Cisco Nexus 5600 Series Release Notes, Release 7.x

First Published: March 20, 2014
Last Modified: August 2, 2023
Current Release: Cisco NX-OS Release 7.3(14)N1(1)

This document describes the features, caveats, and limitations for the Cisco Nexus 5600 Series switches and the Cisco Nexus 2000 Series Fabric Extenders (FEXs). Use this document in combination with documents listed in the "Obtaining Documentation and Submitting a Service Request" section on page 147.

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

Note Release notes are sometimes updated with new information about restrictions and caveats. See the following website for the latest version of the Cisco Nexus 5600 Series and Cisco Nexus 2000 Series Release Notes:
http://www.cisco.com/en/US/docs/switches/datacenter/nexus5600/sw/release/notes/Nexus_5600_Release_Notes.html

Table 1 shows the new and changed history for this document.

Table 1 New and Changed Information

Date	Description
August 2, 2023	Created NX-OS Release 7.3(14)N1(1) release notes.
April 28, 2023	Added CSCwf04604 to the Open Caveats section.
February 13, 2023	Created NX-OS Release 7.3(13)N1(1) release notes.
August 03, 2022	Created NX-OS Release 7.3(12)N1(1) release notes.
February 18, 2022	Created NX-OS Release 7.3(11)N1(1) release notes.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table 1 New and Changed Information

Date	Description
July 23, 2021	Created NX-OS Release 7.3(10)N1(1) release notes.
February 12, 2021	Created NX-OS Release 7.3(9)N1(1) release notes.
July 30, 2020	Created NX-OS Release 7.3(8)N1(1) release notes.
June 1, 2020	Created NX-OS Release 7.3(7)N1(1b) release notes.
April 20, 2020	Created NX-OS Release 7.3(7)N1(1a) release notes.
March 31, 2020	Added CSCvt58479 to the Open Caveats section.
February 6, 2020	Created NX-OS Release 7.3(7)N1(1) release notes.
September 16, 2019	Created NX-OS Release 7.3(6)N1(1) release notes.
June 7, 2019	Added CSCvp38432 to the Open Caveats section.
March 26, 2019	Added CSCvo88678 to the Open Caveats section.
February 15, 2019	Created NX-OS Release 7.3(5)N1(1) release notes.
December 20, 2018	Created NX-OS Release 7.1(5)N1(1b) release notes.
September 15, 2018	Created NX-OS Release 7.3(4)N1(1) release notes.
May 9, 2018	Created NX-OS Release 7.3(3)N1(1) release notes.
September 21, 2017	Created NX-OS Release 7.1(5)N1(1) release notes.
August 14, 2017	Added CSCux99818 bug to the Resolved Caveats in Cisco NX-OS Release 7.3(2)N1(1), 7.3(1)N1(1) and 7.2(1)N1(1) sections.
June 14, 2017	Updated the New Software Features and Enhancements in Cisco NX-OS Release 7.3(2)N1(1) section.
May 15, 2017	Created NX-OS Release 7.3(2)N1(1) release notes.
October 11, 2016	Created NX-OS Release 7.3(1)N1(1) release notes.
September 9, 2016	Created NX-OS Release 7.1(4)N1(1) release notes.
February 19, 2016	Created NX-OS Release 7.0(8)N1(1) release notes.
January 08, 2016	Created NX-OS Release 7.3(0)N1(1) release notes.
January 25, 2016	Created NX-OS Release 7.1(3)N1(2) release notes.
November 10, 2015	Created NX-OS Release 7.1(3)N1(1) release notes.
October 15, 2015	Created NX-OS Release 7.2(1)N1(1) release notes.
August 24, 2015	Created NX-OS Release 7.0(7)N1(1) release notes.
July 20, 2015	Created NX-OS Release 7.1(2)N1(1) release notes.
June 04, 2015	Created NX-OS Release 7.2(0)N1(1) release notes.
April 16, 2015	Created NX-OS Release 7.1(1)N1(1) release notes.
April 7, 2015	Created NX-OS Release 7.0(6)N1(1) release notes.
March 2, 2015	Created NX-OS Release 7.1(0)N1(1b) release notes.
January 9, 2015	Added CSCus31100, CSCus39388, CSCus18209 to Resolved Caveats. Added note about CSCus39830 to the ISSU matrix table.
January 8, 2015	Created NX-OS Release 7.1(0)N1(1a) release notes.
January 7, 2015	Added CSCus39388 and CSCus39830 to Open Caveats.

Table 1 New and Changed Information

Date	Description
January 6, 2015	Added CSCus22741 to Open Caveats. Added Open Management Infrastructure to New and Changed Features.
December 23, 2014	Added CSCus31100 to Open Caveats.
December 22, 2014	Created NX-OS Release 7.1(0)N1(1) release notes.
December 22, 2014	Created NX-OS Release 7.0(5)N1(1a) release notes.
October 24, 2014	Created NX-OS Release 7.0(5)N1(1) release notes.
October 2, 2014	Added CSCur09549 to Open Caveats.
September 29, 2014	Created NX-OS Release 7.0(4)N1(1) release notes.
July 25, 2014	Created NX-OS Release 7.0(3)N1(1) release notes.
May 9, 2013	Added Buffer Utilization Histogram to New Software Features.
May 6, 2014	Added CSCuo39454 to Resolved Caveats.
May 5, 2014	Created NX-OS Release 7.0(2)N1(1) release notes.
March 28, 2014	Updated Table 2. Added 20UP LEM to New Hardware Features.
March 27, 2014	Added optics to Table 2. Updated Introduction.
March 20, 2014	Created NX-OS Release 7.0(1)N1(1) release notes.

Contents

This document includes the following sections:

- Introduction, page 3
- System Requirements, page 4
- Online Insertion and Removal Support, page 21
- New and Changed Features, page 21
- Upgrading or Downgrading to a New Release, page 50
- Unsupported Features, page 73
- Limitations, page 73
- Caveats, page 78
- MIB Support, page 146
- Obtaining Documentation and Submitting a Service Request, page 147

Introduction

The Cisco NX-OS software is a data center-class operating system built with modularity, resiliency, and serviceability at its foundation. Based on the industry-proven Cisco NX-OS software, Cisco NX-OS helps ensure continuous availability and sets the standard for mission-critical data center environments. The highly modular design of Cisco NX-OS makes zero-effect operations a reality and enables exceptional operational flexibility.

Several new hardware and software features are introduced for the Cisco Nexus 5600 Series device and the Cisco Nexus 2000 Series Fabric Extender (FEX) to improve the performance, scalability, and management of the product line.

Cisco Nexus 5600 Series Devices

The Cisco Nexus 5600 Series includes 10- and 40-Gigabit Ethernet density in energy-efficient compact form factor switches. The Cisco Nexus 5600 Series Layer 2 and Layer 3 set allow for multiple scenarios such as direct-attach 10- and 40-Gigabit Ethernet access and high-density Cisco Fabric Extender (FEX) aggregation deployments, leaf and spine architectures, or compact aggregation to build scalable Cisco Unified Fabric in the data centers.

Cisco Nexus 5600 Series products use the same set of Cisco application-specific integrated circuits (ASICs) and a single software image across the products within the family, which offers feature consistency and operational simplicity. Cisco Nexus 5600 Series switches support robust Layer 2 and Layer 3 functions, industry-leading FEX architecture with Cisco Nexus 2000 and Cisco Nexus B22 Blade FEX, in-service software upgrades (ISSUs), and Cisco FabricPath. Operational efficiency and programmability are enhanced on the Cisco Nexus 5600 Series through advanced analytics, PowerOn Auto Provisioning (POAP), and Python/Tool Command Language (Tcl) scripting.

The Cisco Nexus devices include a family of line-rate, low-latency, lossless 10-Gigabit Ethernet, Cisco Data Center Ethernet, Fibre Channel over Ethernet (FCoE), and native Fibre Channel devices for data center applications.

For information about the Cisco Nexus 5600 Series, see the *Cisco Nexus 5600 Series Platform Hardware Installation Guide*.

Cisco Nexus 2000 Series Fabric Extenders

The Cisco Nexus 2000 Series Fabric Extender (FEX) is a highly scalable and flexible server networking solution that works with the Cisco Nexus 5600 Series devices to provide high-density and low-cost connectivity for server aggregation. Scaling across 1-Gigabit Ethernet, 10-Gigabit Ethernet, and 40-Gigabit Ethernet, unified fabric, rack, and blade server environments, the FEX is designed to simplify data center architecture and operations.

The FEX integrates with its parent Cisco Nexus device, which allows zero-touch provisioning and automatic configuration. The FEX provides a single point of management that supports a large numbers of servers and hosts that can be configured with the same feature set as the parent Cisco Nexus 5600 switch, including security and quality of service (QoS) configuration parameters. Spanning Tree Protocol (STP) is not required between the Fabric Extender and its parent switch, because the Fabric Extender and its parent switch allow you to enable a large multi-path, loop-free, active-active topology.

Software is not included with the Fabric Extender. Cisco NX-OS software is automatically downloaded and upgraded from its parent switch. For information about configuring the Cisco Nexus 2000 FEX, see the “Configuring the Fabric Extender” chapter in the *Cisco Nexus 5600 Series Layer 2 Switching Configuration Guide*.

System Requirements

This section includes the following topics:

- Hardware Supported, page 5

Hardware Supported

The Cisco NX-OS software supports the Cisco Nexus 5600 Series switch. You can find detailed information about supported hardware in the *Cisco Nexus 5600 Series Hardware Installation Guide*.

Table 2 shows the hardware supported by Cisco NX-OS Release 7.x software.

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software

Cisco NX-OS Release Support						

Hardware	**Part Number**	**7.0(1)N1(1)**	**7.0(2)N1(1)**	**7.0(3)N1(1)**	**7.3(10)N1(1)**
					7.3(9)N1(1)
					7.0(8)N1(1)
					7.0(7)N1(1)
					7.0(6)N1(1)
					7.0(5)N1(1a)
					7.0(5)N1(1)
					7.0(4)N1(1)
						7.3(14)N1(1)
						7.3(13)N1(1)
						7.3(12)N1(1)
						7.3(11)N1(1)
						7.3(10)N1(1)
						7.3(9)N1(1)
						7.3(8)N1(1)
						7.3(7)N1(1b)
						7.3(7)N1(1a)
						7.3(7)N1(1)
						7.3(6)N1(1)
						7.3(5)N1(1)
						7.3(4)N1(1)
						7.3(3)N1(1)
						7.3(2)N1(1)
						7.3(1)N1(1)
						7.3(0)N1(1)
						7.2(1)N1(1)
						7.2(0)N1(1)
						7.1(5)N1(1)
						7.1(4)N1(1)
						7.1(3)N1(2)
						7.1(3)N1(1)
						7.1(2)N1(1)
						7.1(1)N1(1)
						7.1(0)N1(1b)
						7.1(0)N1(1a)

Cisco Nexus 5600 Series						
Cisco Nexus 5624 Switch	N5K-C5624Q	No	No	No	No	Yes
Cisco Nexus 5648 Switch	N5K-C5648Q	No	No	No	No	7.1(1)N1(1) and later.
Cisco Nexus 5696 Switch	N5K-C5696Q	No	No	No	Yes	Yes
Cisco Nexus 5672 Switch	N5K-C5672UP	Yes	Yes	Yes	Yes	Yes
Cisco Nexus 5672-16G Switch	N5K-C5672UP-16G	No	No	No	No	7.3(0)N1(1) and later.

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support						

Hardware	**Part Number**	**7.0(1)N1(1)**	**7.0(2)N1(1)**	**7.0(3)N1(1)**	**7.3(10)N1(1)**
					7.3(9)N1(1)
					7.0(8)N1(1)
					7.0(7)N1(1)
					7.0(6)N1(1)
					7.0(5)N1(1a)
					7.0(5)N1(1)
					7.0(4)N1(1)
						7.3(14)N1(1)
						7.3(13)N1(1)
						7.3(12)N1(1)
						7.3(11)N1(1)
						7.3(10)N1(1)
						7.3(9)N1(1)
						7.3(8)N1(1)
						7.3(7)N1(1b)
						7.3(7)N1(1a)
						7.3(7)N1(1)
						7.3(6)N1(1)
						7.3(5)N1(1)
						7.3(4)N1(1)
						7.3(3)N1(1)
						7.3(2)N1(1)
						7.3(1)N1(1)
						7.3(0)N1(1)
						7.2(1)N1(1)
						7.2(0)N1(1)
						7.1(5)N1(1)
						7.1(4)N1(1)
						7.1(3)N1(2)
						7.1(3)N1(1)
						7.1(2)N1(1)
						7.1(1)N1(1)
						7.1(0)N1(1b)
						7.1(0)N1(1a)

Cisco Nexus 56128 Switch	N5K-C56128P	No	Yes	Yes	Yes	Yes
Cisco Nexus 2000 Series						
Cisco Nexus 2348UPQ FEX	N2K-C2348UPQ	No	No	Yes	Yes	Yes
Cisco Nexus 2348TQ-E FEX	N2K-C2348TQ-E	No	No	No	No	7.3(0)N1(1) and later.
Cisco Nexus 2332TQ FEX	N2K-C2332TQ-10GE	No	No	No	No	7.1(1)N1(1) and later.
Cisco Nexus 2348TQ FEX	N2K-C2348TQ-10GE	No	No	No	No	Yes
Cisco Nexus 2248PQ FEX[1]	N2K-C2248PQ-10GE	Yes	Yes	Yes	Yes	Yes
Cisco Nexus B22 DELL FEX	N2K-B22DELL-P	Yes	Yes	Yes	Yes	Yes
Cisco Nexus B22 Fujitsu FEX	N2K-B22FTS-P	Yes	Yes	Yes	Yes	Yes

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support						

Hardware	**Part Number**	**7.0(1)N1(1)**	**7.0(2)N1(1)**	**7.0(3)N1(1)**	**7.3(10)N1(1)**
					7.3(9)N1(1)
					7.0(8)N1(1)
					7.0(7)N1(1)
					7.0(6)N1(1)
					7.0(5)N1(1a)
					7.0(5)N1(1)
					7.0(4)N1(1)
						7.3(14)N1(1)
						7.3(13)N1(1)
						7.3(12)N1(1)
						7.3(11)N1(1)
						7.3(10)N1(1)
						7.3(9)N1(1)
						7.3(8)N1(1)
						7.3(7)N1(1b)
						7.3(7)N1(1a)
						7.3(7)N1(1)
						7.3(6)N1(1)
						7.3(5)N1(1)
						7.3(4)N1(1)
						7.3(3)N1(1)
						7.3(2)N1(1)
						7.3(1)N1(1)
						7.3(0)N1(1)
						7.2(1)N1(1)
						7.2(0)N1(1)
						7.1(5)N1(1)
						7.1(4)N1(1)
						7.1(3)N1(2)
						7.1(3)N1(1)
						7.1(2)N1(1)
						7.1(1)N1(1)
						7.1(0)N1(1b)
						7.1(0)N1(1a)

Cisco Nexus B22 HP FEX	N2K-B22HP-P	Yes	Yes	Yes	Yes	Yes
Cisco Nexus B22 IBM FEX	N2K-B22IBM-P	Yes	Yes	Yes	Yes	Yes
Cisco Nexus 2232TM-E FEX	N2K-C2232TM-E-10GE	Yes	Yes	Yes	Yes	Yes
Cisco Nexus 2232TM FEX	N2K-C2232TM-10GE	Yes	Yes	Yes	Yes	Yes
Cisco Nexus 2232PP FEX	N2K-C2232PP-10GE	Yes	Yes	Yes	Yes	Yes
Cisco Nexus 2248TP-E FEX	N2K-C2248TP-E-1GE	Yes	Yes	Yes	Yes	Yes
Cisco Nexus 2248TP FEX	N2K-C2248TP-1GE	Yes	Yes	Yes	Yes	Yes
Cisco Nexus 2224TP FEX	N2K-C2224TP-1GE	Yes	Yes	Yes	Yes	Yes
Cisco Nexus 2148T FEX	N2K-C2148T-1GE	No	No	No	No	No

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support						

Hardware	**Part Number**	**7.0(1)N1(1)**	**7.0(2)N1(1)**	**7.0(3)N1(1)**	**7.3(10)N1(1)**
					7.3(9)N1(1)
					7.0(8)N1(1)
					7.0(7)N1(1)
					7.0(6)N1(1)
					7.0(5)N1(1a)
					7.0(5)N1(1)
					7.0(4)N1(1)
						7.3(14)N1(1)
						7.3(13)N1(1)
						7.3(12)N1(1)
						7.3(11)N1(1)
						7.3(10)N1(1)
						7.3(9)N1(1)
						7.3(8)N1(1)
						7.3(7)N1(1b)
						7.3(7)N1(1a)
						7.3(7)N1(1)
						7.3(6)N1(1)
						7.3(5)N1(1)
						7.3(4)N1(1)
						7.3(3)N1(1)
						7.3(2)N1(1)
						7.3(1)N1(1)
						7.3(0)N1(1)
						7.2(1)N1(1)
						7.2(0)N1(1)
						7.1(5)N1(1)
						7.1(4)N1(1)
						7.1(3)N1(2)
						7.1(3)N1(1)
						7.1(2)N1(1)
						7.1(1)N1(1)
						7.1(0)N1(1b)
						7.1(0)N1(1a)

Linecard Expansion Modules						
100 Gigabit Ethernet Line Card Expansion Module (LEM)	N5696-M4C	No	No	No	No	Yes
Cisco Nexus 5696Q 40 Gigabit Ethernet Line Card Expansion Module (LEM)	N5696-M12Q	No	No	No	Yes	Yes
Cisco Nexus 5696Q 20UP LEM N6004X-M20UP	N5696-M20UP	No	No	No	Yes	Yes
Cisco Nexus 24x10GE Unified Port + 2xQSFP 40GE.[2]	N56-M24UP2Q	No	Yes	Yes	Yes	Yes
Cisco Nexus 5648Q Gigabit Ethernet Line Card Expansion Module (12-port QSFP module)	N56-M12Q	No	No	No	No	Yes

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support						

Hardware	**Part Number**	**7.0(1)N1(1)**	**7.0(2)N1(1)**	**7.0(3)N1(1)**	**7.3(10)N1(1)**
					7.3(9)N1(1)
					7.0(8)N1(1)
					7.0(7)N1(1)
					7.0(6)N1(1)
					7.0(5)N1(1a)
					7.0(5)N1(1)
					7.0(4)N1(1)
						7.3(14)N1(1)
						7.3(13)N1(1)
						7.3(12)N1(1)
						7.3(11)N1(1)
						7.3(10)N1(1)
						7.3(9)N1(1)
						7.3(8)N1(1)
						7.3(7)N1(1b)
						7.3(7)N1(1a)
						7.3(7)N1(1)
						7.3(6)N1(1)
						7.3(5)N1(1)
						7.3(4)N1(1)
						7.3(3)N1(1)
						7.3(2)N1(1)
						7.3(1)N1(1)
						7.3(0)N1(1)
						7.2(1)N1(1)
						7.2(0)N1(1)
						7.1(5)N1(1)
						7.1(4)N1(1)
						7.1(3)N1(2)
						7.1(3)N1(1)
						7.1(2)N1(1)
						7.1(1)N1(1)
						7.1(0)N1(1b)
						7.1(0)N1(1a)

Cisco Nexus 5624Q Gigabit Ethernet Line Card Expansion Module (12-port QSFP module)	N56-M12Q	No	No	No	No	Yes
Transceivers						
QSFP Transceivers						
QSFP-4X10G-LR-S	QSFP-4X10G-LR-S	No	No	No	No	7.3(1)N1(1) and later.
LR4 Optics—WSP-Q40GL R4L	QSFP40G-LR4-LITE	No	No	No	No	Yes
Cisco QSFP40G BiDi Short-reach Transceiver	QSFP-40G-SR-BD	Yes	Yes	Yes	Yes	Yes
Cisco QSFP 40GBASE-LR4 Transceiver Module, LC, 10KM	QSFP-40GE-LR4	Yes	Yes	Yes	Yes	Yes

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support						

Hardware	**Part Number**	**7.0(1)N1(1)**	**7.0(2)N1(1)**	**7.0(3)N1(1)**	**7.3(10)N1(1)**
					7.3(9)N1(1)
					7.0(8)N1(1)
					7.0(7)N1(1)
					7.0(6)N1(1)
					7.0(5)N1(1a)
					7.0(5)N1(1)
					7.0(4)N1(1)
						7.3(14)N1(1)
						7.3(13)N1(1)
						7.3(12)N1(1)
						7.3(11)N1(1)
						7.3(10)N1(1)
						7.3(9)N1(1)
						7.3(8)N1(1)
						7.3(7)N1(1b)
						7.3(7)N1(1a)
						7.3(7)N1(1)
						7.3(6)N1(1)
						7.3(5)N1(1)
						7.3(4)N1(1)
						7.3(3)N1(1)
						7.3(2)N1(1)
						7.3(1)N1(1)
						7.3(0)N1(1)
						7.2(1)N1(1)
						7.2(0)N1(1)
						7.1(5)N1(1)
						7.1(4)N1(1)
						7.1(3)N1(2)
						7.1(3)N1(1)
						7.1(2)N1(1)
						7.1(1)N1(1)
						7.1(0)N1(1b)
						7.1(0)N1(1a)

40GBASE-SR4 QSFP Transceiver	QSFP-40G-SR4	Yes	Yes	Yes	Yes	Yes
QSFP 4x10GBASE-SR Transceiver	QSFP-40G-CSR4	Yes	Yes	Yes	Yes	Yes
QSFP 40GBASE-LR4 Transceiver, LC, 10KM	QSFP-40G-LR4	Yes	Yes	Yes	Yes	Yes
Cisco 40GBase-AOC QSFP direct-attach Active Optical Cable, 1-meter	QSFP-H40G-AOC1M	Yes	Yes	Yes	Yes	Yes
Cisco 40GBase-AOC QSFP direct-attach Active Optical Cable, 2-meter	QSFP-H40G-AOC2M	Yes	Yes	Yes	Yes	Yes
Cisco 40GBase-AOC QSFP direct-attach Active Optical Cable, 3-meter	QSFP-H40G-AOC3M	Yes	Yes	Yes	Yes	Yes

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support						

Hardware	**Part Number**	**7.0(1)N1(1)**	**7.0(2)N1(1)**	**7.0(3)N1(1)**	**7.3(10)N1(1)**
					7.3(9)N1(1)
					7.0(8)N1(1)
					7.0(7)N1(1)
					7.0(6)N1(1)
					7.0(5)N1(1a)
					7.0(5)N1(1)
					7.0(4)N1(1)
						7.3(14)N1(1)
						7.3(13)N1(1)
						7.3(12)N1(1)
						7.3(11)N1(1)
						7.3(10)N1(1)
						7.3(9)N1(1)
						7.3(8)N1(1)
						7.3(7)N1(1b)
						7.3(7)N1(1a)
						7.3(7)N1(1)
						7.3(6)N1(1)
						7.3(5)N1(1)
						7.3(4)N1(1)
						7.3(3)N1(1)
						7.3(2)N1(1)
						7.3(1)N1(1)
						7.3(0)N1(1)
						7.2(1)N1(1)
						7.2(0)N1(1)
						7.1(5)N1(1)
						7.1(4)N1(1)
						7.1(3)N1(2)
						7.1(3)N1(1)
						7.1(2)N1(1)
						7.1(1)N1(1)
						7.1(0)N1(1b)
						7.1(0)N1(1a)

Cisco 40GBase-AOC QSFP direct-attach Active Optical Cable, 5-meter	QSFP-H40G-AOC5M	Yes	Yes	Yes	Yes	Yes
Cisco 40GBase-AOC QSFP direct-attach Active Optical Cable, 7-meter	QSFP-H40G-AOC7M	Yes	Yes	Yes	Yes	Yes
Cisco 40GBase-AOC QSFP direct-attach Active Optical Cable, 10-meter	QSFP-H40G-AOC10M	Yes	Yes	Yes	Yes	Yes
Cisco QSFP Adapter Module, 1G(GLC-T, SX,LH) and 10G with 10G-SFP-SR, 10G-SFP-LR and 10G-SFP-ZR	CVR-QSFP-SFP10G	Yes	Yes	Yes	Yes	Yes
SFP+ Optical						

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support						

Hardware	**Part Number**	**7.0(1)N1(1)**	**7.0(2)N1(1)**	**7.0(3)N1(1)**	**7.3(10)N1(1)**
					7.3(9)N1(1)
					7.0(8)N1(1)
					7.0(7)N1(1)
					7.0(6)N1(1)
					7.0(5)N1(1a)
					7.0(5)N1(1)
					7.0(4)N1(1)
						7.3(14)N1(1)
						7.3(13)N1(1)
						7.3(12)N1(1)
						7.3(11)N1(1)
						7.3(10)N1(1)
						7.3(9)N1(1)
						7.3(8)N1(1)
						7.3(7)N1(1b)
						7.3(7)N1(1a)
						7.3(7)N1(1)
						7.3(6)N1(1)
						7.3(5)N1(1)
						7.3(4)N1(1)
						7.3(3)N1(1)
						7.3(2)N1(1)
						7.3(1)N1(1)
						7.3(0)N1(1)
						7.2(1)N1(1)
						7.2(0)N1(1)
						7.1(5)N1(1)
						7.1(4)N1(1)
						7.1(3)N1(2)
						7.1(3)N1(1)
						7.1(2)N1(1)
						7.1(1)N1(1)
						7.1(0)N1(1b)
						7.1(0)N1(1a)

Cisco DWDM 10G SFP	DWDM-SFP10G-XX.XX[3]	No	No	No	No	7.3(2)N1(1) and later.
Cisco CWDM 10G SFP	CWDM-SFP10G-XXXX[4]	No	No	No	No	7.3(2)N1(1) and later.
Cisco ZR 10G SFP	SFP-10G-ZR[5]	No	No	No	No	7.3(2)N1(1) and later.
Cisco 40GBASE ER4 Optics	QSFP-40G-ER4	No	No	No	No	7.1(1)N1(1) and later.
QSFP to 4xSFP 10G Passive Copper Splitter Cable, 1M	QSFP-4SFP10G-CU1M	Yes	Yes	Yes	Yes	Yes
QSFP to 4xSFP 10G Passive Copper Splitter Cable, 3M	QSFP-4SFP10G-CU3M	Yes	Yes	Yes	Yes	Yes
QSFP to 4xSFP 10G Passive Copper Splitter Cable, 5M	QSFP-4SFP10G-CU5M	Yes	Yes	Yes	Yes	Yes

Table 2 *Hardware Supported by Cisco NX-OS Release 7.x Software (continued)*

Cisco NX-OS Release Support						

Hardware	**Part Number**	**7.0(1)N1(1)**	**7.0(2)N1(1)**	**7.0(3)N1(1)**	**7.3(10)N1(1)**
					7.3(9)N1(1)
					7.0(8)N1(1)
					7.0(7)N1(1)
					7.0(6)N1(1)
					7.0(5)N1(1a)
					7.0(5)N1(1)
					7.0(4)N1(1)
						7.3(14)N1(1)
						7.3(13)N1(1)
						7.3(12)N1(1)
						7.3(11)N1(1)
						7.3(10)N1(1)
						7.3(9)N1(1)
						7.3(8)N1(1)
						7.3(7)N1(1b)
						7.3(7)N1(1a)
						7.3(7)N1(1)
						7.3(6)N1(1)
						7.3(5)N1(1)
						7.3(4)N1(1)
						7.3(3)N1(1)
						7.3(2)N1(1)
						7.3(1)N1(1)
						7.3(0)N1(1)
						7.2(1)N1(1)
						7.2(0)N1(1)
						7.1(5)N1(1)
						7.1(4)N1(1)
						7.1(3)N1(2)
						7.1(3)N1(1)
						7.1(2)N1(1)
						7.1(1)N1(1)
						7.1(0)N1(1b)
						7.1(0)N1(1a)

QSFP to 4xSFP10G Active Copper Splitter Cable, 7M	QSFP-4SFP10G-AC7M	Yes	Yes	Yes	Yes	Yes
QSFP to 4xSFP10G Active Copper Splitter Cable, 10M	QSFP-4X10G-AC10M	Yes	Yes	Yes	Yes	Yes
Cisco 40GBASE-CR4 QSFP+ to 4 10GBASE-CU SFP+ direct-attach breakout 7-meter cable, active	QSFP-4X10G-AC7M	Yes	Yes	Yes	Yes	Yes
Cisco 40GBASE-CR4 QSFP+ to 4 10GBASE-CU SFP+ direct-attach breakout 10-meter cable, active	QSFP-4X10G-AC10M	Yes	Yes	Yes	Yes	Yes
10-Gigabit Ethernet SFP (for Cisco Nexus 2000 Series to Cisco Nexus 5600 Series connectivity)	FET-10G(=)	Yes	Yes	Yes	Yes	Yes

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support						

Hardware	**Part Number**	**7.0(1)N1(1)**	**7.0(2)N1(1)**	**7.0(3)N1(1)**	**7.3(10)N1(1)**
					7.3(9)N1(1)
					7.0(8)N1(1)
					7.0(7)N1(1)
					7.0(6)N1(1)
					7.0(5)N1(1a)
					7.0(5)N1(1)
					7.0(4)N1(1)
						7.3(14)N1(1)
						7.3(13)N1(1)
						7.3(12)N1(1)
						7.3(11)N1(1)
						7.3(10)N1(1)
						7.3(9)N1(1)
						7.3(8)N1(1)
						7.3(7)N1(1b)
						7.3(7)N1(1a)
						7.3(7)N1(1)
						7.3(6)N1(1)
						7.3(5)N1(1)
						7.3(4)N1(1)
						7.3(3)N1(1)
						7.3(2)N1(1)
						7.3(1)N1(1)
						7.3(0)N1(1)
						7.2(1)N1(1)
						7.2(0)N1(1)
						7.1(5)N1(1)
						7.1(4)N1(1)
						7.1(3)N1(2)
						7.1(3)N1(1)
						7.1(2)N1(1)
						7.1(1)N1(1)
						7.1(0)N1(1b)
						7.1(0)N1(1a)

40-Gigabit Ethernet QSFP+ (for Cisco Nexus 2000 Series to Cisco Nexus 5600 Series connectivity)	FET-40G	Yes	Yes	Yes	Yes	Yes
Gigabit Ethernet SFP, LH transceiver	GLC-LH-SMD	Yes	Yes	Yes	Yes	Yes
Gigabit Ethernet SFP, EX transceiver	GLC-EX-SMD	6.0(2)N1(2) and later.	6.0(2)N1(2) and later.	6.0(2)N1(2) and later.	6.0(2)N1(2) and later.	6.0(2)N1(2) and later.
Cisco GE SFP, LC connector SX transceiver	GLC-SX-MM	Yes	Yes	Yes	Yes	Yes
40-Gigabit CU QSFP module	QSFP-H40G-CU1M	Yes	Yes	Yes	Yes	Yes
40-Gigabit CU QSFP module	QSFP-H40G-CU3M	Yes	Yes	Yes	Yes	Yes
40-Gigabit CU QSFP module	QSFP-H40G-CU5M	Yes	Yes	Yes	Yes	Yes

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support						

Hardware	**Part Number**	**7.0(1)N1(1)**	**7.0(2)N1(1)**	**7.0(3)N1(1)**	**7.3(10)N1(1)**
					7.3(9)N1(1)
					7.0(8)N1(1)
					7.0(7)N1(1)
					7.0(6)N1(1)
					7.0(5)N1(1a)
					7.0(5)N1(1)
					7.0(4)N1(1)
						7.3(14)N1(1)
						7.3(13)N1(1)
						7.3(12)N1(1)
						7.3(11)N1(1)
						7.3(10)N1(1)
						7.3(9)N1(1)
						7.3(8)N1(1)
						7.3(7)N1(1b)
						7.3(7)N1(1a)
						7.3(7)N1(1)
						7.3(6)N1(1)
						7.3(5)N1(1)
						7.3(4)N1(1)
						7.3(3)N1(1)
						7.3(2)N1(1)
						7.3(1)N1(1)
						7.3(0)N1(1)
						7.2(1)N1(1)
						7.2(0)N1(1)
						7.1(5)N1(1)
						7.1(4)N1(1)
						7.1(3)N1(2)
						7.1(3)N1(1)
						7.1(2)N1(1)
						7.1(1)N1(1)
						7.1(0)N1(1b)
						7.1(0)N1(1a)

40-Gigabit CU QSFP module	QSFP-H40G-ACu7M	Yes	Yes	Yes	Yes	Yes
40-Gigabit CU QSFP module	QSFP-H40G-ACu10M	Yes	Yes	Yes	Yes	Yes
Cisco 10GBASE-AOC SFP+ Cable 1 Meter	SFP-10G-AOC1M	Yes	Yes	Yes	Yes	Yes
Cisco 10GBASE-AOC SFP+ Cable 2 Meter	SFP-10G-AOC2M	Yes	Yes	Yes	Yes	Yes
Cisco 10GBASE-AOC SFP+ Cable 3 Meter	SFP-10G-AOC3M	Yes	Yes	Yes	Yes	Yes
Cisco 10GBASE-AOC SFP+ Cable 5 Meter	SFP-10G-AOC5M	Yes	Yes	Yes	Yes	Yes
Cisco 10GBASE-AOC SFP+ Cable 7 Meter	SFP-10G-AOC7M	Yes	Yes	Yes	Yes	Yes
Cisco 10GBASE-AOC SFP+ Cable 10 Meter	SFP-10G-AOC10M	Yes	Yes	Yes	Yes	Yes

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support						

Hardware	Part Number	7.0(1)N1(1)	7.0(2)N1(1)	7.0(3)N1(1)	7.3(10)N1(1)
					7.3(9)N1(1)
					7.0(8)N1(1)
					7.0(7)N1(1)
					7.0(6)N1(1)
					7.0(5)N1(1a)
					7.0(5)N1(1)
					7.0(4)N1(1)
						7.3(14)N1(1)
						7.3(13)N1(1)
						7.3(12)N1(1)
						7.3(11)N1(1)
						7.3(10)N1(1)
						7.3(9)N1(1)
						7.3(8)N1(1)
						7.3(7)N1(1b)
						7.3(7)N1(1a)
						7.3(7)N1(1)
						7.3(6)N1(1)
						7.3(5)N1(1)
						7.3(4)N1(1)
						7.3(3)N1(1)
						7.3(2)N1(1)
						7.3(1)N1(1)
						7.3(0)N1(1)
						7.2(1)N1(1)
						7.2(0)N1(1)
						7.1(5)N1(1)
						7.1(4)N1(1)
						7.1(3)N1(2)
						7.1(3)N1(1)
						7.1(2)N1(1)
						7.1(1)N1(1)
						7.1(0)N1(1b)
						7.1(0)N1(1a)

Cisco 40GBase-AOC QSFP to 4 SFP+ Active Optical breakout Cable, 1-meter	QSFP-4X10G-AOC1M	Yes	Yes	Yes	Yes	Yes
Cisco 40GBase-AOC QSFP to 4 SFP+ Active Optical breakout Cable, 2-meter	QSFP-4X10G-AOC2M	Yes	Yes	Yes	Yes	Yes
Cisco 40GBase-AOC QSFP to 4 SFP+ Active Optical breakout Cable, 3-meter	QSFP-4X10G-AOC3M	Yes	Yes	Yes	Yes	Yes
Cisco 40GBase-AOC QSFP to 4 SFP+ Active Optical breakout Cable, 5-meter	QSFP-4X10G-AOC5M	Yes	Yes	Yes	Yes	Yes
Cisco 40GBase-AOC QSFP to 4 SFP+ Active Optical breakout Cable, 7-meter	QSFP-4X10G-AOC7M	Yes	Yes	Yes	Yes	Yes

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support						

Hardware	**Part Number**	**7.0(1)N1(1)**	**7.0(2)N1(1)**	**7.0(3)N1(1)**	**7.3(10)N1(1)**
					7.3(9)N1(1)
					7.0(8)N1(1)
					7.0(7)N1(1)
					7.0(6)N1(1)
					7.0(5)N1(1a)
					7.0(5)N1(1)
					7.0(4)N1(1)
						7.3(14)N1(1)
						7.3(13)N1(1)
						7.3(12)N1(1)
						7.3(11)N1(1)
						7.3(10)N1(1)
						7.3(9)N1(1)
						7.3(8)N1(1)
						7.3(7)N1(1b)
						7.3(7)N1(1a)
						7.3(7)N1(1)
						7.3(6)N1(1)
						7.3(5)N1(1)
						7.3(4)N1(1)
						7.3(3)N1(1)
						7.3(2)N1(1)
						7.3(1)N1(1)
						7.3(0)N1(1)
						7.2(1)N1(1)
						7.2(0)N1(1)
						7.1(5)N1(1)
						7.1(4)N1(1)
						7.1(3)N1(2)
						7.1(3)N1(1)
						7.1(2)N1(1)
						7.1(1)N1(1)
						7.1(0)N1(1b)
						7.1(0)N1(1a)

Cisco 40GBase-AOC QSFP to 4 SFP+ Active Optical breakout Cable, 10-meter	QSFP-4X10G-AOC10M	Yes	Yes	Yes	Yes	Yes
CXP Optics						
100 GB SR10 Optic	CXP-100G-SR10	No	No	No	No	Yes
100 GB SR12 Optic	CXP-100G-SR12	No	No	No	No	Yes
SFP+ Copper						
10GBASE-CU SFP+ Cable (7 meters)	SFP-H10GB-ACU7M(=)	Yes	Yes	Yes	Yes	Yes
10GBASE-CU SFP+ Cable (10 meters)	SFP-H10GB-ACU10M(=)	Yes	Yes	Yes	Yes	Yes
Cisco 1000 BASE-T SFP transceiver module for Category 5 copper wire, extended operating temperature range, RJ-45 connector	SFP-GE-T(=)	Yes	Yes	Yes	Yes	Yes

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support						

Hardware	**Part Number**	**7.0(1)N1(1)**	**7.0(2)N1(1)**	**7.0(3)N1(1)**	**7.3(10)N1(1)**
					7.3(9)N1(1)
					7.0(8)N1(1)
					7.0(7)N1(1)
					7.0(6)N1(1)
					7.0(5)N1(1a)
					7.0(5)N1(1)
					7.0(4)N1(1)
						7.3(14)N1(1)
						7.3(13)N1(1)
						7.3(12)N1(1)
						7.3(11)N1(1)
						7.3(10)N1(1)
						7.3(9)N1(1)
						7.3(8)N1(1)
						7.3(7)N1(1b)
						7.3(7)N1(1a)
						7.3(7)N1(1)
						7.3(6)N1(1)
						7.3(5)N1(1)
						7.3(4)N1(1)
						7.3(3)N1(1)
						7.3(2)N1(1)
						7.3(1)N1(1)
						7.3(0)N1(1)
						7.2(1)N1(1)
						7.2(0)N1(1)
						7.1(5)N1(1)
						7.1(4)N1(1)
						7.1(3)N1(2)
						7.1(3)N1(1)
						7.1(2)N1(1)
						7.1(1)N1(1)
						7.1(0)N1(1b)
						7.1(0)N1(1a)

Cisco 10GBASE-CU SFP+ cable 1 meter, passive	SFP-H10GB-CU1M	Yes	Yes	Yes	Yes	Yes
10GBASE CU SFP+ cable, 1.5 meter, passive	SFP-H10GB-CU1.5M	Yes	Yes	Yes	Yes	Yes
10GBASE CU SFP+ cable, 2 meters, passive	SFP-H10GB-CU2M	Yes	Yes	Yes	Yes	Yes
10GBASE CU SFP+ cable, 2.5 meters, passive	SFP-H10GB-CU2.5M	Yes	Yes	Yes	Yes	Yes
Cisco 10GBASE-CU SFP+ cable, 3 meters, passive	SFP-H10GB-CU3M	Yes	Yes	Yes	Yes	Yes
Cisco 10GBASE-CU SFP+ Cable, 5 meters, passive	SFP-H10GB-CU5M	Yes	Yes	Yes	Yes	Yes
Fibre Channel						

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support						

Hardware	Part Number	7.0(1)N1(1)	7.0(2)N1(1)	7.0(3)N1(1)	7.3(10)N1(1)
					7.3(9)N1(1)
					7.0(8)N1(1)
					7.0(7)N1(1)
					7.0(6)N1(1)
					7.0(5)N1(1a)
					7.0(5)N1(1)
					7.0(4)N1(1)
						7.3(14)N1(1)
						7.3(13)N1(1)
						7.3(12)N1(1)
						7.3(11)N1(1)
						7.3(10)N1(1)
						7.3(9)N1(1)
						7.3(8)N1(1)
						7.3(7)N1(1b)
						7.3(7)N1(1a)
						7.3(7)N1(1)
						7.3(6)N1(1)
						7.3(5)N1(1)
						7.3(4)N1(1)
						7.3(3)N1(1)
						7.3(2)N1(1)
						7.3(1)N1(1)
						7.3(0)N1(1)
						7.2(1)N1(1)
						7.2(0)N1(1)
						7.1(5)N1(1)
						7.1(4)N1(1)
						7.1(3)N1(2)
						7.1(3)N1(1)
						7.1(2)N1(1)
						7.1(1)N1(1)
						7.1(0)N1(1b)
						7.1(0)N1(1a)

8-Gbps Fibre Channel—short wavelength	DS-SFP-FC8G-SW(=)	Yes	Yes	Yes	Yes	Yes
8-Gbps Fibre Channel—long wavelength	DS-SFP-FC8G-LW(=)	Yes	Yes	Yes	Yes	Yes
4-Gbps Fibre Channel—short wavelength	4DS-SFP-FC4G-SW(=)	Yes	Yes	Yes	Yes	Yes
4-Gbps Fibre Channel—long wavelength	4DS-SFP-FC4G-LW(=)	Yes	Yes	Yes	Yes	Yes
16-Gbps Fibre Channel-short wavelength	DS-SFP-FC16G-SW	No	No	No	No	7.3(0)N1(1) and later.
16-Gbps Fibre Channel-long wavelength	DS-SFP-FC16G-LW	No	No	No	No	7.3(0)N1(1) and later.

