F3 interfaces goes to Hardware Failure after creating SVI
CSCvm44595	N7K Aclmgr memory leak on show ip access-list expanded cmd
CSCvm65736	N7k: ELAM release may trigger clp_elam crash/LC reload

Table 41 Cisco NX-OS Release 7.3(3)D1(1) Resolved Caveats

Identifier	Description
CSCvm67806	FabricPath - use PURGE instead of DELETE when LSA expire
CSCvm70503	With MT enabled, all the routes shows as pending ((nil), 0) and URIB update failure for Topo 2
CSCvn01786	remove "show tech all binary" from "show tech fex"
CSCvc26766	IPv6 routes/rnh missing in UFDM/FIB after issu.
CSCuc35049	need syslog to match error state of fabric modules
CSCvh77171	N7K M2 - multicast traffic to CPU blackholed due to RL and CoPP dropping all packets
CSCvh95329	N7K "ipfib"crashed.
CSCvg44192	bfd based static route not getting deleted during interface shut.

Resolved Caveats—Cisco NX-OS Release 7.3(2)D1(3a)

Table 42 Cisco NX-OS Release 7.3(2)D1(3a) Resolved Caveats

Record Number	Description
CSCva16707	F3 - static MAC programmed for TCAM Bucket0
CSCvb74706	N7K: F3 2s convergence time on module OIR
CSCvb93995	Cisco NX-OS Software removes ACL from VTY interface
CSCvc55528	WCCP crashed due to memory leak - WCCP_MEM_msg_control_packet
CSCvd10140	Dynamic Mac address has wrong DI (Destination index) on M2
CSCve07101	N7k/6.2(16) BGP not prepending as-path for certain prefixes in a prefix-list
CSCve10859	NXOS Default prefix LSA handling change
CSCve40271	N7K crashes while opening startup-config
CSCve46211	ethpcm crash when trying to allocate memory
CSCve54480	ARP ACL not working on M3 card
CSCvf87011	M3 - Ncpinfraclnt Crash
CSCvg10842	Input discards after issu to 7.3 or 8.x code, egress throughput reduction for F3-100gig/40gig ports.
CSCvg38672	vpc self-isolation:vpc legs are up on local after all modules up when MCT down
CSCuc35049	need syslog to match error state of fabric modules

Resolved Caveats—Cisco NX-OS Release 7.3(2)D1(3)

Table 43 Cisco NX-OS Release 7.3(2)D1(3) Resolved Caveats

Record Number	Description
CSCux87740	N7K uses wrong MAC address for BFD when peer switches mac address.
CSCve51700	Cisco FX-OS and NX-OS System Software CLI Command Injection Vulnerability.
CSCve99197	N7k/PIM/8.2(0.80S2): PIM assert prevents (S,G)s to age out even in absence of mcast data traffic.
CSCve99902	Cisco Nexus Series Switches CLI Command Injection Vulnerability.
CSCvf31178	N77/M3/VPLS/PIM: PIM-3-AVL_ERROR: AVL-tree operation ravl_insert() failed for PIM Assert FSM.
CSCvf36683	N7K-SUP2/E: eUSB Flash Failure or Unable to Save Configuration.
CSCvg04072	Cisco NX-OS System Software Patch Installation Command Injection Vulnerability.
CSCvg70868	Nexus 7k Sees "ipfib" Crash on N77-F348XP-23 Linecard.
CSCvg92062	Post ISSU from 7.3.1 to 8.1.2 image, record templates show junk values
CSCvg92363	F3:fln_em watchdog timer improvements.
CSCvh89092	N7K - adding kernel nvram-messages to show tech.
CSCvi09055	BGP neighbor flap or slow convergence with outbound route-map coupled with aggressive timers.
CSCvi77191	N7K - adding kernel messages to OBFL for hung state.
CSCvj19911	Incorporate new firmware into NX-OS due to logflash mount unsuccessful.

