Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes, Cisco NX-OS Release 5.2

Release Date: December 7, 2012
Date Last Modified: January 21, 2019
Current Release: Cisco NX-OS Release 5.2(1)N1(9b)

This document describes the features, caveats, and limitations for the Cisco Nexus 5000 Series switches and the Cisco Nexus 2000 Series Fabric Extenders in the following software releases:

- Cisco NX-OS Release 5.2(1)N1(9b)
- Cisco NX-OS Release 5.2(1)N1(9a)
- Cisco NX-OS Release 5.2(1)N1(9)
- Cisco NX-OS Release 5.2(1)N1(8b)
- Cisco NX-OS Release 5.2(1)N1(8a)
- Cisco NX-OS Release 5.2(1)N1(8)
- Cisco NX-OS Release 5.2(1)N1(7)
- Cisco NX-OS Release 5.2(1)N1(6)
- Cisco NX-OS Release 5.2(1)N1(5)
- Cisco NX-OS Release 5.2(1)N1(4)
- Cisco NX-OS Release 5.2(1)N1(3)
- Cisco NX-OS Release 5.2(1)N1(2a)
- Cisco NX-OS Release 5.2(1)N1(2)
- Cisco NX-OS Release 5.2(1)N1(1b)
- Cisco NX-OS Release 5.2(1)N1(1a)
- Cisco NX-OS Release 5.2(1)N1(1)

Use this document in combination with documents listed in the “Related Documentation” section on page 47.

Cisco Systems, Inc.
www.cisco.com

Note Release notes are sometimes updated with new information about restrictions and caveats. See the following website for the most recent version of the Cisco Nexus 5000 Series and Cisco Nexus 2000 Series release notes: http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/release/notes/Nexus_5000_Release_Notes.html

Note Table 1 shows the online change history for this document.

Table 1 Online History Change

Date	Description
July 13, 2012	Created NX-OS Release 5.2(1)N1(1) release notes.
July 16, 2012	Updated Hardware Supported section.
July 22, 2012	Added Cisco Nexus B22F FEX.
July 31, 2012	Updated Supported Upgrade and Downgrade Paths.
August 24, 2012	Created NX-OS Release 5.2(1)N1(1a) release notes.
September 4, 2012	Updated Hardware Supported.
September 6, 2012	Added three routing protocols to IPv6 Support for Additional Features.
September 25, 2012	Created NX-OS Release 5.2(1)N1(1b) release notes. CSCuc37925
September 27, 2012	Added CSCuc37925 to Open Caveats.
October 5, 2012	Added CSCuc37057 to Open Caveats.
October 19, 2012	Created NX-OS Release 5.2(1)N1(2) release notes.
October 22, 2012	Added CSCuc80263 to Open Caveats.
October 23, 2012	Created NX-OS Release 5.2(1)N1(2a) release notes.
November 6, 2012	Updated the SFP+ Optical information in Table 2.
December 7, 2012	Created NX-OS Release 5.2(1)N1(3) release notes.
December 17, 2012	Added power supply support.
January 24, 2013	Revised the limitation about Cisco Nexus 5548UP and Cisco Nexus 5598UP switches with Fibre Channel connections to HP Virtual Connect modules in the "Limitations" section.
March 22, 2013	Created NX-OS Release 5.2(1)N1(4) release notes.
April 3, 2013	Added CSCud72948 to Resolved Caveats in Cisco NX-OS Release 5.2(1)N1(4).
July 1, 2013	Created NX-OS Release 5.2(1)N1(5) release notes.
July 2, 2013	Added more detailed information and table related to DOM polling for NX-OS Releases 5.2(1)N1(5) and earlier releases.
October 14, 2013	Created NX-OS Release 5.2(1)N1(6) release notes.

Table 1 Online History Change

Date	Description
October 18, 2013	Updated New Software Features text.
November 12, 2013	Added CSCul27686 to Open Caveats.
February 7, 2014	Created NX-OS Release 5.2(1)N1(7) release notes.
June 27, 2014	Created NX-OS Release 5.2(1)N1(8) release notes.
July 15, 2014	Added CSCup74438 to Open Caveats. Moved CSCuj46069 from Resolved to Open.
August 8, 2014	Created NX-OS Release 5.2(1)N1(8a) release notes.
October 24, 2014	Created NX-OS Release 5.2(1)N1(9) release notes.
October 30, 2014	Changed the release number from 5.2(1)N1(9) to 5.2(1)N1(8b) in the whole document.
April 20, 2015	Created NX-OS Release 5.2(1)N1(9) release notes.
March 18, 2016	Created NX-OS Release 5.2(1)N1(9a) release notes.
February 12, 2017	Created NX-OS Release 5.2(1)N1(9b) release notes.
January 21, 2019	Updated the "Limitations" section to include the limitation while upgrading from Cisco NX-OS Release 5.1 to Cisco NX-OS Release 5.2 due to fcoe-npv feature.