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support						

Hardware	**Part Number**	**7.0(1)N1(1)**	**7.0(2)N1(1)**	**7.0(3)N1(1)**	**7.3(10)N1(1)**
					7.3(9)N1(1)
					7.0(8)N1(1)
					7.0(7)N1(1)
					7.0(6)N1(1)
					7.0(5)N1(1a)
					7.0(5)N1(1)
					7.0(4)N1(1)
						7.3(14)N1(1)
						7.3(13)N1(1)
						7.3(12)N1(1)
						7.3(11)N1(1)
						7.3(10)N1(1)
						7.3(9)N1(1)
						7.3(8)N1(1)
						7.3(7)N1(1b)
						7.3(7)N1(1a)
						7.3(7)N1(1)
						7.3(6)N1(1)
						7.3(5)N1(1)
						7.3(4)N1(1)
						7.3(3)N1(1)
						7.3(2)N1(1)
						7.3(1)N1(1)
						7.3(0)N1(1)
						7.2(1)N1(1)
						7.2(0)N1(1)
						7.1(5)N1(1)
						7.1(4)N1(1)
						7.1(3)N1(2)
						7.1(3)N1(1)
						7.1(2)N1(1)
						7.1(1)N1(1)
						7.1(0)N1(1b)
						7.1(0)N1(1a)

16-Gbps Cisco Fibre Channel Extended Longwave SFP+	DS-SFP-FC16G-ELW	No	No	No	No	7.3(0)N1(1) and later.
8-Gbps Cisco Fibre Channel Extended Reach SFP+	DS-SFP-FC8G-ER	No	No	No	No	7.3(0)N1(1) and later.
8-Gbps Cisco CWDM Fibre Channel SFP+ (2/4/8-Gbps)	DS-CWDM8G-xxxx	No	No	No	No	7.3(0)N1(1) and later.
4-Gbps Fibre Channel-short wavelength	DS-SFP-FC4G-SW(=)	No	No	No	No	7.3(0)N1(1) and later.

[1] The Cisco Nexus 2248PQ FEX does not support Gen1 cables.

[2] This LEM is installed in the N56128P.

[3] The DWDM-SFP10G-XX.XX optic is supported only on Cisco Nexus N5672UP(only UP ports), N56128P(24UP + 2Q GEM) and N5696Q(20UP LEM).

[4] The CWDM-SFP10G-XXXX optic is supported across all platforms except in a FEX.

[5] The SFP-10G-ZR optic is supported only on Cisco Nexus N5672UP(only UP ports), N56128P(24UP + 2Q GEM) and N5696Q(20UP LEM).

Online Insertion and Removal Support

Online Insertion and Removal (OIR) is supported on the Cisco Nexus 5600 and 6000 series switches. However, before OIR, the module being removed must be powered off. To power off the corresponding module, use the **poweroff module** command in global configuration mode.

Note Hot swap of a module is not supported.

New and Changed Features

This section describes the new features introduced in Cisco NX-OS Release 7.x.

- New Software Features and Enhancements in Cisco NX-OS Release 7.3(14)N1(1), page 23
- New Hardware Features in Cisco NX-OS Release 7.3(14)N1(1), page 23
- New Software Features and Enhancements in Cisco NX-OS Release 7.3(13)N1(1), page 23
- New Hardware Features in Cisco NX-OS Release 7.3(13)N1(1), page 23
- New Software Features and Enhancements in Cisco NX-OS Release 7.3(12)N1(1), page 23
- New Hardware Features in Cisco NX-OS Release 7.3(12)N1(1), page 23
- New Software Features and Enhancements in Cisco NX-OS Release 7.3(11)N1(1), page 24
- New Hardware Features in Cisco NX-OS Release 7.3(11)N1(1), page 24
- New Software Features and Enhancements in Cisco NX-OS Release 7.3(10)N1(1), page 24
- New Hardware Features in Cisco NX-OS Release 7.3(10)N1(1), page 24
- New Software Features and Enhancements in Cisco NX-OS Release 7.3(9)N1(1), page 24
- New Hardware Features in Cisco NX-OS Release 7.3(9)N1(1), page 24
- New Software Features and Enhancements in Cisco NX-OS Release 7.3(8)N1(1), page 24
- New Hardware Features in Cisco NX-OS Release 7.3(8)N1(1), page 24
- New Software Features and Enhancements in Cisco NX-OS Release 7.3(7)N1(1b), page 25
- New Hardware Features in Cisco NX-OS Release 7.3(7)N1(1b), page 25
- New Software Features and Enhancements in Cisco NX-OS Release 7.3(7)N1(1a), page 25
- New Hardware Features in Cisco NX-OS Release 7.3(7)N1(1a), page 25
- New Software Features and Enhancements in Cisco NX-OS Release 7.3(7)N1(1), page 25
- New Hardware Features in Cisco NX-OS Release 7.3(7)N1(1), page 25
- New Software Features and Enhancements in Cisco NX-OS Release 7.3(6)N1(1), page 25
- New Hardware Features in Cisco NX-OS Release 7.3(6)N1(1), page 25
- New Software Features and Enhancements in Cisco NX-OS Release 7.3(5)N1(1), page 25
- New Hardware Features in Cisco NX-OS Release 7.3(5)N1(1), page 26
- New Software Features and Enhancements in Cisco NX-OS Release 7.3(4)N1(1), page 26
- New Hardware Features in Cisco NX-OS Release 7.3(4)N1(1), page 26
- New Software Features and Enhancements in Cisco NX-OS Release 7.3(3)N1(1), page 26

- New Hardware Features in Cisco NX-OS Release 7.3(3)N1(1), page 26
- New Software Features and Enhancements in Cisco NX-OS Release 7.3(2)N1(1), page 26
- New Hardware Features in Cisco NX-OS Release 7.3(2)N1(1), page 27
- New Software Features and Enhancements in Cisco NX-OS Release 7.3(1)N1(1), page 27
- New Hardware Features in Cisco NX-OS Release 7.3(1)N1(1), page 27
- New Software Features and Enhancements in Cisco NX-OS Release 7.3(0)N1(1), page 27
- New Hardware Features in Cisco NX-OS Release 7.3(0)N1(1), page 34
- New Software Features and Enhancements in Cisco NX-OS Release 7.2(1)N1(1), page 34
- New Hardware Features in Cisco NX-OS Release 7.2(1)N1(1), page 35
- New Software Features and Enhancements in Cisco NX-OS Release 7.2(0)N1(1), page 35
- New Hardware Features in Cisco NX-OS Release 7.2(0)N1(1), page 39
- New Software Features and Enhancements in Cisco NX-OS Release 7.1(5)N1(1b), page 39
- New Hardware Features in Cisco NX-OS Release 7.1(5)N1(1b), page 39
- New Software Features and Enhancements in Cisco NX-OS Release 7.1(5)N1(1), page 39
- New Hardware Features in Cisco NX-OS Release 7.1(5)N1(1), page 39
- New Software Features and Enhancements in Cisco NX-OS Release 7.1(4)N1(1), page 39
- New Hardware Features in Cisco NX-OS Release 7.1(4)N1(1), page 41
- New Software Features and Enhancements in Cisco NX-OS Release 7.1(3)N1(2), page 41
- New Hardware Features in Cisco NX-OS Release 7.1(3)N1(2), page 41
- New Software Features and Enhancements in Cisco NX-OS Release 7.1(3)N1(1), page 41
- New Hardware Features in Cisco NX-OS Release 7.1(3)N1(1), page 41
- New Software Features and Enhancements in Cisco NX-OS Release 7.1(2)N1(1), page 41
- New Hardware Features in Cisco NX-OS Release 7.1(2)N1(1), page 42
- New Software Features and Enhancements in Cisco NX-OS Release 7.1(1)N1(1), page 42
- New Hardware Features in Cisco NX-OS Release 7.1(1)N1(1), page 43
- New Software Features and Enhancements in Cisco NX-OS Release 7.1(0)N1(1b), page 44
- New Hardware Features in Cisco NX-OS Release 7.1(0)N1(1b), page 44
- New Software Features and Enhancements in Cisco NX-OS Release 7.1(0)N1(1a), page 44
- New Hardware Features in Cisco NX-OS Release 7.1(0)N1(1a), page 46
- New Software Features and Enhancements in Cisco NX-OS Release 7.0(8)N1(1), page 47
- New Hardware Features in Cisco NX-OS Release 7.0(8)N1(1), page 47
- New Software Features and Enhancements in Cisco NX-OS Release 7.0(7)N1(1), page 47
- New Hardware Features in Cisco NX-OS Release 7.0(7)N1(1), page 47
- New Software Features and Enhancements in Cisco NX-OS Release 7.0(6)N1(1), page 47
- New Hardware Features in Cisco NX-OS Release 7.0(6)N1(1), page 47
- New Software Features and Enhancements in Cisco NX-OS Release 7.0(6)N1(1), page 47
- New Hardware Features in Cisco NX-OS Release 7.0(5)N1(1a), page 48
- New Software Features and Enhancements in Cisco NX-OS Release 7.0(5)N1(1), page 48

- New Hardware Features in Cisco NX-OS Release 7.0(5)N1(1), page 48
- New Software Features and Enhancements in Cisco NX-OS Release 7.0(4)N1(1), page 48
- New Hardware Features in Cisco NX-OS Release 7.0(4)N1(1), page 48
- New Software Features and Enhancements in Cisco NX-OS Release 7.0(3)N1(1), page 48
- New Hardware Features in Cisco NX-OS Release 7.0(3)N1(1), page 49
- New Software Features and Enhancements in Cisco NX-OS Release 7.0(2)N1(1), page 49
- New Hardware Features in Cisco NX-OS Release 7.0(2)N1(1), page 49
- New Software Features and Enhancements in Cisco NX-OS Release 7.0(1)N1(1), page 49
- New Hardware Features in Cisco NX-OS Release 7.0(1)N1(1), page 50

New Software Features and Enhancements in Cisco NX-OS Release 7.3(14)N1(1)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.3(14)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.3(13)N1(1)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.3(13)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.3(12)N1(1)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.3(12)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.3(11)N1(1)

Secure Erase

The Secure Erase feature is introduced to erase all customer information for Nexus 5600 series switches from Cisco NX-OS Release 7.3(11)N1(1).

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

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

New Hardware Features in Cisco NX-OS Release 7.3(11)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.3(10)N1(1)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.3(10)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.3(9)N1(1)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.3(9)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.3(8)N1(1)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.3(8)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.3(7)N1(1b)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.3(7)N1(1b)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.3(7)N1(1a)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.3(7)N1(1a)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.3(7)N1(1)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.3(7)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.3(6)N1(1)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.3(6)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.3(5)N1(1)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.3(5)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.3(4)N1(1)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.3(4)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.3(3)N1(1)

There are no new software features in this release. The following CLI is introduced in this release:

hardware v6-ns ll-gl-ucast-enable

Note For the **hardware v6-ns ll-gl-ucast-enable** command to become functional, you need to clear the IPv6 routes, using the **clear ipv6 route vrf all*** command after configuring the **hardware v6-ns ll-gl-ucast-enable** command.

RMAC Learning

Starting with Cisco NX-OS Release 7.3(3)N1(1), RMAC Learning feature is also supported on FabricPath VLANs with the knob **mac address-table router-mac learn-enable**.

New Hardware Features in Cisco NX-OS Release 7.3(3)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.3(2)N1(1)

Cisco NX-OS Release 7.3(2)N1(1) includes bug fixes and the following software features and enhancements:

- Soft Reload, page 26
- Auto Negotiation, page 27

Soft Reload

The Soft Reload feature provides a best effort mechanism for a switch to gracefully be brought up with minimal impact to production traffic when a process crash occurs. You can also use the **soft-reload** command to trigger a manual soft reload of the switch.

For more information about the Soft Reload feature, refer to the *Cisco Nexus 5600 Series NX-OS Security Configuration Guide, Release 7.x*.

Auto Negotiation

The following commands are introduced on the Cisco Nexus 2000 Series Fabric Extenders:

- The **no negotiation auto** command is enabled on the Cisco Nexus 2232PP, 2248PQ, and 2348UPQ Fabric Extenders.

Note You can disable auto negotiation with a 1-Gigabit Ethernet SFP-based interface, using the **no negotiation auto** command in global configuration mode.

- The **speed 100** command is enabled on the Cisco Nexus 2348UPQ Fabric Extender's GLC-T SFP module to support 100 megabit speed for the SFP module.
- The **speed auto 100** command is enabled on the Cisco Nexus 2248TP-E Fabric Extender to advertise 100 megabit speed during the auto negotiation in the FEX.

New Hardware Features in Cisco NX-OS Release 7.3(2)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.3(1)N1(1)

There are no new features for this release. Cisco NX-OS Release 7.3(1)N1(1) includes the following programmable fabric enhancements:

- vPC Convergence
- vPC Orphan Port Command
- eBGP Underlay Support

For details, refer to the *Cisco Programmable Fabric with VXLAN BGP EVPN Release Notes*.

New Hardware Features in Cisco NX-OS Release 7.3(1)N1(1)

Cisco NX-OS Release 7.3(1)N1(1) supports the following new hardware:

QSFP-4X10G-LR-S

New Software Features and Enhancements in Cisco NX-OS Release 7.3(0)N1(1)

Cisco NX-OS Release 7.3(0)N1(1) includes bug fixes and the following software features and enhancements:

- Lightweight DHCPv6 Relay Agent (LDRA), page 29
- Fiber Channel Support on Cisco Nexus 2348UPQ with N5600 Switches as Parent, page 29
- N5672UP-16G, page 29

- Implicit Bind vFC, page 29
- LACP Fast Hello, page 29
- Enhancements to CB-QoS-MIB, page 29
- L3 over vPC, page 30
- 63-Character Hostname, page 30
- EXEC Banner, page 30
- 128-Character VLAN Name, page 30
- Login Block Per User, page 30
- VRRPv3 Enablement, page 30
- GIR Enhancement, page 30
- PIM SSM with vPC, page 30
- Netconf Enhancements, page 31
- Reserved VLAN Range, page 31
- L3 FEX Scale Enhancement, page 31
- Runtime Protection as part of CSDL (X-SPACE), page 31
- Product Security Baseline (PSB) Enhancements, page 31
- Product Security Baseline (PSB) 5.0 Passphrase Enhancements, page 32
- Support for Usernames Starting with _(underscore), page 32
- Chef and Puppet Support, page 32
- SHA-512 Algorithm Support for Verifying OS, page 32
- NTP Authentication Key Length Enhancement, page 32
- VXLAN Leaf Switching/Routing, page 33
- VXLAN Border Leaf/Border Spine Switching/Routing, page 33
- VXLAN Fabric OAM, page 33
- LLDP Auto-configuration Trigger, page 33
- Per-Port Auto-configuration Trigger, page 33
- VM Tracker Auto-configuration Trigger, page 33
- VXLAN (L2/L3 gateway and BGP EVPN), page 33
- ACL-Object Group, page 34
- Standards-based BGP EVPN and VXLAN, page 34

Note When you upgrade from an older NX-OS release to Cisco NX-OS release 7.3(0)N1(1), then an additional configuration line, **no lacp suspend-individual**, is seen in the **show** command output of the **show running-config interface port-channel** *number* command. See CSCut55084 for more details.

Lightweight DHCPv6 Relay Agent (LDRA)

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.

Fiber Channel Support on Cisco Nexus 2348UPQ with N5600 Switches as Parent

Cisco Nexus 2348UPQ Fabric Extender (FEX) supports native Fiber Channel (FC) ports. You can convert and use the HIF ports as FC ports. You can configure the HIF ports to run 2, 4, 8, or 16 Gigabit fibre channel (FC). HIF ports are unified ports that enable a combination of 1-Gigabit or 10-Gigabit Ethernet and 2-Gigabit, or 4-Gigabit, or 8-Gigabit, or 16-Gigabit FC interfaces.

N5672UP-16G

The Cisco Nexus 5672UP-16G Switch is a 1RU 2-,4-, 8-, and 16-Gbps Fibre Channel and 10 and 40 Gigabit Ethernet (40-Gbps on uplink and network-facing ports) switch offering wire-speed performance for up to twenty-four 16-Gbps Fibre Channel or seventy-two 10 Gigabit Ethernet ports (using QSFP breakout cables). The Cisco Nexus 5672UP-16G offers 48 fixed 1 and 10 Gigabit Ethernet ports, of which the last 24 ports (highlighted in orange on the chassis for easy identification) are unified ports that support 16-, 8-, 4-, and 2-Gbps Fibre Channel. All 48 fixed ports support classical Ethernet and FCoE.

Implicit Bind vFC

This feature enables you to create a virtual Fibre Channel (vFC), and implicitly bind it to an Ethernet interface or a port-channel using a single command. You must make sure that the vFC identifier matches the Ethernet interface or port-channel identifier. The Ethernet interface can be a module (slot/port) or a Fabric Extender (FEX) interface (chassis/slot/port).

LACP Fast Hello

This feature is enhanced to change the LACP short-timeout value for the **lacp fast rate** command to modify the duration of the LACP Fast Rate timeout. Earlier to this enhancement, even when the rate is set to fast (1 second), the timeout was still 15 seconds. This enhancement introduces a configurable short-timeout with a range of 3 to 15 seconds.

Enhancements to CB-QoS-MIB

Beginning with Cisco NX-OS Release 7.3(0)N1(1), the following cbQoSMIB tables are also supported by QoS policies:

- cbQosClassMapStats
- cbQosMatchStmtStats
- cbQosQueueingStats

L3 over vPC

Beginning with Cisco NX-OS Release 7.3(0)N1(1), a layer 3 device can form peering adjacency between both the vPC peers in a vPC domain. Traffic sent over the peer link will not have TTL decremented. The L3 device can form peering adjacency with both vPC peers. This enhancement is not applicable for vPC+ and is applicable only for unicast (not multicast).
Note that L3 over vPC+ is supported on Cisco Nexus 5600 switches from Cisco Nexus 7.0 release.

63-Character Hostname

Starting with Cisco NX-OS Release 7.3(0)N1(1), the character limit for a switch name and a host name is increased from 32 to 63 alphanumeric characters.

EXEC Banner

Starting with Cisco NX-OS Release 7.3(0)N1(1), the EXEC banner is displayed after a user logs in to a switch. This banner can be used to post reminders to the network administrators.

128-Character VLAN Name

Beginning with Cisco NX-OS Release 7.3(0)N1(1), the length of a VLAN name that you can configure has been increased from 32 to 128 characters.

Login Block Per User

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

VRRPv3 Enablement

VRRP version 3 (VRRPv3) enables a group of switches to form a single virtual switch to provide redundancy and reduce the possibility of a single point of failure in a network. The LAN clients can then be configured with the virtual switch as their default gateway.

GIR Enhancement

Starting with Cisco NX-OS Release 7.3(0)N1(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.
You can use GIR to perform maintenance and software upgrade of the switches and the connected FEXs. A FEX group is added to optimize the procedure to bring up or take down the FEX.

PIM SSM with vPC

Starting with Cisco NX-OS Release 7.3(0)N1(1), PIM SSM traffic is supported.

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. Cisco NX-OS Release supports the following capabilities in NETCONF on Nexus 5000 and 6000 platforms:

- get-config
- copy-config
- validate
- Enhancements in *edit-config* to support Default Operation and Operations (Actions); Rollback on Error, Stop on Error and Continue on Error; Candidate config.
- commit
- lock
- unlock
- Logging of all the Netconf operations and its status in syslog.

Reserved VLAN Range

Starting with Cisco NX-OS Release 7.3(0)N1(1), the number of reserved VLANs has been increased from 80 to 82. The VLAN range is from 3968 to 4049. The two new VLANs are 4048 and 4049.

L3 FEX Scale Enhancement

The L3 FEX support for N5696Q has increased from 24 to 32 with this release. For more details, refer to the *Verified Scalability guide for Cisco NX-OS Release 7.3(0)N1(1).*

Runtime Protection as part of CSDL (X-SPACE)

The general category of runtime protections describes many technologies and techniques. Runtime protections provide increased resiliency to a product while it is running, typically allowing the software to detect and correct certain types of undesirable behavior, or allowing the product to terminate or restart to regain its integrity. These technologies help defend against malicious software gaining a foothold in a system.

  - No-Execute (X-SPACE)—Marks certain areas of memory as “no execute”, that is, it cannot be executed on the CPU. This is normally enabled on areas of memory that are writable, thus preventing an attacker from writing memory during exploitation of a vulnerability, and then subsequently executing the written data. The internal program name in Cisco is X-Space.

X-SPACE cannot be disabled by the customer and has no impact on the normal functioning of the Cisco Nexus 5000/6000 switches.

Product Security Baseline (PSB) Enhancements

Beginning with Cisco NX-OS Release 7.3(0)N1(1), as part of the PSB 5.0 mandatory requirements adherence, the following password authentication commands were introduced:

- **change-password**—Non-admin users can use the **change-password** command to authenticate with the old password and then enter the new password.

- **password secure-mode**—The **password secure-mode** command is enabled by default; non-admin users must use the old password for authentication before changing the password. Admin users can disable the password using the **no password secure-mode** command and then change the password without authenticating with old password.
- **show password secure-mode**—This command displays if secure-mode is enabled or not.

Product Security Baseline (PSB) 5.0 Passphrase Enhancements

Beginning with Cisco NX-OS Release 7.3(0)N1(1), as part of the PSB 5.0 mandatory requirements adherence, the following PSB passphrase enhancements were introduced:

- Passphrase time values—With every username command (except 'admin'), there is a username passphrase configuration command, which lists the lifetime, warn time, and grace time of the passphrase.
- Lock user-account—An administrator can lock or unlock any user account using the **username** *username* **lock-user-account** and **unlock locked-users** commands. The **show locked-users** command displays all the locked users.
- Invalid username logging—The administrator can ensure non-logging or logging of invalid usernames in logs during an authentication failure. By default, invalid usernames during an authentication failure are not logged.

Support for Usernames Starting with _(underscore)

Effective from Cisco NX-OS release 7.3(0)N1(1), usernames starting with _(underscore) is supported.

Chef and Puppet Support

Starting from Cisco NX-OS release 7.3(0)N1(1), Cisco Nexus 5600 and Cisco Nexus 6000 series switches will support open agents, such as Chef and Puppet. 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.

SHA-512 Algorithm Support for Verifying OS

Beginning with Cisco NX-OS Release 7.3(0)N1(1), support for SHA-512 algorithm has been added. The **show file** *filename* command will display an option to calculate the sha512sum and the **show file** *bootflash:file* **sha512sum** command will display the sha512 checksum for the input file.

NTP Authentication Key Length Enhancement

Beginning with Cisco NX-OS Release 7.3(0)N1(1), you can use up to 32 alphanumeric characters for the MD5 string.

VXLAN Leaf Switching/Routing

These features describe the functioning of the VXLAN programmable 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/decapsulating VXLAN packets from/to the end hosts. VTEPS also perform Integrated Route/Bridge (IRB), in that 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 handoff scenarios include classical ethernet handoff for layer 2, and handoff to MPLS L3VPN and LISP enabled networks.

VXLAN 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.

LLDP Auto-configuration Trigger

Auto-configuration for bare metal severs provides a touchless orchestration to dynamically allocate or deallocate resources for every tenant. LLDP auto-configuration trigger can be enabled using the **lldp fabric auto-config** command.

Per-Port Auto-configuration Trigger

For auto-configuration, interfaces connecting to the host or server workloads must be configured to specify the desired auto-configuration trigger. By default, auto-configuration trigger is not enabled on the interface. The auto-configuration trigger must be explicitly configured on the interface and only one auto-configuration trigger can be configured per interface. The per-port auto-configuration trigger can be configured by using the **encapsulation dynamic {dot1q | vdp | lldp | vmtracker}** command.

VM Tracker Auto-configuration Trigger

VM Tracker connects with VMware vCenter and collects information about the VMs that are connected to each host. VM Tracker auto-configuration trigger can be enabled using the **vmtracker fabric auto-config** command.

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 5600 series switch acting as leaf switch (L2/L3 Gateway with Distributed Anycast Gateway and vPC) border-leaf switch (L2/L3 Gateway, LISP, MPLS, VRF-lite, and Classic Ethernet Layer2 with and without vPC) and spine switch with and without route-reflector. For VXLAN multi-destination traffic, bidirectional PIM is required.

ACL-Object Group

ACL-Object group feature enables you to create a rule, where you can specify the object groups instead of IP addresses or ports. Using object groups while configuring IPv4 or IPv6 ACLs can help reduce the complexity of updating ACLs when you want to add or remove addresses or ports from the source or destination of rules. For example, if three rules are referencing the same IP address group object, you can add an IP address to the object instead of changing all the three rules.

Standards-based BGP EVPN and VXLAN

For details, refer to the *Cisco Programmable Fabric with VXLAN BGP EVPN Release Notes*.

New Hardware Features in Cisco NX-OS Release 7.3(0)N1(1)

Cisco NX-OS Release 7.3(0)N1(1) supports the following new hardware:

- Cisco Nexus 5672UP-16G switch (N5K-C5672UP-16G).
- Cisco Nexus 2348TQ-E FEX (N2K-C2348TQ-E).
- Cisco Nexus 2248PQ support for CVR-QSFP-SFP10G (FET-10G, SFP-10G-SR, SFP-10G-LR, SFP-10G-ER, AOC).

New Software Features and Enhancements in Cisco NX-OS Release 7.2(1)N1(1)

NX-OS Patching

NX-OS patching 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.
- Only 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 the process to be patched cannot be restarted, then the patch will be deployed either by reload or ISSU and on the other hand, software can be patched simply by restarting the process for process-restart patch.

Behavior Change in LACP Suspend-Individual

This release has the following behavior change:
When you upgrade from an older NX-OS release to Cisco NX-OS release 7.2(1)N1(1), then an additional configuration line, **no lacp suspend-individual**, is seen in the **show** command output of the **show running-config interface port-channel** *number* command. See CSCut55084 for more details.

New Hardware Features in Cisco NX-OS Release 7.2(1)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.2(0)N1(1)

Cisco NX-OS Release 7.2(0)N1(1) includes bug fixes and the following software features and enhancements:

- Secure Login Enhancements, page 35
- Auto-Config: Support for Routable Loopback Address, page 36
- Extend DHCP Server Support, page 36
- LLDP Support for VM Tracker, page 36
- PoAP Diagnostics, page 36
- NX-API Support, page 36
- Dynamic VLAN Based on MAC-Based Authentication (MAB), page 36
- NTP over IPv6 Support, page 37
- QoS ACL Statistics Per Entry, page 38
- Shared Buffer QoS Command, page 37
- vIP HSRP Enhancement, page 37
- QoS Drop Counter History, page 37
- FEX HIF as SPAN Destination, page 37
- VTPv3/VTP Pruning, page 37
- ACL-Based QoS Classification Offload, page 37
- Queue Limit Change, page 38
- Auto-Config: Logging of Profile Instantiation for Compliance and Accounting, page 38
- Border Leaf Conversational Learning, page 38
- Four-Port vPC, page 38
- Egress Multicast Buffering, page 38
- RMAC Learning, page 38
- Behavior Change in vn-segment Configuration, page 39

Secure Login Enhancements

The following requirements are supported for Cisco NX-OS release 7.2(0)N1(1):

- Configuring Login Parameters (Secure Login feature)
- Restricting Sessions Per User (Per User Per login)
- Password should use algorithm (Hash or Symmetric-key) for secure writing (SHA256 password hashing).
- Password length configuration (Min, Max)
- Enabling the password prompt for user name.
- Configuring Shared Key Value for using RADIUS/TACACS.

Auto-Config: Support for Routable Loopback Address

This feature provides support for the VRF profile to be updated on the leaf resulting in the loopback routable IP address being auto-configured under that vrf as well as advertised using MP-BGP to all leaf nodes.

Extend DHCP Server Support

This feature enables you to have common DHCP servers (for example, Microsoft Windows) for IP address assignments within dynamic fabric automation (DFA).

LLDP Support for VM Tracker

Starting with Cisco NX-OS release 7.2(0)N1(1), Link Layer Discovery Protocol (LLDP) is supported on VM Tracker.

PoAP Diagnostics

PoAP failure can be detected with locator LED. When the PoAP process starts, the locator-LED will flash the pattern 21 (flashing twice, short pause, flashing once, long pause) to indicate that PoAP is in progress.

NX-API Support

On Cisco Nexus devices, command-line interfaces (CLIs) are run only on the device. NX-API improves the accessibility of these CLIs by making them available outside of the switch by using HTTP/HTTPS. You can use this extension to the existing Cisco Nexus CLI system on the Cisco Nexus 5000 and 6000 Series devices. NX-API supports show commands and configurations.

NX-API supports JSON-RPC.

Dynamic VLAN Based on MAC-Based Authentication (MAB)

The Cisco Nexus 5000 and 6000 series switches supports dynamic VLAN assignment. After the 802.1x authentication or MAB is completed; before bringing up the port, you may want to (as part of authorization) allow the peer/host to be placed into a particular VLAN based as a result of the authentication. The RADIUS server typically indicates the desired VLAN by including tunnel attributes within the Access-Accept message. This procedure of getting the VLAN an binding it to the port constitutes to Dynamic VLAN assignment.

NTP over IPv6 Support

The Network Time Protocol (NTP) is a protocol designed to time-synchronize a network of machines. IPv6 support is added for NTP in the Nexus 5000 and 6000 series switches. This allows IPv6 NTP servers/peers to be configured for time synchronization.

ACL-Based QoS Classification Offload

The ACL-based QoS Policy Offload is supported on the N2348TQ and N2348UPQ Fabric Extender 6x40G QSFP 48x10G SFP+ FEX.

Shared Buffer QoS Command

The **queue-limit** *queue-size* **bytes** is extended to set the queue limit size for 40G interfaces also.

vIP HSRP Enhancement

This feature is enhanced to support the following:

- Support for HSRP VIP configuration to be in a different subnet than that of interface subnet.
- Enhanced ARP to source with VIP from SUP for hosts when hosts are in VIP subnet or referenced by static route to VLAN configuration.
- Periodic ARP synchronization support to VPC peer.
- Allows use of the VIP address as L3 source address and gateway address for all communications with DHCP server.

QoS Drop Counter History

To correlate the QoS drops with the potential buffer usage, a new set of commands are introduced. The drop history on each interface is recorded and implemented in the following commands:

- **show hardware internal bigsur port** *interface* **qos-drop-history brief**
- **show hardware internal bigsur all-ports qos-drop-history brief**
- **show hardware internal bigsur port** *interface* **qos-drop-history details**
- **clear hardware internal bigsur port** *interface* **qos-drop-history details**

FEX HIF as SPAN Destination

This feature enables HIF and Virtual Ethernet (Veth) ports as SPAN destination.

VTPv3/VTP Pruning

VTP Version 3 (VTPv3) was introduced in Cisco NX-OS release 7.2(0)N1(1) and has the following features:

- Provides interoperability with switches configured with VTP version 1 or 2.
- Allows only the primary server to make VTP configuration changes.
- Supports 4K VLANs.

- Permits feature-specific primary servers. A switch can be a primary server for a specific feature database such as MST or for the entire VLAN database.
- Provides enhanced security with hidden and secret passwords.
- Provides interoperability with private VLANs (PVLAN). PVLANs and VTPs are no longer mutually exclusive.

QoS ACL Statistics Per Entry

This feature supports QoS ACL statistics per-entry to verify per QoS class-map classification. Counters are shown per ACE for QoS ACL, and statistics per QoS ACL entry can be viewed.

Queue Limit Change

Cisco Nexus N2348UPQ Fabric Extender (48x10G SFP+ 6x40G QSFP Module) is supported from Cisco NX-OS release 7.2(0)N1(1).

Auto-Config: Logging of Profile Instantiation for Compliance and Accounting

The enhanced syslogs are generated when profile apply, profile un-apply, and profile refresh are performed and it contains details about the host that triggers the profile events.

Border Leaf Conversational Learning

You can enable conversational learning on all leaf nodes by using the **fabric forwarding conversational-learning all** command. For this 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.

Four-Port vPC

In Cisco Nexus 5600 and 6000 Series Switches, the 4-port vPC provides the capability to associate the vFC interface to an individual member of a port-channel that has multiple port members. This feature is supported only for Cisco Nexus 2300 Series switches that are connected to Cisco Nexus 5600 and 6000 Series switches.

Egress Multicast Buffering

The Cisco Nexus 5600 and 6000 Series Switches support Egress Multicast Buffering, which is a process that provides additional cells to multicast traffic at Egress. When there is heavy multicast traffic at Egress, buffer space (cells) is borrowed from the unicast pool. The pool provides a specific number of cells to enhance the traffic and minimize traffic drops at Egress side.

RMAC Learning

On Cisco Nexus 5600 and 6000 series switches, the RMAC Learning feature allows the default MAC address (RMAC) of a VLAN interface to be dynamically learned on another VLAN interface over a bridged interface.

Behavior Change in vn-segment Configuration

Beginning with Cisco NX-OS Release 7.2(0)N1(1), modifying vn-segment of a VLAN with existing vn-segment configuration is disabled. From this release onwards, you must remove the existing vn-segment configuration under the VLAN, and then configure the new vn-segment.

New Hardware Features in Cisco NX-OS Release 7.2(0)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.1(5)N1(1b)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.1(5)N1(1b)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.1(5)N1(1)

There are no new software features for this release.

New Hardware Features in Cisco NX-OS Release 7.1(5)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.1(4)N1(1)

There are no new features for this release. Cisco NX-OS Release 7.1(4)N1(1) includes the following enhancements:

Serviceability Enhancements

Sup-region TCAM Monitoring

The Sup-region Ternary Content-Addressable Memory (TCAM) Monitoring feature is a monitoring mechanism that enables detection, reporting, and correction of sup-region TCAM entry corruption.

The following Sup TCAM commands are introduced in this release:

- **hardware sup-tcam monitoring enable**
- **hardware sup-tcam monitoring timer-expiry**
- **hardware sup-tcam monitoring trigger-detection**

- **show platform afm info sup-tcam monitoring info**
- **show platform afm info tcam access stats**

For more information about sup-region TCAM monitoring, refer to the *Cisco Nexus 5600 Series NX-OS Security Configuration Guide, Release 7.x*.

Forwarding Manager PSS Consistency Checker

To detect any inconsistencies in the Forwarding Manager Persistent Storage Service (PSS), use the following Forwarding Manager PSS consistency checkers before performing a nondisruptive upgrade:

- **show platform fwm info pss runtime_consistency**
- **show platform fwm info pss runtime_consistency_report**

For more information about Forwarding Manager PSS consistency checker, refer to the *Cisco Nexus 6000 Troubleshooting guide*.

Forwarding Manager L2MP Hardware Software Consistency Checker

The Forwarding Manager Layer 2 Multipathing (L2MP) hardware and software consistency checker provides inputs on inconsistencies between the L2MP data structures and the corresponding hardware–programmed entries. Use the following Forwarding Manager L2MP hardware–software consistency checkers to view the inconsistencies:

- **show consistency-checker l2mp**
- **show consistency-checker l2mp module**

For more information about Forwarding Manager L2MP hardware–software consistency checker, refer to the *Cisco Nexus 6000 Troubleshooting Guide*.

FEX ISSU Upgrade Enhancement

The **install fex** *fex-id* command is introduced to address a Fabric Extender's nondisruptive upgrade failure during a regular upgrade.

For more information about FEX ISSU upgrade, refer to the *Cisco Nexus 5000/6000 Series NX-OS Fabric Extender Command Reference Guide*.

From Cisco NX-OS Release 7.1(4)N1(1) onwards, if one or more FEXs fail during a nondisruptive upgrade process, the install process will display the upgrade failure of that particular FEX, but will continue the upgrade process for other FEXs.

Link Debounce Time Enhancement

The **link debounce link-up time** command is introduced to configure the debounce linkup time for an interface.

For more information about link debounce, refer to the *Cisco Nexus 5600 Series NX-OS Interfaces Command Reference*.

Firmware Version Upgrade

On a Cisco Nexus 56128P switch with an N56-M24UP2Q module, the firmware version is upgraded from 1.15 to 1.16. For more information on Version 1.15 issue, refer to the CSCva12553 caveat.

To upgrade the firmware version, perform the following steps:

1. Load Cisco NX-OS Release 7.1(4)N1(1) with firmware Version 1.16 on a switch and reload the switch.
2. Power off and power on the module for the new version to start working.

Hardware Unicast VOQ Enhancement

The **hardware unicast voq-limit-sup** command is introduced to limit the number of control packets that can be buffered on a supervisor before the packets can be sent to egress ports. The **hardware unicast voq-limit-sup** command helps in managing the virtual output queuing (VOQ) to prevent one blocked receiver from affecting traffic that is being sent to other noncongested receivers (head-of-line blocking).

For more information about the **hardware unicast voq-limit-sup** command, refer to the *Cisco Nexus 5600 Series NX-OS QoS Command Reference*.

New Hardware Features in Cisco NX-OS Release 7.1(4)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.1(3)N1(2)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.1(3)N1(2)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.1(3)N1(1)

There are no new software features in this release.

Note Although this release has no new features, the following is a changed behavior:
When you upgrade from an older NX-OS release to Cisco NX-OS release 7.1(3)N1(1), then an additional configuration line, **no lacp suspend-individual**, is seen in the **show** command output of the **show running-config interface port-channel** *number* command. See CSCut55084 for more details.

New Hardware Features in Cisco NX-OS Release 7.1(3)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.1(2)N1(1)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.1(2)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.1(1)N1(1)

Cisco NX-OS Release 7.1(1)N1(1) includes bug fixes and the following software features and enhancements:

- Flex link Support, page 42
- IEEE 1588v2 PTP, page 42
- ERSPAN v3 with PTP Timestamp, page 42
- CoPP (Control Plane Policing) Extended Rate, page 43
- Class-Based Quality-of-Service MIB (cbQoSMIB), page 43
- Intelligent Traffic Director (ITD), page 43
- Remote Integrated Service Engine (RISE), page 43
- 100 Mbps Support on 2348TQ and 2332TQ, page 43

Flex link Support

Flex links are a pair of a Layer 2 interfaces (switch ports or port channels) where one interface is configured to act as a backup to the other. The feature provides an alternative solution to the Spanning Tree Protocol (STP). You can disable STP and still retain basic link redundancy. Flex links are typically configured in service provider or enterprise networks where customers do not want to run STP on the switch. If the switch is running STP, flex links are not necessary because STP already provides link-level redundancy or backup. Flex Links are supported only on Layer 2 ports and port channels, not on VLANs or on Layer 3 ports.

IEEE 1588v2 PTP

PTP is a time synchronization protocol for nodes distributed across a network. Its hardware timestamp feature provides greater accuracy than other time synchronization protocols such as the Network Time Protocol (NTP). PTP is a distributed protocol that specifies how real-time PTP clocks in the system synchronize with each other.

Note PTP is not supported on 100G CLEM.

ERSPAN v3 with PTP Timestamp

Encapsulated remote switched port analyzer (ERSPAN) is used to transport mirrored traffic in an IP network. ERSPAN supports source ports, source VLANs, and destinations on different switches, which provide remote monitoring of multiple switches across your network. ERSPAN uses a generic routing encapsulation (GRE) tunnel to carry traffic between switches.

ERSPAN consists of an ERSPAN source session, routable ERSPAN GRE-encapsulated traffic, and an ERSPAN destination session. You separately configure ERSPAN source sessions and destination sessions on different switches.

There are two types of ERSPAN—Type II (default) and type III. Type III supports all of ERSPAN type II features and adds the following enhancements:

- Provides timestamp information in the ERSPAN Type III header that can be used to calculate the packet latency among edge, aggregate, and core switches.
- Identifies possible traffic sources using the ERSPAN Type III header fields.
- ERSPAN Type III provides configurable switch IDs that can be used to identify traffic flows across multiple switches.

CoPP (Control Plane Policing) Extended Rate

Beginning with Cisco Nexus 7.1(1)N1(1) release, you can configure an extended CoPP committed information rate (CIR) limit of up to 61,440 Kbps for each customized CoPP profile.

Class-Based Quality-of-Service MIB (cbQoSMIB)

This feature provides the Simple Network Management Protocol (SNMP) MIB that enables retrieval of class-map and policy-map configuration and statistics.

Intelligent Traffic Director (ITD)

Intelligent Traffic Director (ITD) is an intelligent, scalable clustering and load-balancing engine that addresses the performance gap between a multi-terabit switch and gigabit servers and appliances. The ITD architecture integrates Layer 2 and Layer 3 switching with Layer 4 to Layer 7 applications for scale and capacity expansion to serve high-bandwidth applications.

ITD provides adaptive load balancing to distribute traffic to an application cluster. With this feature on the Cisco Nexus 5000 Series switches, you can deploy servers and appliances from any vendor without a network or topology upgrade.