Resolved Caveats—Cisco NX-OS Release 7.3(2)D1(2)

Table 44 Cisco NX-OS Release 7.3(2)D1(2) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCuu06969	Bootvar core @ sha512_compress with Sup high CPU
CSCva16707	F3 - static MAC programmed for TCAM Bucket0
CSCvb33380	Running tac-pac causes M3 card ncpinfraclnt core
CSCvb74706	N7K: F3 2s convergence time on module OIR
CSCvb86962	N7K40GM3: Service SAP Qosmgr SAP for slot 6 returned error on reload
CSCvc47920	N7K - snmpd memory leaks snmp_pss_parse_context_map_entry
CSCvc55528	WCCP crashed due to memory leak - WCCP_MEM_msg_control_packet
CSCvc58707	N7K - snmpd memory leaks in functions pss_restore_runtime() and sdwrap_dbg_init()
CSCvd10140	Dynamic Mac address has wrong DI (Destination index) on M2
CSCve07101	N7k/6.2(16) BGP not prepending as-path for certain prefixes in a prefix-list

Table 44 Cisco NX-OS Release 7.3(2)D1(2) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCve10859	NXOS Default prefix LSA handling change
CSCve40271	N7K crashes while opening startup-config
CSCve46211	ethpcm crash when trying to allocate memory
CSCve52403	F3 - xbar local links might fail to sync with spine after reload or power-on
CSCve54480	ARP ACL not working on M3 card
CSCve60708	7.3.2 mem leak in mibgroup/Rmon during longevity run, realloc, event_Clone, ROWAPI_get_clone
CSCvf04693	Orphan ports enabled with "vpc orphan-port suspend" remain down post autorecovery
CSCvf33147	F3 - xbar sync failed during module bringup after upgrade N77-F312CF-26 ver 1.1
CSCvf63612	Possible cause of sync Loss between Line card to Fabric in 7.3.2.D1.1 release
CSCvf87011	M3 - Ncpinfraclnt Crash
CSCvg10842	After ISSU to 7.3(2)D1(1) egress credited traffic is limited to 50G

Resolved Caveats—Cisco NX-OS Release 7.3(2)D1(1)

Table 45 Cisco NX-OS Release 7.3(2)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCve06320	Netflow - netflow/nfm not responding msg stuck in MTS Buffer
CSCuy04933	Wrong timestamps in netflow data
CSCvc70292	N77-M324FQ-25L powered down due to fatal error in device DEV_SLF_PL
CSCvb40562	N7K: F3 module crash in ncpinfraclnt service during FIB update
CSCva97361	OSPFv3 crash on Post-ISSU SSO
CSCuz40287	adbm service not responding if secure ldap fails to connect to ldap server continuously
CSCve34578	Nexus 7000: cts hap reset on 7.3(1)D1(1) triggered when ASA failover happens
CSCva84959	F2 1G port fails to recover after remote end comes back up
CSCvd13580	Fatal interrupt does not get logged into OBFL logs
CSCvd25258	Bogus DHCP GIADDR being used for DHCP Smart Relay post ISSU
CSCvd74225	N7K/F3: Constant EOBC heartbeat failure
CSCvb90273	Some F3 cards can get bricked upon EPLD downgrade
CSCvc78278	NXOS/ETHPM: Traffic not forwarded after port change from Channeling to Individual
CSCvb23556	MDSNG : callhome crashed sig6 while replaying configs
CSCvb57997	SSTE: GLBP service crash due to heartbeat failure

Table 45 Cisco NX-OS Release 7.3(2)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCva94583	FP: Anycast HSRP stuck in Init state after VDC/Switch reload
CSCvd53833	N7K: “IFTMC PD commit db search failed” error msg post ISSU to 7.2
CSCvb62669	"ipqosmgr" crashed after QoS configuration change
CSCvb27539	Nexus 7004 6.2.14 IPv6 connected L3 interface not showing up in RIB
CSCvc69075	MAC address mismatch between SUP and LC after a VPLS failover.
CSCvb64844	N7k/vPC+ - L2 loop cause FP core Port not copy CE MAC address
CSCva13788	post ISSU, bfdc crashed due session data structure corruption
CSCvc16783	ipfib crashed on reloading vdc on bl
CSCvb84395	M3 module failure with log enabled deny policies
CSCvb02616	Some N77-F348XP-23 modules do not boot up on 6.2 code
CSCvd29280	MSDP TCP connection doesn't establish properly neighbor stuck in listening
CSCvb79504	PIM SG timer expiry not refreshing with continuous traffic when MRIB is updated by MSDP
CSCvc66498	multicast over PIM SSM over VPC for L3 orphan ports drops every 3 min
CSCvc46102	N7K - PIM/RPM Parses Deny Entry In Route-Map On Static RP Configuration As Permit Following ISSU
CSCvc53438	Shared tree takes up to 60 seconds to be pruned after 2nd receiver joins
CSCvc36844	PIM Join List in nexus doesn't contain all Rcvrs - Pruned
CSCvc42895	N7K: MPLS LDP "advertise-labels interface" missing after reload.
CSCvc92277	NFP crash after associating netflow-original flow record to active flow monitor
CSCvc44582	F3 Module crashing multiple times after removing and re-adding flow monitor command
CSCvc62084	STP BA Inconsistent on port-channel interface when native vlan does not exist
CSCvc23468	Evaluation of N9k/N7k/N5k/N3k/MDS for NTP November 2016
CSCvc65466	OTV fails to advertise mac after a mac move
CSCvc13106	LC SMU activation fails due to “file exist” after performing “install activate ... test”
CSCvd17129	RBH mis programmed after removing interfaces from vpc and reusing the interface as standalone port
CSCvb93551	Nexus7k Memory Leak On IPQOSMGR
CSCvc44767	hashlib.py not found in 7.3(1)1D1(1)
CSCve57887	res_mgr crashes when doing an snmp get on CISCO-VDC-MIB with a null VDC ID
CSCvb44776	BGP crashes due heartbeat failure after asserts
CSCva79760	IPV6 link local only BGP peering leads to installing wrong adjacency
CSCvb11563	Leaked Vrf route from Global not changing next-hop
CSCvd86332	EIGRP routers stopped propagating default route.