Contents

This document includes the following sections:

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 MDS 9000 SAN-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 5000 Series switch and the Cisco Nexus 2000 Series Fabric Extender (FEX) to improve the performance, scalability, and management of the product line. Cisco NX-OS Release 5.2 also supports all hardware and software supported in Cisco NX-OS Release 5.1, Cisco NX-OS Release 5.0, and Cisco NX-OS Software Release 4.2.

Cisco Nexus 5000 Series Switches

The Cisco Nexus 5000 Series switches 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 switches for data center applications. The Cisco Nexus 5000 Series includes the Cisco Nexus 5500 Platform and the Cisco Nexus 5000 Platform.

For information about the Cisco Nexus 5000 Series, see the *Cisco Nexus 5000 Series and Cisco Nexus 5500 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 5000 Series switches to provide high-density and low-cost connectivity for server aggregation. Scaling across 1-Gigabit Ethernet, 10-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 5000 Series switch, 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 5000 Series 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 5000 Series Layer 2 Switching Configuration Guide*.

System Requirements

This section includes the following topics:

Hardware Supported

The Cisco NX-OS software supports the Cisco Nexus 5000 Series switch. You can find detailed information about supported hardware in the *Cisco Nexus 5000 Series Hardware Installation Guide*.

Table 2 shows the hardware supported by Cisco NX-OS Release 5.2(x) software.

Table 2 Hardware Supported by Cisco NX-OS Release 5.2(x) Software

Cisco NX-OS Release Support								
Hardware	**Part Number**	**5.2(1)N1(9b) 5.2(1)N1(9a) 5.2(1)N1(9) 5.2(1)N1(8b) 5.2(1)N1(8a) 5.2(1)N1(8) 5.2(1)N1(7) 5.2(1)N1(6) 5.2(1)N1(5) 5.2(1)N1(4) 5.2(1)N1(3) 5.2(1)N1(2a) 5.2(1)N1(2) 5.2(1)N1(1b) 5.2(1)N1(1a) 5.2(1)N1(1)**	**5.1(3)N2(1c) 5.1(3)N2(1b) 5.1(3)N2(1a) 5.1(3)N2(1)**	**5.1(3)N1(1b) 5.1(3)N1(1a) 5.1(3)N1(1)**	**5.0(3)N2(2a) 5.0(3)N2(2) 5.0(3)N2(1)**	**5.0(3) N1(1)**	**5.0(2) N2(1)**	**5.0(2) N1(1)**
Cisco Nexus 5000 Series								
Cisco Nexus 5596T switch[1]	N5K-C5596T-FA	Yes	No	No	No	No	No	No
Cisco Nexus 5596UP switch	N5K-C5596UP-FA	Yes	Yes	Yes	Yes	Yes	No	No

Table 2 Hardware Supported by Cisco NX-OS Release 5.2(x) Software (continued)

Cisco NX-OS Release Support								
Hardware	**Part Number**	**5.2(1)N1(9b) 5.2(1)N1(9a) 5.2(1)N1(9) 5.2(1)N1(8b) 5.2(1)N1(8a) 5.2(1)N1(8) 5.2(1)N1(7) 5.2(1)N1(6) 5.2(1)N1(5) 5.2(1)N1(4) 5.2(1)N1(3) 5.2(1)N1(2a) 5.2(1)N1(2) 5.2(1)N1(1b) 5.2(1)N1(1a) 5.2(1)N1(1)**	**5.1(3)N2(1c) 5.1(3)N2(1b) 5.1(3)N2(1a) 5.1(3)N2(1)**	**5.1(3)N1(1b) 5.1(3)N1(1a) 5.1(3)N1(1)**	**5.0(3)N2(2a) 5.0(3)N2(2) 5.0(3)N2(1)**	**5.0(3) N1(1)**	**5.0(2) N2(1)**	**5.0(2) N1(1)**
Cisco Nexus 5548UP switch	N5K-C5548UP-FA	Yes	Yes	Yes	Yes	Yes	No	No
Cisco Nexus 5548P switch	N5K-C5548P-FA	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco Nexus 5020P switch	N5K-C5020P-BF	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco Nexus 5010P switch	N5K-C5010P-BF	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco Nexus 2000 Series								
Cisco Nexus B22DELL P FEX[2]	N2K-B22DELL-P	Yes	No	No	No	No	No	No
Cisco Nexus 2232TM-E FEX[3]	N2K-C2232TM-E-10GE	Yes	No	No	No	No	No	No
Cisco Nexus B22F FEX	N2K-B22FTS-P	Yes	No	No	No	No	No	No
Cisco Nexus B22HP FEX[4]	N2K-B22HP-P	Yes	Yes	Yes	Yes			
Cisco Nexus 2232TM FEX	N2K-C2232TM-10GE	Yes	Yes	Yes	Yes	No	No	No
Cisco Nexus 2232PP FEX	N2K-C2232PP-10GE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco Nexus 2248TP E FEX	N2K-C2248TP-E-1GE	Yes	Yes	Yes	No	No	No	No
Cisco Nexus 2248TP FEX	N2K-C2248TP-1GE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco Nexus 2224TP FEX	N2K-C2224TP-1GE	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 2 Hardware Supported by Cisco NX-OS Release 5.2(x) Software (continued)