Remote Integrated Service Engine (RISE)

Cisco RISE is an architecture that logically integrates an external (remote) service appliance, such as a Citrix NetScaler Application Delivery Controller (ADC), so that the appliance appears and operates as a service module (remote line card) within the Cisco Nexus switch. The Cisco NX-OS software in which RISE is supported supports the Cisco Nexus 5500, 5600, and 6000 Series switches.

100 Mbps Support on 2348TQ and 2332TQ

The Cisco Nexus Release 7.1(1)N1(1) supports 100 Mbps speed on the host interfaces of Cisco Nexus 2348TQ and 2332TQ.

To see the autonegotiation matrix details for the N2K-C2348TQ-10GE and N2K-C2332TQ-10GE fabric extenders, refer to the section titled *Speed and Duplex Mode* in the “Configuring the Fabric Extenders” chapter of *Cisco Nexus 5600 Series NX-OS Layer 2 Switching Configuration Guide, Release 7.x*.

New Hardware Features in Cisco NX-OS Release 7.1(1)N1(1)

Cisco NX-OS Release 7.1(1)N1(1) supports the following new hardware:

- Cisco Nexus N5648Q—Support for 48 QSFP 40G ports. It has 24 fixed QSFP ports and support for two GEM slots that can support an additional 12 QSFP ports per GEM slot.
- Cisco Nexus N2332TQ—FEX supporting 32 10GBaseT host ports and 4 QSFP+ network ports.

New Software Features and Enhancements in Cisco NX-OS Release 7.1(0)N1(1b)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.1(0)N1(1b)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.1(0)N1(1a)

Cisco NX-OS Release 7.1(0)N1(1a) includes bug fixes and the following software features and enhancements:

- BPDU Guard Enhancement, page 44
- CTS with FabricPath, page 45
- Dynamic ARP Inspection Enhancement, page 45
- IPv6 vPC/vPC+ Keepalive Support, page 45
- Graceful Insertion and Removal (GIR) Enhancement, page 45
- ISSU Modifications, page 45
- Long Distance Support, page 45
- MET Sharing, page 45
- Open Management Infrastructure, page 45
- Password Length Enhancement, page 45
- Syslog Message as SNMP Trap, page 46
- Unified Fabric Solution (previously called Dynamic Fabric Automation (DFA)), page 46
- VLAN Translation, page 46
- VM Tracker, page 46
- VXLAN Bridging and Routing, page 46

BPDU Guard Enhancement

BPDU Guard can be can be activated on disallowed edge trunk VLANs. This is done by configuring both sides of the link as either trunks or access interfaces.

CTS with FabricPath

The Cisco TrustSec security architecture has been extended to support Cisco FabricPath environments including those using vPC+. CTS packet classification can occur before or as traffic enters the fabric, at which point packet tags are preserved through the fabric for the purpose of applying security policy to the data path.

Dynamic ARP Inspection Enhancement

Dynamic ARP Inspection (DAI) can validate ARP packets against user-configured ARP access control lists (ACLs). DAI can be configured to drop ARP packets when the IP/MAC addresses in the packets are invalid. This is done by configuring ARP-based ACLs.

IPv6 vPC/vPC+ Keepalive Support

IPv6 support for vPC/vPC+ provides IPv6 capabilities for the vPC/vPC+ keepalive from the mgmt0 out-of-band interface and also from the built-in front ports using SVI.

Graceful Insertion and Removal (GIR) Enhancement

Provides the ability to gracefully eject a switch and isolate it from the network so that debugging or an upgrade can be performed. The switch is removed from the regular switching path and put into a maintenance mode. Once maintenance on the switch is complete, you can bring the switch into full operational mode.

ISSU Modifications

In service software updates (ISSUs) are limited to the three previous releases.

Long Distance Support

Long distance support (20 km/10G & 3 km/40G) for FCoE.

MET Sharing

Improves efficiency in the usage of Multicast Expansion Table (MET) entries in the hardware.

Open Management Infrastructure

Open Management Infrastructure (OMI) is no longer supported.

Password Length Enhancement

The following commands have been added to provide the ability to configure the minimum and maximum length of a password:

- **userpassphrase min-length** *length*
- **userpassphrase max-length** *length*

- **show userpassphrase length**

Syslog Message as SNMP Trap

The following features has been added:

- User Interface for Persistent Logging
- Syslog SNMP Traps
- History Logging
- Syslog Message Format

Unified Fabric Solution (previously called Dynamic Fabric Automation (DFA))

This software release is the second release to support enhancements to Cisco's Unified Fabric Solution.

Unified Fabric focuses on simplifying, optimizing, and automating data center fabric environments by offering an architecture based on four major pillars: Fabric Management, Workload Automation, Optimized Networking, and Virtual Fabrics.

Each of these pillars provides a set of modular functions that can be used together, or independently, for ease of adoption of new technologies in the data center environment.

Note Each vPC pair must use different vPC Domain ID within a given fabric. Together with unique Fabric Identifier (per fabric) will ensure unique SOO generated by vPC leaf node throughout entire domain.

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

VLAN Translation

Allows for the merging of separate Layer 2 domains that might reside in a two data centers that are connected through some form of Data Center Interconnect (DCI).

VM Tracker

Supports automatic VLAN provisioning.

VXLAN Bridging and Routing

VXLAN technology provides a mechanism to extend the reachability of virtual segments within a data center and increases scale of number of segments by removing the restriction of 4096 VLANs that can be deployed in a data center. The feature provides the ability to switch traffic in a VXLAN segment as well as route traffic between VXLAN segments as well as between VXLAN and VLAN segments.

New Hardware Features in Cisco NX-OS Release 7.1(0)N1(1a)

Cisco NX-OS Release 7.1(0)N1(1a) supports the following new hardware:

- Cisco Nexus 5624Q switch— (N5K-C5624Q, N5624-B-24Q, N56-M12Q)

- Cisco Nexus 2348TQ FEX— (N2K-C2348TQ-10GE)
- Cisco 100G Line Card Expansion Module—(N5696-M4C)
  - To enable 100G LEM N5696-M4C, the required BIOS version is 2.8.0 or above for EF chassis. If the LEM's BIOS version is lower than 2.8.0, ISSU is required as it facilitates a built-in BIOS update procedure.
  - For EF-CR chassis, the required BIOS version is 2.1.0 or above.
  - For Microcontroller Firmware—The required version is 1.2.0.2 or above for EF-CR chassis and 1.1.0.4 or above for EF chassis.
  - For N5696Q, native support has been added for 100G LEM N5696-M4C.
  - Added support for 100G LEM N5696-M4C with N6004EF chassis. 100G LEM N5696-M4C module must have BIOS version 2.8.0 or above for N6004EF chassis.
- H7 Power Supply Support—support for forward air flow (FAF) (NXA-PHV-1100W) and reverse air flow (RAF) (NXA-PHV-1100W-B) with both AC and DC power source.
- LR4 Optics—WSP-Q40GLR4L (QSFP40G-LR4-LITE)

New Software Features and Enhancements in Cisco NX-OS Release 7.0(8)N1(1)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.0(8)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.0(7)N1(1)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.0(7)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.0(6)N1(1)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.0(6)N1(1)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.0(5)N1(1a)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.0(5)N1(1a)

There are no new hardware features in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.0(5)N1(1)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.0(5)N1(1)

There is no new hardware in this release.

New Software Features and Enhancements in Cisco NX-OS Release 7.0(4)N1(1)

There are no new software features in this release.

New Hardware Features in Cisco NX-OS Release 7.0(4)N1(1)

Cisco NX-OS Release 7.0(4)N1(1) supports the following new hardware:

- Cisco Nexus 5696Q Switch (N5696Q)
- Cisco Nexus 5696Q 40 Gigabit Ethernet Line Card Expansion Module (N5696-M12Q)
- Cisco Nexus 5696Q Unified Port Linecard Expansion Module (N5696-M20UP)
- Cisco Nexus 2348UPQ support for QSA (FET-10G, SFP-10G-SR, SFP-10G-ER)

New Software Features and Enhancements in Cisco NX-OS Release 7.0(3)N1(1)

Cisco NX-OS Release 7.0(3)N1(1) is a maintenance release that includes bug fixes and the following software features and enhancements:

- Dynamic FCoE Over DFA, page 48
- FEX Based ACL Classification, page 49

Dynamic FCoE Over DFA

Dynamic Fibre Channel over Ethernet (FCoE) over DFA enables I/O consolidation. It permits both LAN and SAN traffic to coexist on the same switch and the same wire.

FEX Based ACL Classification

The FEX-based ACL Classification feature uses TCAM resources on a FEX to perform ACL-based packet classification of incoming packets on the switch. When QoS policies are processed on a FEX, the policies are enforced on the switch and on the associated FEX or FEXs.

New Hardware Features in Cisco NX-OS Release 7.0(3)N1(1)

Cisco NX-OS Release 7.0(3)N1(1) supports the following new hardware:

- Cisco Nexus 2348UPQ Fabric Extender (N2K-C2348UPQ)

New Software Features and Enhancements in Cisco NX-OS Release 7.0(2)N1(1)

Cisco NX-OS Release 7.0(2)N1(1) is a maintenance release that includes bug fixes and the following software features and enhancements:

- Buffer Utilization Histogram, page 49

Buffer Utilization Histogram

The Buffer Utilization Histogram feature enables you to analyze the maximum queue depths and buffer utilization in the system in real time.

New Hardware Features in Cisco NX-OS Release 7.0(2)N1(1)

Cisco NX-OS Release 7.0(2)N1(1) supports the following new hardware:

- Cisco Nexus 56128 (N5K-C56128P)
- Cisco Nexus 24x10GE Unified Port + 2xQSFP 40GE (N56-M24UP2Q)

New Software Features and Enhancements in Cisco NX-OS Release 7.0(1)N1(1)

Cisco NX-OS Release 7.0(1)N1(1) is a maintenance release that includes bug fixes and the following software features and enhancements:

- ACL Logging for IPv6 ACLs, page 49
- Dynamic FCoE Using FabricPath, page 50
- Layer 2 CTS Support, page 50

ACL Logging for IPv6 ACLs

The ACL logging feature allows you to monitor IPv6 ACL flows and to log dropped packets on an interface.

Dynamic FCoE Using FabricPath

Dynamic FCoE extends the capability and reliability of storage networks by leveraging FabricPath technology to create logical separation of SAN A and SAN B. FCoE VFCs and Interswitch-Links (ISLs) are dynamically configured, simplifying the multihop FCoE deployments in leaf-spine topologies.

Layer 2 CTS Support

The Cisco TrustSec security architecture builds secure networks by establishing clouds of trusted network devices. Cisco TrustSec also uses the device information acquired during authentication for classifying, or coloring, the packets as they enter the network. This packet classification is maintained by tagging packets on ingress to the Cisco TrustSec network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path.

New Hardware Features in Cisco NX-OS Release 7.0(1)N1(1)

Cisco NX-OS Release 7.0(1)N1(1) supports the following new hardware:

- Cisco Nexus 5672UP N5K-C5672UP
- Cisco Nexus 6004 20UP LEM N6004X-M20UP

Upgrading or Downgrading to a New Release

This section describes the upgrade and downgrade possibilities and BIOS revision for the different Cisco NX-OS 7.x releases.

- Upgrade and Downgrade Guidelines, page 51
- Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(14)N1(1), page 52
- Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(13)N1(1), page 54
- Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(12)N1(1), page 55
- Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(10)N1(1), page 58
- Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(9)N1(1), page 59
- Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(8)N1(1), page 60
- Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(7)N1(1b), page 62
- Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(7)N1(1a), page 63
- Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(7)N1(1), page 64
- Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(6)N1(1), page 65
- Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(5)N1(1), page 66
- Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(4)N1(1), page 67
- BIOS Revision for Cisco NX-OS Release 7.3(1)N1(1), page 68
- BIOS Revision for Cisco NX-OS Release 7.3(0)N1(1), page 68
- Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.2(1)N1(1), page 69
- Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 7.1(5)N1(1b), page 70

- Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.1(5)N1(1), page 70
- BIOS Revision for Cisco NX-OS Release 7.1(4)N1(1), page 71
- Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.0(8)N1(1), page 72
- BIOS Revision for Cisco NX-OS Release 7.0(8)N1(1), page 72

Upgrade and Downgrade Guidelines

The following guidelines apply to Cisco NX-OS Release 7.x for Cisco Nexus devices:

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.

Note If a supported upgrade or downgrade path is not taken, then certain configurations, especially related to unified ports, Fibre Channel (FC) ports, breakout, and FEX may be lost.

Note Upgrading Cisco NX-OS Software by changing the boot-variables and performing a reload is not supported in Cisco Nexus 5000 and 6000 Series Switches. This may result in loss of configuration and forwarding issues.

Note Doing a disruptive upgrade between incompatible images can result in loss of configurations such as unified ports, Fibre Channel (FC) ports, breakout, and FEX configurations, and VLAN database (VTP mode client/server). See CSCul22703 for details.

Note On Cisco Nexus 5672, 56128, and 5696 switches, nondisruptive upgrade may fail and will need manual intervention to recover the systems. See CSCux76799 for details.

Note If you are performing a nondisruptive ISSU from Cisco NX-OS release 7.0(6)N1(1) to 7.0(7)N1(1) and later release, or from Cisco NX-OS release 7.0(6)N1(1) to a 7.1, 7.2, or 7.3 release, then you must reload the switch for the CSCur26244 fix to be effective; alternatively, you must perform a disruptive ISSU.

Note When a switch is connected to Cisco Nexus 2348UPQ, 2348TQ, and 2332TQ Fabric Extender, and if you perform a nondisruptive upgrade to Cisco NX-OS Release 7.0(7)N1(1), 7.1(2)N1(1), 7.2(0)N1(1), or 7.3(0)N1(1) and later, then you must reload the mentioned FEXs after the nondisruptive upgrade for the CSCut90356 fix to be effective; alternatively, you must do a disruptive upgrade for these releases.

Note When you upgrade from an earlier release to Cisco NX-OS releases 7.1(3)N1(1), 7.1(3)N1(2), 7.1(4)N1(1), 7.1(5)N1(1), 7.2(1)N1(1), 7.3(1)N1(1), 7.3(2)N1(1) and later releases with the config-sync feature enabled, changes to the default LACP suspend-individual configuration might cause interface configuration to get locked out. See the bug CSCvh75595 for more details.

Note If you want to upgrade from a release, that is not listed in the "Current Cisco NX-OS Release" column under the "Supported Upgrade and Downgrade Paths for a Cisco NX-OS Release 7.x" section to the latest Cisco NX-OS release version, then you must first upgrade to a release that is listed in the "Current Cisco NX-OS Release" column and then to the latest release version.

Note If you want to upgrade from a release, that is not listed in the "Current Cisco NX-OS Release" column under the "Supported Upgrade and Downgrade Paths for a Cisco NX-OS Release" section to the latest Cisco NX-OS release version, then you must first upgrade to a release that is listed in the "Current Cisco NX-OS Release" column and then to the latest release version.

Note When you upgrade from Cisco NX-OS releases 7.3(3)N1(1), 7.3(2)N1(1), and 7.3(1)N1(1), ensure to upgrade to Cisco NX-OS release 7.3(8)N1(1) and then to Cisco NX-OS release 7.3(13)N1(1).

Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(14)N1(1)

Table 3 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 7.3(14)N1(1). For more information, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.3(14)N1(1)*.

For other 7.3 releases, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide* specific for that release at:

https://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-guides-list.html.

Table 3 Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 7.3(14)N1(1)

Current Cisco NX-OS Release	Upgrade to NX-OS Release 7.3(14)N1(1)	Downgrade from NX-OS Release 7.3(14)N1(1)
7.3(13)N1(1)	Nondisruptive upgrade (ISSU)	Disruptive downgrade[1]
7.3(12)N1(1)		
7.3(11)N1(1)		
7.3(10)N1(1)		
7.3(9)N1(1)		
7.3(8)N1(1)		
7.3(7)N1(1b)		
7.3(7)N1(1a)		
7.3(6)N1(1)		
7.3(5)N1(1)		
7.3(4)N1(1)		
7.3(3)N1(1)		
7.3(2)N1(1)		
7.1(5)N1(1)		
7.1(4)N1(1)		

[1] In-service software downgrade (ISSD) from Cisco NX-OS Release 7.3.x to any earlier releases is not supported. All incompatible configurations will be lost in the target release. Performing a downgrade will also result in loss of certain configurations such as unified ports, breakout, and FEX configurations. See CSCul22703 for details. For more information on restoring the configuration, see the "Restoring the Configuration" section in the *Cisco Nexus 5600 Series Software Upgrade and Downgrade Guide, Release*.

Note If you want to upgrade from a release on Cisco NX-OS release 7.1 train or earlier, you must first upgrade to Cisco NX-OS release 7.3(8)N1(1) and then to 7.3(14)N1(1). If you want to upgrade from a release on Cisco NX-OS release 7.3(4) to 7.3(7b), you must first upgrade to Cisco NX-OS release 7.3(8)N1(1) and then to 7.3(14)N1(1). If you want to upgrade from a release on Cisco NX-OS release 7.3(8) or later, you can upgrade to 7.3(14)N1(1).

Note If you upgrade from an earlier release to Cisco NX-OS release 7.3(2)N1(1), the older BIOS version will be upgraded to the current release BIOS version. For the new BIOS version to take effect, you need to reload the device.

Note If Cisco Nexus 5624Q and 5648Q switches have an older BIOS version, then ISSU to Cisco NX-OS release 7.3(2)N1(1) may be disruptive for some releases. To avoid the disruptive upgrade, upgrade the BIOS version manually before you upgrade the release version. For assistance, please contact the Cisco Technical Assistance Center (TAC).

Starting with Cisco NX-OS Release 7.3(2)N1(1), during a nondisruptive upgrade if any port on a Cisco Nexus switch or a peer switch retries for an errdisable recovery for more than two times, then the port will be brought down, that is, it will not be recovered after two retries. The port will be recovered after the completion of the nondisruptive ISSU.

Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(13)N1(1)

Table 4 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 7.3(13)N1(1). For more information, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.3(13)N1(1)*.

For other 7.3 releases, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide* specific for that release at:

https://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-guides-list.html.

Table 4 Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 7.3(13)N1(1)

Current Cisco NX-OS Release	Upgrade to NX-OS Release 7.3(13)N1(1)	Downgrade from NX-OS Release 7.3(13)N1(1)

7.3(12)N1(1)
7.3(11)N1(1)
7.3(10)N1(1)
7.3(9)N1(1)
7.3(8)N1(1)
7.3(7)N1(1b)
7.3(7)N1(1a)
7.3(6)N1(1)
7.3(5)N1(1)
7.3(4)N1(1)
7.3(3)N1(1)
7.3(2)N1(1)
7.1(5)N1(1)
7.1(4)N1(1)
	Nondisruptive upgrade (ISSU)	Disruptive downgrade[1]

[1] In-service software downgrade (ISSD) from Cisco NX-OS Release 7.3.x to any earlier releases is not supported. All incompatible configurations will be lost in the target release. Performing a downgrade will also result in loss of certain configurations such as unified ports, breakout, and FEX configurations. See CSCul22703 for details. For more information on restoring the configuration, see the "Restoring the Configuration" section in the *Cisco Nexus 5600 Series Software Upgrade and Downgrade Guide, Release*.

Note If you want to upgrade from a release on Cisco NX-OS release 7.1 train or earlier, you must first upgrade to Cisco NX-OS release 7.3(8)N1(1) and then to 7.3(13)N1(1). If you want to upgrade from a release on Cisco NX-OS release 7.3(4) to 7.3(7b), you must first upgrade to Cisco NX-OS release 7.3(8)N1(1) and then to 7.3(13)N1(1). If you want to upgrade from a release on Cisco NX-OS release 7.3(8) or later, you can upgrade to 7.3(13)N1(1).

Note If you upgrade from an earlier release to Cisco NX-OS release 7.3(2)N1(1), the older BIOS version will be upgraded to the current release BIOS version. For the new BIOS version to take effect, you need to reload the device.

Note If Cisco Nexus 5624Q and 5648Q switches have an older BIOS version, then ISSU to Cisco NX-OS release 7.3(2)N1(1) may be disruptive for some releases. To avoid the disruptive upgrade, upgrade the BIOS version manually before you upgrade the release version. For assistance, please contact the Cisco Technical Assistance Center (TAC).

Starting with Cisco NX-OS Release 7.3(2)N1(1), during a nondisruptive upgrade if any port on a Cisco Nexus switch or a peer switch retries for an errdisable recovery for more than two times, then the port will be brought down, that is, it will not be recovered after two retries. The port will be recovered after the completion of the nondisruptive ISSU.

Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(12)N1(1)

Table 5 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 7.3(12)N1(1). For more information, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.3(12)N1(1)*.

For other 7.3 releases, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide* specific for that release at:

https://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-guides-list.html.

Table 5 Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 7.3(12)N1(1)

Current Cisco NX-OS Release	Upgrade to NX-OS Release 7.3(12)N1(1)	Downgrade from NX-OS Release 7.3(12)N1(1)

7.3(11)N1(1)
7.3(10)N1(1)
7.3(9)N1(1)
7.3(8)N1(1)
7.3(7)N1(1b)
7.3(7)N1(1a)
7.3(6)N1(1)
7.3(5)N1(1)
7.3(4)N1(1)
7.3(3)N1(1)
7.3(2)N1(1)
7.1(5)N1(1)
7.1(4)N1(1)
	Nondisruptive upgrade (ISSU)	Disruptive downgrade[1]

[1] In-service software downgrade (ISSD) from Cisco NX-OS Release 7.3.x to any earlier releases is not supported. All incompatible configurations will be lost in the target release. Performing a downgrade will also result in loss of certain configurations such as unified ports, breakout, and FEX configurations. See CSCul22703 for details. For more information on restoring the configuration, see the "Restoring the Configuration" section in the *Cisco Nexus 5600 Series Software Upgrade and Downgrade Guide, Release*.

Note You cannot upgrade non-disruptively to Cisco NX-OS Release 7.3(12)N1(1) from Cisco NX-OS Release 7.3(7)N1(1) because of the issue due to CSCvt58479.

Note If you want to upgrade from a release on Cisco NX-OS release 7.1 train or earlier, you must first upgrade to Cisco NX-OS release 7.1(4)N1(1) and then to 7.3(12)N1(1). If you want to upgrade from a release on Cisco NX-OS release 7.2 train or earlier, you must first upgrade to Cisco NX-OS release 7.3(2)N1(1) and then to 7.3(12)N1(1).

Note If you upgrade from an earlier release to Cisco NX-OS release 7.3(2)N1(1), the older BIOS version will be upgraded to the current release BIOS version. For the new BIOS version to take effect, you need to reload the device.

Note If Cisco Nexus 5624Q and 5648Q switches have an older BIOS version, then ISSU to Cisco NX-OS release 7.3(2)N1(1) may be disruptive for some releases. To avoid the disruptive upgrade, upgrade the BIOS version manually before you upgrade the release version. For assistance, please contact the Cisco Technical Assistance Center (TAC).

Starting with Cisco NX-OS Release 7.3(2)N1(1), during a nondisruptive upgrade if any port on a Cisco Nexus switch or a peer switch retries for an errdisable recovery for more than two times, then the port will be brought down, that is, it will not be recovered after two retries. The port will be recovered after the completion of the nondisruptive ISSU.

Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(11)N1(1)

Table 6 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 7.3(11)N1(1). For more information, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.3(11)N1(1)*.

For other 7.3 releases, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide* specific for that release at:

https://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-guides-list.html.

Table 6 Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 7.3(11)N1(1)

Current Cisco NX-OS Release	Upgrade to NX-OS Release 7.3(11)N1(1)	Downgrade from NX-OS Release 7.3(11)N1(1)

7.3(10)N1(1)
7.3(9)N1(1)
7.3(8)N1(1)
7.3(7)N1(1b)
7.3(7)N1(1a)
7.3(6)N1(1)
7.3(5)N1(1)
7.3(4)N1(1)
7.3(3)N1(1)
7.3(2)N1(1)
7.1(5)N1(1)
7.1(4)N1(1)
	Nondisruptive upgrade (ISSU)	Disruptive downgrade[1]

[1] In-service software downgrade (ISSD) from Cisco NX-OS Release 7.3.x to any earlier releases is not supported. All incompatible configurations will be lost in the target release. Performing a downgrade will also result in loss of certain configurations such as unified ports, breakout, and FEX configurations. See CSCul22703 for details. For more information on restoring the configuration, see the "Restoring the Configuration" section in the *Cisco Nexus 5600 Series Software Upgrade and Downgrade Guide, Release*.

Note You cannot upgrade non-disruptively to Cisco NX-OS Release 7.3(11)N1(1) from Cisco NX-OS Release 7.3(7)N1(1) because of the issue due to CSCvt58479.

Note If you want to upgrade from a release on Cisco NX-OS release 7.1 train or earlier, you must first upgrade to Cisco NX-OS release 7.1(4)N1(1) and then to 7.3(11)N1(1). If you want to upgrade from a release on Cisco NX-OS release 7.2 train or earlier, you must first upgrade to Cisco NX-OS release 7.3(2)N1(1) and then to 7.3(11)N1(1).

Note If you upgrade from an earlier release to Cisco NX-OS release 7.3(2)N1(1), the older BIOS version will be upgraded to the current release BIOS version. For the new BIOS version to take effect, you need to reload the device.

Note If Cisco Nexus 5624Q and 5648Q switches have an older BIOS version, then ISSU to Cisco NX-OS release 7.3(2)N1(1) may be disruptive for some releases. To avoid the disruptive upgrade, upgrade the BIOS version manually before you upgrade the release version. For assistance, please contact the Cisco Technical Assistance Center (TAC).

Starting with Cisco NX-OS Release 7.3(2)N1(1), during a nondisruptive upgrade if any port on a Cisco Nexus switch or a peer switch retries for an errdisable recovery for more than two times, then the port will be brought down, that is, it will not be recovered after two retries. The port will be recovered after the completion of the nondisruptive ISSU.

Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(10)N1(1)

Table 7 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 7.3(10)N1(1). For more information, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.3(10)N1(1).*

For other 7.3 releases, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide* specific for that release at:

https://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-guides-list.html.

Table 7 Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 7.3(10)N1(1)

Current Cisco NX-OS Release	Upgrade to NX-OS Release 7.3(10)N1(1)	Downgrade from NX-OS Release 7.3(10)N1(1)

7.3(9)N1(1)
7.3(8)N1(1)
7.3(7)N1(1b)
7.3(7)N1(1a)
7.3(6)N1(1)
7.3(5)N1(1)
7.3(4)N1(1)
7.3(3)N1(1)
7.3(2)N1(1)
7.1(5)N1(1)
7.1(4)N1(1)
	Nondisruptive upgrade (ISSU)	Disruptive downgrade[1]

[1] In-service software downgrade (ISSD) from Cisco NX-OS Release 7.3.x to any earlier releases is not supported. All incompatible configurations will be lost in the target release. Performing a downgrade will also result in loss of certain configurations such as unified ports, breakout, and FEX configurations. See CSCul22703 for details. For more information on restoring the configuration, see the "Restoring the Configuration" section in the *Cisco Nexus 5600 Series Software Upgrade and Downgrade Guide, Release*.

Note You cannot upgrade non-disruptively to Cisco NX-OS Release 7.3(10)N1(1) from Cisco NX-OS Release 7.3(7)N1(1) because of the issue due to CSCvt58479.

Note If you want to upgrade from a release on Cisco NX-OS release 7.1 train or earlier, you must first upgrade to Cisco NX-OS release 7.1(4)N1(1) and then to 7.3(10)N1(1). If you want to upgrade from a release on Cisco NX-OS release 7.2 train or earlier, you must first upgrade to Cisco NX-OS release 7.3(2)N1(1) and then to 7.3(10)N1(1).

Note If you upgrade from an earlier release to Cisco NX-OS release 7.3(2)N1(1), the older BIOS version will be upgraded to the current release BIOS version. For the new BIOS version to take effect, you need to reload the device.

Note If Cisco Nexus 5624Q and 5648Q switches have an older BIOS version, then ISSU to Cisco NX-OS release 7.3(2)N1(1) may be disruptive for some releases. To avoid the disruptive upgrade, upgrade the BIOS version manually before you upgrade the release version. For assistance, please contact the Cisco Technical Assistance Center (TAC).

Starting with Cisco NX-OS Release 7.3(2)N1(1), during a nondisruptive upgrade if any port on a Cisco Nexus switch or a peer switch retries for an errdisable recovery for more than two times, then the port will be brought down, that is, it will not be recovered after two retries. The port will be recovered after the completion of the nondisruptive ISSU.

Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(9)N1(1)

Table 8 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 7.3(9)N1(1). For more information, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.3(9)N1(1)*.

For other 7.3 releases, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide* specific for that release at:

https://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-guides-list.html.

Table 8 Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 7.3(9)N1(1)

Current Cisco NX-OS Release	Upgrade to NX-OS Release 7.3(9)N1(1)	Downgrade from NX-OS Release 7.3(9)N1(1)

7.3(8)N1(1)
7.3(7)N1(1b)
7.3(7)N1(1a)
7.3(6)N1(1)
7.3(5)N1(1)
7.3(4)N1(1)
7.3(3)N1(1)
7.3(2)N1(1)
7.1(5)N1(1)
7.1(4)N1(1)
	Nondisruptive upgrade (ISSU)	Disruptive downgrade[1]

[1] In-service software downgrade (ISSD) from Cisco NX-OS Release 7.3.x to any earlier releases is not supported. All incompatible configurations will be lost in the target release. Performing a downgrade will also result in loss of certain configurations such as unified ports, breakout, and FEX configurations. See CSCul22703 for details. For more information on restoring the configuration, see the "Restoring the Configuration" section in the *Cisco Nexus 5600 Series Software Upgrade and Downgrade Guide, Release*.

Note You cannot upgrade non-disruptively to Cisco NX-OS Release 7.3(9)N1(1) from Cisco NX-OS Release 7.3(7)N1(1) because of the issue due to CSCvt58479.

Note If you want to upgrade from a release on Cisco NX-OS release 7.1 train or earlier, you must first upgrade to Cisco NX-OS release 7.1(4)N1(1) and then to 7.3(9)N1(1). If you want to upgrade from a release on Cisco NX-OS release 7.2 train or earlier, you must first upgrade to Cisco NX-OS release 7.3(2)N1(1) and then to 7.3(9)N1(1).

Note If you upgrade from an earlier release to Cisco NX-OS release 7.3(2)N1(1), the older BIOS version will be upgraded to the current release BIOS version. For the new BIOS version to take effect, you need to reload the device.

Note If Cisco Nexus 5624Q and 5648Q switches have an older BIOS version, then ISSU to Cisco NX-OS release 7.3(2)N1(1) may be disruptive for some releases. To avoid the disruptive upgrade, upgrade the BIOS version manually before you upgrade the release version. For assistance, please contact the Cisco Technical Assistance Center (TAC).

Starting with Cisco NX-OS Release 7.3(2)N1(1), during a nondisruptive upgrade if any port on a Cisco Nexus switch or a peer switch retries for an errdisable recovery for more than two times, then the port will be brought down, that is, it will not be recovered after two retries. The port will be recovered after the completion of the nondisruptive ISSU.

Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(8)N1(1)

Table 9 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 7.3(8)N1(1). For more information, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.3(8)N1(1)*.

For other 7.3 releases, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide* specific for that release at:

https://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-guides-list.html.

Table 9 Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 7.3(8)N1(1)

Current Cisco NX-OS Release	Upgrade to NX-OS Release 7.3(8)N1(1)	Downgrade from NX-OS Release 7.3(8)N1(1)

7.3(7)N1(1b)
7.3(7)N1(1a)
7.3(6)N1(1)
7.3(5)N1(1)
7.3(4)N1(1)
7.3(3)N1(1)
7.3(2)N1(1)
7.1(5)N1(1)
7.1(4)N1(1)
	Nondisruptive upgrade (ISSU)	Disruptive downgrade[1]

[1] In-service software downgrade (ISSD) from Cisco NX-OS Release 7.3.x to any earlier releases is not supported. All incompatible configurations will be lost in the target release. Performing a downgrade will also result in loss of certain configurations such as unified ports, breakout, and FEX configurations. See CSCul22703 for details. For more information on restoring the configuration, see the "Restoring the Configuration" section in the *Cisco Nexus 5600 Series Software Upgrade and Downgrade Guide, Release*.

Note You cannot upgrade non-disruptively to Cisco NX-OS Release 7.3(8)N1(1) from Cisco NX-OS Release 7.3(7)N1(1) because of the issue due to CSCvt58479.

Note If you want to upgrade from a release on Cisco NX-OS release 7.1 train or earlier, you must first upgrade to Cisco NX-OS release 7.1(4)N1(1) and then to 7.3(8)N1(1). If you want to upgrade from a release on Cisco NX-OS release 7.2 train or earlier, you must first upgrade to Cisco NX-OS release 7.3(2)N1(1) and then to 7.3(8)N1(1).

Note If you upgrade from an earlier release to Cisco NX-OS release 7.3(2)N1(1), the older BIOS version will be upgraded to the current release BIOS version. For the new BIOS version to take effect, you need to reload the device.

Note If Cisco Nexus 5624Q and 5648Q switches have an older BIOS version, then ISSU to Cisco NX-OS release 7.3(2)N1(1) may be disruptive for some releases. To avoid the disruptive upgrade, upgrade the BIOS version manually before you upgrade the release version. For assistance, please contact the Cisco Technical Assistance Center (TAC).

Starting with Cisco NX-OS Release 7.3(2)N1(1), during a nondisruptive upgrade if any port on a Cisco Nexus switch or a peer switch retries for an errdisable recovery for more than two times, then the port will be brought down, that is, it will not be recovered after two retries. The port will be recovered after the completion of the nondisruptive ISSU.

Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(7)N1(1b)

Table 10 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 7.3(7)N1(1b). For more information, see the *Cisco Nexus 6000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.3(7)N1(1b)*.

For other 7.3 releases, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide* specific for that release at:

https://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-guides-list.html.

Table 10 Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 7.3(7)N1(1b)

Current Cisco NX-OS Release	Upgrade to NX-OS Release 7.3(7)N1(1b)	Downgrade from NX-OS Release 7.3(7)N1(1b)

7.3(7)N1(1a)
7.3(6)N1(1)
7.3(5)N1(1)
7.3(4)N1(1)
7.3(3)N1(1)
7.3(2)N1(1)
7.1(5)N1(1)
7.1(4)N1(1)
	Nondisruptive upgrade (ISSU)	Disruptive downgrade[1]

[1] In-service software downgrade (ISSD) from Cisco NX-OS Release 7.3.x to any earlier releases is not supported. All incompatible configurations will be lost in the target release. Performing a downgrade will also result in loss of certain configurations such as unified ports, breakout, and FEX configurations. See CSCul22703 for details. For more information on restoring the configuration, see the “Restoring the Configuration” section in the *Cisco Nexus 5600 Series Software Upgrade and Downgrade Guide, Release*.

Note You cannot upgrade non-disruptively to Cisco NX-OS Release 7.3(7)N1(1b) from Cisco NX-OS Release 7.3(7)N1(1) because of the issue due to CSCvt58479.

Note If you want to upgrade from a release on Cisco NX-OS release 7.1 train or earlier, you must first upgrade to Cisco NX-OS release 7.1(4)N1(1) and then to 7.3(7)N1(1b). If you want to upgrade from a release on Cisco NX-OS release 7.2 train or earlier, you must first upgrade to Cisco NX-OS release 7.3(2)N1(1) and then to 7.3(7)N1(1b).

Note If you upgrade from an earlier release to Cisco NX-OS release 7.3(2)N1(1), the older BIOS version will be upgraded to the current release BIOS version. For the new BIOS version to take effect, you need to reload the device.

Note If Cisco Nexus 5624Q and 5648Q switches have an older BIOS version, then ISSU to Cisco NX-OS release 7.3(2)N1(1) may be disruptive for some releases. To avoid the disruptive upgrade, upgrade the BIOS version manually before you upgrade the release version. For assistance, please contact the Cisco Technical Assistance Center (TAC).

Starting with Cisco NX-OS Release 7.3(2)N1(1), during a nondisruptive upgrade if any port on a Cisco Nexus switch or a peer switch retries for an errdisable recovery for more than two times, then the port will be brought down, that is, it will not be recovered after two retries. The port will be recovered after the completion of the nondisruptive ISSU.

Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(7)N1(1a)

Table 11 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 7.3(7)N1(1a). For more information, see the *Cisco Nexus 6000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.3(7)N1(1a)*.

For other 7.3 releases, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide* specific for that release at:

https://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-guides-list.html.

Table 11 Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 7.3(7)N1(1a)

Current Cisco NX-OS Release	Upgrade to NX-OS Release 7.3(7)N1(1a)	Downgrade from NX-OS Release 7.3(7)N1(1a)

7.3(6)N1(1)
7.3(5)N1(1)
7.3(4)N1(1)
7.3(3)N1(1)
7.3(2)N1(1)
7.1(5)N1(1)
7.1(4)N1(1)
	Nondisruptive upgrade (ISSU)	Disruptive downgrade[1]

[1] In-service software downgrade (ISSD) from Cisco NX-OS Release 7.3.x to any earlier releases is not supported. All incompatible configurations will be lost in the target release. Performing a downgrade will also result in loss of certain configurations such as unified ports, breakout, and FEX configurations. See CSCul22703 for details. For more information on restoring the configuration, see the “Restoring the Configuration” section in the *Cisco Nexus 5600 Series Software Upgrade and Downgrade Guide, Release*.

Note You cannot upgrade non-disruptively to Cisco NX-OS Release 7.3(7)N1(1a) from Cisco NX-OS Release 7.3(7)N1(1) because of the issue due to CSCvt58479.

Note If you want to upgrade from a release on Cisco NX-OS release 7.1 train or earlier, you must first upgrade to Cisco NX-OS release 7.1(4)N1(1) and then to 7.3(7)N1(1a). If you want to upgrade from a release on Cisco NX-OS release 7.2 train or earlier, you must first upgrade to Cisco NX-OS release 7.3(2)N1(1) and then to 7.3(7)N1(1a).

Note If you upgrade from an earlier release to Cisco NX-OS release 7.3(2)N1(1), the older BIOS version will be upgraded to the current release BIOS version. For the new BIOS version to take effect, you need to reload the device.

Note If Cisco Nexus 5624Q and 5648Q switches have an older BIOS version, then ISSU to Cisco NX-OS release 7.3(2)N1(1) may be disruptive for some releases. To avoid the disruptive upgrade, upgrade the BIOS version manually before you upgrade the release version. For assistance, please contact the Cisco Technical Assistance Center (TAC).

Starting with Cisco NX-OS Release 7.3(2)N1(1), during a nondisruptive upgrade if any port on a Cisco Nexus switch or a peer switch retries for an errdisable recovery for more than two times, then the port will be brought down, that is, it will not be recovered after two retries. The port will be recovered after the completion of the nondisruptive ISSU.

Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(7)N1(1)

Table 12 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 7.3(7)N1(1). For more information, see the *Cisco Nexus 6000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.3(7)N1(1)*.

For other 7.3 releases, see the *Cisco Nexus 6000 Series NX-OS Software Upgrade and Downgrade Guide* specific for that release at:

http://www.cisco.com/c/en/us/support/switches/nexus-6000-series-switches/products-installation-guides-list.html.

Table 12 Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 7.3(7)N1(1)

Current Cisco NX-OS Release	Upgrade to NX-OS Release 7.3(7)N1(1)	Downgrade from NX-OS Release 7.3(7)N1(1)

7.3(6)N1(1)
7.3(5)N1(1)
7.3(4)N1(1)
7.3(3)N1(1)
7.3(2)N1(1)
7.1(5)N1(1)
7.1(4)N1(1)
	Nondisruptive upgrade (ISSU)	Disruptive downgrade[1]

[1] In-service software downgrade (ISSD) from Cisco NX-OS Release 7.3.x to any earlier releases is not supported. All incompatible configurations will be lost in the target release. Performing a downgrade will also result in loss of certain configurations such as unified ports, breakout, and FEX configurations. See CSCul22703 for details. For more information on restoring the configuration, see the “Restoring the Configuration” section in the *Cisco Nexus 6000 Series Software Upgrade and Downgrade Guide, Release*.

Note If you want to upgrade from a release on Cisco NX-OS release 7.1 train or earlier, you must first upgrade to Cisco NX-OS release 7.1(4)N1(1) and then to 7.3(7)N1(1). If you want to upgrade from a release on Cisco NX-OS release 7.2 train or earlier, you must first upgrade to Cisco NX-OS release 7.3(2)N1(1) and then to 7.3(7)N1(1).

Note If you upgrade from an earlier release to Cisco NX-OS release 7.3(2)N1(1), the older BIOS version will be upgraded to the current release BIOS version. For the new BIOS version to take effect, you need to reload the device.

Note If Cisco Nexus 5624Q and 5648Q switches have an older BIOS version, then ISSU to Cisco NX-OS release 7.3(2)N1(1) may be disruptive for some releases. To avoid the disruptive upgrade, upgrade the BIOS version manually before you upgrade the release version. For assistance, please contact the Cisco Technical Assistance Center (TAC).

Starting with Cisco NX-OS Release 7.3(2)N1(1), during a nondisruptive upgrade if any port on a Cisco Nexus switch or a peer switch retries for an errdisable recovery for more than two times, then the port will be brought down, that is, it will not be recovered after two retries. The port will be recovered after the completion of the nondisruptive ISSU.

Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(6)N1(1)

Table 13 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 7.3(6)N1(1). For more information, see the *Cisco Nexus 6000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.3(6)N1(1).*

For other 7.3 releases, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide* specific for that release at:

https://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-guides-list.html.