Table 45 Cisco NX-OS Release 7.3(2)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCvb99376	N7K send Candidate Default bit in the EIGRP update
CSCva83066	Nexus EIGRP loop, route not flushed from topology table
CSCvc45002	Multiple switches in FP domain crash due to __inst_001__isis_fabricpath hap reset
CSCvc81179	Nexus7k ISIS crash at txlist_tq_remove_node
CSCuz18971	old/inactive area-ids are not cleared from the ospf db
CSCvc30847	OSPF LSA not withdrawn from Nexus when interface is down
CSCut93487	OTV: AED stays inactive for all VLANs
CSCvd08029	SNMPD crash when RIPv2 authentication is enabled and RIPv2-MIB::rip2IfConfAuthType is being polled
CSCuz72951	Conditional default originate broken for IPv6 BGP
CSCuz51928	icmpv6 crashes because of access to a non-readable memory region.
CSCvb93309	NXOS/n7k-pi: URIB crash during show ip route
CSCvb48568	Evaluation of N9k/N7k/N5k/N3k/MDS September 2016 CVEs
CSCvc03725	Change CSCun41202 to allow weak ciphers also
CSCvb32808	statsprofiler crash with no space in sap STATSPROFILER SAP
CSCvb76929	N7k: ACL's are not programmed into tcam
CSCvb93865	Nexus77: routing failover time increased 1sec after version up from 6.2(14) to 7.3(1)D1(1)
CSCvd74634	UFDM does not download route to line card after ISSU SMU
CSCve68247	Stale TCAM entries with SXP session torn down
CSCvb93352	N7K - Loops VTP v3 update on peer-link between vPC peers
CSCvd07149	N5K6K - VPC VTEP Keeps Advertising Secondary IP When VPC's Are Suspended For Dual Active

Resolved Caveats—Cisco NX-OS Release 7.3(1)D1(1)

Table 46 Cisco NX-OS Release 7.3(1)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCuy55178	Cisco Nexus 7000 F3 ncpinfraclnt crash
CSCux65494	ACLLOG memory leak crash at ACLLOG_MEM_filter_info_t
CSCuz82625	Change the heap size in aclqos.conf
CSCui51401	HW acl entries are not correct when having IPv6 RACL with BFD enabled
CSCuw03713	N7K: Layer 2 (L2) packet not dropped on length mismatch
CSCui49066	N7K: Storm Control syslog is not getting generated on M2 module

Table 46 Cisco NX-OS Release 7.3(1)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCuy49752	N7K-C7700 : Unable to manually walk nexus coppoids cbQosPoliceStatsTable
CSCux93185	n7k/COPP - move mcast exception connected to dedicated class
CSCux79495	Need to change CTS logging level to 5 to notify user for SXP flapping
CSCva63315	M2 module reset by val_usd process
CSCuy02586	vPC+ both switches learn mac address on peer-link on receiving garp
CSCuz10518	Nexus got dot1x hap reset
CSCuy31610	EEM: Configuration failed with: 0x412c000d validation timed out
CSCva65703	M2/F3- elo_io process high on LC CPU without Ethernet OAM
CSCuz58822	ELTMC crash when running 'show tech detail'
CSCuy54998	F3 port-sec static mac inserted into HW table regardless of int state
CSCuz83088	Configuring PVLAN on FEX Isolated Ports fail after ISSU
CSCuw76844	N77-F348XP-23 may reload on executing some show CLI on down-rev firmware
CSCva66159	debounce timer not honored for 1G/SGMII mode on 10/1 F3 module
CSCuy51156	Port stuck in authorization pending state after link flaps
CSCuo05800	HIF of N2232PP 1G link can't up with 3rd device
CSCuy89705	4 way HSRP does not work on Nexus 5k/6k switches
CSCva24715	Nexus Anycast HSRP crashes when VLAN string is more than 1000
CSCuw61229	Bringing up new L3 interface may break BFD redirect adj with new int lif
CSCuw49932	F3 - drop adjacency in FIB involving PBR policy recursive vrf map
CSCuy40322	IGMP Leave causes MAC flap between GPC and FP SWID
CSCva55599	L2 HIFPC h/w not programmed after module reload of one FPC member module
CSCuz54906	LIF not published to SDB for port-channel on VRF removal
CSCuw51522	Mac learnt on ES ID for host vpc+ port operating in individual mode
CSCva74462	N7K w/ Sup 2 Engine Incorrectly Punts MPLS Traffic to Control Plane
CSCux86505	Suppress Kickstart/System Image Warning message when doing POAP
CSCuy49391	netstack cores when rebind of interfaces with new vdc
CSCuz03208	IGMP Queries not forwarded out of MVR interfaces
CSCuy02120	Memory leak caused by restarting OSPF process
CSCux87583	Nexus: Multiple hung SSH sessions
CSCva31220	'sh hard queuing drops ingress' makes LC memory leak.
CSCuz33019	diag_port_lb HAP reset
CSCuz67556	Incorrect label stack after MPLS TE FRR optimization in lfib
CSCuz89143	N77M3: LC /tmp at 100% due to PC_CTS.log, disable internal logging
CSCuv82106	Multicast traffic gets blackholed when MVR configured
CSCux38743	VPC - IGMP membership query is leaked to IGMP router port

Table 46 Cisco NX-OS Release 7.3(1)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCva58027	N7k - show vpc cli hangs
CSCuz83616	vpc command added automatically on some FEX HIFs (vpc_num > 4096)
CSCuy93686	vpc+: fabricpath STP type-1 configuration incompatible msg
CSCuy15221	vPC: F3 module reload delay to unset VSL bit
CSCuw10951	NXOS/F3: Multicast convergence improvement
CSCva52387	Nexus 7700 Netstack Crash When Packet Unexpectedly Takes MPLS IPv6 Path
CSCuz53597	N7K does not advertise implicit-null label as an Edge-LSR should do
CSCuy94988	For FEX scale we are using old scale numbers in Software
CSCuy62745	Master Bug to port fix for 2348 Issues from N5k to N7k,N9k
CSCuy11493	Errors ""tlvu_table_convert_tlv_to_indv_field" when issuing startup
CSCuz92661	Evaluation of N3k,N5k,N7k,N9k, N8K for NTP June 2016
CSCuz44147	Evaluation of n7k/N5k/n9k/n3k/MDS for NTP_April_2016
CSCux95101	Evaluation of N9k/N5k/N3k/MDS for NTP_January_2016
CSCuz34593	N7K: Incorrect filename when issuing 'copy run ftp'
CSCuz98928	NX-OS: pipe not recognized as special character by 'exclude' cli filter
CSCuz77805	"switchport trunk allowed vlan" not programmed in HW
CSCuy08128	Cut through Threshold change on Tiburon FEX's on 40gb NIF's
CSCva75937	port-profile configuration missed after reload
CSCuz05950	N2232TM: Tail drops not mapped to interface counters
CSCuz00514	Rollback removes switchport mode trunk in port-profile
CSCva75358	VRF export maps applied to denied prefixes
CSCuz67278	VXLAN-EVPN:two RMAC are transported as transitive community,but shouldnt
CSCuy07502	In show running, ffff is missing from the v4 mapped v6 address.
CSCuy64775	EIGRP redistributed routes wedged in topology table
CSCva31129	"Unable to resolve NH" on peer in Unicast OTV after switchover
CSCuy77045	configuring "mpls ldp sync" removes "mpls traffic-eng router-id" command
CSCuz67595	Incorect IGP metric calculation for ISIS
CSCut19221	OTV Unicast Flooding MAC Entry Lost
CSCux98493	Need to block ISSU to 7.3 if OTV data-group mask is </24
CSCuy89746	OTV VDC crashes after remote command "reload ascii"
CSCuy38146	RIP keep advertising route even though original route source is down
CSCuy83572	RIP routes not installed when RIP packet has same sequence as previous
CSCuz74998	igmp static-oif fails when using route-map
CSCuw29235	"restart igmp" command or ND ISSU results in "igmp hap reset"
CSCva35217	IPv6 Route not installed in RIB when learned via eBGP IPv6 Link Local