Table 13 Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 7.3(6)N1(1)

Current Cisco NX-OS Release	Upgrade to NX-OS Release 7.3(6)N1(1)	Downgrade from NX-OS Release 7.3(6)N1(1)

7.3(5)N1(1)
7.3(4)N1(1)
7.3(3)N1(1)
7.3(2)N1(1)
7.1(5)N1(1)
7.1(4)N1(1)
	Nondisruptive upgrade (ISSU)	Disruptive downgrade[1]

[1] In-service software downgrade (ISSD) from Cisco NX-OS Release 7.3.x to any earlier releases is not supported. All incompatible configurations will be lost in the target release. Performing a downgrade will also result in loss of certain configurations such as unified ports, breakout, and FEX configurations. See CSCul22703 for details. For more information on restoring the configuration, see the “Restoring the Configuration” section in the *Cisco Nexus 6000 Series Software Upgrade and Downgrade Guide, Release 7.3(6)N1(1)*.

Note If you want to upgrade from a release on Cisco NX-OS release 7.1 train or earlier, you must first upgrade to Cisco NX-OS release 7.1(4)N1(1) and then to 7.3(6)N1(1). If you want to upgrade from a release on Cisco NX-OS release 7.2 train or earlier, you must first upgrade to Cisco NX-OS release 7.3(2)N1(1) and then to 7.3(6)N1(1).

Note If you upgrade from an earlier release to Cisco NX-OS release 7.3(2)N1(1), the older BIOS version will be upgraded to the current release BIOS version. For the new BIOS version to take effect, you need to reload the device.

Note If Cisco Nexus 5624Q and 5648Q switches have an older BIOS version, then ISSU to Cisco NX-OS release 7.3(2)N1(1) may be disruptive for some releases. To avoid the disruptive upgrade, upgrade the BIOS version manually before you upgrade the release version. For assistance, please contact the Cisco Technical Assistance Center (TAC).

Starting with Cisco NX-OS Release 7.3(2)N1(1), during a nondisruptive upgrade if any port on a Cisco Nexus switch or a peer switch retries for an errdisable recovery for more than two times, then the port will be brought down, that is, it will not be recovered after two retries. The port will be recovered after the completion of the nondisruptive ISSU.

Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(5)N1(1)

Table 14 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 7.3(5)N1(1). For more information, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.3(5)N1(1)*.

For other 7.3 releases, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide* specific for that release at:

https://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-guides-list.html.

Table 14 Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 7.3(5)N1(1)

Current Cisco NX-OS Release	Upgrade to NX-OS Release 7.3(5)N1(1)	Downgrade from NX-OS Release 7.3(5)N1(1)

7.3(4)N1(1)
7.3(3)N1(1)
7.3(2)N1(1)
7.1(5)N1(1)
7.1(4)N1(1)
	Nondisruptive upgrade (ISSU)	Disruptive downgrade[1]

[1] In-service software downgrade (ISSD) from Cisco NX-OS Release 7.3.x to any earlier releases is not supported. All incompatible configurations will be lost in the target release. Performing a downgrade will also result in loss of certain configurations such as unified ports, breakout, and FEX configurations. See CSCul22703 for details. For more information on restoring the configuration, see the "Restoring the Configuration" section in the *Cisco Nexus 5600 Series Software Upgrade and Downgrade Guide, Release 7.3(4)N1(1)*.

Note If you want to upgrade from a release on Cisco NX-OS release 7.1 train or earlier, you must first upgrade to Cisco NX-OS release 7.1(4)N1(1) and then to 7.3(5)N1(1). If you want to upgrade from a release on Cisco NX-OS release 7.2 train or earlier, you must first upgrade to Cisco NX-OS release 7.3(2)N1(1) and then to 7.3(5)N1(1).

Note If you upgrade from an earlier release to Cisco NX-OS release 7.3(2)N1(1), the older BIOS version will be upgraded to the current release BIOS version. For the new BIOS version to take effect, you need to reload the device.

Note If Cisco Nexus 5624Q and 5648Q switches have an older BIOS version, then ISSU to Cisco NX-OS release 7.3(2)N1(1) may be disruptive for some releases. To avoid the disruptive upgrade, upgrade the BIOS version manually before you upgrade the release version. For assistance, please contact the Cisco Technical Assistance Center (TAC).

Starting with Cisco NX-OS Release 7.3(2)N1(1), during a nondisruptive upgrade if any port on a Cisco Nexus switch or a peer switch retries for an errdisable recovery for more than two times, then the port will be brought down, that is, it will not be recovered after two retries. The port will be recovered after the completion of the nondisruptive ISSU.

Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.3(4)N1(1)

Table 15 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 7.3(4)N1(1). For more information, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.3(4)N1(1)*.

For other 7.3 releases, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide* specific for that release at:

http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-guides-list.html

Table 15 Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 7.3(4)N1(1)

Current Cisco NX-OS Release	Upgrade to NX-OS Release 7.3(4)N1(1)	Downgrade from NX-OS Release 7.3(4)N1(1)

7.3(3)N1(1)
7.3(2)N1(1)
7.1(5)N1(1)
7.1(4)N1(1)
	Nondisruptive upgrade (ISSU)	Disruptive downgrade[1]

[1] In-service software downgrade (ISSD) from Cisco NX-OS Release 7.3.x to any earlier releases is not supported. All incompatible configurations will be lost in the target release. Performing a downgrade will also result in loss of certain configurations such as unified ports, breakout, and FEX configurations. See CSCul22703 for details. For more information on restoring the configuration, see the "Restoring the Configuration" section in the *Cisco Nexus 5600 Series Software Upgrade and Downgrade Guide, Release 7.3(4)N1(1)*.

Note If you want to upgrade from a release on Cisco NX-OS release 7.1 train or earlier, you must first upgrade to Cisco NX-OS release 7.1(4)N1(1) and then to 7.3(3)N1(1). If you want to upgrade from a release on Cisco NX-OS release 7.2 train or earlier, you must first upgrade to Cisco NX-OS release 7.3(2)N1(1) and then to 7.3(4)N1(1).

Note If you upgrade from an earlier release to Cisco NX-OS release 7.3(2)N1(1), the older BIOS version will be upgraded to the current release BIOS version. For the new BIOS version to take effect, you need to reload the device.

Note If Cisco Nexus 5624Q and 5648Q switches have an older BIOS version, then ISSU to Cisco NX-OS release 7.3(2)N1(1) may be disruptive for some releases. To avoid the disruptive upgrade, upgrade the BIOS version manually before you upgrade the release version. For assistance, please contact the Cisco Technical Assistance Center (TAC).

Note Starting with Cisco NX-OS Release 7.3(2)N1(1), during a nondisruptive upgrade if any port on a Cisco Nexus switch or a peer switch retries for an errdisable recovery for more than two times, then the port will be brought down, that is, it will not be recovered after two retries. The port will be recovered after the completion of the nondisruptive ISSU.

BIOS Revision for Cisco NX-OS Release 7.3(1)N1(1)

For Cisco NX-OS Release 7.3(1)N1(1), the BIOS versions have been revised. The following table shows the latest BIOS versions for the various Cisco Nexus 5600 and Nexus 6000 series platforms.

Note For Cisco NX-OS Release 7.3(2)N1(1) and later releases, the BIOS versions have not been revised, and the following table shows the latest BIOS versions for the various Nexus 5600 and Nexus 6000 series platforms.

.

Table 16 BIOS Revision for Cisco NX-OS Release 7.3(1)N1(1)

Platform	Latest BIOS Version	ISSU	Reload Required?
Cisco Nexus 5672 UP	2.1.7	Nondisruptive	Yes
Cisco Nexus 6001 (Base-T supervisor)	2.5.0	Nondisruptive	Yes
Cisco Nexus 6004	3.3.0	Nondisruptive	Yes
Cisco Nexus 6001	2.5.0	Nondisruptive	Yes
Cisco Nexus 5696	2.6.0	Nondisruptive	Yes
Cisco Nexus 56128P	3.7.0	Nondisruptive	Yes
Cisco Nexus 5624Q	1.1.6	Nondisruptive	Yes
Cisco Nexus 5648Q	1.1.7	Nondisruptive	Yes
Cisco Nexus 5672UP-16G	0.2.0	Nondisruptive	Yes

BIOS Revision for Cisco NX-OS Release 7.3(0)N1(1)

For Cisco NX-OS Release 7.3(0)N1(1), the BIOS versions have been revised. The following table shows the latest BIOS versions for the various Cisco Nexus 5600 and Nexus 6000 series platforms.

.

Table 17 BIOS Revision for Cisco NX-OS Release 7.3(0)N1(1)

Platform	Latest BIOS Version	ISSU	Reload Required?
Cisco Nexus 5672	2.1.5	Nondisruptive	No
Cisco Nexus 6001 (Base-T supervisor)	2.2.0	Nondisruptive	No
Cisco Nexus 6001	2.2.0	Nondisruptive	No
Cisco Nexus 6004	2.3.0	Nondisruptive	No
Cisco Nexus 5696	2.6.0	Nondisruptive	Yes
Cisco Nexus 56128	3.3.0	Nondisruptive	No
Cisco Nexus 5624Q	1.1.3	Nondisruptive	Yes
Cisco Nexus 5648Q	1.1.4	Nondisruptive	Yes

Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.2(1)N1(1)

Table 18 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 7.2(1)N1(1). For more information, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.2(1)N1(1)*.

For other 7.2 releases, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide* specific for that release at:

http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-guides-list.html.

Table 18 Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 7.2(1)N1(1)

Current Cisco NX-OS Release	Upgrade to NX-OS Release 7.2(1)N1(1)	Downgrade from NX-OS Release 7.2(1)N1(1)

7.2(0)N1(1)[1]
7.1(1)N1(1)—7.1(3)N1(2)
7.1(0)N1(1b)
7.1(0)N1(1a)
7.0(8)N1(1)
7.0(7)N1(1)
7.0(6)N1(1)
	Nondisruptive upgrade	Disruptive downgrade[2]

[1] Possibility of disruptive upgrade if FC or FCoE is enabled and upgrade is from Cisco NX-OS release 7.2(0)N1(1) or earlier. See CSCuq94445 for more details.

[2] In-service software downgrade (ISSD) from Cisco NX-OS Release 7.2.x to any earlier releases is not supported. All incompatible configurations will be lost in the target release. Performing a downgrade will also result in loss of certain configurations such as unified ports, breakout, and FEX configurations. See CSCul22703 for details. For more information on restoring the configuration, see the “Restoring the Configuration” section in the *Cisco Nexus 5600 Series Software Upgrade and Downgrade Guide, Release 7.2(0)N1(1)*.

Note Disruptive upgrade is required before configuring VLAN translation on FEX for Cisco NX-OS Release 7.1(0)N1(1a).

Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 7.1(5)N1(1b)

Table 19 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 7.1(5)N1(1b). For more information, see the *Cisco Nexus 5500 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.1(5)N1(1b)*.

For other 7.1 releases, see the *Cisco Nexus 5500 Series NX-OS Software Upgrade and Downgrade Guide* specific for that release at:
http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-guides-list.html.

Table 19 Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 7.1(5)N1(1b)

Current Cisco NX-OS Release	Upgrade to NX-OS Release 7.1(5)N1(1b)	Downgrade from NX-OS Release 7.1(5)N1(1b)

7.1(1)N1(1)—7.1(4)N1(1)[1]
7.1(5)N1(1a)
7.1(0)N1(1b)
7.1(0)N1(1a)
7.0(4)N1(1)—7.0(8)N1(1)
	Nondisruptive upgrade (ISSU)	Disruptive downgrade

[1] Possibility of disruptive upgrade if FC or FCoE is enabled and upgrade is from Cisco NX-OS release 7.1(3)N1(2) or earlier. See CSCuq94445 for more details.

Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.1(5)N1(1)

Table 20 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 7.1(5)N1(1). For more information, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.1(5)N1(1)*.

For other 7.1 releases, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide* specific for that release at:

http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-guides-list.html.

Table 20 Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 7.1(5)N1(1)

Current Cisco NX-OS Release	Upgrade to NX-OS Release 7.1(5)N1(1)	Downgrade from NX-OS Release 7.1(5)N1(1)

7.1(1)N1(1)—7.1(4)N1(1)[1]
7.1(0)N1(1b)
7.1(0)N1(1a)
7.0(4)N1(1)—7.0(8)N1(1)
	Nondisruptive upgrade (ISSU)	Disruptive downgrade

1. Possibility of disruptive upgrade if FC or FCoE is enabled and upgrade is from Cisco NX-OS release 7.1(3)N1(2) or earlier. See CSCuq94445 for more details.

Note When you perform a nondisruptive upgrade from an earlier release to Cisco NX-OS Release 7.1(4)N1(1), you might experience traffic loss in the Straight-Through FEXs on a vPC secondary device. This issue occurs when the **max-lsp-lifetime** command value is less than 90 seconds. We recommend that you increase the **max-lsp-lifetime** command value to more than that of the upgrade time or set a default value of 1200 seconds. To configure the **max-lsp-lifetime** command, you must first configure the **fabricpath domain default** command.

Note When you perform a nondisruptive upgrade from an earlier release to Cisco NX-OS Release 7.1(4)N1(1), you might experience Forwarding Manager crash. See CSCva39744 and CSCuu81208 caveats for more details.

Note When you perform a disruptive upgrade from Cisco NX-OS release 7.0.x to 7.1.x, 7.2.x, or 7.3.x, with the **hardware ethernet store-and-fwd-switching** command configured, there might be some traffic loss. To avoid the above scenario, we recommend that you create a /mnt/pss/qd_sf_sdb file with content as 1 before upgrading. If you have upgraded from Cisco NX-OS release 7.0.x to 7.1.x, 7.2.x, or 7.3.x, with the **hardware ethernet store-and-fwd-switching** command configured, after the upgrade, remove the **hardware ethernet store-and-fwd-switching** command configuration, reconfigure the command again, and reload the switch. See CSCvj22890 for more details.

BIOS Revision for Cisco NX-OS Release 7.1(4)N1(1)

For Cisco NX-OS Release 7.1(4)N1(1), the BIOS versions have been revised. The following table shows the latest BIOS versions for the various Cisco Nexus 5600 and Cisco Nexus 6000 series platforms.

Note Refer to the Field Notice before performing an upgrade.

.

Table 21 BIOS Revision for Cisco NX-OS Release 7.1(4)N1(1)

Platform	Latest BIOS Version	ISSU	Reload Required?
Cisco Nexus 5672 UP	2.1.7	Nondisruptive	Yes
Cisco Nexus 6001	2.5.0	Nondisruptive	Yes
Cisco Nexus 6004	3.3.0	Nondisruptive	Yes
Cisco Nexus 6001 (Base-T supervisor)	2.5.0	Nondisruptive	Yes
Cisco Nexus 5696	2.6.0	Nondisruptive	Yes
Cisco Nexus 56128P	3.7.0	Nondisruptive	Yes
Cisco Nexus 5624Q	1.1.6	Disruptive	No
Cisco Nexus 5648Q	1.1.7	Disruptive	No

Note For the BIOS upgrade to be effective, a reload is required. A switch requires a BIOS upgrade only if it encounters a PCI error issue. Refer to CSCUt56888.

Note On Cisco Nexus 5624Q and 5648Q switches, by default ISSU will go for a disruptive upgrade process. To avoid a disruptive process, upgrade the BIOS version manually before upgrading the release version. Contact the Cisco Technical Assistance Center (TAC) for assistance with this option.

Note On Cisco Nexus 5648Q switches, ISSU will go for the disruptive upgrade process because BIOS version and Input/Output Field-Programmable Gate Array (IOFPGA) version have to be upgraded. This cannot be avoided, as manually upgrading the IOFPGA will result in disruptive ISSU.

Supported Upgrade and Downgrade Path for Cisco NX-OS Release 7.0(8)N1(1)

Table 22 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 7.0(8)N1(1). For more information, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.0(8)N1(1)*.

For other 7.0 releases, see the *Cisco Nexus 5600 Series NX-OS Software Upgrade and Downgrade Guide* specific for that release at:

http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-guides-list.html.

Table 22 Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 7.0(8)N1(1)

Current Cisco NX-OS Release	Upgrade to NX-OS Release 7.0(8)N1(1)	Downgrade from NX-OS Release 7.0(8)N1(1)
7.0(0)N1(1)—7.0(7)N1(1)[1]	Nondisruptive upgrade.	Disruptive downgrade.

[1] Possibility of ISSU failure if you are upgrading to Cisco NX-OS release 7.0(6)N1(1) or earlier when multi-step ISSU is performed. For multi-step ISSU, it is recommended to upgrade directly to Cisco NX-OS Release 7.0(7)N1(1) or 7.0(8)N1(1). See CSCuw78727 for details.

Note When you upgrade (ISSU upgrade or non-ISSU upgrade) from Cisco NX-OS Release 6.0(2)N2(7) to Cisco NX-OS Release 7.0(6)N1(1) or later releases, Dynamic Host Configuration Protocol (DHCP) OFFER packets get dropped. We recommend you disable the **ip dhcp relay** command and reconfigure it after the upgrade.

BIOS Revision for Cisco NX-OS Release 7.0(8)N1(1)

For Cisco NX-OS Release 7.0(8)N1(1), the BIOS versions have been revised. The following table shows the latest BIOS versions for the various Cisco Nexus 5600 and Nexus 6000 series platforms.

.

Table 23 BIOS Revision for Cisco NX-OS Release 7.0(8)N1(1)

Platform	Latest BIOS Version	ISSU	Reload Required?
Cisco Nexus 5672	2.1.5	Nondisruptive	Yes
Cisco Nexus 6001	2.2.0	Nondisruptive	Yes
Cisco Nexus 56128	3.3.0	Nondisruptive	Yes
Cisco Nexus 6004	2.3.0	Nondisruptive	Yes

Unsupported Features

Beginning with Cisco NX-OS release 7.3(0)N1(1), the One Platform Kit (onePK) feature is not supported on Cisco Nexus 5000 and 6000 series switches.

Limitations

This section describes the limitations for Cisco NX-OS Release 7.x.

- Starting with Cisco NX-OS Release 7.3(2)N1(1), during a nondisruptive upgrade if any port on a Cisco Nexus switch or a peer switch retries for an errdisable recovery for more than two times, then the port will be brought down, that is, it will not be recovered after two retries. The port will be recovered after the completion of the nondisruptive ISSU.
- PTP—In case of a nondisruptive ISSU from a release earlier than Cisco NX-OS release 7.1(1)N1(1) to the latest release, you must perform a reload before enabling the PTP feature.
- BGP—In Cisco Nexus 5600 and 6000 series switches, if both the **send-community** and **send-community extended** commands are in the configuration for Cisco NX-OS 6.0(2) or an earlier release and an ISSU is performed, then only **send-community extended** will be present in the configuration for a Cisco NX-OS 7.0(x) or later release after the ISSU. You must manually reconfigure the **send-community** command. The running configuration will show **send-community both** instead of both commands.
- Beginning with Cisco NX-OS release 7.1(2)N1(1), the per interface limit of VLAN mapping configurations is 170 per switch. If you want to configure more than 170 VLAN mappings per switch, you must configure more number of port channels, each having VLAN mapping configurations. For example, if you want to achieve 1000+ VLAN mappings per switch, you must configure 6 or more port channels with a maximum of 170 VLAN mappings for each port channel.
- When **fabricpath-oam**, **traceroute**, or **mtrace** commands are used on a Cisco Nexus 5600 switch in a Programmable Fabric topology by including the option ‘use-host-vlan’, the command times out. This is due to a hardware limitation on Nexus 5600 switches that causes the FabricPath-OAM packet format to be misaligned compared to the protocol specification.
- If you are connecting a Cisco Nexus 5600 switch to an M1 interface using 1000 base-LH SFP, then beginning with Cisco NX-OS release 7.1(1)N1(1), to configure the **no negotiate auto** command, you must change the speed and duplex to a fixed speed and duplex. You cannot configure the **no negotiate auto** command when the speed and duplex is set to AUTO.
- Downgrading from Cisco NX-OS release 7.0(2)N1(1) to 5.2(1)N1(8a) is not supported. This may result in the removal of the Fabricpath feature-set.

- On Cisco Nexus 5000 and 6000 series switches, the device manager (DM) is not downloadable and cannot be enabled. In case you need to use the DM, you must install the DCNM application and launch the device manager using the DCNM application.
- Netflow export is not supported for the following parameters:
  - Source or destination autonomous system (AS) number of the local device or the peer.
  - BGP next-hop IPv4 or IPv6 address.
- Netflow export may result in packet drops at the time of surge in ingress data traffic. This state is temporary and the process will recover automatically after some time. See CSCuu96337 for more details.
- If you are migrating from Cisco NX-OS Release 7.1(0)N1(1a) or 7.1(0)N1(1b) to Cisco NX-OS Release 7.2(0)N1(1) or to 7.1(1)N1(1) (which is supposed to be a nondisruptive ISSU) for the switches that have the N2348TQ FEX connected, then the ISSU might fail and upgrade to Cisco NX-OS Release 7.2(0)N1(1) or to 7.1(1)N1(1) will be disruptive. This will result in loss of certain configurations such as unified ports, breakout, and FEX configurations. For details, see CSCuu76648. Refer to the "Restoring the Configuration" section in the *Cisco Nexus 5600 Series Software Upgrade and Downgrade Guide, Release 7.2(0)N1(1)* to restore the configuration if the configurations contain interface breakout or unified port configurations.
- Loading a new license or reloading existing license on a Cisco Nexus 5624Q switch is not supported. For details, see CSCus41273.
- The Server Virtualization Switch (SVS) connection is not deleted during a rollback when NIV is enabled. To resolve this issue, delete the current SVS connection and reapply the original SVS connection.
- If you configure a Cisco Nexus 2248TP port to 100 Mbps instead of autonegotiation, then autonegotiation does not occur, which is the expected behavior. Both sides of the link should be configured to both hardwired speed or both autonegotiate.

  no speed—Autonegotiates and advertises all speeds (only full duplex).

  speed 1000—Autonegotiates only for an 802.3x pause.

  speed 100—Does not autonegotiate; pause cannot be advertised. The peer must be set to not autonegotiate and fix at 100 Mbps (similar to the N2248TP). For details, see CSCte81998.
- If you connect a Cisco switch (with 1 Gigabit Ethernet interfaces) to a Cisco Nexus 5600 Series switch or a Cisco Nexus 6000 Series switch using supported 1 Gigabit (GLC-SX-MM) or 10 Gigabit (SFP-10G-SR) transceiver modules and the **auto-negotiate** command is enabled, there may be connectivity issue between the devices. To avoid this issue, we recommend that you configure the **speed 1000** command on that switch interface.
- When a private VLAN port is configured as a TX (egress) SPAN source, the traffic seen at the SPAN destination port is marked with the VLAN of the ingressed frame. There is no workaround.
- In large-scale configurations, some Cisco Nexus 2000 Series Fabric Extenders might take up to 3 minutes to appear online after entering the **reload** command. A configuration can be termed large scale when the maximum permissible Cisco Nexus 2000 Series Fabric Extenders are connected to a Cisco Nexus 5600 Series switch, all host-facing ports are connected, and each host-facing interface has a large configuration that supports the maximum permissible ACEs per interface.
- The Cisco Nexus 2148 Fabric Extender does not support frames with the dot1q vlan 0 tag.

- VACLs of more than one type on a single VLAN are unsupported. Cisco NX-OS software supports only a single type of VACL (either MAC, IPv4, or IPv6) applied on a VLAN. When a VACL is applied to a VLAN, it replaces the existing VACL if the new VACL is a different type. For instance, if a MAC VACL is configured on a VLAN and then an IPv6 VACL is configured on the same VLAN, the IPv6 VACL is applied, and the MAC VACL is removed.
- A MAC ACL is applied only on non-IP packets. Even if there is a **match eth type = ipv4** statement in the MAC ACL, it does not match an IP packet. To avoid this situation, use IP ACLs to apply access control to the IP traffic instead of using a MAC ACL that matches the EtherType to IPv4 or IPv6.
- Multiple **boot kickstart** statements in the configuration are not supported.
- If you configure Multiple Spanning Tree (MST) on a Cisco Nexus 5600 Series switch, avoid partitioning the network into a large number of regions.
- By design, vEth interfaces do not share the underlying behavior of a vPC port. As a result, a VLAN is not suspended when the peer switch suspends it. For example, when you shut a VLAN on a primary switch, the VLAN continues to be up on the secondary switch when the vEth interface is on a FEX. When the VLAN on the primary switch goes down, the VLAN on the vEth interface on the primary is suspended, but the vEth on the secondary switch remains up because it is an active VLAN on the secondary switch.
- The packet length in the IP GRE header of a packet exiting from the switch is not equal to the MTU value configured in the ERSPAN source session. This is true for SPAN or ERSPAN. The Cisco Nexus 5600 switch terminates in multiples of 16 bytes. If MTU is configured as 100 bytes, then the actual truncated packet is 96 bytes.
- Unknown unicast packets in FabricPath ports are counted as multicast packets in interface counters. This issue occurs when unknown Unicast packets are sent and received with a reserved multicast address (that floods to a VLAN) in the outer FabricPath header, and the Cisco Nexus 5600 Series switch increments the interface counter based on the outer FabricPath header. As a result, Multicast counters are incremented. There is no workaround for this issue.
- In an emulated switch setup, an inband keepalive does not work. The following steps are recommended for peer keepalive over SVI when a switch is in FabricPath mode:
  - Use a dedicated front panel port as a vPC+ keepalive. The port should be in CE mode.
  - Use a dedicated VLAN to carry the keepalive interface. The VLAN should be a CE VLAN.
  - Enter the **dual-active exclude interface-vlan** *keepalive-vlan* command to prevent the SVI from going down on the secondary when a peer-link goes down.
- The limit of the table that holds the Router MAC and Virtual MAC entries for determining packet routing or switching is 500 entries. The Virtual MAC entries, the MAC used for HSRP/VRRP that is also programmed in this table, can be shared across multiple Layer 3 interfaces. If SVIs 1–100 all have the same group number configured, just one entry needs to be programmed in this table. We recommend that you configure the same group ID across all or multiple Layer 3 interfaces/SVIs. If multiple group IDs are configured on an Layer 3 interface, we recommend that you configure the same set of group IDs across all or multiple Layer 3 interfaces. This configuration supports HSRP/VRRP on more interfaces.
- The maximum IP MTU that can be set on Layer 3 interfaces running Layer 3 protocols is 9192 because of the internal header used inside the switch. The related network-qos policy must be set to 9216.
- If there are unified ports configured as Fiber Channel (FC) and a disruptive upgrade is performed, then the FC interfaces must be reconfigured, and the switch will require a second reload.

- On Cisco Nexus 56128P and 5672UP Switches, running Cisco NX-OS Release 7.0(1)N1(1) or later release, you will see an increase in the BIG_DROP_INGRESS_PAUSE and BIG_DROP_INGRESS_ACL counter drops for an ASIC. These drops do not impact the performance of the switch. To view the counter drops for an ASIC, use the **show platform fwm info pif fc2/24 | i drop** and **show platform fwm info pif fc2/24 | i drop** commands.
- In a vPC topology, when a Hot Standby Router Protocol (HSRP) pair is in Active/Standby mode, and FabricPath is enabled on them, you will not be able to ping from the standby switch to the virtual IP address (VIP).
- Under certain unique conditions packets between the Cisco Nexus 2300 Series FEX and the parent Cisco Nexus 5600 or 6000 switches can get corrupted. See CSCux93803 for more information.
- By default, auto-recovery is enabled on vPC. If you choose to disable auto-recovery and reload the switch, the disabled auto-recovery mode will be reset and auto-recovery will be enabled again after the switch reloads.

Limitations on the Cisco Nexus 5600

The limitations on the Cisco Nexus 5600 switch are as follows:

- SPAN Limitations on Fabric Extender Ports, page 76
- Layer 3 Limitations, page 77
- Stuck Ingress and Egress Buffers in a vPC Environment, page 77

SPAN Limitations on Fabric Extender Ports

The SPAN limitations on Fabric Extender ports are as follows:

- On a Cisco Nexus device, if the SPAN source is a FEX port, the frames will always be tagged when leaving the SPAN destination.
- On a Cisco Nexus 5600 switch, if the SPAN source is on an access port on the switch port, the frames will not be tagged when leaving the SPAN destination.
- Ports on a FEX can be configured as a tx-source in one session only.

  If two ports on the same FEX are enabled to be tx-source, the ports need to be in the same session. If you configure a FEX port as a tx-source and another port belonging to the same FEX is already configured as a tx-source on a different SPAN session, an error is displayed on the CLI.

  In the following example, Interface Ethernet100/1/1 on a FEX 100 is already configured as a tx-source on SPAN session-1:

```
swor28(config-monitor)# show running-config monitor
      version 7.0(1)N1(1)
      monitor session 1
          source interface Ethernet100/1/1 tx
          destination interface Ethernet1/37
          no shut
```

  If you add an interface Ethernet100/1/2 as a tx-source to a different SPAN session (session-2) the following error appears:

```
swor28(config)# monitor session 2
swor28(config-monitor)# source interface ethernet 100/1/2 tx
ERROR: Eth100/1/2: Ports on a fex can be tx source in one session only
swor28(config-monitor)#
```

- When a FEX port is configured as a tx-source, the multicast traffic is spanned on all VLANs that the tx-source port is a member of. The FEX port sends out only multicast packets that are not filtered by IGMP snooping. For example, if FEX ports 100/1/1–12 are configured on VLAN 11 and the switch port 1/5 sends multicast traffic on VLAN 11 in a multicast group, and hosts connected to FEX ports 100/1/3–12 are interested in receiving that multicast traffic (through IGMP), then that multicast traffic goes out on FEX ports 100/1/3–12, but not on 100/1/1–2.

  If you configure SPAN Tx on port 100/1/1, although the multicast traffic does not egress out of port 100/1/1, the SPAN destination does receive that multicast traffic, which is due to a design limitation.
- When a FEX port is configured as both SPAN rx-source and tx-source, broadcast non-IGMP Layer-2 multicast frames as well as unknown unicast frames originating from that port might be seen twice on the SPAN destination: once on the ingress and once on the egress path. On the egress path, the frames are filtered by the FEX to prevent them from going out on the same port on which they were received. For example, if FEX port 100/1/1 is configured on VLAN 11 and is also configured as SPAN rx-source and tx-source and a broadcast frame is received on that port, the SPAN destination recognizes two copies of the frame, even though the frame is not sent back on port 100/1/1.
- For releases prior to Cisco NX-OS release 7.2(0)N1(1), a FEX port cannot be configured as a SPAN destination. Only a switch port can be configured and used as a SPAN destination. FEX HIF as SPAN destination is supported from Cisco NX-OS release 7.2(0)N1(1) onwards.
- With a SPAN on Latency session, FEX ports cannot be configured as source or destination.

Layer 3 Limitations

Asymmetric Configuration

In a vPC topology, two Cisco Nexus 5600 switches configured as vPC peer switches need to be configured symmetrically for Layer 3 configurations such as SVIs, a peer gateway, routing protocol and policies, and RACLs.

Note vPC consistency check does not include Layer 3 parameters.

Stuck Ingress and Egress Buffers in a vPC Environment

A Cisco Nexus 5600 Series switch enabled for switching-mode store-and-forward may experience a egress ASIC buffer stuck under the following conditions:

- An unsolicited **write erase** command is issued. Additional parameters are configured that have impact on the forwarding decision, which means a new VLAN or VNI is created.
- A **copy running-configuration startup configuration** command is issued after the extra parameters are configured, and then additional new VLAN or VNI parameters are configured again.
- In the reported instance of this problem the switch was configured as a vPC peer switch and the issue affected the ASIC that holds the connection to the vPC peer-link.

To avoid this problem do not use random **write-erase** commands. If such a command was issued in error, immediately run the **copy running-configuration startup-configuration** command.

Caveats

This section includes the open and resolved caveats for this release. Each caveat has a link to the Bug Toolkit, where you can find details.

This section includes the following topics:

- Open Caveats, page 79
- Resolved Caveats n Cisco NX-OS Release 7.3(14)N1(1), page 82
- Resolved Caveats in Cisco NX-OS Release 7.3(13)N1(1), page 82
- Resolved Caveats in Cisco NX-OS Release 7.3(12)N1(1), page 82
- Resolved Caveats in Cisco NX-OS Release 7.3(11)N1(1), page 83
- Resolved Caveats in Cisco NX-OS Release 7.3(10)N1(1), page 83
- Resolved Caveats in Cisco NX-OS Release 7.3(9)N1(1), page 84
- Resolved Caveats in Cisco NX-OS Release 7.3(8)N1(1), page 86
- Resolved Caveats in Cisco NX-OS Release 7.3(7)N1(1b), page 87
- Resolved Caveats in Cisco NX-OS Release 7.3(7)N1(1a), page 87
- Resolved Caveats in Cisco NX-OS Release 7.3(7)N1(1), page 88
- Resolved Caveats in Cisco NX-OS Release 7.3(6)N1(1), page 89
- Resolved Caveats in Cisco NX-OS Release 7.3(5)N1(1), page 91
- Resolved Caveats in Cisco NX-OS Release 7.3(4)N1(1), page 92
- Resolved Caveats in Cisco NX-OS Release 7.3(3)N1(1), page 94
- Resolved Caveats in Cisco NX-OS Release 7.3(2)N1(1), page 97
- Resolved Caveats in Cisco NX-OS Release 7.3(1)N1(1), page 106
- Resolved Caveats in Cisco NX-OS Release 7.3(1)N1(1), page 106
- Resolved Caveats in Cisco NX-OS Release 7.3(0)N1(1), page 109
- Resolved Caveats in Cisco NX-OS Release 7.2(1)N1(1), page 110
- Resolved Caveats in Cisco NX-OS Release 7.2(0)N1(1), page 113
- Resolved Caveats in Cisco NX-OS Release 7.1(5)N1(1b), page 114
- Resolved Caveats in Cisco NX-OS Release 7.1(5)N1(1), page 114
- Resolved Caveats in Cisco NX-OS Release 7.1(4)N1(1), page 118
- Resolved Caveats in Cisco NX-OS Release 7.1(3)N1(2), page 125
- Resolved Caveats in Cisco NX-OS Release 7.1(2)N1(1), page 128
- Resolved Caveats in Cisco NX-OS Release 7.1(1)N1(1), page 132
- Resolved Caveats in Cisco NX-OS Release 7.1(0)N1(1b), page 135
- Resolved Caveats in Cisco NX-OS Release 7.1(0)N1(1a), page 135
- Resolved Caveats in Cisco NX-OS Release 7.0(8)N1(1), page 135
- Resolved Caveats in Cisco NX-OS Release 7.0(7)N1(1), page 137
- Resolved Caveats in Cisco NX-OS Release 7.0(6)N1(1), page 140
- Resolved Caveats in Cisco NX-OS Release 7.0(5)N1(1a), page 144

- Resolved Caveats in Cisco NX-OS Release 7.0(5)N1(1), page 144
- Resolved Caveats in Cisco NX-OS Release 7.0(4)N1(1), page 144
- Resolved Caveats in Cisco NX-OS Release 7.0(3)N1(1), page 145
- Resolved Caveats in Cisco NX-OS Release 7.0(2)N1(1), page 145
- Resolved Caveats in Cisco NX-OS Release 7.0(1)N1(1), page 145

Open Caveats

Caveats describe unexpected behavior in a product. The Open Caveats section lists open caveats that apply to the current release and may apply to previous releases. A caveat that is open for a prior release and is still unresolved applies to all future releases until it is resolved.

The Bug Search Tool (BST), which is the online successor to the Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data, such as bug details, product, and version. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat whose ID you do not have, perform the following procedure:

1. Access the BST using your Cisco user ID and password at https://tools.cisco.com/bugsearch/
2. In the Bug search window that is displayed, enter the necessary information in the corresponding fields.

For more information about how to use the Cisco Bug Search Tool effectively, including how to set email alerts for bugs and to save bugs and searches, see the Bug Search Tool Help and FAQ page.

Table 24 lists descriptions of open caveats in Cisco NX-OS Release 7.x.

To view the details of the software bugs pertaining to your product, click the Caveat ID/Bug ID number in the table. The corresponding Bug Search Tool page is displayed with details of the Caveat ID/Bug ID.