Table 46 Cisco NX-OS Release 7.3(1)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCuy85875	Moved host route does not get installed in HW in LISP IGP Assist in ASM
CSCva10977	URIB fails to push to FIB silently. Need logs / traces for chg list.
CSCuw55057	urib not updating FIB when the RP has the same admin distance as AM
CSCuw85884	N7K snmpd process seg fault crash
CSCuy07280	Evaluation of N3k,N5k,N7k,N9k for OpenSSL January 2016
CSCuy54488	Evaluation of n7k/n5k/MDS/n9k/n3k/n3500 for OpenSSL March 2016
CSCux41326	Evaluation of NX-OS for OpenSSL December 2015 vulnerabilities
CSCuy89690	"show accounting log" shows the community string on plain text
CSCuz22196	Nexus: snmpd Program terminated with signal 8, Arithmetic exception.
CSCuz84286	SNMP crash on 6.2(10) with netsnmp_wrap_up_request
CSCux44698	SVI's go down on VPC primary, when peer-link is down
CSCuz21326	Aclmgr Crashes on 6214
CSCux54465	BFD Stuck in Down state & BFD Session is not initialized On N6000
CSCva13713	Error 0x40870004 while copying tac-pac to ftp server
CSCuy16372	N7K No autostate on admin down SVI brings it into operationally up state
CSCuy71149	show logging log mixed old and new log after logging monitor command
CSCuy52663	6.2(16) (S40) - ipfib core @ fln_ufib_pd_ecmp_adj_handles_pss_insert
CSCuz39613	F3: null0-routed traffic hits CPU with IP redirects enabled
CSCuz68780	FLN_FIB_LSMET_EXHAUSTED show command can be misleading
CSCuz91706	Username limited to 28 characters causes issue for vmtracker feature
CSCuz77139	sac_usd hap rest on standby supervisor
CSCuy70246	Error while collecting show tech-supp detail Size mismatch.

Resolved Caveats—Cisco NX-OS Release 7.3(0)DX(1)

Table 47 Cisco NX-OS Release 7.3(0)DX(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCuw21167	Archive Job status column not getting updated for all jobs after Upgrade
CSCus59551	Template cannot be imported if properties is defined
CSCun65251	Config Delivery -Incorrect Job status
CSCur95202	Cannot import template definition
CSCut48826	Notify Border Leaf option on BL/ER pairing is cleared in remote DB case
CSCuv76463	VRF-common-universal profile can be edited & deleted when instantiated
CSCuu08025	Need DB password in encrypted for some files
CSCux03524	N7k: Multicast traffic not transmitted towards FEX on same FE as source

Table 47 Cisco NX-OS Release 7.3(0)DX(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCty30696	Changes in IFTMC for Flanker ASIC
CSCux77234	F3 packets are flooded for 2-3 sec during receiving gratuitous arp
CSCut36702	F3 / 4-Way HSRP / VMAC Programmed To sup-eth31 On Listen Members
CSCuv75088	Phyport vPC with Esxi does not come up thr FEX
CSCuy07224	Physical VPC on FEX port stays suspended (suspended(LACP misconfig))
CSCuy57603	Wrong return value for MACAddress and SystemID in IEEE8023-LAG-MIB
CSCuy90969	N7K Eompls decap uses wrong MTU
CSCux99818	pim process crash at pim_get_rp_by_rp
CSCuq14012	MFIB stops updating multicast hardware hit counters
CSCuw07827	Vxlan Details not showing and Vxlan-Vlan mapping missing
CSCuw48283	High CPU Ficon due to flush sync loop
CSCuc27353	Not able to format bootflash or check bootflash or fix bootflash errors
CSCuy51899	default logging level mvrp 2 shown with show run
CSCux01711	N7k / N77k - Interface (HIF) counters on Nexus 2348 may be erroneous
CSCus96878	Nexus7700 FEX interface link flap with FET-10G
CSCuy47125	cshcNetflowResourceUsageTable return incorrect values in SNMP
CSCuw92095	NXAPI: json "show monitor session" destination interfaces incomplete
CSCux31915	N7K:vsh crash on Linecard while collecting tacpac
CSCux35766	Incorrect power mode w supplies are shutdown on N7k PS-Redundant config
CSCux94893	N77: There is difference to detect removing linecard by slot number
CSCuy30270	LISP: synch leads to frequent uRIB writes, which block route reads
CSCux54153	Deletion of route-map seq doesn't trigger OSPF external LSA deletion
CSCuy61699	ospfv3 route has not got advertised to another area
CSCux59834	Limit OTV data-group configuration to /24
CSCux49719	pam_aaa_motd:cannot open motd file : /vdc_4/etc/motd - dcos_sshd
CSCut84271	IP SLA control protocol communication may fail if loopback address used
CSCux14926	Nexus 7000 - SLA udp-jitter IP TOS not reflected by Responder
CSCux47262	STP stuck on LRN state after upgrade
CSCuw86555	N7K Silent/Unknown supervisor switchover
CSCut29799	Privilege escalation with o+w files and directories
CSCuy14048	SNMP nonoperational status from a Nexus7700 7.2(1)D1(1)
CSCuy43188	In "F2E F3" VDC, IPSG entries being pushed on F3 rather than F2E
CSCuy99701	N77 - N77-F3 modules not populated for cshcMacUsageTable
CSCuu26045	Add MiniUCS FI OUI 0x74a02f to MDS list of recognized Cisco OUIs

Resolved Caveats—Cisco NX-OS Release 7.3(0)D1(1)

Table 48 Cisco NX-OS Release 7.3(0)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCux37999	ISSU from Cisco NX-OS Release 7.2 to Cisco NX-OS Release 7.3, F3 and F2 cards fail to upgrade to 7.3.
CSCux78871	After ISSU from Cisco NX-OS Release 7.2(1)D1(1) to Cisco NX-OS Release 7.3(0)D1(1) (195s0) peer-link flap same vni two Diff BD's
CSCuv12718	G bit set for HSRP VMAC in vPC setup with state Listen/Listen
CSCuw40994	Acl logging not supported under admin vdc in Cisco Nexus 7700 series
CSCuv61321	Cisco Nexus 7000 ARP Denial of Service (DoS) Vulnerability
CSCuw58529	repeating aclqos crashes caused Cisco Nexus 7000 module hap reset
CSCuw78785	ARP packets loop with dynamic arp inspection in Fabricpath network
CSCux03956	ARP Reply for VIP is dropped in hardware on egress path
CSCuu38613	ARP response to wrong interface when sender mac not equal to source mac
CSCuv05073	HMM hosts learnt on peer-link after control plane stress test
CSCux42981	Display issue in running-config for FP vlans
CSCut50593	BFD config showing large inaccurate nums in startup config
CSCuw10915	MPLS ldp sync disappears after interface flap
CSCuv22121	ISL drops seen when congestion timeout mode edge is configured.
CSCux63641	EEM script not being deleted from running-config
CSCux23763	EEM_POLICY_DIR: device crash while executing Phyton script
CSCuw95078	M2 VLAN Translation Missing after Module Reload
CSCuw20002	Cisco Nexus 7000 Temperature sensors stalls for linecards after EPLD update
CSCuw51036	%ETHPORT-3-IF_UNSUPPORTED_TRANSCEIVER:” for LOROM twinax cable
CSCuv22195	Need to add command for show system default interface
CSCuw71136	Static Mac address assigned on interface after default interface command
CSCuw62175	F3 - MTM FE Timer Expired after Gross Interrupt Threshold Exceeded
CSCuv42487	show tech-support fcoe needs to contain all pertinent FC information
CSCux03757	"fabric forwarding mode anycast-gateway" command gone after SW upgrade
CSCux23216	Auto-pull - refresh does not work after copy r s + reload on VPC
CSCuu24295	DFA: Profile flags and state are not being correctly set during failover
CSCuw16411	HSRP state Active/Active after removing Anycast
CSCuu39555	Sometimes few HSRPVIP removed ISSU 6.0.2.N2(7)>7.0.6.N1(1)>7.2.0.N1(1)
CSCuw25153	Traffic loss during HSRP Recovery
CSCuw97457	SVI interfaces are not displayed in “show interface description”
CSCuu71254	IPv4 Traffic Completely Dropped After ISSU from 6210 to 7.2
CSCuu11282	ITD probe with frequency configuration less than 5 seconds reverts to 60 seconds