Table 24 Open Caveats in Cisco NX-OS Release 7.x

Caveat ID	Open Caveat Headline	Known Affected Release	Known Resolved Release
CSCwf04604	N5k/N6k - cannot pre-provision FEX or expansion module interfaces after upgrading to 7.3.11	7.3(13)N1(1)	

CSCun66310	Cisco Nexus 5596:System fails to boot after a power cycle	7.2(1)N1(1)
		7.1(3)N1(1)	

CSCur86623	Cisco N24Q Performance: Drops seen at L2/L3 Fullmesh Multicast.	7.1(0)N1(1)	
CSCur95371	VXLAN for working on Cisco Nexus 5696-M4C.	7.1(0)N1(1)	
CSCus78963	Inconsistent behavior of System LED during error state.	7.1(1)N1(1)	7.3(2)N1(1)
CSCut63393	Border Leaf needs to advertise hash-len for BSR	7.2(0)N1(1)	7.3(0)N1(1)

Table 24 Open Caveats in Cisco NX-OS Release 7.x (continued)

CSCuv92470	Traffic loss of 9 seconds, while doing vPC shutdown on vPC primary in FP	7.2(1)N1(1)	
CSCuw64344	Pre-provisioning does not for FC FEX ports	7.3(0)N1(1)	
CSCux14029	10G Auto-negotiation issue between 2232TM-E FEX and 10G partners	7.1(2)N1(1)	
CSCuy16934	Fix the error string when ports go to errDisabled state on “no-fcoe”	7.3(0)N1(1)	

CSCuz70693	Cisco Nexus 5600 - BUM traffic with CRC error is cut-through switched	7.1(3)N1(1)
		7.1(0)N1(1)
			7.3(2)N1(1)

CSCuz73561	Access map config generating error in config sync	7.1(4)N1(1)	
CSCuz97563	KERN-3-SYSTEM_MSG: [373.500345] FCP_ERRFCP_PORT: gat_fcp_add_port@1212	7.3(2)N1(1)	7.3(3)N1(1)
CSCva47977	Switch-profile database not in sync after defaulting the interface	7.1(4)N1(1)	7.3(3)N1(1)

CSCva88817	Auto-Config stuck in PPM-Resp wait state due to copy run start failure	7.3(1)N1(1)
		7.2(1)N1(1)
			7.3(2)N1(1)

CSCva96705	First time net-flow configuration after ISSU may not work	7.1(4)N1(1)	7.3(2)N1(1)
CSCvb26949	DFA auto-config profile refresh failure due to IPv6 address change	7.3(0)N1(1)	7.3(2)N1(1)
CSCvd04299	VLAN tags are not present when span destination is a FEX HIF	7.3(2)N1(1)	

CSCvd38629	AA FEX going to &quot;Chk Upg Seq&quot; while flapping HIFs on switch undergoing ND ISSU	7.3(2)N1(1)
		7.1(5)N1(1)	

CSCvd40670	2248PQ fex: SNMP walk on ENTITY SENSOR MIB shows incorrect values for Control sensor	7.3(2)N1(1)	7.3(6)N1(1)
CSCvd58130	Unable to clear QoS statistics on the FEX host interface ports	7.3(2)N1(1)	
CSCvd97805	VTP datafile is not receiving vtp mode change update in vtp version 2	7.3(2)N1(1)	
CSCvi50709	Port-security mac added as “PEER_STATIC” on vPC primary and causes traffic failure	7.3(3)N1(1)	

CSCvi57566	Exception test : fwm hap reset with TCAM exhaustion and triggers (crs, vlan del/add)	7.3(3)N1(1)
		7.3(2)N1(1)	

CSCvk56504	Crash due to fwm heartbeat failure	7.1(4)N1(1)	
CSCvk69720	N7K F3 to N6K: 1 min link up delay	7.3(3)N1(1)	

Table 24 Open Caveats in Cisco NX-OS Release 7.x (continued)

CSCvm02123	N5k can't save config: Service “snmpd” failed to store its configuration (error-id 0x00000006)	7.3(1)N1(1)	
CSCvm08488	N2K-B22IBM FEX crash due to kernel panic	7.3(2)N1(1)	

CSCvm09038	“switchport trunk mode on” causes existing FC san-port-channel to go down and not recover	7.3(2)N1(1)
		7.1(4)N1(1)
			7.3(5)N1(1)

CSCvm23492	SVI interfaces can not be displayed in “show interface description”	7.3(3)N1(1)
		7.3(2)N1(1)
			7.3(5)N1(1)

CSCvm39490	Nexus 5K and 6K should perform “link reset failed nonempty receive queue”	7.3(3)N1(1)	
CSCvm41235	Fex(N2K-C2248TP) does not negotiate speed with WSA (UCS C220-M4) RPC port	7.3(3)N1(1)	
CSCvo88678	Extraneous line in show ip bgp output	7.3(5)N1(1)	7.3(6)N1(1)
CSCvp38432	N5K crash in fwm hap reset 1 minute after ISSU from 7.1(4)N1(1) to 7.3(4)N1(1)	7.3(4)N1(1)	
CSCvr05880	When reload N2K-C2232PP-10GE with GLC-T, peer NIC comes up & down before nxos takes control the FEX	7.3(7)N1(1a)	7.3(8)N1(1)
CSCvt58479	FEX N2K-C2232TM Fails after upgrading to 7.3(7)N1(1)	7.3(7)N1(1)	7.3(7)N1(1a)
CSCwd76790	Loopback configuration unable to add or delete on nexus 6000 running code 7.3.12.N1.1	7.3(12)N1(1)	

Resolved Caveats n Cisco NX-OS Release 7.3(14)N1(1)

Table 25 Resolved Caveats in Cisco NX-OS Release 7.3(14)N1(1)

Caveat ID Number	Description
CSCwe54747	San-Port-Channel or trunk with Cisco switch OUI 0x802DBF fails to come up
CSCwf04604	N5k/N6k - cannot pre-provision FEX or expansion module interfaces after upgrading to 7.3.12
CSCvt84013	Interface-vlan process crash or stale ifindex entries in queue when SNMP used to shut down SVIs

Resolved Caveats in Cisco NX-OS Release 7.3(13)N1(1)

Table 26 Resolved Caveats in Cisco NX-OS Release 7.3(13)N1(1)

Caveat ID Number	Description
CSCwc98158	PFM process crashed while processing SNMP req for FEX & switch went for reload
CSCwd23720	Unable to configure vfc interfaces when aaa TACACS+ is also configured in the switch
CSCwd12326	Changing switch OOB causes Nexus to reload

Resolved Caveats in Cisco NX-OS Release 7.3(12)N1(1)

Table 27 Resolved Caveats in Cisco NX-OS Release 7.3(12)N1(1)

Caveat ID Number	Description
CSCun63493	OVH:arp to diff sunet not generated
CSCvf24911	ARP memory leak @ LIBBL_MEM_bitfield_malloc_t & LIBSLAB_MEM_create_slab
CSCvn30912	Snmpd process may crash due to memory leak during the long run
CSCwb26794	Unexpected Reload on a N5k device due to a AFM hap reset
CSCwb30111	Traffic dropped post LACP PO member P to I state logical transition with no lacp suspend-individual
CSCwb58131	N6K crash due to ethpm when load config
CSCwb94829	LLDP Port Description Value Incorrect
CSCwc13512	NXOS CLI command accepted when invalid
CSCwc37089	Cannot remove `logging level user 6` from configuration - 7.3(11)N1(1)

Resolved Caveats in Cisco NX-OS Release 7.3(11)N1(1)

Table 28 Resolved Caveats in Cisco NX-OS Release 7.3(11)N1(1)

Caveat ID Number	Description
CSCve13331	syslogs aren't generated by EEM with scale-limit monitor feature enabled
CSCvj70275	N7K%SYSMGR-2-VOLATILE_DB_FULL: high usage in /dev/shm
CSCvw45465	Nexus TACACS crash due to SHA1 memory leak
CSCvz14369	EEM script with Cron timer configuration randomly stop working
CSCvz32435	bios_daemon hap reset silent reload Exit code: (null) (255) no core file
CSCvz43090	N5K vsh core - VSHD-2-VSHD_SYSLOG_EOL_ERR
CSCvz47694	Nexus Switch unexpectedly reboots due to private-vlan process.
CSCvz60527	N5K uses wrong MAC address for BFD when replace peer switch
CSCvz73221	N5K: VXLAN EVPN L2 multicast interrupt on local leaf node
CSCvz87980	VTP hap reset due to memory leak
CSCvz94985	N5596: False SNMP values for transceiver details
CSCvz97066	SYSMGR-2-SERVICE_CRASHED: Service “eth_port_sec”
CSCwa12071	N2K-C2348: CFG_PORT_ID mis programming after HIF link flaps
CSCwa32959	64 bytes of garbage message at the end of a decrypted snmp v3 response packet from Nexus5k
CSCwa34646	Nexus OSPF process crash in N5k
CSCwa40815	FEX links flapping due to TFTP failure could cause an unexpected reload
CSCwa42205	EEM that redirects CLI output piped to XML/JSON to file does not work

Resolved Caveats in Cisco NX-OS Release 7.3(10)N1(1)

Table 29 Resolved Caveats in Cisco NX-OS Release 7.3(10)N1(1)

Caveat ID Number	Description
CSCui72164	CFS process may core following a hardware failure on vPC peer
CSCvc44877	Everest: IGMP Entries not removed with Continuous Leave stream on L2/L3 Interface
CSCvf30935	Eigrp routes flap if OSPF is removed from the switch
CSCvo90653	Graceful SPT switch-over
CSCvw88122	Nexus switch reloads due to "fwm hap reset" due to corrupted vlan id.
CSCvw91793	FIP CVL should be sent to Enode MAC instead of the VN_Port MAC
CSCvx59326	AAA process crash due to HAP reset.
CSCvx69757	N55-PDC-1100W PSUs on Nexus 5648Q intermittently reported as failed and recovering immediately

Table 29 Resolved Caveats in Cisco NX-OS Release 7.3(10)N1(1)

Caveat ID Number	Description
CSCvx72821	Port-Channel with Cisco switch OUI 0xDC774C or 0x4CE176 or 0x3C13CC does not come up or trunk.
CSCvx75284	DFA: host mobility not working between DCs if leaves are VPC
CSCvx89955	N5672UP-16G Incorrect transceiver sync and transmit fault count at 16G link speed.
CSCvx91633	show logging commands result in not enough memory
CSCvy07033	N5K: 'VLAN to VNI mapping is incorrect' log generates by non VXLAN enabled device
CSCvy28073	PIM crashes after configuring - ip pim rp-candidate
CSCvy32857	N5600/N6000- After disabling / re-enabling LLDP, DCBX info missing from PDU
CSCvy57499	Kernel Panic in fc2

Resolved Caveats in Cisco NX-OS Release 7.3(9)N1(1)

Table 30 Resolved Caveats in Cisco NX-OS Release 7.3(9)N1(1)

Caveat ID Number	Description
CSCvp52698	N56k switches do not automatically save core files to bootflash:
CSCvu39910	IPv6 routes redistributed from BGP missing after changing to MT
CSCvu76363	dhcp_snoop hap reset when configuring dhcp after ND-ISSU
CSCvv11854	HSRP vmac is learn from wrong ports on switch in hsrp Listen state
CSCvv14476	Interface is removed after removal command fails TACACS command authorization
CSCvv17429	SNMP does not show interface stats when we have FC configured on same module
CSCvv30267	Radius using md5 authentication is not supported by FIPS standard, add CLI warning if configured.
CSCvv33602	PFMA HAP Reset in N5K
CSCvv55432	689710350 UNIVERSITY: N5K-C5596UP-FA -N5K zoneset interface number wrong
CSCvv72593	Storm control doesn't take affect even when the traffic on FEX HIF is higher than broadcast level
CSCvv80013	Macs stuck or lost after rapid flap in VXLAN
CSCvv99626	Nexus5k crashed due to afm hap reset
CSCvw11909	N56K: Certain third party 40G to 10G breakout cables not recognized 5624,5648 and 5672UP-16G
CSCvw15198	N5K Service “__inst_001__rip” (PID 4884) hasn't caught signal 11 (core will be saved)
CSCvw15473	MPLS LDP IGP SYNC is not working properly on N7K/8.4.3/M3 with ISIS.
CSCvw18496	“cisco id is --” in show interface transceiver | Nexus 5672UP
CSCvw27543	PTP Grandmaster flapping issue due to SNMP polling
CSCvw45963	Nexus 5K crash in AAA process after multiple login failures
CSCvw59656	TLVU: Memory Leak when 'show system internal vpcm info vpc' is used
CSCvw60214	EEM script blocks certain PTS and after 32 blocked terminal logging stops working

Table 30 Resolved Caveats in Cisco NX-OS Release 7.3(9)N1(1)

Caveat ID Number	Description
CSCvw71912	Improper error message printing causing RPM crash
CSCvw76960	N5K: port-profile crash with abort raised from ppm_strncat_wrapper on large vlan lists
CSCvw82110	In 7.3(8)N1(1), VFC bound to HIF-port-channel is getting MAC from pcfcfmac pool
CSCvw88122	Nexus switch reloads due to “fwm hap reset” due to corrupted vlan id.
CSCvw91793	FIP CVL should be sent to Enode MAC instead of the VN_Port MAC
CSCvx03056	Nexus 5500 reports incorrect storm control traffic type and threshold
CSCvx06215	Traceback: vtp hap reset due to malloc

Resolved Caveats in Cisco NX-OS Release 7.3(8)N1(1)

Table 31 Resolved Caveats in Cisco NX-OS Release 7.3(8)N1(1)

Caveat ID Number	Description
CSCum31127	PIM/IGMP: MTS buffers become full when high IGMP/PIM traffic rate received by device
CSCur23755	edge-port config does not work w/o mac addr-table loop-detect port-down
CSCvi75064	MTS buffer stuck when configuring “logging source interface” on N5K/N6K
CSCvj07101	Copying SNMP MIB using IPV6 causes a reload
CSCvk68792	NXOS: Netstack crash observed with active timer library in heap_extract_min
CSCvr05880	When reload N2K-C2232PP-10GE with GLC-T/GLC-TE, peer NIC comes up & goes down on boot up
CSCvr96953	Users cannot authenticate against RADIUS/TACACS+ if custom role offered was recently modified
CSCvs77848	Nexus 5K - M2RIB not updated when flex-link co-learned port becomes primary
CSCvs80995	Vlan Manager crash due to heartbeat failure
CSCvs84839	PTP core when configuring PTP on M20UP module for N5696
CSCvs98307	Periodic stats collections at AFM delay PTP TCAM disable and enable functionality.
CSCvt13079	Unable to disable unknown multicast blocking on switchport
CSCvt21707	CFS Process Crashes Due to Memory Exhaustion
CSCvt25511	DFA multicast flow between vpc pair, both mc rec and mc src on orphan ports in same vlan, not work
CSCvt58479	FEX N2K-C2232TM Fails after upgrading to 7.3(7)N1(1)
CSCvt64497	Add OUI 10:B3:D5 to the default OUI list (MDS customer bug)
CSCvt73484	no power trap is sent when unplug the power supply of the fex.
CSCvt82666	traffic loss when fex-fabric reconnected with N2348
CSCvu00553	OSPF Sets Type-5 FA for local routes
CSCvu02581	Newly added normal-range vlans lost after reloading if VTP enabled
CSCvu06665	Storm-control does not detect IPv6 multicast on 5672 running 7.3(7)N1(1)
CSCvu10626	"Suspended due to port binding" error for Fex FC ports while upgrading to 7.3(6)N1(1) version
CSCvu20245	PIM crash when freeing memory
CSCvu25056	Show tech includes 'show platform fwm mem-stats detail' but the command doesn't work
CSCvu40307	Process MIB always returns the physical index as 1 for N5K
CSCvu43036	EIGRP adjacency not coming up in VPC+
CSCvu59829	incomplete UDLD status via SNMP Nexus 5600
CSCvu63081	FEX 2248 dropping multicast during IGMP update from client on a different FEX

Table 31 Resolved Caveats in Cisco NX-OS Release 7.3(8)N1(1)

Caveat ID Number	Description
CSCvu65037	fc san-port-channel member port sometimes in init state with 2 or more ports in the san-port-channel
CSCvu65455	show diff command doesn't work with startup-config
CSCvu66012	N5K- Passwordless SCP is not working inside an EEM script
CSCvu70864	Nexus 5596 continuous VSH process crash
CSCvu95003	Nexus FWM crash during ND upgrade
CSCvu90705	isis ipv6 routes are shown as pending ((nil), 0) for MT-IPV6-UNICAST topology

Resolved Caveats in Cisco NX-OS Release 7.3(7)N1(1b)

Refer to the following security advisory:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ipip-dos-kCT9X4

Resolved Caveats in Cisco NX-OS Release 7.3(7)N1(1a)

Table 32 Resolved Caveats in Cisco NX-OS Release 7.3(7)N1(1a)

Caveat ID Number	Description
CSCvt25511	DFA multicast flow between vpc pair, both mc rec and mc src on orphan ports in same vlan, not work.
CSCvt58479	FEX N2K-C2232TM Fails after upgrading to 7.3(7)N1(1)
CSCvs98307	Periodic stats collections at AFM delay PTP TCAM disable and enable functionality.

Resolved Caveats in Cisco NX-OS Release 7.3(7)N1(1)

Table 33 Resolved Caveats in Cisco NX-OS Release 7.3(7)N1(1)

Caveat ID Number	Description
CSCvc42886	N56xx - No SSH possible to device when root directory is full due to nxapi request
CSCvn95489	show running-config diff still displays diff after 'copy run start' command
CSCvr05880	When reload N2K-C2232PP-10GE with GLC-T, peer NIC comes up & down before nxos takes control the FEX
CSCvr06481	NVE library not initialized by client syslog during host delete/re-add in DFA fabric
CSCvr08343	Forwarding manager Daemon crash due to Heartbeat Failure
CSCvr20115	VPC Orphan Suspend reinit is seen for invalid interfaces - "port not present"
CSCvr31887	fwm crash when applying 4042 as FCOE/VSAN config
CSCvr40993	FEX 103 started to flap,SDP timeout/SFP Mismatch
CSCvr49513	OID is not increasing for entSensorType
CSCvr53123	After reload with mac address-table router-mac learn-enable, SVI macs are not programmed on GEM
CSCvr74305	Nexus pim hap reset
CSCvr75968	change in JSON format for the output "show interface transceiver details | json"
CSCvr93847	Ingress BUM traffic dropped due to incorrect rpf vector programming for overlay port-channel
CSCvs01424	Nexus56128P - kernel panic in fcpc process
CSCvs07988	Nexus crashes just after configuring FEX ports as L2 trunk
CSCvs22600	FWM crash when bringing up VPC link
CSCvs31019	switch powered down due to configured fan policy
CSCvs50363	disabling port-channel takes up to 20 seconds in VPC environment
CSCvs56311	NX-OS Crash in SNMPd Process Due to signal 8, Arithmetic exception.
CSCvs71045	FPOAM crash on all spines when running traceroute fabricpath CLI from Leaf
CSCvn05569	Port-Channel remains suspended
CSCvs41591	Handle SUNNYVALE ASIC errors
CSCvp54881	Unable to create San Port Channel between UCS & Nexus 56128p
CSCvr19956	cefcModuleOperStatus is not responding for N55-M160L3-V2

Resolved Caveats in Cisco NX-OS Release 7.3(6)N1(1)

Table 34 Resolved Caveats in Cisco NX-OS Release 7.3(6)N1(1)

Caveat ID Number	Description
CSCus75293	Nexus 5000 add interface status down due to invalid QoS
CSCuy87611	Need to suppress vtp_ascii_gen_cb() logs in vtp_debug.log
CSCvc49591	Missing IGMP Entries after N7K joining vPC domain
CSCvd14248	evpn ESI local host mac-ip incorrectly flagged as static - mac out of sync in l2irb
CSCvd21524	N5K: snmp trap connUnitPortStatusChange is sent for Eth interface down
CSCvd40670	2248PQ fex: SNMP walk on ENTITY SENSOR MIB shows incorrect values for Control sensor
CSCvd52503	FC Transceiver details warning and alarm symbols
CSCvf31178	N77/M3/VPLS/PIM: PIM-3-AVL_ERROR: AVL-tree operation ravl_insert() failed for PIM Assert FSM
CSCvi93291	MAC learning issue with dhcp relay after host migration
CSCvm65905	(N2348TQ) FEX gets disconnected due SATMGR when executing "show alog"
CSCvn37301	With passive TWINAX cable N2K-C2348TQ-10G-E reports the Fan Failure
CSCvn98850	N2k psoc_mgr crash
CSCvn99156	Incorrect number of prefixes sent if Candidate-RP list packet length greater than configured PIM MTU
CSCvo03719	FWM process crash when trying to program 40G Port-channel member table
CSCvo15674	crash because of memory leak in bfd process
CSCvo19738	BFD neighbor on static route does not up if one end SVI is bounced
CSCvo20196	Stale host route stuck in UFIB after multicast traffic received on source tree.
CSCvo20669	Port-profile database corrupted after adding new vlans
CSCvo29736	SNMP polling of transceiver DOM values intermittently returns wrong values
CSCvo31748	MAC addresses flapping of DHCP client and relay agents
CSCvo47512	"show mac address-table" incorrect in show tech
CSCvo51233	FWM crash with full MAC address table.
CSCvo54734	N5K/6K: After ISSU, Fabricpath VLANs not part of flood list on core facing interfaces
CSCvo56362	Nexus 5k crashed due to fabric_mcast hap reset
CSCvo71558	Incorrectly printing "%STP-2-VLAN_PORT_LIMIT_EXCEEDED: The number of vlan-port instances"
CSCvo87478	n5k // "Duplicate entry found in PPM database" when addding new command to port-profile
CSCvo88678	Extraneous line in show ip bgp output
CSCvp05588	When polling ENTITY-MIB, FEX related data is not being returned

Table 34 Resolved Caveats in Cisco NX-OS Release 7.3(6)N1(1)

Caveat ID Number	Description
CSCvp05823	Constant NTPd (non-sysmgr) Crash on NX-OS 7.3(5)N1(1), Recurrence of CSCuu13856
CSCvp08694	Stale arp entry/route after VM move from one VPC domain to other due to HMM update failure
CSCvp16499	VPC Orphan Suspend - Reinit failed "port not present" on reload
CSCvp18771	fc interface zoning shows erroneous swwns in the active zoneset
CSCvp45375	N5672UP has reloaded after "inherit port-profile NAME" command
CSCvp52300	N5K/7.3(5)N1(1): %FCNS-3-BAD_FRAME: %$VSAN 99%$: Invalid CT command code <<no interface and CT code
CSCvp58845	After remove/add VRF, remote host routes not installed to URIB and report 'remote nh not installed'
CSCvp64501	Enhancement to retry reading PS Presence during PSU failures
CSCvp67180	Crash CLI thread at the moment of deleting a SVI
CSCvp70317	N2K-C2232PP-10GE(with N5/6/7/9K parents) GLC-TE/T SFP is not recognized after reseating.
CSCvp75032	VRF missing after upgrade to 7.3(5)N1(1)
CSCvp75413	N5K/6K: logging server <hostname> uses old IP address
CSCvp76175	FC traffic through 2348UPQ FEX is interrupted when Eth.int configured for FCoE on same FEX is shut.
CSCvp90218	N55-M8P8FP module: FC SFP transceiver details isn't working correctly
CSCvp93415	psoc_mgr memory corruption for B22 DELL fex
CSCvq02173	dhcp_snoop reset on nexus 5000
CSCvq07847	N5k Fex process crashes after FEX uplink flaps repeatedly
CSCvq21920	Nexus 56K console loop on username/password prompt
CSCvq35994	N5600 overwrites incorrectly GM clock variance in PTP announce message
CSCvq36736	ipqosmgr crash on Nexus 5696
CSCvq37608	sh fex 'fex num' transceiver - shows "sfp is present but not supported"
CSCvq42668	nexus7k heartbeat failure IGMP crash
CSCvq53154	mrib crash when collecting mcast show tech with N7K in SDA border role.
CSCvq54180	kernel panic in fcpc process
CSCvq56346	N56128 crashed due to cdp hap reset running 7.3(5)N1(1)
CSCvq69480	pvlan crashed on fex scale setup with snmpwalk on oid iso.3.6.1.4.1.9.9.82.1.11.2
CSCvq72873	entSensorThresholdNotification is sent after fex becomes online
CSCvq79234	N5K orphan ports came up momentarily even with 'vpc orphan-port suspend' after switch reload
CSCvq91588	Nexus 5500 - 7.3(5)N1(1) and prior - VFC interface "no shut" causes fwm hap reset

Table 34 Resolved Caveats in Cisco NX-OS Release 7.3(6)N1(1)

Caveat ID Number	Description
CSCum46904	Errdisable recovery cause dcvx cli not seen in running
CSCus37253	Turning on Port-track feature throws error

Resolved Caveats in Cisco NX-OS Release 7.3(5)N1(1)

Table 35 Resolved Caveats in Cisco NX-OS Release 7.3(5)N1(1)

Caveat ID Number	Description
CSCvb24457	T2:123: %LIBOSC-2-OSC_ERR: DATACORRUPTION-DATAINCONSISTENCY EIGRP
CSCvb34336	Link stays up even after removing cable after ND ISSU from 6.0 to 7.0
CSCvc43642	L3 traffic from secondary vlan to regular vlan is getting flooded instead of routed causing drops
CSCvd61694	GARP for Anycast HSRP VIP is sent with non-zero LID
CSCvd79462	Mem leak in confcheck process when executing "show install all impact" command
CSCve00906	vlan mutex locked when config range of vlans with automated tool
CSCvh04052	LISP: directed broadcasts cause false positive host detections
CSCvh87828	lisp punt route nexthop not deleted/updated for all interfaces/routes after BGP nexthop change
CSCvi11059	F2 linecard goes into a booting loop when more than 200 "vpc orphan-port suspend" are configured.
CSCvi11432	N5600 per link BFD session may not come up after interface no shut
CSCvi88404	N5K: var/tmp is full with csm_sh_run_acfg files
CSCvj14664	BFD CoS markings are not preserved from its DSCP
CSCvk36753	N5k :: SNMP RBAC not working
CSCvk43520	Snmp counter are increasing after several snmp walk.
CSCvk67894	Feature flexlink is disabled after Software Upgrade to 7.3.3
CSCvm02579	Incorrect code fix of CSCuu39555 for N5K causes HSRP VIP subnet issue after upgrade
CSCvm09038	"switchport trunk mode on" causes existing FC san-port-channel to go down and not recover
CSCvm23492	SVI interfaces can not be displayed in "show interface description"
CSCvm46998	N5600: DHCP OFFER looping after upgrade to 7.3(3)N1(1)
CSCvm48443	Nexus 5k FEX - Show Run vs Show Run All Discrapancy
CSCvm53809	After upgrading Nexus 5k switch from 5.x to 7.x, system CPU usage has increased by 10-20% in pktmgr
CSCvm54522	n5k cli counter for output error is not consistent with snmp ifOutErrors

Table 35 Resolved Caveats in Cisco NX-OS Release 7.3(5)N1(1)

Caveat ID Number	Description
CSCvm55640	FEX not process NIF down when parent's ports shutdown or power off
CSCvm65175	N2348TQ HIF's PHY firmware upgrade -10G Auto-negotiation
CSCvm65636	nexus 56128 snmp ifInUcastPkts reports 0 for 10g breakout interfaces
CSCvm69385	Clear ip mroute leaves entry in MFIB
CSCvm75648	AFM reset due to heartbeat failure
CSCvm81228	NXOS: Kernel panic in igmp:igmp-cli-t
CSCvm86801	N5K running 7.1(5)N1(1) Service "snmpd" crash
CSCvm96110	N55-PDC-1100W intermittently reported as failed or shutdown, and recovering immediately afterwards
CSCvm96743	N5600/N6000: SVI MAC not installed in myipr table
CSCvn17202	Unable to decode core file after unexpected reload - Nexus 5000
CSCvn18744	N2K-C2232PP-10GE GLC-TE= SFP is not recognized in ports 9,10,24,26,28
CSCvn25659	vxlan+vpc env, some server can't ping successful after reloading module of one leaf
CSCvn25729	N6k :: configure profile commands missing after disruptive software upgrade
CSCvn27038	qd hap reset due to memory leak
CSCvn35480	After upgrade the fex reports the same "MajorThresh" and "MinorThres" temperature thresholds

Resolved Caveats in Cisco NX-OS Release 7.3(4)N1(1)

Table 36 Resolved Caveats in Cisco NX-OS Release 7.3(4)N1(1)

Caveat ID Number	Description
CSCvj84775	PIM6 Anycast-RP failling to send Register-Stop
CSCvk41424	fabric-access process crash on N5K-C5696Q
CSCsz95889	"BB credit transitions from zero" counter not incrementing during periods of congestion
CSCul25498	remove-private AS does not remove 4-byte private ASN's
CSCup42901	"no power resource" in the output of show environment fex command
CSCuq83491	5548UP timeout drops not showing up under output discards
CSCuv49772	Cisco part number and pid not displayed for FC SFP on N5k/N6k
CSCvc81065	N5K: FC/FCoE OID 1.3.6.1.3.94.1.6 timeouts
CSCve01571	Memory leak in "fcpc" -- FU_MEM_fu_msg_id_node_wrap_t
CSCve33644	N5K: ETHPM buffer leak on FEX HIF after L2 loop
CSCve52503	"ETHPORT-3-IF_NON_CISCO_TRANSCEIVER: Non-Cisco" for some twinax cables

Table 36 Resolved Caveats in Cisco NX-OS Release 7.3(4)N1(1)

Caveat ID Number	Description
CSCvf79399	2232PP FEX module Crash when inserting 4 GLC-TE transceivers into FEX HIF port
CSCvh69943	Nexus: Errors Seen in Ranged "show accounting log" Outputs After Configuring Daylight Saving Time
CSCvi14840	Nexus might crash after creating multiple MSDP mesh groups
CSCvi96969	Static VPC port-channel enabled prematurely on bootup
CSCvj01313	N5K/N6K PTP Process crash with NULL pointer mts_wrap_p
CSCvj08973	snmpd hap reset crash when snmpwalk on OID stpxMSTInstanceVlansMapped2k
CSCvj24868	MTS buffers' leak while constantly polling objects in BRIDGE-MIB
CSCvj39629	Ifmgr to return success for lc_remove seq when module is not existent
CSCvj44528	N5600-M12-Q and N5600-48Q-12Q-FIX modules may remain offline after switch reload
CSCvj61755	Dynamic vfc should not allow "switchport mode F"
CSCvj67123	N56xx / N6k: multiple interrupts on BIGSUR when using 1Gig SFP and the port is down.
CSCvj69502	Nexus doesn't send remote address in command authorization packets for non-interactive ssh sessions
CSCvj69510	Nexus doesn't send remote address in command authorization packets for nxapi calls
CSCvj83542	N5K ethpm HAP reset after memory depletion
CSCvj88104	VLAN mapping configuration not applied to port-channel members and causing flapping of interfaces.
CSCvk17715	N5k :: cannot save configuration due to "Service "AAA Daemon" failed to store its configuration"
CSCvk22067	Crash due to fwm hap reset
CSCvk25746	fcoe fcf mac address should not be checked out for non fcoe port-channel when vpc is enabled
CSCvk29478	ARP is not learnt on non-directly connected VPC peer for the Orphan host in a VXLAN EVPN setup.
CSCvk35035	logging server vrf name in startup-config changed after reload
CSCvk72224	Nexus 5k: Port Profile Memory Leak
CSCvm06361	Python shell cli execution throws 'cisco.cli_execution_error:'
CSCvm07315	Add 'show tech fwm' to show tech detail
CSCvm12103	intermittent Unicast traffic dropped on FTAG-1 root switch when reloaded, high scale setup.
CSCvm16677	PSS memory leak in igmp_snoop for key type 0x04 and 0x0d

Resolved Caveats in Cisco NX-OS Release 7.3(3)N1(1)

Table 37 Resolved Caveats in Cisco NX-OS Release 7.3(3)N1(1)

Caveat ID Number	Description
CSCvj22890	Disruptive upgrade from 7.0.3 to 7.1.4/.5/7.3.2 changes store and forward, cut through settings.
CSCve87569	SNMPUSER CLI cannot create the user in the User database
CSCux87740	N7k uses wrong MAC address for BFD when peer switches mac address
CSCvf05783	N5k (5548) pipe to JSON returns empty output.
CSCvh78863	n56128 fwm hap reset with multicast routing enabled
CSCvf50659	Service "eem_policy_dir" (PID 4233) is forced exit during ISSU
CSCum48625	eth_port_sec hap reset seen on removing the static secured mac
CSCve62895	Nexus 5000: upgrade to 7.3(2)N1(1) firmware version info unable to Sync with PI
CSCve86927	Nexus 5000: fwm hap reset when configuring erspan on fex
CSCvg60756	FHR not sending register to RP due to SGR prune
CSCvg71991	ARP Entries Are Flapping in vPC VXLAN EVPN Setup
CSCve47401	N3K/N9K/N7K OSPF Rogue LSA with maximum sequence number vulnerability
CSCvf14879	Cisco Nexus Series Switches CLI Command Injection Vulnerability
CSCvf14926	Cisco NX-OS System Software CLI Command Injection Vulnerability
CSCvg04072	Cisco NX-OS System Software Patch Installation Command Injection Vulnerability
CSCvg41173	Cisco NX-OS Software removes ACL from VTY interface
CSCua04911	Entering '@' symbol during console authentication removes previous text
CSCup79623	EEM:S5: show eem history events: not over writing after 50 applets
CSCur48104	fcoe fcf mac address should not be checked out for non fcoe port-channel
CSCut52109	Nexus5600/Nexus6000 ->40G-> sh int fex XX transceiver - SFP present but does not support
CSCuy22022	N2K-B22IBM-P FEX temperature sensor failed
CSCuy90720	Nexus5000/Nexus6000 Kernel Panic / Watchdog Timeout due to usb_stor_control_thread.
CSCuz81712	ENH: snmpCommunityTable to use alphanumerical index values (ASCII) only
CSCuz97563	FCP_ERRFCP_PORT Error Messages seen when enabled for or making changes in FCoE Configuration
CSCva47977	Switch-profile database not in sync after defaulting the interface
CSCvb15891	Post ND ISSU sh vlan id <> shows promiscuous trunk po123 for all vlans
CSCvb86787	Cisco Nexus 5K/6K/7K/9K/9500-R/MDS CLI Command Injection Vulnerability
CSCvb91037	CTS: N6K(5672_up) rejecting LACP BPDUs due to CMD tag
CSCvc16208	Nexus6000 Enumeration limit for output of "show interface fex-fabric".

CSCvc44767	hashlib.py not found in 7.3(1)1D1(1)
CSCvc81119	Better logging in syslogs and enhance error correction for SUN_FI_NEW_C5_INT_2_XGXS_rx1_fifo_err
CSCvc84738	Nexus 5548 Kernel Panic Due to Corruption in mtsbuf
CSCvc90796	Sync with NTP servers lost intermittently
CSCvd19871	Terminal monitor not showing any output
CSCvd23076	TACACS crashes when buffer limit (>2072) is crossed for valid command arguments
CSCvd29390	TAH ISSU : ISSU failed during saving MTS state
CSCvd36242	ISIS crashes in isis_srm_stop_timer_next
CSCvd42177	Nexus5000/Nexus6000 : Cannot Save Running Config + Bootflash in read-only state
CSCvd48146	psoc_mgr process to save log file in /tmp directory to bootflash when B22 FEX crashes.
CSCvd90058	FC memory leak causing the devices to go unstable
CSCve13020	tftp_si_entries is read-only
CSCve21005	"show sprom sup" is not showing correct Hardware version for Nexus 5000
CSCve25225	N5K-C5672 zombie process [fh_ttyd] <defunct> increasing when trigger EEM applet
CSCve41802	Duplicate syslog messages for Interface x/y is down.
CSCve56063	Nexus5000 Watchdog at pfm_norcal_driver_nmi_cb
CSCve57871	Nexus5600 vPC FEX MAC not updated through GARP after move
CSCve63609	Crash due to Fwm heartbeat failure
CSCve72490	Offline port RSCN not sent
CSCve93651	Broken VRF Due to RD Change in BGP
CSCve93863	Cisco FX-OS and NX-OS System Software CLI Command Injection Vulnerability
CSCvf02937	Nexus5000 crash when pushing zone change from DCNM
CSCvf06777	2348TQ FEX black holing ingress traffic during online sequence due to early linkup on HIF
CSCvf09556	Nexus5000 XML stops working post upgrade
CSCvf15167	Cisco NX-OS System Software CLI Command Injection Vulnerability
CSCvf15198	Cisco NX-OS Python Parser Escape Vulnerability
CSCvf29419	Cisco Nexus 5000/6000 Series Switches Privilege Escalation via Sudo
CSCvf31132	Cisco NX-OS System Software Management Interface Denial of Service Vulnerability
CSCvf35481	fwm hap-reset after ISSU when no shut on vlan translation enabled port
CSCvf35575	When using 'clock source ptp', time shown in outputs is offset by TAI/UTC difference
CSCvf36902	N5K-C5672 eem_policy_dir memory usage increasing after long time get no response

CSCvf42847	Nexus 5000 sh lldp neighbors | xml > conversion failed due to conv error
CSCvf43404	Stale Entries in NIF ASIC causing BIG_DROP_SRC_VLAN_MBR Drops
CSCvf44671	False positive SNMP traps generated for unknown Fex Fan
CSCvf44985	DHCP Relay does not recalculate UDP checksum of relayed packets if their GIADDR is non-zero
CSCvf49466	ISSU from 7.1(4)N1(1) to 7.1(4)N1(1e) : FEXes did not come online after SUP ISSU
CSCvf50699	switchport trunk allowed vlan add removes existing vlans from a trunk interface
CSCvf53881	Device connected N2K-C2348TQ-10G-E HIF port not going down when FEX HIF is admin down state
CSCvf60485	Nexus 5000/7.1(4)N1(1) - Nexus intermittently showing wrong values for SFP sensors
CSCvf62005	PFMA segmentation fault due to RR index out of bounds
CSCvf66000	static ARP might point to wrong physical interface
CSCvf66491	PIM crash when freeing memory
CSCvf73400	Nexus5000/6000 -> Repeated worker process: check_tty:could not get tty - nxapi syslog
CSCvf75697	Nexus 5000 Crashes During CTS (Cisco TrustSec) Server Update
CSCvf77327	ARP Performance Improvement when ARP suppression is enabled
CSCvf79399	FEX module Crash when inserting 4 GLC-TE transceivers into FEX HIF port
CSCvf80455	2348UPQ FEX brings up certain HIF links ahead of time during NX-OS upgrade
CSCvf83485	Link interruption caused crash of isis_fabricpath
CSCvf90675	Unable to create SVI when using local user with read-write custom role
CSCvf97641	Nexus 5548 - show tech-support fex command drop TELNET and SSH session
CSCvg07980	FWM crashes when FEX connected to 2 cards on N5K or unplug one cable from 2 cards
CSCvg11339	SHOW TECH-SUPPORT DETAILS - Access Control Table For VSAN: xxx corrupted, incorrect
CSCvg19150	Nexus5000/6000: Clear ip mroute can cause FWM process to crash
CSCvg19370	Nexus 5672 crash due to port-profile when HIF config change
CSCvg27448	Invalid command message Instead of incomplete command message
CSCvg31154	Nexus5000/6000 unable to toggle CFS for syslogd
CSCvg34238	fcFeModuleFxPortCapacity does not return expected values
CSCvg34243	SW WA for N6K not responding to NS to GL from link-local
CSCvg36035	Non-Default FC-map causes mis-programming of MAC Addresses for FC and FCOE hosts and targets
CSCvg42136	Nexus5000 : Port-security MAC address programmed on a peer-link for a non-up port
CSCvg49250	ARP Entries Are Flapping in vPC VXLAN Setup
CSCvg63685	EEM Script can not run completely after upgrade from 7.1 to 7.3
CSCvg66767	DOC: N5k SNMP Polling causes device reboot

CSCvg72033	Process FEX infinite loop on processing corrupted packet causes crash
CSCvg74817	Nexus5000/6000: PS failure not detected
CSCvg80137	SNMP traps CLIs are missing after Upgrade
CSCvg87171	AFM process crash
CSCvg88176	Nexus6000 sends PTP packets with TTL 1
CSCvg94995	XMLization for "show interface brief" command returns inconsistent output w/ FC and VFC ports
CSCvh01841	Slack memory leak in /lib/libglib-2.0.so.0.1600.3
CSCvh10932	after issu to 7.3(2)N1(1c) when remove or add a vlan on a trunk get error message (cosmetic only)
CSCvh24664	"interface-vlan hap reset" reload due to memory leak in "interface-vlan Daemon"
CSCvh30000	N56K:ifSpeed/ifHighSpeed does not return the actual BW
CSCvh31138	Incorrect CDCE mac programming in few bigsur ASIC instances upon mac moves in Vxlan setup
CSCvh32749	Port Manager memory leak @ PM_MEM_fu_fc2_frame_t
CSCvh55370	%SYSMGR-3-CFGWRITE_FAILED: Configuration copy failed (error-id 0x401E0000) when copy r s
CSCvh58010	CRC 10b to 10d option doesn't appear in the CLI for 5624 and 5648 Platform
CSCvh58035	Nexus5000/6000::fix for CSCvg34243 does not work with "hardware ipv6 glean throttle" command configured
CSCvh61832	Nexus 5672-16G platform: PLOGI failing in case of San-Port-channel in NP mode
CSCvh73021	Nexus5000- Unable to delete/add port-channels
CSCvh77328	N5600: VPC cannot get port-channel STP status on bootup with 8 linecards
CSCvh92726	Nexus5000: vxlan evpn prevents internal communication with FEX
CSCvi07117	MTS buffers leak on SAP 407 CoPP from SAP 27 SNMP Response opcode 7679
CSCvi09328	Nexus 5600/6000: IGMP snooping mrouter ports are not VLAN aware
CSCvi33605	SNMP ColdStart Trap is sent, when the snmpd process is crashed

Resolved Caveats in Cisco NX-OS Release 7.3(2)N1(1)

Table 38 Resolved Caveats in Cisco NX-OS Release 7.3(2)N1(1)

Caveat ID Number	Description
CSCux99818	pim process crash due to corruption caused by lmemory depletion
CSCto57719	"spanning-tree port-priority" changed to "0" from "128" in show run all"
CSCtw96661	N5K not able to suppress Sev5 syslog messages related with connected FEX
CSCtz05620	O2-96-T:Kernel Panic when provision GEM modules & sw got reset
CSCua04442	Nexus 5000: vFC down does not trigger callhome alert

Table 38 Resolved Caveats in Cisco NX-OS Release 7.3(2)N1(1) (continued)

Caveat ID Number	Description
CSCub14112	UDLD clean up for fex-fabric ports
CSCub16077	FRAME DISCARD message seen after bringing up multi-hop FCoE vfc intf
CSCue41816	"sh hardware internal fc-mac <> port <> statistics" clear enhancement
CSCue76773	"ip routing multicast software-replicate" Support for N5K/N6k platform
CSCuh78381	SAN Port-channel reports as going down when a member link fails
CSCuh90262	'hsrp bfd' config is not indented under interface vlan after ISSU
CSCuj36664	SYSMGR-2-SERVICE cfs crashed unexpectedly
CSCuj70799	Powered-down due to fan policy trigger after SFP insert
CSCun30488	N 55K series switch does not show more than 255 tx credits on fc int
CSCuo03534	dcos-telnetd crash with SIG3
CSCuo24670	N5K/FEX FEX Interface Incrementing output discards rapidly
CSCuo37471	N7k/RIB displays HSRP VIP route incorrectly
CSCuo49098	show flogi event-history is broken when using FPORT SAN-Port-Channel.
CSCuo66649	bigsurusd core on adding member port to portchannel
CSCuo79180	copy run start fails: Service "flogi" failed to store its configuration
CSCuo95666	N5K/6K: Enhance logging capabilities for ASIC failures
CSCup76173	240/249 ERROR: Timer expired on replay config cfs hap reset at syscall()
CSCuq60111	Incorrect Type 1 vPC consistency for "vPC card type" in Enhanced vPC
CSCuq72020	Forwarding ASIC Diag Error not forcing links to go down completely
CSCur13534	ptplc reset while copy ptp config followed by poweroff & no poweroff mod
CSCur22079	Cisco Nexus 2K Fabric Extender Software Default Credential Vulnerability
CSCur59733	IPv6 TACACS Auth Fails On N7K/N9K Over Mgmt VRF
CSCur89779	(S, G) not timing out even if there is no traffic
CSCus22583	Changing the port type doesn't remove the configuration from startup
CSCus44812	SS Fex:Bootup diag detected major event: Forwarding ASIC failure
CSCus67475	FCNS cores due to fcns hap reset
CSCus71581	need to copy cores from show cores into bootflash by default
CSCus73291	Kernel Panic for process fcoe_mgr
CSCus78963	Twinpeak:Incosistent behaviour of System LED during error state
CSCut11150	OSPF max-metric doesn't work when startup timer value is default
CSCut17708	san-port-channel not load-balanced on Nexus 6000 and 5600
CSCut29890	User role hierarchy not working correctly,interfac deny overrides permit
CSCut52535	vlan mapping under vPC port cause link up delay
CSCut56888	PCI error reporting in 5K/6K products
CSCut60043	N5K/6K - 40G transceivers have delay for link-up on module boot/reload

Table 38 Resolved Caveats in Cisco NX-OS Release 7.3(2)N1(1) (continued)

Caveat ID Number	Description
CSCut64996	Nexus5548 _Ethernet ports is lost in running-config after reload
CSCut76080	N6k doesn't accept hardware profile tcam feature interface-qos limit 224
CSCut89123	Kernel panic due to "insmod" process
CSCut92989	EVPC+ peer drops FTAG2 traffic while other VPC peer initializes the FEX
CSCut93487	OTV: AED stays inactive for all VLANs
CSCut94161	EEM: Configuration failed with: 0x412c000d validation timed out
CSCuu00863	Storm Control syslog needs to specify traffic type
CSCuu10667	Multicast-routing not disabled on mgmt0 interface after disabling CFS
CSCuu21817	High convergence time for multicat/broadcast trf during vPC Primary ISSU
CSCuu31064	All Nexus Tech supports should include some basic information
CSCuu38577	N55xx,N56xx and N600x : link debounce timer may not work as configured
CSCuu65506	N5k/N6k-No support for SNMP OID access restriction / SNMP views
CSCuu70111	FWM service crash at FWM_FWIM_IF_GET_NEXT_LIF
CSCuv01780	Mgmt0 with Crossover cable and hardcoded speed 100/duplex full is down
CSCuv61110	N5K/N6K: Errors when modifying vlan allowed list in port-profile on FEX
CSCuv74091	Add predefined FCoE+Jumbo QoS policy
CSCuv74260	Add ieee8021PFCMib specification to Nexus 5k/6k platform
CSCuv82106	Multicast traffic gets blackholed when MVR configured
CSCuw15860	SSH Multiplexing on N9k can cause client applications to hang
CSCuw23628	[KK_113]: NFM HAP reset on performing copy r s - N56128
CSCuw26728	Enh: N5K/6K Log syslog message if ingress/egress buffer gets stuck
CSCuw40711	Nexus - in.dcos-telnetd service crash
CSCuw59277	FEX 2348 A-A: Packets send to wrong FEX HIF interface
CSCuw68009	Do not allow sampling mode of 1 out-of 1 for netflow on Nexus 6000
CSCuw71143	"no neg auto" on 2232PP,2248PQ 2348UPQ and 100M GLC-T support on 2348UPQ
CSCuw73492	N5K crash due to Service: stp hap reset
CSCuw83670	N5k/6k - AFM Errors - unknown policy - Port error disabled
CSCuw92095	NXAPI: json "show monitor session" destination interfaces incomplete
CSCuw92560	N6K kernel panic crash qh_urb_transaction
CSCuw92582	Add syslog to notify L3 interface with sub-interface limit exhausted
CSCux00981	few pkt drops when shut/no shut given on PO cfged
CSCux05255	Interface running-configuration may incorrectly show 'shutdown'
CSCux06997	inherit port-profile fails due to vpc orphan-port suspend
CSCux06999	N5K Config-Sync shows "in sync" despite "sh run switch-profile" differs
CSCux09380	IP PIM MTU to increase AUTORP packet size

Table 38 Resolved Caveats in Cisco NX-OS Release 7.3(2)N1(1) (continued)

Caveat ID Number	Description
CSCux09406	Null L2 destination address in ACC(PLOGI) frame
CSCux17060	N5K xmlma hap reset
CSCux22638	show fabric database host needs date
CSCux28524	Nexus 5K crashed due to "QD" process.
CSCux29893	"Police cir" is not limiting the traffic correctly
CSCux40274	Multicast traffic dropped due to cell usage stuck for ingress buffer
CSCux44029	XML support for show interface fcx/y transceiver details
CSCux46963	N5K kernel panic crash usd_mts_kthread Part II
CSCux47933	FEX2348 EVPC: HIF PO seconds of traffic drops after NIF failure
CSCux51705	interface counters stucked in 0
CSCux65366	MCM memory leak @ libacfg.so
CSCux68595	FWM crashes while executing "show platform load-balance forwarding-path"
CSCux75794	HA policy of Reset - Crash in port_mgr after successful ISSU
CSCux76255	vpc hap reset during ISSU from 7.0(5)N1(1) to 7.0.7.N1.1
CSCux76712	FC interface disabled due to 'bit error rate too high' when rate is low
CSCux76799	Nexus 5600: Non disruptive ISSU can fail on certain systems.
CSCux78294	Crash on router when removing L2VPN
CSCux85363	N5K/N6K : IGMP GSQ are not sent out in response to IGMP leaves
CSCux95740	port-channel member interface with vpc orphan-port suspend configured
CSCux95821	show tech-support fcoe needs to contain all pertinent FC information
CSCuy01302	IPv6 multicast traffic blackholing when ipv6 static route configured
CSCuy03675	Nexus crash in FCS process
CSCuy07502	In show running, ffff is missing from the v4 mapped v6 address.
CSCuy07577	N5600/6000 HSRP VMAC not removed after SVI delete
CSCuy08128	Cut through Threshold change on Tiburon FEX's on 40gb NIF's
CSCuy11722	N5k/6k - HSRP VMAC wrongly installed as Static in 4-way setup/VPC
CSCuy14677	Logfile "/var/tmp/ppm_logfile" taking up space in /var/tmp
CSCuy16875	CLI enhancement 'show tech afm'
CSCuy21070	Nexus5500 7.2 or 7.3 after reload, vsan down on vfc interface
CSCuy22769	VXLAN-EVPN with suppress-arp, ARP for silent destination is flooded back
CSCuy23998	N5k pbr next-hop adjacency not updated in hardware
CSCuy33905	n5600 delay in processing ethpm mts after reload
CSCuy36538	N6K: AA-FEX HIF Suspension on Parent Replacement with FEX Pre-Provision
CSCuy37201	Vlan remains in error disable state when created in fabric path and VPC
CSCuy37831	FEXs are getting reloaded, due to non reception of async notification msg

Table 38 Resolved Caveats in Cisco NX-OS Release 7.3(2)N1(1) (continued)

Caveat ID Number	Description
CSCuy43572	N5K/6K:VPC+ Peer-link going into suspend state during switch replacement
CSCuy44608	N5K -Multiple Issues with "snmp-server source-interface informs" command
CSCuy44866	ACL logging not working for egress (packet manager change)
CSCuy49328	N5596 kernel panic on carmelusd process
CSCuy58226	Remove feature to store VMAN sdwrap debug logs in a memory mapped file
CSCuy61164	fwm core with "no int po102" after seeing "%ETHPORT-2-IF_SEQ_ERROR"
CSCuy61591	Radius crash on dot1x authentication with multiple flap of authed ports
CSCuy62490	N5k: qd hap reset at qd_bigsur_lc_remove
CSCuy63746	BFD Stuck in Down state &BFD Session is not initialized On N6k-VMM issue
CSCuy65138	After ISSU from 7.1(0)N1(1b) to 7.1(3)N1(1), unused HIF will not come up
CSCuy68868	N5k/N6k VxLAN: FWM crash observed while deleting vlan to vni mapping
CSCuy69670	Nexus 5k/6k Priority Flow Control 'Off' when Interface is 'Up'
CSCuy73026	sh run for ascii-cfg not displayed correctly
CSCuy79971	9 micro sec offset corrections on N5548 switches
CSCuy79978	N5672 ptp state stuck in "Uncalibrated" State
CSCuy80838	"errdisable recovery cause security-violation" for N5k/N6k
CSCuy81174	N5K/6K: Abort install if running version of BIOS is empty
CSCuy83222	Snmp polling cause pfstats MTS buffer leak
CSCuy83572	RIP routes not installed when RIP packet has same sequence as previous
CSCuy85524	Bios image should be md5 verified after extraction prior to application
CSCuy90720	nexus 5600 kernel panic crash usb-storage usb_stor_control_thread
CSCuy91379	Nexus 5K crash at dleft_sprint_table_info
CSCuy91714	N5K-C5596UP FWM Crash During ISSU to 7.2(1)N1(1)
CSCuy93128	N5K ttyd process core when ISSU to 7.0(7)N1(1)
CSCuy94627	N5K-C5596UP FWM Crash During ISSU to 7.0(6)N1(1)
CSCuy99477	Change metrictype of redistributed routes from MPBGP-OSPF from E2 to E1
CSCuz04086	ntp source-interface does not work as expected on 7.1 images
CSCuz18971	old/inactive area-ids are not cleared from the ospf db
CSCuz22196	Nexus: snmpd Program terminated with signal 8, Arithmetic exception.
CSCuz23976	DHCP Snooping not working correctly if broadcast flag is set
CSCuz27269	N5K aclmgr hap reset when saving config
CSCuz29352	copp config isn't in show run all
CSCuz29569	Error during pre-provisioning the module of type N5696-M20UP
CSCuz40287	adbm service not responding if secure ldap fails to connect to ldap server continuously
CSCuz40720	Crash with L2MP and ECMP configured

Table 38 Resolved Caveats in Cisco NX-OS Release 7.3(2)N1(1) (continued)

Caveat ID Number	Description
CSCuz42053	N5K Crash in ethpm Due to Memory Leak in libutils.so.0.0.0
CSCuz46078	AFM: TCAM Carving of Layer 3 Card-facing UPC may cause traffic drops
CSCuz51928	icmpv6 crashes because of access to a non-readable memory region.
CSCuz52171	N5K/N6K: PVLAN HIFs Suspended/Inactive on vPC Peer Replacement
CSCuz58307	Syslog missing for %VPC-6-PEER_VPC_UP event
CSCuz58321	Enhancement: Syslog for VPC-3-PEER_REACHABLE: Remote Switch Reachable
CSCuz58351	SNMP OID - Location of FEX power supplies are not programmed correctly
CSCuz58396	Enhancement: Include domain id in %VPC-3-VPC_PEER_LINK_DOWN or UP syslog
CSCuz59030	Nexus 5000 chap protocol actually does PAP
CSCuz62143	Service not responding while enable feature fcoe in 5596UP
CSCuz68056	logging server vrf changes to vrf default after ND-ISSU
CSCuz70693	N5600 - BUM traffic with CRC error is cut-through switched
CSCuz72951	Conditional default originate broken for IPv6 BGP
CSCuz78217	DFA: Fabric database clock is not in sync with device clock
CSCuz86712	port-security programmed mac doesn't match with configured mac
CSCuz86879	Config/Unconfig Speed Inconsistency at NIF PO,make it down & FEX Offline
CSCuz94239	%VPC-6-LOG_LIBSVI_SVI_MCEC_TYPE2_FAILED should be warning or error level
CSCva07077	Changing MST cost is not reflecting in "sh spanning-tree mst int detail"
CSCva07536	FWM core on N5K
CSCva16041	N7K: HSRP holdtimer doesn't reset when receiving HSRP hello
CSCva19355	ADM corruption while upgrade causes switch to get Bricked
CSCva21856	include-profile missing as bgp asn is queried during bgp process restart
CSCva37287	[N56K] N56128 Gem Module: N56-M24UP2Q 40G ports-Cisco QSFP unsupported
CSCva37484	N2K temp sensors incorrectly label airflow dir w/ type B supplies/fans
CSCva59260	satctrl crashed while trying to modify a QoS policy
CSCva60485	N5k/6k - AFM Errors - unknown policy - Port error disabled the second
CSCva61424	Port-profile crashing with core and system going for reset
CSCva61637	Port-profile configuration missing in startup configuration
CSCva64010	show run takes long to execute due to very large device-alias database
CSCva79760	IPV6 link local only BGP peering leads to installing wrong adjcaency
CSCva80745	CLIS memory leaks caused frequent crashes
CSCva81366	BFD session doesn't go down if the IP address on the BFD peer is removed
CSCva83066	N9k/ Eigrp loop, route not flushed from topology table
CSCva83732	Need correction for Licenses warning message when enabling hsrp/vrrp.

Table 38 Resolved Caveats in Cisco NX-OS Release 7.3(2)N1(1) (continued)

Caveat ID Number	Description
CSCva86453	Converged Code N7k regression: RP candidate with prefix-list option
CSCva88817	N5k / N6k - Auto-Config stuck in PPM-Resp wait / PPM del wait state due to copy run start failure
CSCva89987	config line is greater than 223 symbols causing merge failure
CSCva90035	VRRP VIP not Programmed
CSCva94583	FP: Anycast HSRP stuck in Init state after VDC/Switch reload
CSCva98029	ethpm mts queue build up and ethpm hap reset after pvlan creation
CSCvb02494	N7K OTV with BFD configured / BFD Session Flaps on System Switchover
CSCvb12173	EIGRP default summary route not working as expected in Nexus 9000
CSCvb14650	dhcp_snoop hap reset on nexus 6000
CSCvb14785	OSPF Authentication Failure key-id 0 upgrade to 7.0(3)i3(1)
CSCvb16035	NxOS ABR in OSPF totally stubby area does not originate default LSA
CSCvb18486	fwm core after vpc reload
CSCvb20502	n5k vpc - when multicast is received over the VPC PL - DR delays PIM Reg
CSCvb22794	N5K VRRPv3: VIP is not reachable from Backup node
CSCvb23804	Routing changes cased IPFIB crash on N5k
CSCvb38749	N5K/6K: show interface status fex <> lists FC/VFC interfaces
CSCvb39963	N5K:port-security:sticky secure MAC address not removed
CSCvb39993	n7k/hsrp anycast: incorrect active hold timer after timer config change
CSCvb42221	Nexus5600: non-UP port may fail to link up at 1G
CSCvb43958	[KK-mr1] sh policy-map int eth 1/1 input type que command throw error
CSCvb44776	BGP crashes due heartbeat failure after asserts
CSCvb47408	Nexus 5K :seeing FSM ASSERT FAILURE messages on the console
CSCvb48309	AAA: "show logging log" displays user password in clear text
CSCvb48568	Evaluation of N9k/N7k/N5k/N3k/MDS for OpenSSL September 2016 CVEs
CSCvb50456	Nexus 6k crashes when issuing "show ip pim rp"
CSCvb50503	Nexus 5K/6K reloads multiple times with "eth_port_sec hap reset" @ avl_do_walk.
CSCvb51287	N5K-C5696Q: Interface number in storm control log is incorrect.
CSCvb51638	sysmgr reset reason 'service' string formatting error
CSCvb57997	SSTE: GLBP service crash due to heartbeat failure
CSCvb64583	N5k crashes when authenticating via TACACS
CSCvb71555	N5K/6K: DHCPOFFER storm if received over Fabricpath core ports.
CSCvb77224	Expedite SPF calculation based on internal events (Do not delay SPF calculation)
CSCvb79504	PIM SG timer expiry not refreshing with continuous traffic when MRIB is updated by MSDP
CSCvb80772	N5K/6K: DFA Leafs Routing into SMAC of all 0s

Table 38 Resolved Caveats in Cisco NX-OS Release 7.3(2)N1(1) (continued)

Caveat ID Number	Description
CSCvb81261	Including "show tech-support flogi" in "show tech-support details"
CSCvb84735	NTP sync issue with ntp distribute upon image upgrade due to incorrect vrf id
CSCvb93309	NXOS/n7k-pi: URIB crash during show ip route
CSCvb97556	SNMPD process crash on 7.3.0.N1.1 due to port_manager polling
CSCvc01442	FWM crash: Memory leak in ipfib library after HW adjacency table exhaustion
CSCvc02193	packets not routed after PBR policy removal from SVI
CSCvc02580	Interface based zoning with domain-id results in an error
CSCvc03364	NXOS/FP: MDT move for FTAG 1 cause packet drop in unicast packets
CSCvc04281	DHCP ACK looping in Nexus 5648 vpc set up
CSCvc10943	FWM hap reset due to leak fwmpd_handle_scan_addrs_common
CSCvc17025	OSPF sessions stuck in EXCHANGE/DR state for long time
CSCvc17970	VXLAN packets black-holing in ECMP (Multipath) scenario after reload
CSCvc21896	Hitless Upg Fail fex not coming up even on new uplink ports
CSCvc23468	Evaluation of N9k/N7k/N5k/N3k/MDS for NTP November 2016
CSCvc23614	USB1 / slot 0 format prompts for password when logged in with network-admin user privilege
CSCvc24535	"snmpd" crash with signal 11
CSCvc30847	OSPF LSA not withdrawn from Nexus when interface is down
CSCvc36844	PIM Join List in nexus doesn't contain all Rcvrs - Pruned
CSCvc37953	using "show platform fwm info stm-stats clear" on N56k will create CFS MAC Sync problems
CSCvc41571	Jumbled and strange ACL log displayed for Egress direction if port-type is FEX
CSCvc42571	VTP traffic flooded over VPC when received over peer-link
CSCvc44015	address-family ipv4 multicast path invalid in BGP but present in URIB
CSCvc44767	hashlib.py not found in 7.3(1)1D1(1)
CSCvc45002	Multiple switches in FP domain crash due to __inst_001__isis_fabricpath hap reset
CSCvc46102	N7K - PIM/RPM Parses Deny Entry In Route-Map On Static RP Configuration As Permit Following ISSU
CSCvc48029	default route from outside the fabric allowed inside the fabric
CSCvc52883	N6000/N5600: NON-STOMP CRC errors on random 40 Gig BiDi port after reload
CSCvc52992	N5K: CFS service crashses @ tcp_wait_msg_manage_eintr
CSCvc53438	Shared tree takes up to 60 seconds to be pruned after 2nd receiver joins
CSCvc54099	N5K: FC uplinks using ports higher than 64 with trunking enabled go into err disabled
CSCvc58162	fex hap reset
CSCvc58714	Incorrect placement of OSPF rfc1583compatibility command under VRF configuration

Table 38 Resolved Caveats in Cisco NX-OS Release 7.3(2)N1(1) (continued)

Caveat ID Number	Description
CSCvc58786	Duplicate multicast packets in vPC domain.
CSCvc59435	VRF gets stuck in DOWN state
CSCvc65466	OTV fails to advertise mac after a mac move
CSCvc66498	multicast over PIM SSM with VPC for L3 orphan ports drops every 3 min
CSCvc69321	'install all' command blocked after original 'install' command session is terminated
CSCvc69751	Unexpected reload of the Supervisor due to LDP service crashed
CSCvc70579	PPM: Port-profile config takes precedence over direct interface config
CSCvc70733	2348TQ fex with many 100mbit ports does not come online
CSCvc72531	N5K returns 0 when SNMP tries to get "ifOutErrors" MIB
CSCvc81179	Nexus7k ISIS crash at txlist_tq_remove_node
CSCvc84376	FEX N2K-C2348TQ-10GE Reset
CSCvc85082	N5K: statsprofiler hap reset
CSCvc85365	n5k :: HSRP MAC misprogrammed after loop was detected
CSCvc85922	SVI counters incrementing rapidly
CSCvc87518	ISSU upgrade results in fabricpath commands lost from cli
CSCvc88287	SVI generating group-specific-queries to 224.0.0.x reserved multicast address
CSCvc90944	NOHMS-2-NOHMS_DIAG_ERR_PS_FAIL: System minor alarm on power supply
CSCvc93954	Allowed VLAN list add/remove using a nested port-profile is not working correctly
CSCvc99945	Unidirectional L3 connectivity due to having the same IP address configured on multiple interfaces
CSCvd07149	N5K6K - VPC VTEP Keeps Advertising Secondary IP When VPC's Are Suspended For Dual Active
CSCvd07578	SNMPD process crash parsing port info
CSCvd09440	ISIS not sending a MTS_OPC_OTV_STALE_ISIS_DATA notification to OTV
CSCvd09807	KK-MR2: Server connected Maywood HIF port not going down when FEX offline
CSCvd15679	IntMacRx-Er increased on Xmit-Err
CSCvd15697	show interface counter error snmp not shows error count
CSCvd21496	N5K:afm hap reset due to afm memory leak by nat
CSCvd22339	N5k: Monitoring LACP groupd via SNMP always returns value of 1
CSCvd28640	n5k SNMP ifSpeed returns speed as 3705032704 instead of max 4294967295
CSCvd29280	MSDP TCP connection doesn't establish properly neighbour stuck in listening
CSCvd29708	Multiple FEX reload due to Watchdog Timeout
CSCvd36289	ethpc core on 2348 fex with with remote pc flap along with adding sytem Jumbo MTU
CSCvd43419	"router ospf <>" on N5k creates multiple OSPF process
CSCvd53354	Nexus 5672UP-16G no output for show hardware internal fc-mac all-ports

Table 38 Resolved Caveats in Cisco NX-OS Release 7.3(2)N1(1) (continued)

Caveat ID Number	Description
CSCvd58108	&quot;show hardware profile tcam resource template default&quot; shows incorrect TCAM usage
CSCvd62198	mroute OIL is removed on vpc DR failure resulting in 90 sec multicast outage
CSCvd83606	Nexus 5600: not honoring UTC offset on GM failure
CSCvd90219	N6K/N56K No traffic after No shut member in NPV to NPIV san-port-channel
CSCvd95927	EEM script times out at 100s mark in 7.2/7.3

Resolved Caveats in Cisco NX-OS Release 7.3(1)N1(1)

Table 39 Resolved Caveats in Cisco NX-OS Release 7.3(1)N1(1)

Caveat ID	Resolved Caveat Headline
CSCux99818	pim process crash due to corruption caused by lmemory depletion
CSCva70369	Nondisruptive ISSU secondary upgrade failed due to fwm core
CSCuw69419	VIP used as src ip in data path causing traffic to drop at the dest. leaf
CSCuv53931	aaa commands doesn't appear in sh run
CSCuz85110	vsh crashes @ create_snmpv3_user_after_aaa_authenticate
CSCuz27269	Cisco Nexus5000 aclmgr hap reset when saving config
CSCuz02835	PBR -Applied PBR doesn't match the last ACE of the called ACL
CSCux29893	"Police cir" is not limiting the traffic correctly
CSCva97304	AFM Hap rest is seen while applying ACL containing object group
CSCva69077	Cisco Nexus5000 might crash due to afm hap reset
CSCuw83670	Cisco Nexus5000/6000 - AFM Errors - unknown policy - Port error disabled
CSCva60485	Cisco Nexus5000/6000 - AFM Errors - unknown policy - Port error disabled the second
CSCur99346	PPM_VSH_MAX_CMD_BUF_SIZE 4K limitation
CSCuy71942	Absolute time-out causes PPM's background VSH sessions to end
CSCva76684	Misconfigured param-list instances or parameters for auto-config setups
CSCuy33905	Cisco Nexus5600 delay in processing ethpm mts after reload
CSCuy96713	VSH process crashes with "show" commands collected by script
CSCux95887	port-security internal information not cleared on feature de-activation
CSCva41231	Cisco Nexus5596UP switch crash upon bringing up fc ports with port-monitor enabled
CSCuy03675	Nexus crash in FCS process
CSCva18410	Error disabled due to Flexlink error, Reason: Interface does not exist
CSCva48982	PTP Crash on Nexus5000 upon Interface flaps

Table 39 Resolved Caveats in Cisco NX-OS Release 7.3(1)N1(1) (continued)

Caveat ID	Resolved Caveat Headline
CSCux86505	Suppress Kickstart/System Image Warning message when doing POAP
CSCup45280	kernel panic in ethpm
CSCuy27650	Cisco Nexus5000 kernel panic seen with e1000_get_hw_semaphore_generic
CSCuw92560	Cisco Nexus6000 kernel panic crash qh_urb_transaction
CSCuy11722	Cisco Nexus5000/6000 - HSRP VMAC wrongly installed as Static in 4-way setup/VPC
CSCva31928	Cisco Nexus5000/6000: PIM SSM with vPC does not work for L3 orphan ports
CSCuw96116	vPC - HSRP VMAC Points to Router With SVI in Admin Down State
CSCux87583	Nexus: Multiple hung SSH sessions
CSCux00981	few pkt drops when shut/no shut given on PO cfged
CSCva15568	Cisco Nexus5000/6000: Device reload causes unrelated LACP member to flap
CSCur23918	Logging Level config for LLDP does not appear in Startup
CSCuy43572	Cisco Nexus5000/6000:VPC+ Peer-link going into suspend state during switch replacement
CSCuz84691	Allow vlan list per port honored when dot1q auto-config trigger enabled
CSCuy13405	crash on "no mac address-table static" command execution
CSCva07047	Dual-home FEX forces crash on eVPC peer
CSCuw59277	FEX 2348 A-A: Packets send to wrong FEX HIF interface
CSCuw33676	fwm core at fwm_fwim_disassociate_pif_from_pc_int -kk 131
CSCux83653	FWM hap reset after upgrade to 7.0(7)N1(1)
CSCuy42776	Microburst Monitoring cause failure on interface
CSCux30403	Cisco Nexus6000 vn-segment FabricPath Leaf not forwarding for Vlan not created
CSCuq60111	Incorrect Type 1 vPC consistency for "vPC card type" in Enhanced vPC
CSCva37021	Cisco Nexus6000 vPC unknown unicast loop during reload
CSCuz91342	vpc hap reset after upgrade
CSCuv99658	VPC peer link is not coming up after peer-link flap
CSCuy44866	ACL logging not working for egress (packet manager change)
CSCuy93985	Control-Plane Egress QoS - CoS markings are not preserved from its DSCP
CSCuy22769	VXLAN-EVPN with suppress-arp, ARP for silent destination is flooded back
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

Table 39 Resolved Caveats in Cisco NX-OS Release 7.3(1)N1(1) (continued)

Caveat ID	Resolved Caveat Headline
CSCuy08128	Cut through Threshold change FEX's on 40gb NIF's
CSCuy30027	Need reload mechanism for 2348 FEX when CRC errors are seen
CSCva12553	N56-M24UP2Q in N5K-C56128P-SUP does not recognize media type of SFPs
CSCuv44148	Ports status "down (SFP not inserted)" although SFP present
CSCuy27585	Cisco Nexus5000: Incorrect startup for allowed vlans in port-profile type ethernet
CSCux42280	BFD session randomly flaps on Cisco Nexus6000
CSCvb28917	Display "qos statistics" in the running-config
CSCux28524	Cisco Nexus5000 crashed due to "QD" process.
CSCuy28938	One Server sending continous RX pause can cause Buffer lock
CSCva13731	RADIUS Daemon crash on Cisco Nexus5000
CSCux30880	Auto-config profile stuck PPM Del Wait ascii-cfg-server rollback request
CSCux40274	Multicast traffic dropped due to cell usage stuck for ingress buffer
CSCva11572	copy bootflash:<file> startup-config cannot restore the ssh key config
CSCuy07280	Evaluation of N3k,N5k,N7k,N9k for OpenSSL January 2016
CSCuy54488	Evaluation of n7k/n5k/MDS/n9k/n3k/n3500 for OpenSSL March 2016
CSCuz52394	Evaluation of N7k/N5k/N9k/N3k/MDS for OpenSSL May 2016
CSCuu49957	Fex connected Power supply should respond proper status
CSCuq45360	LinkUP SNMP Trap not sent on LinkUp events for FEX Fabric Port-Channel
CSCuz43145	DCNM, DM or SSH login to switch fails - "Unknown User or Password"
CSCux86332	N3k/N6K/N7K/N9K/MDS January 2016 OpenSSH Vulnerabilities
CSCuv42794	SSH 'no matching cipher found' message missing source IP address
CSCuy83222	N5696+N5696-M12Q with sub-interf;Snmppolling Cause MTS Buff leak-pfstats
CSCum57545	Peer-link STP inconsistency due to corrupt BPDU does not clear
CSCuw89504	Nexus 6000 crashes with memory leak in bfd_app
CSCuy11847	TACACS Daemon Hap Reset When Adding an SSH Key
CSCux72134	Vlan not getting programmed as vn-seg capable
CSCuv75852	AA dual-homed FEX HIF suspended due to speed during server boot process
CSCva57357	Vlans pruned due to lack of VTP join when vtp pruning enabled
CSCva67085	VTP hap reset during the VTP timer message handling

Resolved Caveats in Cisco NX-OS Release 7.3(0)N1(1)

Table 40 Resolved Caveats in Cisco NX-OS Release 7.3(0)N1(1)

Caveat ID	Resolved Caveat Headline
CSCuy08558	Feature VTP incompatibility issue on fabric
CSCuq94445	ISSU failed. Maximum downtime exceeded
CSCur72846	Multi mobility domain and FCoE co-existence does not work
CSCuu59941	FC ports error disabled with non-Cisco SFPs after upgrade to Cisco NX-OS Release 6.x/7.x
CSCux20846	Cisco Nexus 6000: IGMP HAP Reset during "install all" upgrades with IGMPv3.
CSCut99511	BFD flaps with the 50 ms default timer.
CSCuu07598	Cisco Nexus 5548P/N55-M16P : After Upgrade Interface Down & Unrecoverable
CSCuv04979	Cisco Nexus 5000, 6000 series Platform: netstack crash while saving tech-support in bootflash
CSCut68629	Nexus 5000: customized CoPP config back to default after reload
CSCum62759	CTS: Nexus 5000 ignores CTS timers from ISE
CSCur37987	Cisco NX-OS crash in "show system internal im info module "non existing slot"
CSCut94326	Cisco Nexus 5596UP as FC switch: cannot change FSPF cost under fc interface
CSCul85203	Cisco Nexus 5000 Port in Internal-Fail errDisable : fu ha standby message queued
CSCuv24827	FCoE feature failed with POAP template in cpom/dcnm
CSCuw70493	State/Reason error and Generic error Missing ACL cause crash. span monitor
CSCur72846	Multi mobility domain and FCOE coexistance does not work
CSCuw02271	Cisco Nexus 2348:Incorrect CFG_PORT_ID programming causing Traffic-Blackholing
CSCux14987	Cisco Nexus 5000, 6000 switch crashes with "lacp hap reset"
CSCux23707	FWM hap reset with uplink-FO cfg on Maywood HIFs connctd to UCS VIC1225T
CSCur20769	sh fex 'fex num' transceiver -shows sfp is present but not supported
CSCux10337	Cisco Nexus 2348TQ fex devices crash repeatedly
CSCuo93650	Enh: Speed up module 2 bring up in Cisco Nexus 6001
CSCuu37102	Cisco Nexus 5000 kernel Panic on AIPC driver causing crash
CSCux41730	Cisco NX-OS changes with regard to BIOS change for CSCuw58510
CSCuw73332	VTPv3 mode changes from client to transparent after PVLAN creation
CSCux33230	"ipqosmgr hap reset" during upgrade from Cisco NX-OS Release 7.1(2)N1(1) to 7.1(3)N1(1)

Table 40 Resolved Caveats (continued) in Cisco NX-OS Release 7.3(0)N1(1)

Caveat ID	Resolved Caveat Headline
CSCuw13812	iscm memory leak
CSCup75270	FC interfaces are not listed in IF-MIB snmp walk
CSCud56630	Not able to unload mib using 'no snmp-server load-mib' command
CSCuv54185	SNMPd keeps logging "svi_counter_cache_fetch: destroying stale results"
CSCuv32204	SNMPd Memory Leak in libport_mgr_common
CSCuv42326	SPAN destination on HIF port does not work for A/A FEXes.
CSCun34005	Cisco Nexus 2k/5k/6k: Continuous memory leak messages seen for ethpm
CSCut35608	Traffic loss during recovery when dVP is enabled for xlated VLAN(Cisco Nexus 6000)
CSCuv48304	vPC hap reset during auto-config
CSCur15707	Cisco Nexus 5000: VLANs learned via VTP not created
CSCuw51093	WCCP redirection should be applied for the Layer 3 routed packets

Resolved Caveats in Cisco NX-OS Release 7.2(1)N1(1)

Table 41 Resolved Caveats in Cisco NX-OS Release 7.2(1)N1(1)

Caveat ID	Resolved Caveat Headline
CSCux99818	pim process crash due to corruption caused by lmemory depletion
CSCut55653	interface-vlan info is not propagated to vPC leading to inconsistency
CSCus93963	Cisco Nexus 5000- After Reload Local Authorization Fails when mgmt0 int is down
CSCut42246	ACL used for ERSPAN filter not removed
CSCul00229	Cisco Nexus 6000 - PIM Registers Misclassified as PIM Hellos by COPP
CSCus28695	WCCP - ACL Remark breaks TCAM redirection entry
CSCut75399	update rdecode.sh to support n3k/5k
CSCuo02240	Cisco Nexus 5000 carmel usd core
CSCus75696	Cisco Nexus N55-M4Q GEM module port1 and port2 stay down after reboot
CSCus64364	Cisco Nexus 5000: carmelusd component got cored on O2 switch
CSCuu07598	Cisco Nexus 5548P/N55-M16P : After Upgrade Interface Down and Unrecoverable
CSCut07668	Cisco Nexus 5000: Cisco IP phone voice vlan not working
CSCuq25291	REOP on Cisco Nexus 6000: CSCtk37170: CDP IPv4 address is reported incorrectly
CSCuu06028	interface config doesn't apply properly after Disruptive Downgrade
CSCuv04979	Cisco Nexus 5000, 6000 Platform: netstack crash while saving tech-support in bootflash

Table 41 Resolved Caveats in Cisco NX-OS Release 7.2(1)N1(1)

Caveat ID	Resolved Caveat Headline
CSCut92605	"port-profile hap reset" after switch-profile commit
CSCut65095	Cisco Nexus may reload due to port-profile hap reset
CSCuu04623	Parsing error while importing lengthy configuration to switch profile
CSCuv58843	port-profile reset when committing a VLAN change
CSCut68629	Cisco Nexus 5000: customized CoPP config back to default after reload
CSCuu67017	Cisco Nexus 6000 /Nexus 5600 CoPP arp/ipv6-nd policy CIR set to 8000
CSCut21777	DHCP Packets flooded to VPC peer with DHCP snooping configuration
CSCuu97262	Lot of unwanted packets seen on debug dhcp all
CSCuu09610	Switch sends large number of DHCPv4 packets in response
CSCut94161	EEM: Configuration failed with: 0x412c000d validation timed out
CSCtz26764	Cisco Nexus 5000 - After removing GEM, interfaces still remain in the show start
CSCul25050	Cisco N2K-B22HP-P: Down interface are logged ETHPORT-5-IF_DOWN_ERROR_DISABLED
CSCuo58150	Cisco Nexus 6000: QinQ capability not enabled after nondisruptive ISSU
CSCus17580	eth_port_channel hap reset
CSCuv01812	Cisco Nexus 6000: port-security err-disables HIF after switch/fex reload
CSCuu04099	Cisco Nexus 6000: SAN port-channel has output discards when member links are added
CSCur10558	Trunk Protocol Enable does not show in running config when disabled
CSCup96375	crash flogi process on both Cisco Nexus 5000 at the same time due to null pointer
CSCup70139	Cisco Nexus 5000 fwm hap reset
CSCut83532	Cisco Nexus 5600 vPC Pair loops back unknown unicast packets
CSCuc93691	Fwm hap reset as soon as FEX is connected
CSCut39135	Traffic loss during recovery when dVP is enabled for xlated Vlan(HMM PI)
CSCus50291	Cisco Nexus 5000, 6000: IGMP General Queries are not sent out mvr receiver port
CSCuw38972	Fabricpath ECMP not working after ISSU
CSCuv27318	IGMP packets are sourced from Anycast SWID instead of emulated switch id
CSCuo56514	In vPC+ Nexus 5500 ARP reply may be sourced from SID, rather then ESID
CSCuu00391	Cisco Nexus 5000, 6000: BCAST flag missing for FTAG 2
CSCue08601	Show interface trunk shows all interfaces as fabric path forwarding
CSCut55084	Cisco Nexus 5000, 6000: Need to make LACP suspend individual default for base ports
CSCuu84449	IGMP snooping entries age out in AA FEX topologies

Table 41 Resolved Caveats in Cisco NX-OS Release 7.2(1)N1(1)

Caveat ID	Resolved Caveat Headline
CSCut75242	ISSU upgrade: IGMP HAP reset
CSCue76773	"ip routing multicast software-replicate" Support for Cisco Nexus 5000, 6000 platform
CSCuv54348	fwm aborted due to heartbeat failure
CSCut19721	Logging source-interface loopback does not work for ipv6
CSCut46788	Cisco Nexus 5600: Log on prompt not correct when hostname begins with number
CSCus97195	Cisco Nexus 5K/6k - FEX HIF port down delay when FEX Fabric member links down
CSCuo28747	Cisco Nexus 5000, 6000: FWM core during ISSU
CSCuu96337	Cisco N5672UP NFM crash after config change
CSCut36200	Ports towards the Cisco N2K-B22HP-P do not come up after a server reboot
CSCus89917	Ethanalyzer interprets packets as Malformed LLC
CSCuv40217	Excessive NMI on root port due to correctable error not if causing reboot
CSCus89890	Link state will not change after ISSU to Cisco NX-OS Release 7.0 from 6.0(2)
CSCuo46284	Cisco Nexus 55xxUP showing SFP uC: Module 1: v0.0.0.0
CSCut86026	Cisco Nexus 5000, 6000: /var/tmp directory getting full with lcuc log file
CSCuu37102	Cisco Nexus 5000: kernel Panic on AIPC driver causing crash
CSCun33975	'ppm' process crashes soon after upgrading Cisco Nexus 5000
CSCup86425	Crash after entering "no port-profile type ethernet uplink"
CSCur80754	Incorrect show run for allowed vlans in port-channel type port-profiles
CSCur18043	Cisco Nexus 6000 "ntp access-group peer" wont show up in running config
CSCuw13812	iscm memory leak
CSCut99251	Rollback fails when "speed 1000" for port-channel member ports
CSCut51575	VPC breaks due to incorrect emulated switch-id after ISSU upgrade
CSCut38855	Cisco Nexus 5000 DR does not register S,G when acting as first hop router
CSCuv08448	Cisco Nexus 5000 VDC Authenticated Privilege Escalation Vulnerability
CSCuv92830	RADIUS login only assigned network-operator role
CSCuv82719	Unable to login with new passwd reset from switch(boot) prompt
CSCuu69510	Cisco Nexus 5000/6000 snmp 64 bit counters for svi interface dont work
CSCut82544	SNMP MIB entPhysicalVendorType does not send the correct value
CSCuf57781	%STP-2-BLOCK_DETECTED_PVST_PEER message is not output on Nexus5000
CSCtu54802	Syslog server cannot see origin-id from Cisco Nexus 5000
CSCur49785	Inconsistency between running and startup config

Table 41 Resolved Caveats in Cisco NX-OS Release 7.2(1)N1(1)

Caveat ID	Resolved Caveat Headline
CSCuv25016	sh forwarding internal message counts - N6K/N5K switch reloads: fwm core
CSCut57364	DFA Autoconf/Profile-refresh failing if using vlan name in the profile
CSCut55133	N5672: cant't save config after configuring vlan mapping more than 200
CSCut35608	Traffic loss during recovery when dVP is enabled for xlated Vlan(N6K)
CSCut52768	dvp interface command should appear with "show run interface all"
CSCum93892	VSAN is stuck in operational state down, but state is active.
CSCuj39540	Port Cores After Running Script - Compliance Test - CISCO-FC-FE-MIB.
CSCuv72180	auto-config profile stuck in PPM Del Wait.
CSCus09017	ERROR: no free label Message for ACL modification
CSCus92242	counter in show queuinter interface not removed after n5k reload.
CSCuq96601	PPM should block 'copy r s' if auto-config is going on in the background.

Resolved Caveats in Cisco NX-OS Release 7.2(0)N1(1)

Table 42 Resolved Caveats in Cisco NX-OS Release 7.2(0)N1(1)

Caveat ID	Resolved Caveat Headline
CSCug90187	SFP and QSFP support for FEX.
CSCuu06028	Interface config doesn't apply properly after Disruptive Downgrade
CSCuu33047	Roll back failed while applying allowed vlan command to a interface
CSCut86729	vPC Multicast optimization doesn't work after disable/enable the CLI.
CSCuu39555	Sometimes few HSRPVIP removed ISSU Cisco NX-OS Release 6.0.2.N2(7) > 7.0.6.N1(1) > 7.2.0.N1(1).
CSCum83908	Port-security is not learning all addresses on changing the port mode.
CSCus04748	vlan mapping is not installed for one of the 2 FEX's hosting a 2lvpc PO.
CSCus16779	FEX vlan translation with multiple HIF PO flaps may stop L2 vlan fwding
CSCut55443	FWM mac trace buffer memory corruption
CSCuq56923	Logging level virtual-service reverts to default after a NX-OS upgrade
CSCus22741	DRAP process crash after FP domain restart
CSCur07245	Cisco Nexus switch may see repeated crashes of ntpd process
CSCur12364	Cisco Nexus 5000: ISSU fails 5.1(3)Nx(x)/5.2(1)N1(x) -> 6.0(2)Nx(x) -> 7.0(x)N1(1)
CSCuu06719	Profile re-apply between universal and individual profiles does not work.