Table 48 Cisco NX-OS Release 7.3(0)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCuv12718	G bit set for HSRP VMAC in vPC setup with state Listen/Listen
CSCux62214	L2FM consistency checker can cause memory leak / crash
CSCut10399	MAC address flooding on F3 linecard
CSCuw39946	MAC learnt on non existent F2e port
CSCur44677	BGP not putting routes in urib on mac address change
CSCui90811	Traffic drop on VC in disposition, imposition directions after OIR
CSCux50627	%MTM-SLOT10-0-FE_TIMER_EXPIRED: FE timer expired
CSCut75457	HSRP VACL Filter Broken
CSCuw40711	Nexus - in.dcos-telnetd service crash
CSCuv75088	Phyport vPC with Esxi does not come up thr FEX
CSCuw73046	Vinci MT-full L2 extension on Borderleaf requires configuration of BDI
CSCuh44088	Need to prevent mrouter on ports on FEX HIFs due to PIM hellos
CSCux20846	Nexus 6k: IGMP HAP Reset during "install all" upgrades with IGMPv3
CSCux09435	MSDP SA information not exchange after reload
CSCuw01105	multicast duplicate packets or loop on border leafs
CSCux28796	OIL is not copied from (*,G) to (S,G)
CSCuw82347	PIM Assert Storm on pair of N6Ks with Egress VPC and ECMP in L3 Core
CSCuv34380	vPC switch keeps sending (S, G) joins even after (*, G) entry gone.
CSCuv76460	Multicast counters getting rolled at 32 bit for IPMCAST-MIB
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	M1/M2 Egress Queuing behavior post 6.2(x) for control plane packet
CSCut83347	MFDM crashes due to HB loss
CSCux48649	OTV with F3 can only support 50 data-groups after AED failover
CSCux60618	BGP RR doesn't send update
CSCuw16936	Removing/Adding tunnel dest. throws %LDP-3-OIM_SDB_OPEN: Error
CSCux19294	MPLS TE - RSVP BW incorrect for 40G and 100G interfaces
CSCuv42308	MST Disputes VPC peer-switch secondary peer sending cost of 250
CSCur57084	FEX Core Fails to Upload in Non-default VDC - No Workaround on NPE Image
CSCux01711	Cisco Nexus 7000/ Cisco Nexus 7700- Interface (HIF) counters on Nexus 2348 may be erroneous
CSCus96878	Cisco Nexus 7700 FEX interface link flap with FET-10G
CSCuv64056	Cisco Nexus 7000/Cisco Nexus 7700 support NX-OS mechanism to upgrade firmware on eUSB flash
CSCuw92095	NXAPI: json “show monitor session” destination interfaces incomplete
CSCuv55905	Can configure ntp server <name> use-vrf w/o name server configuration.

Table 48 Cisco NX-OS Release 7.3(0)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtz59354	cNTP ACL Does Not Continue Processing After Matching Deny Entry
CSCuw84708	Evaluation of Cisco Nexus 9000, Cisco Nexus 3000, mds, Cisco Nexus 7000 and Cisco Nexus 5000 infra for NTP
CSCuv06177	copy run to sftp on linux server fails
CSCuu39870	NAM Module flooding accounting log
CSCur00089	vdc-admin on Cisco Nexus 7000 can break out of vsh-"chroot" using symbolic links
CSCut98473	PortLoopback test fails following EOBC congestion
CSCuv95316	Pixmc core being observed after insert new sup or reload chassis
CSCuv88508	Crash in the pltfm_config process
CSCuv45849	FEX HIF Po load-balancing issue when connected to Cisco Nexus 7700 F3 module
CSCuw80185	ISSU causes inconsistent internal RLs (rate limiters) to be implemented
CSCuw70817	"port-profile type <type>" should not be expected in the rollback diff.
CSCuu06999	adding a large number of Vlans to a port-profile failing.
CSCut18591	tshark: Segmentation Violation with IP Protocol 89 Capture Filter
CSCuw37373	Python: Script with stdin, input, raw_input does not show the message
CSCuw86978	F2E 6.2.(14) upgrade fail %VMM-2-VMM_SERVICE_ERR: VDC1: Service SAP
CSCuv44967	Unable to modify access-list using config session
CSCuv80499	BGP flapping with same AS-PATH ACL matched in two or more route-map seqs
CSCuv50831	BGP is installing route with AD 255 in URIB
CSCuw81067	Multicast SG join state missing in BGP
CSCuv82966	L3 DCI autoconfig: VRF stuck in Delete Holddown
CSCux55826	NXOS/BGP: routers not redistributed after ATTR and prefix list change
CSCuu78729	EIGRP can install non-successor to RIB in case of ECMP paths
CSCux11029	Route tag lost on internal routes when using eigrp wide metric on Nexus
CSCut46889	OV intf stuck at "Cleanup in Progress" when bouncing overlay interface
CSCuw74438	L3vm crash during ISSU
CSCux77347	LISP: map-cache on the standby HSRP is not cleared when dyn host returns
CSCux47285	LISP: race condition LISP/RIB when programming FIB
CSCuw90721	LISP: RNH notifies for db RLOCs gone when coincide with map-cache RLOCs
CSCuv66399	Forwarding address not set in OSPF for routes w/ different prefix length
CSCuv56604	ospf pushing BFD into admin down state
CSCuw03410	Nexus 6.2.x OSPF taking long time in LSA generation
CSCux09020	NSSA intern router originate default not ASBR post ISSU 6.2.8a to 6.2.12
CSCuv81861	OSPF NSSA sending type 7 LSA after converted to regular area
CSCuu22255	LL shouldn't be installed in u6rib by ospfv3