Resolved Caveats in Cisco NX-OS Release 7.1(5)N1(1b)

Table 43 Resolved Caveats in Cisco NX-OS Release 7.1(5)N1(1b)

Identifier	Description
CSCvb93309	NXOS/n7k-pi: URIB crash during show ip route

Resolved Caveats in Cisco NX-OS Release 7.1(5)N1(1)

Table 44 Resolved Caveats in Cisco NX-OS Release 7.1(5)N1(1)

Caveat ID Number	Description
CSCuz59030	Nexus 5000 chap protocol actually does PAP
CSCvc85365	n5k :: HSRP MAC mis-programmed after loop was detected
CSCva98029	ethpm mts queue build up and ethpm hap reset after pvlan creation
CSCvb48309	AAA: "show logging log" displays user password in clear text
CSCuz02835	PBR -Applied PBR doesn't match the last ACE of the called ACL
CSCvd21496	afm hap reset due to afm memory leak by nat
CSCva59260	satctrl crashed while trying to modify a QoS policy
CSCuu10667	Multicast-routing not disabled on mgmt0 interface after disabling CFS
CSCvc52992	CFS service crashes @ tcp_wait_msg_manage_eintr
CSCuu31064	All Nexus Tech supports should include some basic information
CSCve00906	vlan mutex locked when config range of vlans with automated tool
CSCvb14650	dhcp_snoop hap reset on nexus 6000
CSCvb71555	N5K/6K: DHCPOFFER storm if received over Fabricpath core ports.
CSCvd15679	IntMacRx-Er increased on Xmit-Err
CSCve33644	N5K: ETHPM buffer leak on FEX HIF after L2 loop
CSCvb39963	N5K:port-security:sticky secure MAC address not removed
CSCvb50503	Nexus 5K/6K reloads multiple times with "eth_port_sec hap reset" @ avl_do_walk.
CSCvb38749	N5K/6K: show interface status fex <> lists FC/VFC interfaces
CSCuz10788	N5k transceiver det. show incorrect link length supported for OM3 cable
CSCuw27142	Need CLI to clear snmp counters for Nexus switches
CSCvd53354	Nexus 5672UP-16G no output for show hardware internal fc-mac all-ports
CSCvd07578	SNMPD process crash parsing port info
CSCvd90219	N6K/N56K No traffic after No shut member in NPV to NPIV san-port-channel
CSCvb81261	Including "show tech-support flogi" in "show tech-support details"
CSCvc47673	show feature | xml returns plain output

Table 44 Resolved Caveats (continued)in Cisco NX-OS Release 7.1(5)N1(1)

Caveat ID Number	Description
CSCvd29708	Multiple FEX reload due to Watchdog Timeout
CSCuw66815	Nexus 5K / 6K Crashes Due to "fex hap reset" When Issuing "show fex" with an Offline FEX
CSCvf24911	ARP memory leak @ LIBBL_MEM_bitfield_malloc_t & LIBSLAB_MEM_create_slab
CSCvd79462	Mem leak in confcheck process when executing "show install all impact" command
CSCve41802	Duplicate syslog messages for Interface x/y is down.
CSCve37631	Packet drops are seen with increased PPS on 7.3.0
CSCvc69321	'install all' command blocked after original 'install' command session is terminated
CSCvb22794	N5K VRRPv3: VIP is not reachable from Backup node
CSCvb80772	N5K/6K: DFA Leafs Routing into SMAC of all 0s
CSCuo03534	dcos-telnetd crash with SIG3
CSCuw40711	Nexus - in.dcos-telnetd service crash
CSCvb66156	Nexus 56k/6k PIM dr-priority ignored after re-applying 'ip pim sparse-mode'
CSCvb50456	Nexus 6k crashes when issuing "show ip pim rp"
CSCve56212	PIM bidir stops forwarding traffic when the route to RP changes
CSCvc58786	Duplicate multicast packets in vPC domain.
CSCvb18486	fwm core after vpc reload
CSCvc10943	FWM hap reset due to leak fwmpd_handle_scan_addrs_common
CSCva09533	vPC Primary suspends vlans when secondary is back online after reload
CSCux08353	vrrpv3 configuration failed after default interface
CSCuz58396	Enhancement: Include domain id in %VPC-3-VPC_PEER_LINK_DOWN or UP syslog
CSCuz58321	Enhancement: Syslog for VPC-3-PEER_REACHABLE: Remote Switch Reachable
CSCux06997	inherit port-profile fails due to vpc orphan-port suspend
CSCvf22937	Dynamic NAT entries not getting cleared
CSCvd61694	GARP for Anycast HSRP VIP is sent with non-zero LID
CSCvc41571	Jumbled and strange ACL log displayed for Egress direction if port-type is FEX
CSCvc23468	Evaluation of N9k/N7k/N5k/N3k/MDS for NTP November 2016
CSCvb84735	NTP sync issue with ntp distribute upon image upgrade due to incorrect vrf id
CSCvc70733	2348TQ fex with many 100mbit ports does not come online
CSCvd36289	ethpc core on 2348 fex with remote pc flap along with adding system Jumbo MTU

Table 44 Resolved Caveats (continued)in Cisco NX-OS Release 7.1(5)N1(1)

Caveat ID Number	Description
CSCvc58162	fex hap reset
CSCvc84376	FEX N2K-C2348TQ-10GE Reset
CSCvc21896	Hitless Upg Fail fex not coming up even on new uplink ports
CSCva37484	N2K temp sensors incorrectly label airflow dir w/ type B supplies/fans
CSCus78963	Inconsistent behavior of System LED during error state
CSCvc90944	NOHMS-2-NOHMS_DIAG_ERR_PS_FAIL: System minor alarm on power supply
CSCvc17025	OSPF sessions stuck in EXCHANGE/DR state for long time
CSCve13020	tftp_si_entries is read-only
CSCvd66631	display of show run interface command is not correct upon applying port-profile inherit
CSCva88817	N5k / N6k - Auto-Config stuck in PPM-Resp wait / PPM del wait state due to copy run start failure
CSCva61637	Port-profile configuration missing in startup configuration
CSCva89987	config line is greater than 223 symbols causing merge failure
CSCuv74091	Add predefined FCoE+Jumbo QoS policy
CSCuz70693	N5600 - BUM traffic with CRC error is cut-through switched
CSCve72490	Offline port RSCN not sent
CSCve87784	BGP Process Crash when receiving AS Path longer than 255
CSCur60325	EIGRP can lead to routing loops in some cases
CSCvb54096	EIGRP default Route churns when adding summary-address
CSCuy64775	EIGRP redistributed routes wedged in topology table
CSCus28099	Redistributed routes become internal on neighbor when withdrawn from EIGRP
CSCut01798	Retransmission of SIA-Query leads to SIA
CSCvc45002	Multiple switches in FP domain crash due to __inst_001__isis_fabricpath hap reset
CSCuu08990	CVE-2015-2808 RC4 Cipher used with SSL/TLS protocol could be insecure
CSCvb48573	Evaluation of nexus-5000-all for Openssl September 2016
CSCuu65506	N5k/N6k-No support for SNMP OID access restriction / SNMP views
CSCvc52926	OID is not increasing for entSensorType
CSCvd15697	show interface counter error snmp not shows error count
CSCvc81103	snmpd crash
CSCvb86787	Cisco Nexus 5K/6K/7K/9K/9500-R/MDS CLI Command Injection Vulnerability
CSCva07077	Changing MST cost is not reflecting in "sh spanning-tree mst int detail"
CSCuz24753	auto_root_file_deletion_log.txt growing in size in /var/tmp

Table 44 Resolved Caveats (continued)in Cisco NX-OS Release 7.1(5)N1(1)

Caveat ID Number	Description
CSCux65366	MCM memory leak @ libacfg.so
CSCur59733	IPv6 TACACS Auth Fails On N7K/N9K Over Mgmt VRF
CSCvb64583	N5k crashes when authenticating via TACACS
CSCvb23804	Routing changes cased IPFIB crash on N5k
CSCub14112	UDLD clean up for fex-fabric ports
CSCvc01442	FWM crash: Memory leak in ipfib library after HW adjacency table exhaustion
CSCvc24535	"snmpd" crash with signal 11
CSCvc42571	VTP traffic flooded over VPC when received over peer-link
CSCvb51287	N5K-C5696Q: Interface number in storm control log is incorrect.
CSCvc06145	afm crashed while executing afm commands
CSCvc04281	DHCP ACK looping in Nexus 5648 vpc set up
CSCut17708	san-port-channel not load-balanced on Nexus 6000 and 5600
CSCvd83606	Nexus 5600: not honoring UTC offset on GM failure
CSCuz95629	mac learning issue with dhcp relay in wifi roaming situation.
CSCvc37953	using "show platform fwm info stm-stats clear" on N56k will create CFS MAC Sync problems
CSCuw68009	Do not allow sampling mode of 1 out-of 1 for netflow on Nexus 6000
CSCva71034	access port based SVI ACL logging not working for egress
CSCvc02193	packets not routed after PBR policy removal from SVI
CSCuy85524	Bios image should be md5 verified after extraction prior to application
CSCvb34336	Link stays up even after removing cable after ND ISSU from 6.0 to 7.0
CSCuo95666	N5K/6K: Enhance logging capabilities for ASIC failures
CSCvc52883	N6000/N5600: NON-STOMP CRC errors on random 40 Gig BiDi port after reload
CSCvc02603	Nexus 5600 - 7.3(0)N1(1) - Netflow packet sysUpTime incorrect (SysUptime = 0)
CSCvb42221	Nexus5600: non-UP port may fail to link up at 1G
CSCve72379	hardware unicast voq-limit-sup command not working after reload
CSCvb72921	N6k: vPC Type-1 consistency failure for incorrect vn-segment mapping
CSCut68601	PIM hap reset seen on multiple switches with Auto-RP configurations
CSCva85659	Pvlan Trunk config cannot be removed from PortChannel

Resolved Caveats in Cisco NX-OS Release 7.1(4)N1(1)

Table 45 Resolved Caveats in Cisco NX-OS Release 7.1(4)N1(1)

Caveat ID Number	Description
CSCve92402	hardware unicast voq-limit-sup needs to become default on bigsur based platforms
CSCvd28463	Nexus 5000/6000 Latency Monitoring reporting an incorrect maximum value
CSCuw23628	NFM HAP reset on performing copy r s - N56128
CSCuq94445	ISSU failed. Maximum downtime exceeded
CSCus44812	SS Fex: Bootup diag detected major event: Forwarding ASIC failure
CSCva37287	Cisco N56128 Gem Module: N56-M24UP2Q 40G ports-Cisco QSFP unsupported
CSCuc62084	Show accounting log / show log output is missing initial
CSCto41862	Cisco Nexus 5000: 'authorization config-commands' causes garbled output
CSCux46009	Cisco Nexus 802.1x: suffix delimited with @ is not sent in RADIUS request
CSCuz85110	vsh crashes @ create_snmpv3_user_after_aaa_authenticate
CSCuz27269	Cisco Nexus 5000: aclmgr hap reset when saving config
CSCuu62888	Cisco Nexus 5000/6000: ISIS Neighbor with network type p2p adjacency not coming up
CSCux29893	"Police cir" is not limiting the traffic correctly
CSCuz46078	AFM: TCAM Carving of Layer 3 Card-facing UPC may cause traffic drops
CSCva60485	Cisco Nexus 5000/6000 - AFM Errors - unknown policy - Port error disabled the second
CSCux03956	ARP Reply for VIP is dropped in hardware on egress path
CSCuw09852	BFD not sent over FP core ports on Cisco Nexus 56128
CSCuw09193	%CDP-4-NATIVE_VLAN_MISMATCH message not logged on Cisco Nexus 5600
CSCuj36664	SYSMGR-2-SERVICE cfs crashed unexpectedly
CSCuz24931	copy run to sftp on linux server fails
CSCuw24856	Cisco Nexus 5000: vsh core on "show run"
CSCux32552	Cisco Nexus 5000/6000: ascii-cfg hap reset
CSCux69897	Cisco Nexus 5000/6000: vshd crash with EEM CLI regex match
CSCur99346	PPM_VSH_MAX_CMD_BUF_SIZE 4K limitation
CSCuy73026	show run for ascii-cfg not displayed correctly
CSCut29890	User role hierarchy not working correctly, interface deny overrides permit
CSCuy71942	Absolute time-out causes PPM's background VSH sessions to end
CSCuy14677	Logfile "/var/tmp/ppm_logfile" taking up space in /var/tmp
CSCuw51800	unable to delete param-list from config file

Table 45 Resolved Caveats (continued) in Cisco NX-OS Release 7.1(4)N1(1)

CSCup76173	240/249 ERROR: Timer expired on replay config cfs hap reset at syscall()
CSCux06999	Cisco Nexus 5000: Config-Sync shows "in sync" despite "sh run switch-profile" differs
CSCva64010	show run takes long to execute due to very large device-alias database
CSCut49092	[comm:ethpm] WARNING: possible memory leak is detected on peers queue
CSCuz29352	COPP config isn't in show run all
CSCuz23976	DHCP Snooping not working correctly if broadcast flag is set
CSCut75942	dot1x memory leak 24576 bytes with udldLoop with link flap
CSCuz10518	Cisco Nexus got dot1x hap reset
CSCuy80838	"errdisable recovery cause security-violation" for Cisco Nexus 5000/6000
CSCuy63746	BFD Stuck in Down state and BFD Session is not initialized on Nexus 6000-VMM issue
CSCuu38577	Cisco Nexus 55xx, Nexus 56xx and Nexus 600x: link debounce timer may not work as configured
CSCuy33905	Cisco Nexus 5600 delay in processing ethpm mts after reload
CSCuz42053	Cisco Nexus 5000: Crash in ethpm Due to Memory Leak in libutils.so.0.0.0
CSCur37987	Cisco NX-OS crash in "show system internal im info module "non existing slot "
CSCux92689	VMM_TIMEOUT: Service SAP 175 for slot 33 timed out in UPGRADE_READY_SEQ
CSCut01850	MAC violation during failover in Active/Standby server to dual-homed FEX
CSCuv44354	Outage after vlan membership change on AA HIF with port-security
CSCux95887	Port-security internal information not cleared on feature de-activation
CSCuz86712	Port-security programmed mac doesn't match with configured mac
CSCux67319	Memory leak in fabric-access
CSCus22583	Changing the port type doesn't remove the configuration from startup
CSCux76712	FC interface disabled due to 'bit error rate too high' when rate is low
CSCux75794	HA policy of Reset - Crash in port_mgr after successful ISSU
CSCun30488	Cisco Nexus 5500 series switch does not show more than 255 tx credits on fc int
CSCui63827	sh int fc <x/y> capabilities , shows fc <x/y> twice
CSCuu05829	vsh is crashed
CSCux44029	XML support for show interface fcx/y transceiver details
CSCva41231	Cisco Nexus 5596UP switch crash upon bringing up fc ports with port-monitor enabled
CSCue57527	Function fcpc_lcp_get_port_info_hdlr: Error: 0x40290004 ... TLV: 96
CSCuh78381	SAN Port-channel reports as going down when a member link fails
CSCuo49098	show flogi event-history is broken when using FPORT SAN-Port-Channel.

Table 45 Resolved Caveats (continued) in Cisco NX-OS Release 7.1(4)N1(1)

CSCue41816	"sh hardware internal fc-mac <> port <> statistics" clear enhancement
CSCuo79180	copy run start fails: Service "flogi" failed to store its configuration
CSCus67475	FCNS cores due to fcns hap reset
CSCus73291	Kernel Panic for process fcoe_mgr
CSCuw60947	Cisco Nexus 5K/6K RSCN not sent to zone member when zoning change
CSCut94326	Cisco Nexus 5596UP as FC switch: cannot change FSPF cost under fc interface
CSCuy03675	Cisco Nexus crash in FCS process
CSCty11635	Error message after ISSU - FCP_ERRFCP_PORT: gat_fcp_utils_exp_log@30
CSCux24542	FCoE FLOGI from NPV switch gets LS_RJT due to solicit not done
CSCun19774	FCoE-npv: ISSU fails due to disable-fka not set on NP port
CSCub16077	FRAME DISCARD message seen after bringing up multi-hop FCoE vfc intf
CSCuu70111	FWM service crash at FWM_FWIM_IF_GET_NEXT_LIF
CSCul85203	Cisco Nexus 5K Port in Internal-Fail errDisable : fu ha standby message queued
CSCug84860	Cisco Nexus 6K/56K sends wrong FCF-MAC causing N4K server adapter ports to go down
CSCuv20660	NetApp: Response to VLAN Request seen after vfc port was shut
CSCua04442	Cisco Nexus 5000: vFC down does not trigger callhome alert
CSCux09406	Null L2 destination address in ACC(PLOGI) frame
CSCux95821	show tech-support fcoe needs to contain all pertinent FC information
CSCuw09982	Crash on Cisco Nexus 5k after Dell server with Cisco N2K FEX modules inserted is powered on
CSCuw70493	State/Reason error & Generic error Missing ACL cause crash. span monitor
CSCva18410	Error disabled due to Flexlink error, Reason: Interface does not exist
CSCur36713	"in-163" entry for SVI MAC missing in HW-STM table in FWM
CSCur72846	Multi mobility domain and FCOE coexistence does not work
CSCux23216	Auto-pull - refresh does not work after copy r s + reload on VPC
CSCva21856	include-profile missing as bgp asn is queried during BGP process restart
CSCut56970	no spanning tree instance after auto-pull, save and reload
CSCut46713	Unnecessary churn due to secondary not having profiles after reload
CSCuy89705	4 way HSRP does not work on Cisco Nexus 5000/ 6000 switches
CSCuu58251	Missing HSRP VIP v6 link-local after reload of both HSRP routers
CSCuj70799	Powered-down due to fan policy trigger after SFP insert
CSCuy79971	9 micro sec offset corrections on Cisco Nexus 5548 switches
CSCuy79978	Cisco Nexus 5672 ptp state stuck in "Uncalibrated" State

Table 45 Resolved Caveats (continued) in Cisco NX-OS Release 7.1(4)N1(1)

CSCva48982	PTP Crash on Cisco Nexus 5000 upon Interface flaps
CSCuy81174	Cisco Nexus 5000/6000: Abort install if running version of BIOS is empty
CSCux86505	Suppress Kickstart/System Image Warning message when doing POAP
CSCut64996	Cisco Nexus5548 _Ethernet ports is lost in running-config after reload
CSCua78843	SFP validation issue with switchport mode fex-fabric
CSCus84830	Netstack process resets during ACL modification
CSCuz03208	IGMP Queries not forwarded out of MVR interfaces
CSCuv55465	Service "netstack" (PID 3872) hasn't caught signal
CSCut89123	Kernel panic due to "insmod" process
CSCup45280	Kernel panic in ethpm
CSCuy49328	N5596 kernel panic on carmelusd process
CSCuw73492	N5K crash due to Service: stp hap reset
CSCux46963	N5K kernel panic crash usd_mts_kthread Part II
CSCuy27650	N5K kernel panic seen with e1000_get_hw_semaphore_generic
CSCuw92560	N6K kernel panic crash qh_urb_transaction
CSCuy90720	Cisco Nexus 5600 kernel panic crash usb-storage usb_stor_control_thread
CSCtz05620	O2-96-T:Kernel Panic when provision GEM modules & sw got reset
CSCuw92582	Add syslog to notify L3 interface with sub-interface limit exhausted
CSCuy07577	N5672 HSRP vmac remain in mac address table after SVI removed
CSCuy11722	N5k/6k - HSRP VMAC wrongly installed as Static in 4-way setup/VPC
CSCva31928	N5K/6K: PIM SSM with vPC does not work for L3 orphan ports
CSCuw96116	vPC - HSRP VMAC Points to Router With SVI in Admin Down State
CSCuw15860	SSH Multiplexing on N9k can cause client applications to hang
CSCux00981	few pkt drops when shut/no shut given on PO cfged
CSCva15568	N5k/6k: Device reload causes unrelated LACP member to flap
CSCux14987	Cisco Nexus 5k/6k crash with "lacp hap reset"
CSCur23918	Logging Level config for LLDP does not appear in Startup
CSCux20846	Cisco Nexus 6k: IGMP HAP Reset during "install all" upgrades with IGMPv3
CSCuw82347	PIM Assert Storm on pair of N6Ks with Egress VPC and ECMP in L3 Core
CSCuy01302	IPv6 multicast traffic blackholing when ipv6 static route configured
CSCus18893	Crash due to a Kernel Panic at mts_sys_my_node_addr_get
CSCuy43572	N5K/6K:VPC+ Peer-link going into suspend state during switch replacement
CSCuz40720	Crash with L2MP and ECMP configured
CSCva07047	Dual-home FEX forces crash on eVPC peer
CSCuw59277	FEX 2348 A-A: Packets send to wrong FEX HIF interface
CSCuw33676	fwm core at fwm_fwim_disassociate_pif_from_pc_int -kk 131

Table 45 Resolved Caveats (continued) in Cisco NX-OS Release 7.1(4)N1(1)

CSCva07536	FWM core on N5K
CSCuy61164	fwm core with "no int po102" after seeing "%ETHPORT-2-IF_SEQ_ERROR"
CSCux83653	FWM hap reset after upgrade to 7.0(7)N1(1)
CSCux23707	FWM hap reset with uplink-FO cfg on Maywood HIFs connctd to UCS VIC1225T
CSCuy42776	Microburst Monitoring cause failure on interface
CSCue99559	N5K/6K: FWM hap reset during ISSU upgrade
CSCux30403	N6K vn-segment FabricPath Leaf not forwarding for Vlan not created
CSCuy91379	Cisco Nexus 5K crash at dleft_sprint_table_info
CSCuy91714	N5K-C5596UP FWM Crash During ISSU to 7.2(1)N1(1)
CSCuz94239	%VPC-6-LOG_LIBSVI_SVI_MCEC_TYPE2_FAILED should be warning or error level
CSCuz86879	Config/Unconfig Speed Inconsistency at NIF PO,make it down & FEX Offline
CSCuq60111	Incorrect Type 1 vPC consistency for "vPC card type" in Enhanced vPC
CSCuu21983	mts leak between Mcecm SAP and CFS after mct flap followed by reload
CSCuw01221	N5K VPC orphan-port suspend (vpc peerlink is down) w/ peer adjacency OK
CSCva37021	n6k vPC unknown unicast loop during reload
CSCuy36538	N6K: AA-FEX HIF Suspension on Parent Replacement with FEX Pre-Provision
CSCux95740	port-channel member interface with vpc orphan-port suspend configured
CSCuz58307	Syslog missing for %VPC-6-PEER_VPC_UP event
CSCut52535	vlan mapping under vPC port cause link up delay
CSCuy37201	Vlan remains in error disable state when created in fabric path and VPC
CSCux76255	vpc hap reset during ISSU from 7.0(5)N1(1) to 7.0.7.N1.1
CSCuv99658	VPC peer link is not coming up after peer-link flap
CSCuv96234	match datalink mac destination-address use field id 57 for ingress flow
CSCuy44866	ACL logging not working for egress (packet manager change)
CSCuy93985	Control-Plane Egress QoS - CoS markings are not preserved from its DSCP
CSCux85363	N5600/6K : IGMP GSQ are not sent out in response to IGMP leaves
CSCuy22769	VXLAN-EVPN with suppress-arp, ARP for silent destination is flooded back
CSCuz50112	Cisco Nexus 5000 crash with "fpoam hap reset".
CSCuu06239	ACL permit and deny not working on SNMP walk
CSCuy04049	NAT: udp acl matching traffic doesn't get translated
CSCum52148	Distributed reflective denial-of-service vulnerability on NTP server

Table 45 Resolved Caveats (continued) in Cisco NX-OS Release 7.1(4)N1(1)

CSCuz92661	Evaluation of N3k,N5k,N7k,N9k, N8K for NTP June 2016
CSCuz44147	Evaluation of n7k/N5k/n9k/n3k/MDS for NTP_April_2016
CSCuw84708	Evaluation of n9k, n3k, mds, n7k and n5k infra for NTP_October_2015
CSCux95101	Evaluation of N9k/N5k/N3k/MDS for NTP_January_2016
CSCuu13856	N7K/N6k- NTPD Cores fill up /var/sysmgr/
CSCuz04086	ntp source-interface does not work as expected on 7.1 images
CSCuy23998	N5k pbr next-hop adjacency not updated in hardware
CSCuv68967	SNMP Timeout on CISCO-RMON-CONFIG-MIB
CSCuy65138	After ISSU from 7.1(0)N1(1b) to 7.1(3)N1(1), unused HIF will not come up
CSCur20769	sh fex 'fex num' transceiver -shows sfp is present but not supported
CSCuy08128	Cut through Threshold change on Tiburon FEX's on 40gb NIF's
CSCux47933	FEX2348 EVPC: HIF PO seconds of traffic drops after NIF failure
CSCuv46411	HIF ports go down and don't come back up when host reloads
CSCux10337	N2348TQ tiburon fex devices crash repeatedly
CSCuw14656	show-ps satctrl command for N2200-PDC-400W displays status as "FAIL"
CSCux78120	Upgrade failure due to FEX file transfer error
CSCuo66649	bigsurusd core on adding member port to portchannel
CSCuo93650	Enh: Speed up module 2 bring up in Cisco Nexus 6001
CSCuq72020	Forwarding ASIC Diag Error not forcing links to go down completely
CSCux03218	Kernel reload during ISSU/ISSD from KK-191 bin to upg image
CSCuv01780	Mgmt0 with Crossover cable and hardcoded speed 100/duplex full is down
CSCva12553	N56-M24UP2Q in N5K-C56128P-SUP does not recognise media type of SFPs
CSCux41730	N56K/6001: New BIOS to addresses source of correctable PCIE errors
CSCus92726	N5K link flaps with HP StoreEasy x5530
CSCut60043	N5K/6K - 40G transceivers have delay for link-up on module boot/reload
CSCus71581	need to copy cores from show cores into bootflash by default
CSCus09929	Cisco Nexus 55548/5596 detect link up/down without cabling
CSCus89236	Cisco Nexus 5600 1gb link unable to transmit frames after link flap
CSCux76799	Cisco Nexus 5600: Non disruptive ISSU can fail on certain systems.
CSCuo97783	Cisco Nexus 6000: 3-4 Packet loss during power off LEM operation/switch reload
CSCut56888	PCI erros reporting in 5K/6K products
CSCuv44148	Ports status "down (SFP not inserted)" although SFP present
CSCux05255	Interface running-configuration may incorrectly show 'shutdown'
CSCuv61110	N5K/N6K: Errors when modifying vlan allowed list in port-profile on FEX
CSCuy27585	N5K: Incorrect startup for allowed vlans in port-profile type ethernet

Table 45 Resolved Caveats (continued) in Cisco NX-OS Release 7.1(4)N1(1)

CSCuw33247	N6K: SNMP configuration lost after upgrade to 7.0(6)
CSCuw02613	no shut twice when PP with shut is applied to admin down interface
CSCuz29569	Error during pre-provisioning the module of type N5696-M20UP
CSCux83890	N5K/6K: Crash due to provision hap reset- signal 6
CSCux33230	"ipqosmgr hap reset" during ISSU 7.1(2)N1(1)->7.1(3)N1(1)
CSCux42280	BFD session randomly flaps on N6K
CSCuw26728	Enh: N5K/6K Log syslog message if ingress/egress buffer gets stuck
CSCuy62490	N5k: qd hap reset at qd_bigsur_lc_remove
CSCtz94196	Need capability to clear QoS statistics per interface.
CSCux28524	Cisco Nexus 5K crashed due to "QD" process.
CSCuy69670	Cisco Nexus Priority Flow Control 'Off' when Interface is 'Up'
CSCuy28938	One Server sending continuous RX pause can cause Buffer lock
CSCuy61591	Radius crash on dot1x authentication with multiple flap of authed ports
CSCva13731	RADIUS Daemon crash on N5k
CSCux30880	Auto-config profile stuck PPM Del Wait ascii-cfg-server rollback request
CSCuy07502	In show running, ffff is missing from the v4 mapped v6 address.
CSCux40274	Multicast traffic dropped due to cell usage stuck for ingress buffer
CSCup65293	show ip prefix list is not filtering on the basis of name
CSCuz51928	icmpv6 crashes because of access to a non-readable memory region.
CSCuw51328	BGP routes preferred over HMM
CSCua39159	Command injection with CA functionality
CSCva11572	copy bootflash:<file> startup-config cannot restore the ssh key config
CSCux86335	OpenSSH Vulnerabilities
CSCux11097	N5k / N6k- ssh login-attempts 3 results in no ssh login-attempts
CSCux06003	N6K POAP is failing with SSH HOST KEY
CSCux55515	OpenSSH: Evaluation of Multiple OpenSSH CVEs for NX-OS
CSCux17060	N5K xmlma hap reset
CSCuz22196	Cisco Nexus: snmpd Program terminated with signal 8, Arithmetic exception.
CSCut82544	SNMP MIB entPhysicalVendorType does not send the correct value
CSCuz58351	SNMP OID - Location of FEX power supplies are not programmed correctly
CSCuv29391	SNMPD crash on n5k
CSCuv32204	SNMPd Memory Leak in libport_mgr_common
CSCuw76278	NX-OS - Netstack panic crash due to buffer lockup
CSCux51705	interface counters stucked in 0
CSCuy83222	N5696+N5696-M12Q with sub-interf;Snmppolling Cause MTS Buff leak-pfstats

Table 45 Resolved Caveats (continued) in Cisco NX-OS Release 7.1(4)N1(1)

CSCuo24670	N5K/FEX FEX Interface Incrementing output discards rapidly
CSCuw45315	statsclient hap reset seen on stand alone switch
CSCto57719	"spanning-tree port-priority" changed to "0" from "128" in show run all"
CSCuw83023	%STP-2-VLAN_PORT_LIMIT_EXCEEDED on ISSU even when spanning-tree disabled
CSCuo74024	STP BPDU received on vPC secondary not tunneled to vPC primary
CSCum57545	Peer-link STP inconsistency due to corrupt BPDU does not clear
CSCux54465	BFD Stuck in Down state & BFD Session is not initialized On N6000
CSCuw89504	Cisco Nexus 6000 crashes with memory leak in bfd_app
CSCuu77657	Mem leak in fs-daemon process in longevity test
CSCuu21286	n5548UP - Kernel panic while doing ISSU
CSCuz68056	logging server vrf changes to vrf default after ND-ISSU
CSCus95548	N7K - SNMP snmpd core in syslog_mib w handle_notif_clogMessageGenerated
CSCuy93128	N5K ttyd process core when ISSU to 7.0(7)N1(1)
CSCuy11847	TACACS Daemon Hap Reset When Adding an SSH Key
CSCur22877	Traffic drop at BL after vrf extension
CSCun34005	Cisco Nexus2k/5k/6k: Continuous memory leak messages seen for ethpm
CSCux72134	Vlan not getting programmed as vn-seg capable
CSCuw89463	MTS buffer leaks for mcecm on the peer device with MCT flap
CSCuw82759	Cisco Nexus 5600/6000: No LAN_BASE should disable FHRP CLI or throw error
CSCux40246	Cisco Nexus5672 WCCP service not responding when new client connected
CSCuw53377	WCCP process crash
CSCuw51093	WCCP redirection should be applied for layer 3 routed packets
CSCuv14425	Cisco Nexus Unassigned Zone Count Misleading

Resolved Caveats in Cisco NX-OS Release 7.1(3)N1(2)

Table 46 Resolved Caveats in Cisco NX-OS Release 7.1(3)N1(2)

Caveat ID	Resolved Caveat Headline
CSCux33230	"ipqosmgr hap reset" during ISSU 7.1(2)N1(1)->7.1(3)N1(1).
CSCux03218	Kernel reload during ISSU/ISSD from KK-191 bin to upg image.
CSCuw28001	Switch reloads while ND ISSU with LACP failure-maximum downtime exceeded.
CSCux92689	VMM_TIMEOUT: Service SAP 175 for slot 33 timed out in UPGRADE_READY_SEQ.

Resolved Caveats in Cisco NX-OS Release 7.1(3)N1(1)

Table 47 Resolved Caveats in Cisco NX-OS Release 7.1(3)N1(1)

Caveat ID	Resolved Caveat Headline
CSCus84485	Status LED AMBER after upgrading to 7.1(0)N1(1).
CSCuv07607	N5k/N6k - No login possible to device when root directory is full
CSCue80077	FEX: Port flap request from SAP: MTS_SAP_SATMGR
CSCuw83670	N5k/6k - AFM Errors - unknown policy - Port error disabled
CSCut78526	Optimize system qos feature apply code path in AFM
CSCuv05073	HMM hosts learnt on peer-link after control plane stress test
CSCut99511	BFD flaps with the 50 ms default timer
CSCuo02240	N5K carmelusd core
CSCuq25291	REOP on N6K: CSCtk37170: CDP IPv4 address is reported incorrectly
CSCuw30036	Incorrect BGP-3-BADPEERAS: error log after reload
CSCut49617	N5K: 'ip router rip xxx' may disapper from running-config after reboot
CSCuu01961	show run takes long time with large amount of vlans/vsans
CSCuw31547	N5k/N6k stale param-lists in config which user cannot
CSCuq96601	PPM should block 'copy r s' if auto-config is going on in the background
CSCuw61934	N5K Global DB lock after ISSU
CSCuv58843	port-profile reset when committing a VLAN change
CSCuv58091	Verify Fails after importing the running config to Switch-profile
CSCum62759	CTS: N5K ignores CTS timers from ISE
CSCuv69160	N5K: DHCP Snooping binding maintains incorrect port after a client move
CSCtz26764	5K - After removing GEM, interfaces still remain in the show start
CSCuo58150	N6k: QinQ capability not enabled after nondisruptive ISSU
CSCus17580	eth_port_channel hap reset
CSCut53085	mmap error for port-channel services
CSCus52683	Port-channel on FEX down when fex-fabric up
CSCur10558	Trunk Protocol Enable does not show in running config when disabled.
CSCum17923	N5k should not send ELS_RSCN upon mgmt port changes on a connected MDS
CSCuv12447	zoneset is significantly bigger or smaller warning not issued
CSCuu22403	N5K/6K Cosmetic Message: Mac registration with L2FM failed for mac...
CSCuw16411	HSRP state Active/Active after removing Anycast
CSCuv49114	ipAddressPrefix MIB returning wrong object
CSCuu45635	Netstack hap reset after ISSU from 5.2(1) to 7.0(6)N1(1)
CSCuw38972	Fabricpath ECMP not working after ISSU

Table 47 Resolved Caveats (continued)in Cisco NX-OS Release 7.1(3)N1(1)

Caveat ID	Resolved Caveat Headline
CSCuv27318	IGMP packets are sourced from Anycast SWID instead of emulated switch id
CSCuw10906	N5K/N6K vpc ports missing from FTAG tree
CSCut55084	N5K/6K Need to make LACP suspend individual default for base ports
CSCuv82106	Multicast traffic gets blackholed when MVR configured
CSCuw01105	DFA: multicast duplicate packets or loop on border leafs
CSCuv54348	fwm aborted due to heartbeat failure
CSCuu46633	interface vethernet X enters interface range configuration mode
CSCuv37294	2248: Packets getting Blackholed in the HIF VPC port-channel
CSCuv95106	After FEX ISSU interfaces error disabled due Dot1q-tunnel misconfig
CSCut92989	EVPC+ peer drops FTAG2 traffic while other VPC peer initializes the FEX
CSCuq81648	N5K: Po configured as fex-fabric does not work as normal VPC trunk port
CSCus97195	Nexus 5K/6k - FEX HIF port down delay when FEX Fabric member links down
CSCuu14960	Static MAC configuration only allows +-1000 characters
CSCuv35326	N6k :: ICMPv6 related to neighbor discovery punted to the CPU
CSCuu96337	N5672UP NFM crash after config change
CSCui06208	FEX 2232TM-E 10G link flap
CSCuv29358	Interface counters on a Nexus 2348 may be erroneous
CSCut91877	Multiple FEX had fan failure alerts that recover within a second
CSCuv87644	N2348TQ - 10G Auto-negotiation issues
CSCur78132	N2K - Input Align-Err on FEX Host Interfaces
CSCup76628	N2K LED of a PSU blinks green
CSCuu14439	DFE Tuning: Servers not Sending Traffic after Microflap
CSCuv40217	Excessive NMI on root port due to correctable error notif causing reboot
CSCuu27754	N55xx "reload power-cycle" is not resetting ADM
CSCur39762	Nexus 5600: FWM hap reset with "sh hardware internal bigsur asic x eye"
CSCuu33529	Nexus 56128 cannot detect power supply failure
CSCuv03880	Nexus 5696 Cant display DOM of TX RX power reading WSP-Q40GLR4L
CSCuw48559	Nexus 5K: Change fan detection logic
CSCuv79564	Nexus 600x: Hang due to NMI interrupts..
CSCut57707	NX-OS removing pvlan association trunk configuration
CSCus92242	counter in show queuinter interface not removed after n5k reload,
CSCuw13812	iscm memory leak
CSCuv72180	auto-config profile stuck in PPM Del Wait
CSCuw81067	DFA: Multicast SG join state missing in BGP
CSCuv56604	N7K:ospf pushing BFD into admin down state

Table 47 Resolved Caveats (continued)in Cisco NX-OS Release 7.1(3)N1(1)

Caveat ID	Resolved Caveat Headline
CSCut38855	n5k DR does not register S,G when acting as first hop router
CSCuv08448	Cisco Nexus 5000 VDC Authenticated Privilege Escalation Vulnerability
CSCuw28430	Disabling password strength-check does not take effect
CSCuv92830	RADIUS login only assigned network-operator role
CSCuv82719	Unable to login with new passwd reset from switch(boot) prompt
CSCuw75517	Add transceiver direction information to entPhysicalName OID
CSCuu87608	N56-M24UP2Q interfaces are not listed in IF-MIB snmp walk
CSCut82544	SNMP MIB entPhysicalVendorType does not send the correct value
CSCuv54185	SNMPd keeps logging "svi_counter_cache_fetch: destroying stale results"
CSCuw07725	N5k Post-7.1(0)N1(1a) BPDU Guard Not Triggered On Disallowed VLAN
CSCuw07732	N5k Post-7.1(0)N1(1a) BPDU Guard Triggered When Operationally Disabled.
CSCuu92452	Too many MTS flush generated when connecting VPC+ MST to legacy RPVST
CSCur17440	945snmpwalk on cpmCPUTotalTable(1.3.6.1.4.1.9.9.109.1.1.1) failing
CSCuu25462	UDLD NOT to be enabled on the port previously configured fex-fabric
CSCuv25016	sh forwarding internal message counts - N6K/N5K switch reloads: fwm core
CSCut52768	Vinci: dvp interface command should appear with "show run interface all"
CSCuv59999	vlan_mgr Memory Leak on VLAN Addition Removal
CSCuw19708	Nexus 5000 crashes when removing VM tracker config from the interfaces
CSCuv75852	AA dual-homed FEX HIF suspended due to speed during server boot process
CSCut41843	N5000 crash: "vxlan udp port 8472" cause "nve" crash on N5K

Resolved Caveats in Cisco NX-OS Release 7.1(2)N1(1)

Table 48 Resolved Caveats in Cisco NX-OS Release 7.1(2)N1(1)

Caveat ID	Resolved Caveat Headline
CSCuo10554	Cisco Nexus 5000 Message of the Day (MOTD) Telnet Login Vulnerability
CSCus93963	N5K- After Reload Local Authorization Fails when mgmt0 int is down
CSCut79464	unable to login with new passwd reset from switch(boot) prompt
CSCut42246	ACL used for ERSPAN filter not removed
CSCub22567	Error message needs to be cleaned up.
CSCus28695	WCCP - ACL Remark breaks TCAM redirection entry
CSCut75399	update rdecode.sh to support n3k/5k
CSCus75696	N5K N55-M4Q GEM module port1 and port2 stay down after reboot

Table 48 Resolved Caveats in Cisco NX-OS Release 7.1(2)N1(1)

Caveat ID	Resolved Caveat Headline
CSCus64364	N5K: carmelusd component got cored on O2 switch
CSCuu07598	Nexus 5548P/N55-M16P : After Upgrade Interface Down & Unrecoverable
CSCut07668	N5k: Cisco IP phone voice vlan not working
CSCuv04979	N56K Platform: netstack crash while saving tech-support in bootflash
CSCuu01961	show run takes long time with large amount of vlans/vsans
CSCut92605	"port-profile hap reset" after switch-profile commit
CSCut65095	Nexus may reload due to port-profile hap reset
CSCuu04623	Parsing error while importing lengthy configuration to switch profile
CSCut08643	N5K CoPP does not match router ISIS packets
CSCut68629	N5K: customized CoPP config back to default after reload
CSCuu67017	N6K/N56xx CoPP arp/ipv6-nd policy CIR set to 8000
CSCur04843	LLDP with tlv length 0 are dropped
CSCur13337	N5K/6K: LLDP MIB not being responded to in NX-OS 7.0
CSCut50912	DHCP offer is send on vpc orphan port with dhcp snooping enabled
CSCut21777	DHCP Packets flooded to VPC peer with DHCP snooping configuration
CSCut97255	dhcp_snoop reset on nexus 5000
CSCuu09610	Switch sends large number of DHCPv4 packets in response
CSCut94161	EEM: Configuration failed with: 0x412c000d validation timed out
CSCut42878	Ethpm Hap Reset on Nexus 6k/5k
CSCul25050	N2K-B22HP-P: Down interface are logged ETHPORT-5-IF_DOWN_ERROR_DISABLED
CSCus94969	newly added FP vlan is not stp forwarding on the Po interface
CSCuv01812	N6k: port-security err-disables HIF after switch/fex reload
CSCuu04099	N5K: SAN port-channel has output discards when member links are added
CSCuu59941	FC ports error disabled with non-Cisco SFPs after upgrade to 6.x/7.x
CSCup96375	crash flogi process on both N5k's at the same time due to null pointer
CSCur63212	FWM hap reset after issu on restoring fcoe mac addresses
CSCup16103	N7k: Copp fails to rate limit Pause frames from Hosts on 2248TP type FEX
CSCty34142	Enh: Need "show tech fwm" in Nexus 5000/5500
CSCup70139	N5K fwm hap reset
CSCut83532	5600 vPC Pair loops back unknown unicast packets
CSCut36623	crash in fwm with signal 6 fwmpd_delete_int_vlan_to_vni_mapping ()
CSCuc93691	Fwm hap reset as soon as FEX is connected
CSCut13914	N6k: fwm hap reset
CSCus76454	API CFS send failed with Timeout(0x8) in mcec_tl_cb_send_fail
CSCuu24295	DFA: Profile flags and state are not being correctly set during failover

Table 48 Resolved Caveats in Cisco NX-OS Release 7.1(2)N1(1)

Caveat ID	Resolved Caveat Headline
CSCuu73084	HSRP Bundle in INIT state after reload
CSCus57051	Hsrp_Engine crash during ISSU from 6.2(8a) to 6.2.10
CSCuo37471	N7k/RIB displays HSRP VIP route incorrectly
CSCur75712	N5K PTP intermittently sends Delay_Resp with rewinded timestamp
CSCtn18527	ISSU upgrade prints message that switch is reloading.
CSCur20112	%NETSTACK-3-IP_INTERNAL_ERROR: Failed to get IP VRF name 0
CSCus50291	N5k/6K: IGMP General Queries are not sent out mvr receiver port
CSCut45487	Vinci: support for SVI ip secondary with tag 12345
CSCuo56514	In VPC+ N55xx ARP reply may be sourced from SID, rather then ESID
CSCuu00391	N5K/6K: BCAST flag missing for FTAG 2
CSCue08601	Show interface trunk shows all interfaces as fabric path forwarding
CSCut99454	Multiple ip domain-lists not displaying in running-config
CSCur22683	NXOS - VRF aware telnet with "#" in VRF name fails
CSCus45511	Add Debug Messages in MSDP API
CSCur89779	(S, G) not timing out even if there is no traffic
CSCuu29773	Crash in the pim process after exceeding 32K multicast routes
CSCus02026	PIM crash seen on with high scale mcast source on VPC
CSCue76773	"ip routing multicast software-replicate" Support for N5K/N6k platform
CSCus89838	Nexus 5000 'fwm' process crash while updating multicast routes
CSCui97117	"sh int mgmt 0 capabilities " does not give any output
CSCut19721	logging source-interface loopback does not work for ipv6
CSCut46788	Nexus 5600: Logon prompt not correct when hostname begins with number
CSCuu14701	N7k-(6.2.8a) allocate non-null label for loopback used for Anycast RP
CSCuo15015	urib process crash on N7k
CSCur71049	STM thrshold not updated correctly - show platform fwm info stm-stats
CSCut08809	Bug CSCuj56227 gets carried over ISSU upgrade.
CSCuo28747	N5K/6K: FWM core during ISSU
CSCuc72380	Nexus 5500: IGMP Link Local Destination Packet Flooded
CSCus04099	N6k/7k/9k: SSH/Telnet connection refused
CSCun45981	L3 N5K: Inbound and output ICMP frames on different ports
CSCut36200	Ports towards the N2K-B22HP-P do not come up after a server reboot
CSCud02630	Unconnected FEX power supply should show "no power source"
CSCus89917	Ethanalyzer interprets packets as Malformed LLC
CSCus89890	Link state will not change after ISSU to 7.0 from 6.0(2)
CSCuo46284	N55xx showing SFP uC: Module 1: v0.0.0.0 - Install all fails first time

Table 48 Resolved Caveats in Cisco NX-OS Release 7.1(2)N1(1)

Caveat ID	Resolved Caveat Headline
CSCut86026	N56K/6K: /var/tmp directory getting full with lcuc log file
CSCuu37102	N5K kernel Panic on AIPC driver causing crash
CSCun33975	'ppm' process crashes soon after upgrading N5K
CSCup86425	Crash after entering "no port-profile type ethernet uplink"
CSCur80754	Incorrect show run for allowed vlans in port-channel type port-profiles
CSCur18043	N6K "ntp access-group peer" wont show up in running config
CSCua68756	Ingress drop counter value to be displayed for host FEX interface
CSCuq68778	BGP snmp traps cbgpPeer2BkwardTran,cbgpPeer2FsmStChn sent malform inst.
CSCut01933	default route not withdrawn after removing "default originate"
CSCuu70539	N5K bgp process crash after configuring default-originate
CSCus67129	vrf import map doesn't process multiple paths
CSCut51575	VPC breaks due to incorrect emulated switch-id after ISSU upgrade
CSCuo80764	N5K - ISSU upgrade to 7.0.1.N1.1 changing config vrf name to unknown
CSCur12364	N5K:ISSU fails 5.1(3)Nx(x)/5.2(1)N1(x) -> 6.0(2)Nx(x)/5.2 -> 7.0(x)N1(1)
CSCut18721	gbr_422: urib core at urib_chlist_segv_handler
CSCus68473	urib crash after running "clear ip route vrf xxx *"
CSCut64547	LACP port-channel show wrong ifType
CSCuu69510	N5K/N6K snmp 64 bit counters for svi interface dont work
CSCut08818	SNMPD crashes with role with only deny OIDs
CSCut44932	sync-snmp-password failing for user part of the vdc-admin group
CSCuf57781	%STP-2-BLOCK_DETECTED_PVST_PEER message is not output on Nexus5000
CSCut01957	logflash: online and logflash:not present not logged to syslog
CSCts88978	Need explicit log msgs instead of logging 'last msg repeated n times'
CSCtz88781	Fex port showing bpdufilter enabled in port-channel
CSCur49785	Inconsistency between running and startup config
CSCum43366	N5K'Show interface status' output is not aligned correctly in 6.0(2)N2
CSCuq00062	Nexus 5600 7.0(2)N1(1) session limit shows twice in running config
CSCue60401	Telnet disconnect if we have binary characters in the show output
CSCut84977	High cpu and fabricpath mroutes missing after upgrade to 7.0(5)N1(1)
CSCut55133	N5672: cant't save config after configuring vlan mapping more than 200
CSCur47111	Nexus 5500: delay restore value should not be less than 150 for L3 setup
CSCum93892	VSAN is stuck in operational state down, but state is active.

Resolved Caveats in Cisco NX-OS Release 7.1(1)N1(1)

Table 49 Resolved Caveats in Cisco NX-OS Release 7.1(1)N1(1)

Caveat ID	Resolved Caveat Headline
CSCut34556	48Q: RAF fan shows up as FAF syslog on removal during multi OIR
CSCut85787	N5K/6K: NTP received time not to used to update clock.
CSCud02139	Access to nexus7k via vty may get lost at random times with tacacs+
CSCue31348	tacacsd process crash during authentication/authorization
CSCtw85051	Nexus FEX ISSU upgrade fails if FEX link flaps
CSCus23186	CDP gets automatically re-enabled after a reload
CSCur39862	Port-profile config is truncated - "show port-profile" crashes switch
CSCup77720	cts manual command not allowed with fex pre provisioning
CSCus03494	N5K/6K: Cannot import certain config lines longer than 132 characters
CSCur43289	COPP - Ipv6 NA, RA and RS goes to wrong CoPP queue affecting icmpv4
CSCus28101	N5K/6K: Inband TACACS traffic matched against exception-class in CoPP
CSCur41721	DHCP relay is broken over L3 sub-int port-channel
CSCus89196	Trunk ports move to BKN state for native vlan
CSCus19792	"show fcns database", "show fcs ie" not correctly populated after ISSU
CSCuo34512	fwm hap reset with traffic running over the weekend
CSCus95396	fcoe_mgr leak cause a crash
CSCuq31499	N7K FEX satctrl hap reset
CSCua77932	N5k crashes due to fwm hap reset
CSCur30631	Nexus 6000: FWM crash with not enough core files saved
CSCus38422	fwm core triggered due to fex port-channel flap
CSCus94447	DFA-auto-config-recovery-does-not-work
CSCur30305	HMM should learn multiple IPV4/IPV6 address with same MAC
CSCus78223	profile stuck in "Profile halt" status
CSCus52281	Add a PTPLC mem-stats command to Nexus switches
CSCus36208	PTPLC core due to mem leak
CSCuo34379	N5K/6K:NXOS upgrade by changing bootvariables & reload isn't recommended
CSCus22741	DRAP process crash after FP domain restart
CSCus04851	N5k/6k -FP BCAST/MCAST broken on VPC edge ports after remote root change
CSCur01470	N5K/6K fails to respond to unicast ARP request and may loop it back
CSCus16074	N6K: FPOAM process crash
CSCuq45187	L2vpn - Local access circuit DOWN after RELOAD
CSCuq81861	Enabling peer-gateway breaks the fix for CSCui48861
CSCus58726	LACP core + reload on N5K /N6K

Table 49 Resolved Caveats (continued)in Cisco NX-OS Release 7.1(1)N1(1)

Caveat ID	Resolved Caveat Headline
CSCuc61695	port-channel members error disabled due to eltm seq timeout
CSCup85771	Nexus 6000 resets SSH intermittently
CSCuq78422	Fabricpath - 1st CE port bringup places interface in L2G Blocking state
CSCur14220	Netstack core after modifying PBR deleting SVIs and adding back in scale
CSCus11451	N5K: PTP: Core detected due to hwclock crash
CSCuq76383	Can not exit from VTY after using onePK VTY SS
CSCug29190	'ethpc' hap reset tied to SFP diagnostics
CSCun69369	Bigsur FAULTY slot 0 asic 0, bigsur_stm_dma_monitor_timer_hdlr error
CSCun91863	N5K: NOHMS-2-NOHMS_DIAG_ERR_PS_FAIL with DC Power Supply
CSCus70491	N6004 bigsurusd hap reset
CSCuq96902	N6K QSFP-40G-CSR4 shows up as "transceiver is not supported"
CSCur76751	N6K/5K: Need knob to configure mgmt0 interface to operate at auto 10/100
CSCuo23668	N6K: errors "clk_flush: Couldn't Clear Bus" and console unresponsive
CSCus39651	N6k:CRC errors on random 40gig port after reload
CSCuj84269	Nexus 5000 switch reloaded due to gatosusd hap reset
CSCur11599	Nexus 5k/6k - Memory leak in pfstat process causing hap reset
CSCuq66628	VDC-MGR crash on N5k
CSCuq86032	N5k - Same "match cos" value shared between class-fcoe and another class
CSCuq00161	Verizon CoPP: Nexus 5600 Support for CB-QOS MIB
CSCus97571	Rollback Broken in PPM, Auto config breaks while VRF in Delete holddown
CSCus98916	BGP Vinci: For 0.0.0.0/0, BGP installs non-best/multi paths in URIB
CSCup75270	FC interfaces are not listed in IF-MIB snmp walk
CSCus65288	ERSPAN outer ip header length exceeds the maximum limit for a packet
CSCur54642	N5K with ERSPAN enabled may face a slow leak in 'monitor' process
CSCuo71613	IPLUS 152: ISSU ND upg -> bin - FEX module preload failed
CSCur25570	Defined VLANs do not appear in configuration
CSCut09166	fwm hap reset on vlan delete
CSCur39582	vlan_mgr unresponsive on creating or deleting VLAN
CSCus55778	A Nexus 6000 may reload unexpectedly due to a vPC hap reset
CSCup74458	few seconds of packet loss on vpc secondary link bringup
CSCuq42482	N5K dual homed vpc fex, hif speed change not always picked up N5K's
CSCuq27230	IBM Fex: upgrade cmmuc version to 1.10
CSCuq37872	Iplus: Crash in urib segfault in urib_chlist_add_rnh()
CSCuq64886	fabricpath isis bfd requires L3 bfd interval command to adjust timers
CSCuq88206	Increase FCF MAC Allocation for Nexus 6004 Platform to 48.

Table 49 Resolved Caveats (continued)in Cisco NX-OS Release 7.1(1)N1(1)

Caveat ID	Resolved Caveat Headline
CSCuq91075	DFA: DHCP fix for Infoblox.
CSCur09549	Configuration sync rollback failure for failed port channel member.
CSCur16747	satctrl cored after write-erase& applying config with 'FEX-QoS-offload'
CSCur47731	5596UP / Crash, Reload after setting a FC Port shut/no shut
CSCur59789	While configuring vrf Unrecognized IP message minor type 33
CSCur64428	ISIS fails to push MAC entry learned from ISIS peer into local M2RIB
CSCur66262	DFA Leaf should NOT allow auto-pull for core-vlan range/backbone vlan.
CSCur86210	Iplus: motd banner not displayed upon login
CSCus01129	Iplus : vpc status shows "DOWN" in the fex uplink port PoCH output.
CSCus56036	BGP tracebacks or FD read errors along with session flaps
CSCus64947	Vinci Fabric Anchor and Anycast-GW cause ARP-3-DUP_VADDR_SRC_IP msg.
CSCus72900	Knob to Disbable ports after loop is detected not working as expected
CSCus74412	SunnySide fex:Fan is going to 'failure state' even though fan is present
CSCus78102	N6K crashed due to "kernel panic" @ stale pointer
CSCut06901	Traffic blackholing for around 60 secs after new RPF intf comes up
CSCut17968	res mgr crash in n6k/n5k when "show vdc resource" command is given
CSCus77310	vpc hap reset vpc process crashed
CSCus64400	%STP-2-VLAN_PORT_LIMIT_EXCEEDED is output even under verified scalabilty
CSCuq86047	Nexus5k ipForward Object not giving correct results for snmpwalk
CSCuq04309	nexus snmpd crash after mts queue full
CSCur26119	EIGRP prefixes missing after interface flap
CSCuq79790	EIGRP Internal Route does not carry tag that is in the topology
CSCuq68431	EIGRP crash in eigrp_cmi_enqueue
CSCut22554	Workaround for CSCuo46284: Nexus 5500 showing SFP uC: Module 1: v0.0.0.0
CSCus16410	Sometime N6K export as a TCP Src/Dst port is zero.
CSCus68610	N5K/N6K - Silent reset with uC reset code: 0x4800
CSCut35476	Bigsur FAULTY slot 0 asic 3, bigsur_stm_dma_monitor_timer_hdlr
CSCur07245	Nexus switch may see repeated crashes of ntpd process
CSCue56335	N7k - snmpd core dumps during vlanTrunkPortVlansXmitJoined mibwalk
CSCus28969	Nexus 5000 ICMP redirects send with wrong redirect IP gateway
CSCuq56923	Logging level virtual-service reverts to default after a NX-OS upgrade..
CSCut55443	FWM mac trace buffer memory corruption
CSCut03537	QinQ - Double-tag for native/untagged vlan traffic
CSCut74135	Fabricpath mode transit - control packets tagged with internal vlan 4041

Table 49 Resolved Caveats (continued)in Cisco NX-OS Release 7.1(1)N1(1)

Caveat ID	Resolved Caveat Headline
CSCut19714	N2H traffic can drop on a HIF port-channel when another is down
CSCut12023	Port channel service crashes after many 'show run' commands
CSCus29400	FCPC cores and triggers hap reset while allocating response payload
CSCus20646	N5K crash on CDP process

Resolved Caveats in Cisco NX-OS Release 7.1(0)N1(1b)

Table 50 Resolved Caveats in Cisco NX-OS Release 7.1(0)N1(1b)

Caveat ID	Resolved Caveat Headline
CSCus41273	Loading a new license or reloading existing license on 5624Q gives error.

Resolved Caveats in Cisco NX-OS Release 7.1(0)N1(1a)

Table 51 Resolved Caveats in Cisco NX-OS Release 7.1(0)N1(1a)

Caveat ID	Resolved Caveat Headline
CSCup75270	FC interfaces are not listed in IF-MIB snmp walk
CSCus31100	After upgrade to 7.1(0)N1(1), vPCs in down state.
CSCus39388	Alt route missing for vPC.
CSCus18209	FEX VLAN translation with multiple HIF PO flaps might stop Layer 2 VLAN forwarding.
CSCul35819	BPDUGuard not activated on disallowed edge trunk VLANs.
CSCun98175	N6K nfp process crash.

Resolved Caveats in Cisco NX-OS Release 7.0(8)N1(1)

Table 52 Resolved Caveats in Cisco NX-OS Release 7.0(8)N1(1)

Caveat ID	Resolved Caveat Headline
CSCut56888	NMI Error handling in all Nexus 5K/6K products.
CSCuv91102	Interface down after flapping a range of interfaces.
CSCux78120	Upgrade failure due to FEX file transfer error.
CSCux46009	Nexus 802.1x: suffix delimited with @ is not sent in RADIUS request
CSCux03956	ARP Reply for VIP is dropped in hardware on egress path
CSCux32552	N5K/6K ascii-cfg hap reset
CSCuw61934	N5K Global DB lock after ISSU

Table 52 Resolved Caveats in Cisco NX-OS Release 7.0(8)N1(1)

Caveat ID	Resolved Caveat Headline
CSCuw09982	Crash on N5k after Dell server /w N2K FEX modules inserted is powered on
CSCuw40579	inconsistent VRF output cli - sh ip proc vrf all when doing ISSU
CSCux20846	Nexus 6k: IGMP HAP Reset during "install all" upgrades with IGMPv3
CSCuw82347	PIM Assert Storm on pair of N6Ks with Egress VPC and ECMP in L3 Core
CSCus18893	Crash due to a Kernel Panic at mts_sys_my_node_addr_get
CSCue99559	N5K/6K: FWM hap reset during ISSU upgrade
CSCuo95997	no flogis from shared interface vpc legs with native vlan config
CSCuw84708	Evaluation of n9k, n3k, mds, n7k and n5k infra for NTP_October_2015
CSCui06208	FEX 2232TM-E 10G link flap
CSCuv46411	HIF ports go down and don't come back up when host reloads
CSCuv29358	Interface counters on a Nexus 2348 may be erroneous
CSCux10337	N2348TQ tiburon fex devices crash repeatedly
CSCuw75381	Masking of Root Control Register for NMI hang issue
CSCut60043	N5K/6K - 40G transceivers have delay for link-up on module boot/reload
CSCuw48559	Nexus 5K: Change fan detection logic
CSCuv79564	Nexus 600x: Hang due to NMI interrupts..
CSCux41730	NXOS changes wrt BIOS change for CSCuw58510
CSCux83890	N5K/6K: Crash due to provision hap reset- signal 6
CSCux33230	"ipqosmgr hap reset" during ISSU 7.1(2)N1(1)->7.1(3)N1(1)
CSCup10367	N6K/N5K Crashed @MRIB
CSCuw76278	N7K/N5K netstack panic crash after upgrade to 6.2.14/7.2(1)N1(1)
CSCux51705	interface counters stucked in 0
CSCuw83023	%STP-2-VLAN_PORT_LIMIT_EXCEEDED on ISSU even when spanning-tree disabled
CSCuu92452	Too many MTS flush generated when connecting VPC+ MST to legacy RPVST
CSCuu21286	n5548UP - Kernel panic while doing ISSU
CSCuy11847	TACACS Daemon Hap Reset When Adding an SSH Key
CSCuw53377	Nexus5672 WCCP process crash
CSCuv68534	WCCP crashing in the steady state w/o any user induced trigger
CSCuw51093	WCCP redirection should be applied for layer 3 routed packets

Resolved Caveats in Cisco NX-OS Release 7.0(7)N1(1)

Table 53 Resolved Caveats in Cisco NX-OS Release 7.0(7)N1(1)

Caveat ID	Resolved Caveat Headline
CSCuc26047	Nexus 5k/6k reset due to Kernel Panic
CSCuh58418	Ingress drop BIG_DROP_HIT_DROP_PORT_MAP_IDX w/ pbr next-hop is a ce port
CSCup35302	Netstack core in icmp_input on receipt of an ICMP router solicitation
CSCuv58091	Verify Fails after importing the running config to Switch-profile
CSCuu96337	N5672UP NFM crash after config change.
CSCuv24827	StateFarm:FCoE feature failed with POAP template in cpom/dcnm
CSCuu65634	pkt based auto-config access port does not work after profile is removed
CSCul00229	N6K - PIM Registers Misclassified as PIM Hellos by COPP
CSCuq59436	IPQOSMGR-4-QOSMGR_PPF_WARNING: PPF library warning: DDB Error: 0x4117004
CSCut57364	DFA Autoconf/Profile-refresh failing if using vlan name in the profile.
CSCuv07607	N5k/N6k - No login possible to device when root directory is full
CSCut79464	unable to login with new passwd reset from switch(boot) prompt
CSCut42246	ACL used for ERSPAN filter not removed
CSCub22567	Error message needs to be cleaned up.
CSCud07692	Enh: show tech-support enhancements
CSCue80077	FEX: Port flap request from SAP: MTS_SAP_SATMGR
CSCut78526	Optimize system qos feature apply code path in AFM
CSCus28695	WCCP - ACL Remark breaks TCAM redirection entry
CSCuo02240	N5K carmelusd core
CSCus75696	N5K N55-M4Q GEM module port1 and port2 stay down after reboot
CSCus64364	N5K: carmelusd component got cored on O2 switch
CSCuu07598	Nexus 5548P/N55-M16P : After Upgrade Interface Down & Unrecoverable
CSCuh49459	CSCuh49459 %SYSMGR-3-CFGWRITE_FAILED: Configuration copy failed
CSCuu01961	show run takes long time with large amount of vlans/vsans
CSCut92605	"port-profile hap reset" after switch-profile commit
CSCut65095	Nexus may reload due to port-profile hap reset
CSCuu04623	Parsing error while importing lengthy configuration to switch profile
CSCuv58843	port-profile reset when committing a VLAN change
CSCut08643	N5K CoPP does not match router ISIS packets
CSCut68629	N5K: customized CoPP config back to default after reload
CSCuu67017	N6K/N56xx CoPP arp/ipv6-nd policy CIR set to 8000

Table 53 Resolved Caveats in Cisco NX-OS Release 7.0(7)N1(1)

Caveat ID	Resolved Caveat Headline
CSCur13337	N5K/6K: LLDP MIB not being responded to in NX-OS 7.0
CSCur43974	DFA: VLAN Encapsulation error of fabric ports
CSCut50912	DHCP offer is send on vpc orphan port with dhcp snooping enabled
CSCut21777	DHCP Packets flooded to VPC peer with DHCP snooping configuration
CSCut97255	dhcp_snoop reset on nexus 5000
CSCuu97262	Lot of unwanted packets seen on debug dhcp all
CSCug28190	"sh int trunk" doesn't show Vlans Forwarding on FP for all Po members
CSCtz26764	5K - After removing GEM, interfaces still remain in the show start
CSCut42878	Ethpm Hap Reset on Nexus 6k/5k
CSCul25050	N2K-B22HP-P: Down interface are logged ETHPORT-5-IF_DOWN_ERROR_DISABLED
CSCus17580	eth_port_channel hap reset
CSCus94969	newly added FP vlan is not stp forwarding on the Po interface
CSCuv01812	N6k: port-security err-disables HIF after switch/fex reload
CSCuu04099	N5K: SAN port-channel has output discards when member links are added
CSCuu59941	FC ports error disabled with non-Cisco SFPs after upgrade to 6.x/7.x
CSCur10558	Trunk Protocol Enable does not show in running config when disabled.
CSCup96375	crash flogi process on both N5k's at the same time due to null pointer
CSCur63212	FWM hap reset after issu on restoring fcoe mac addresses
CSCur36713	"in-163" entry for SVI MAC missing in HW-STM table in FWM
CSCty34142	Enh: Need "show tech fwm" in Nexus 5000/5500
CSCut74135	Fabricpath mode transit - control packets tagged with internal vlan 4041
CSCup70139	N5K fwm hap reset
CSCua77932	N5k crashes due to fwm hap reset
CSCuu22403	N5K/6K: L2FM messages seen
CSCuv37294	2248: Packets getting Blackholed in the HIF VPC port-channel
CSCut83532	5600 vPC Pair loops back unknown unicast packets
CSCuc93691	Fwm hap reset as soon as FEX is connected
CSCut55443	FWM mac trace buffer memory corruption
CSCuq16049	fwm process crash with heartbeat failure
CSCut13914	N6k: fwm hap reset
CSCuu45148	HMM memleak for unexpected DCNM entry
CSCuo37471	N7k/RIB displays HSRP VIP route incorrectly
CSCur75712	N5K PTP intermittently sends Delay_Resp with rewinded timestamp
CSCut81357	PTP Leap Second : n5k ptp off clock off by 35 seconds
CSCtn18527	ISSU upgrade prints message that switch is reloading.

Table 53 Resolved Caveats in Cisco NX-OS Release 7.0(7)N1(1)

Caveat ID	Resolved Caveat Headline
CSCur20112	%NETSTACK-3-IP_INTERNAL_ERROR: Failed to get IP VRF name 0
CSCus50291	N5k/6K: IGMP General Queries are not sent out mvr receiver port
CSCuu88049	N5K:crash 7.0(6)N1(1) netstack hap reset
CSCus28969	Nexus 5000 ICMP redirects send with wrong redirect IP gateway
CSCuo56514	In VPC+ N55xx ARP reply may be sourced from SID, rather then ESID
CSCuu00391	N5K/6K: BCAST flag missing for FTAG 2
CSCue08601	Show interface trunk shows all interfaces as fabric path forwarding
CSCuq81861	Enabling peer-gateway breaks the fix for CSCui48861
CSCup55118	ORIB buffer exhaustion on IGMP join/leave
CSCut75242	ISSU upgrade: igmp HAP reset
CSCus89838	Nexus 5000 'fwm' process crash while updating multicast routes
CSCui97117	"sh int mgmt 0 capabilities " does not give any output
CSCut19721	logging source-interface loopback does not work for ipv6
CSCut46788	Nexus 5600: Logon prompt not correct when hostname begins with number
CSCut08809	Bug CSCuj56227 gets carried over ISSU upgrade.
CSCuo28747	N5K/6K: FWM core during ISSU
CSCuc72380	Nexus 5500: IGMP Link Local Destination Packet Flooded
CSCus04099	N6k/7k/9k: SSH/Telnet connection refused
CSCun45981	L3 N5K: Inbound and output ICMP frames on different ports
CSCup76628	N2K LED of a PSU blinks green
CSCut36200	Ports towards the N2K-B22HP-P do not come up after a server reboot
CSCuu14439	Connectivity problem with solarflare NIC after server reload
CSCus89917	Ethanalyzer interprets packets as Malformed LLC
CSCuv40217	Excessive NMI on root port due to correctable error notif causing reboot
CSCus89890	Link state will not change after ISSU to 7.0 from 6.0(2)
CSCuo46284	N55xx showing SFP uC: Module 1: v0.0.0.0 - Install all fails first time
CSCuu37102	N5K kernel Panic on AIPC driver causing crash
CSCuq96902	N6K QSFP-40G-CSR4 shows up as "transceiver is not supported"
CSCuu33529	Nexus 56128 cannot detect power supply failure
CSCus68610	Nexus 5672/56128 - Silent reset with uC reset code: 0x4800 or 0x400b
CSCun33975	'ppm' process crashes soon after upgrading N5K
CSCup86425	Crash after entering "no port-profile type ethernet uplink"
CSCur80754	Incorrect show run for allowed vlans in port-channel type port-profiles
CSCuq17992	N5K: PPM crash during FabricPath VLAN config
CSCur18043	N6K "ntp access-group peer" wont show up in running config

Table 53 Resolved Caveats in Cisco NX-OS Release 7.0(7)N1(1)

Caveat ID	Resolved Caveat Headline
CSCua68756	Ingress drop counter value to be displayed for host FEX interface
CSCur26244	Nexus 6000/5600 packet drops with no drop traffic
CSCut51575	VPC breaks due to incorrect emulated switch-id after ISSU upgrade
CSCur12364	N5K:ISSU fails 5.1(3)Nx(x)/5.2(1)N1(x) -> 6.0(2)Nx(x)/5.2 -> 7.0(x)N1(1)
CSCuv08448	Cisco Nexus 5000 VDC Authenticated Privilege Escalation Vulnerability
CSCuv82719	Unable to login with new passwd reset from switch(boot) prompt
CSCut64547	LACP port-channel show wrong ifType
CSCuu87608	N56-M24UP2Q interfaces are not listed in IF-MIB snmp walk
CSCuu69510	N5K/N6K snmp 64 bit counters for svi interface dont work
CSCts88978	Need explicit log msgs instead of logging 'last msg repeated n times'
CSCuu12081	Ethanalyzer fails with capture-ring-buffer
CSCtz88781	Fex port showing bpdufilter enabled in port-channel
CSCur49785	Inconsistency between running and startup config
CSCum43366	N5K'Show interface status' output is not aligned correctly in 6.0(2)N2
CSCuq00062	Nexus 5600 7.0(2)N1(1) session limit shows twice in running config
CSCuv25016	sh forwarding internal message counts - N6K/N5K switch reloads: fwm core
CSCut84977	High cpu and fabricpath mroutes missing after upgrade to 7.0(5)N1(1)
CSCui07482	N5k - CE VLAN's active on FabricPath Core Port
CSCur91350	Port may fail to be add into po due to compatibility check failure
CSCut16773	vlan_mgr crash on creating or deleting VLAN
CSCuv59999	vlan_mgr Memory Leak on VLAN Addition Removal
CSCum93892	VSAN is stuck in operational state down, but state is active.
CSCup35302	Netstack core in icmp_input on receipt of an ICMP router solicitation
CSCuv82106	Multicast traffic gets blackholed when MVR configured.

Resolved Caveats in Cisco NX-OS Release 7.0(6)N1(1)

Table 54 Resolved Caveats in Cisco NX-OS Release 7.0(6)N1(1)

Identifier	Description
CSCur15901	N2K-C2348UPQ FEX does not come up due to "SDP timeout/SFP Mismatch"
CSCup75270	FC interfaces are not listed in IF-MIB snmp walk
CSCud02139	Access to nexus7k via vty may get lost at random times with tacacs+
CSCuc62084	CSCuc62084 Sh accounting log / show log output is missing initial

Table 54 Resolved Caveats in Cisco NX-OS Release 7.0(6)N1(1)

Identifier	Description
CSCtw85051	Nexus FEX ISSU upgrade fails if FEX link flaps
CSCuo67919	SCH : SR creation delayed for more than 6 hours for PSU failure on N5k
CSCuq85982	N55xx link debounce time not working as expected
CSCub20644	cdp core dump in 5.0.3
CSCun70630	Filtering "sh cdp neigh" output does not yield all the entries
CSCun92485	Unable to modify VLAN Failed to run the commands. Please try again later
CSCuq20915	Display of allowed vlan range for FEX HIF breaks in running-config
CSCup77720	cts manual command not allowed with fex pre provisioning
CSCus03494	N5K/6K: Cannot import certain config lines longer than 132 characters
CSCur43289	COPP - Ipv6 NA, RA and RS goes to wrong CoPP queue affecting icmpv4
CSCus28101	N5K/6K: Inband TACACS traffic matched against exception-class in CoPP
CSCul89905	L2 control packets dropped on CTS links with SGT encapsulation
CSCur77280	N6k m2rib missing interfaces from OIFL
CSCun83889	Dual homed FEX interface inactive in FP env.
CSCuf82423	Nexus 5596 ethpm hap reset
CSCur29789	N5k/N6k might unexpectedly reload due to "eth_port_sec hap reset"
CSCuq61301	FEX FCOE FCNS FC4-TYPE:FEATURE incomplete, empty.
CSCue62640	N5K/6K: TCP ports 21, 512-514 are opened after enabling FCoE
CSCun98175	N6K nfp process crash
CSCun80333	pbr-statistics counter issue in multi-sequence PBR
CSCur11378	fwm hap reset with %FWM-2-FWM_ASSERT_FAILURE
CSCuq72386	N5k/6k: Static MAC entries deleted upon STP CBL update
CSCur30631	Nexus 6000: FWM crash with not enough core files saved
CSCuj22176	traffic loss on vPC trunk with 1K vlans after the reload of vPC+ primary
CSCus38422	fwm core triggered due to fex port-channel flap
CSCur30305	HMM should learn multiple IPV4/IPV6 address with same MAC
CSCus36208	PTPLC core due to mem leak
CSCun69659	"m2rib_delete_my_bd_mroutes() failed" when creating FP vlans
CSCuq98419	N5K crash due to kernel panic during ISSU 5.2(1)N1(7)
CSCuo34379	N5K/6K:NXOS upgrade by changing bootvariables & reload isn't recommended
CSCur08894	N5k/6k - FP BCAST broken on VPC edge port after root change on VPC+ peer
CSCus04851	N5k/6k -FP BCAST/MCAST broken on VPC edge ports after remote root change
CSCur01470	N5K/6K fails to respond to unicast ARP request and may loop it back
CSCus16074	N6K: FPOAM process crash

Table 54 Resolved Caveats in Cisco NX-OS Release 7.0(6)N1(1)

Identifier	Description
CSCus58726	LACP core + reload on N5K /N6K
CSCuc61695	port-channel members error disabled due to eltm seq timeout
CSCuq70337	N5K/6K: Bound vrfs lost after upgrade to 7.0
CSCup85771	Nexus 6000 resets SSH intermittently
CSCue56335	N7k - snmpd core dumps during vlanTrunkPortVlansXmitJoined mibwalk
CSCuo39797	fpoam: ping goes into endless loop when max sweep <= min sweep
CSCus15505	clk_mgr process crash due to a memory leak
CSCub90520	CLI threads not exited if 'sh tech <routing_protocol>' is interrupted
CSCug29190	'ethpc' hap reset tied to SFP diagnostics
CSCur12427	5672UP unable to read sensors temperature
CSCun69369	Bigsur FAULTY slot 0 asic 0, bigsur_stm_dma_monitor_timer_hdlr error
CSCum13332	N5K: Changes to input voltage logging
CSCun91863	N5K: NOHMS-2-NOHMS_DIAG_ERR_PS_FAIL with DC Power Supply
CSCus70491	N6004 bigsurusd hap reset
CSCur76751	N6K/5K: Need knob to configure mgmt0 interface to operate at auto 10/100
CSCuo23668	N6K: errors "clk_flush: Couldn't Clear Bus" and console unresponsive
CSCus39651	N6k:CRC errors on random 40gig port after reload
CSCuc26047	Nexus 5000 reset due to Kernel Panic
CSCuj84269	Nexus 5000 switch reloaded due to gatosusd hap reset
CSCur11599	Nexus 5k/6k - Memory leak in pfstat process causing hap reset
CSCuh44248	Nexus 6000: Need to map "reload power-cycle" option to regular reload
CSCuo44979	Nexus 6004: Bios corrupt during reload/power cycle
CSCur02975	Nexus56xx/6k switches may take ~25 sec to respond to some show CLI's
CSCus16410	Sometime N6K export as a TCP Src/Dst port is zero.
CSCuq66628	VDC-MGR crash on N5k
CSCur82368	port-profile hap reset with long trunk allowed vlan list
CSCuq37768	'qd' Segfault at qd_bigsur_print_voq_asic_stats
CSCup64606	FCOE Slow Performance with Nexus N6004.
CSCuq86032	N5k - Same "match cos" value shared between class-fcoe and another class
CSCus97571	Rollback Broken in PPM, Auto config breaks while VRF in Delete holddown
CSCuq68431	EIGRP crash in eigrp_cmi_enqueue
CSCur26119	EIGRP prefixes missing after interface flap
CSCuq39448	Nexus 5K EIGRP crash when distribute list is configured under interface
CSCuq86047	Nexus5k ipForward Object not giving correct results for snmpwalk
CSCus65288	ERSPAN outer ip header length exceeds the maximum limit for a packet

Table 54 Resolved Caveats in Cisco NX-OS Release 7.0(6)N1(1)

Identifier	Description
CSCup99146	Iplus:ERSPAN Type2 & Type3 packet have incorrect outer IP length .
CSCur54642	N5K with ERSPAN enabled may face a slow leak in 'monitor' process
CSCus64400	%STP-2-VLAN_PORT_LIMIT_EXCEEDED is output even under verified scalabilty
CSCuo74024	STP BPDU received on vPC secondary not tunneled to vPC primary
CSCum40651	Tacacs+ per CLI authorization failure upon entering CLI > 64 char
CSCuj90930	Nexus 55xx: crash in ipfib when FIB is exhausted.
CSCur25570	Defined Fabricpath VLANs do not appear in configuration
CSCut09166	fwm hap reset on vlan delete
CSCur39582	vlan_mgr unresponsive on creating or deleting VLAN
CSCup74458	few seconds of packet loss on vpc secondary link bringup
CSCuq42482	N5K dual homed vpc fex, hif speed change not always picked up N5K's
CSCus77310	vpc hap reset vpc process crashed.
CSCum82485	Nexus 5500/6000: L2FM messages seen.
CSCuq39353	IMAINT 133: ascii-cfg hap reset
CSCuq64886	fabricpath isis bfd requires L3 bfd interval command to adjust timers
CSCuq89851	Nexus5672 DFA reboot when mandatory fields in the DCNM are not populated
CSCur16747	satctrl cored after write-erase& applying config with 'FEX-QoS-offload'
CSCur47731	5596UP / Crash, Reload after setting a FC Port shut/no shut
CSCus56036	BGP tracebacks or FD read errors along with session flaps
CSCus66218	Deleted vlans are still showing in show fabricpath output
CSCus78102	N6K crashed due to "kernel panic" @ stale pointer
CSCut06901	Traffic blackholing for around 60 secs after new RPF intf comes up
CSCuq56923	Logging level virtual-service reverts to default after an NX-OS upgrade.
CSCus20646	N5K crash on CDP process
CSCus29400	FCPC cores and triggers hap reset while allocating response payload
CSCuq18021	SNMPset to community strings with special characters cause hap reset
CSCut12023	Port channel service crashes after many 'show run' commands
CSCut17968	res mgr crash in n6k/n5k when "show vdc resource" command is given
CSCut19714	N2H traffic can drop on a HIF port-channel when another is down
CSCut03537	QinQ - Double-tag for native/untagged vlan traffic

Resolved Caveats in Cisco NX-OS Release 7.0(5)N1(1a)

Table 55 Resolved Caveats in Cisco NX-OS Release 7.0(5)N1(1a)

Caveat ID	Resolved Caveat Headline
CSCur12427	5672UP unable to read sensors temperature.

Resolved Caveats in Cisco NX-OS Release 7.0(5)N1(1)

Table 56 Resolved Caveats in Cisco NX-OS Release 7.0(5)N1(1)

Caveat ID	Resolved Caveat Headline
CSCui43663	Python asking for password after write erase reload.
CSCuo17751	Frame drop on egress.
CSCup82567	Config stuck after interface down during vPC bringup.
CSCuq98902	First port on N2K-B22HP-P fails on upgrade to 7.0(3)N1(1).
CSCur01134	Powered down due to fan policy trigger after ISSU.
CSCur09549	Configuration sync rollback failure for failed port channel member.

Resolved Caveats in Cisco NX-OS Release 7.0(4)N1(1)

Table 57 Resolved Caveats in Cisco NX-OS Release 7.0(4)N1(1)

Caveat ID	Resolved Caveat Headline
CSCty86291	MTS buffer exhaustion with sequential add of large VLANs.
CSCuo68435	Programming of updated FabricPath FWD entries to hardware delayed.
CSCup45110	Scale setup error message when clear stats.
CSCup46036	Fan OIR issues.
CSCup87395	Configuration sync failures with no cpd enable and pre-provisioning.
CSCuq27517	QD process crash.
CSCuq27905	The **clear copp stats** command also clears qos statistics.
CSCuq36827	Routing unknown u/c and link local b/c packets.
CSCuq54187	vPC auto-recovery reverts to default delay value after switch reload.
CSCuq61734	ACLMGR crash when show startup-configuration command is entered after access-list deletion.
CSCuq62914	Configuration sync failed for storm-control under FEX interface.
CSCuq70941	The **inherit** command on Nexus is not working with TACACS authorization.

Resolved Caveats in Cisco NX-OS Release 7.0(3)N1(1)

Table 58 Resolved Caveats in Cisco NX-OS Release 7.0(3)N1(1)

Caveat ID	Resolved Caveat Headline
CSCul81869	10Mb FEX:ISSU downgrade from 7.0(1)N1(1) to 6.0(2)N2(1) should be incompatible with Speed 10.
CSCun57615	FP topo includes nonFP VLAN if newly created after non-destructive ISSU from 6.0.2.N2.3.
CSCun74416	Shut/no shut of VE, VF is required after nondisruptive ISSU to release 7.0(1)N1(1).
CSCup70305	Queuing policy on hif not working for l2 mcast traffic.

Resolved Caveats in Cisco NX-OS Release 7.0(2)N1(1)

Table 59 Resolved Caveats in Cisco NX-OS Release 7.0(2)N1(1)

Caveat ID	Resolved Caveat Headline
CSCuo39454	Nexus 56128 QSFP high latency.

Resolved Caveats in Cisco NX-OS Release 7.0(1)N1(1)

Table 60 Resolved Caveats in Cisco NX-OS Release 7.0(1)N1(1)

Record Number	Resolved Caveat Headline
CSCtu31087	BGP update generation blocked because of large number of idle/active peers.
CSCud48710	Layer 2 multicast traffic can be lost up to 1 to 2 minutes upon unshut of the fabric PO in an AA topology. This happens only under the following conditions: • AA topology. • The group is downgraded to V2 of a V3 receiver. • The FEX fabric port is shut on one side. • When the fabric port is unshut, Layer 2 multicast traffic loss may be seen until the next join comes in.
CSCud72942	When all the FEXs are reloaded at the same time, Layer 2 multicast traffic may not recover on one of the HIF ports.
CSCuh36961	A QoS policy with qosCSCun77758-group 1 cannot be applied on a non-FCoE class.

MIB Support

The Cisco Management Information Base (MIB) list includes Cisco proprietary MIBs and many other Internet Engineering Task Force (IETF) standard MIBs. These standard MIBs are defined in Requests for Comments (RFCs). To find specific MIB information, you must examine the Cisco proprietary MIB structure and related IETF-standard MIBs supported by the Cisco Nexus 5600 Series switch.

The MIB Support List is available at the following FTP site:

ftp://ftp.cisco.com/pub/mibs/supportlists/nexus5600/Nexus5600MIBSupportList.html

Related Documentation

Documentation for the Cisco Nexus 5600 Series Switch is available at the following URL:

http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/tsd-products-support-series-home.html

The documentation set is divided into the following categories:

Release Notes

The release notes are available at the following URL:

http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-release-notes-list.html

Installation and Upgrade Guides

The installation and upgrade guides are available at the following URL:

http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-guides-list.html

Command References

The command references are available at the following URL:

http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-command-reference-list.html

Configuration Guides

The configuration guides are available at the following URL:

http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-and-configuration-guides-list.html

Error and System Messages

The system message reference guide is available at the following URL:

http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-system-message-guides-list.html

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus5k-docfeedback@cisco.com. We appreciate your feedback.

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.