Table 48 Cisco NX-OS Release 7.3(0)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCuw27044	OSPFv3 takes 30 min to install route when using link-local addresses
CSCux59834	Limit OTV data-group configuration to /24
CSCuu01234	OTV, next hop pointing to wrong AED - OTV Part
CSCus66235	Match Statements within route-map do not function as AND for table-map
CSCut84448	OSPF type problem when redistribution of static routes
CSCuw03144	OpenSSH: Evaluation of Multiple OpenSSH CVEs for NX-OS
CSCuw10098	FPC members in error disabled state with error as INVALID INTERFACE
CSCut84271	IP SLA control protocol communication may fail if loopback address used
CSCuw56575	SNMP TS is missing show run snmp
CSCuw76278	Cisco Nexus 7000/Cisco Nexus 5000 netstack panic crash after upgrade to 6.2.14/7.2(1)N1(1)
CSCuw96276	CVE-2013-4548 Vulnerability Nexus 7000
CSCus61813	loop in MST environment after ISSU 6.1(4)->6.2(8a)
CSCuu30252	aclmgr: cmd_dynamic_string_add bad item
CSCuv90027	NXOSv Interface ACL config should be blocked until supported
CSCut29799	Privilege escalation with o+w files and directories
CSCur17440	945snmpwalk on cpmCPUTotalTable(1.3.6.1.4.1.9.9.109.1.1.1) failing
CSCux14098	Cisco Nexus 7000/Cisco Nexus 7700: write error: No space left on device
CSCuw62000	Vtpv3: Not updating the vlan info after reload

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

Table 49 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 50 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
CSCui22991	Hardware queuing cfg messed up on removing a policy not in sync with dscp2q map
CSCuz00345	ISSU from 6214 with policy caching does not download >1 ACE's
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
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

Table 50 Cisco NX-OS Release 7.2(2)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
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
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

Table 50 Cisco NX-OS Release 7.2(2)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
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
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 51 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
CSCut17447	SPAN destination port load balancing does not work with M2 module as span src

Table 51 Cisco NX-OS Release 7.2(1)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
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
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

Table 51 Cisco NX-OS Release 7.2(1)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
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
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

Table 51 Cisco NX-OS Release 7.2(1)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
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
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 52 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
CSCus09312	PVLAN:VPC PO member (M1 module) flaps.
CSCus33041	The enable otv stp-synchronization causes the vlans active on all AEDs
CSCus45517	BGP MED not used with LOCAL AS Neighbors.
CSCus77610	N7710G: ports down due to UDLD empty echo after neighbor LC reloaded
CSCus82982	Changing 'is-type' for ISIS configuration de-registers interface as MPLS
CSCun87659	In large vlan scale setup SPM is timing out causing issues
CSCur28450	Rollback to a checkpoint fails verification at FEX SAT PO
CSCur32239	PVLAN add/delete - vlan_mgr event seq timeout
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
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

Table 52 Cisco NX-OS Release 7.2(0)D1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCuq18021	SNMPset to community strings with special characters cause hap reset
CSCur30073	switch table driving wrong multipath

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.