Cisco NX-OS Release Support								
Hardware	**Part Number**	**5.2(1)N1(9b) 5.2(1)N1(9a) 5.2(1)N1(9) 5.2(1)N1(8b) 5.2(1)N1(8a) 5.2(1)N1(8) 5.2(1)N1(7) 5.2(1)N1(6) 5.2(1)N1(5) 5.2(1)N1(4) 5.2(1)N1(3) 5.2(1)N1(2a) 5.2(1)N1(2) 5.2(1)N1(1b) 5.2(1)N1(1a) 5.2(1)N1(1)**	**5.1(3)N2(1c) 5.1(3)N2(1b) 5.1(3)N2(1a) 5.1(3)N2(1)**	**5.1(3)N1(1b) 5.1(3)N1(1a) 5.1(3)N1(1)**	**5.0(3)N2(2a) 5.0(3)N2(2) 5.0(3)N2(1)**	**5.0(3) N1(1)**	**5.0(2) N2(1)**	**5.0(2) N1(1)**
Cisco Nexus 2148T FEX	N2K-C2148T-1GE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Expansion Modules								
12-port 10GBASE-T GEM[5]	N55-M12T	Yes	No	No	No	No	No	No
16-port Universal GEM	N55-M16UP(=)	Yes	Yes	Yes	Yes	Yes	No	No
N5596 Layer 3 GEM	N55-M160L3(=)	Yes	Yes	Yes	Yes	Yes	No	No
N5548 Layer 3 daughter card	N55-D160L3(=)	Yes	Yes	Yes	Yes	Yes	No	No
Layer 3 GEM	N55-M160L3-V2	Yes	Yes	Yes				
Version 2 Layer 3 daughter card	N55-D160L3-V2	Yes	Yes	Yes				
16-port SFP+ Ethernet	N55-M16P(=)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
8 10-Gigabit Ethernet and 8 10-Gigabit FCoE ports	N55-M8P8FP(=)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Transceivers								
Fabric Extender Transceivers								
10-Gigabit Ethernet SFP (for Cisco Nexus 2000 Series to Cisco Nexus 5000 Series connectivity)	FET-10G(=)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SFP+ Optical								
1000BASE-ZX SFP transceiver module for SMF	GLC-ZX-SM(=)	Yes						

Table 2 Hardware Supported by Cisco NX-OS Release 5.2(x) Software (continued)

Cisco NX-OS Release Support								
Hardware	**Part Number**	**5.2(1)N1(9b) 5.2(1)N1(9a) 5.2(1)N1(9) 5.2(1)N1(8b) 5.2(1)N1(8a) 5.2(1)N1(8) 5.2(1)N1(7) 5.2(1)N1(6) 5.2(1)N1(5) 5.2(1)N1(4) 5.2(1)N1(3) 5.2(1)N1(2a) 5.2(1)N1(2) 5.2(1)N1(1b) 5.2(1)N1(1a) 5.2(1)N1(1)**	**5.1(3)N2(1c) 5.1(3)N2(1b) 5.1(3)N2(1a) 5.1(3)N2(1)**	**5.1(3)N1(1b) 5.1(3)N1(1a) 5.1(3)N1(1)**	**5.0(3)N2(2a) 5.0(3)N2(2) 5.0(3)N2(1)**	**5.0(3) N1(1)**	**5.0(2) N2(1)**	**5.0(2) N1(1)**
10-Gigabit Ethernet—short range SFP+ module	SFP-10G-SR(=)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
10-Gigabit Ethernet—long range SFP+ module	SFP-10G-LR(=)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
10-Gigabit Ethernet—extended range SFP+ module	SFP-10G-ER(=)	Yes	Yes	Yes				
1000BASE-T standard	GLC-T(=)	Yes	Yes	Yes	Yes	Yes		
Gigabit Ethernet SFP, LC connector SX transceiver (MMF)	GLC-SX-MM	Yes	Yes	Yes	Yes	Yes		
Gigabit Ethernet SFP, LC connector SX transceiver (MMF), extended temperature range and DOM	GLC-SX-MMD	Yes	Yes	Yes	Yes	Yes		
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF)	GLC-LH-SM	Yes	Yes	Yes	Yes	Yes		
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF), extended temperature range and DOM	GLC-LH-SMD	Yes	Yes	Yes	Yes	Yes		
SFP+ Copper								
10GBASE-CU SFP+ Cable (1 meter)	SFP-H10GB-CU1M(=)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 2 Hardware Supported by Cisco NX-OS Release 5.2(x) Software (continued)

Cisco NX-OS Release Support								
Hardware	**Part Number**	**5.2(1)N1(9b) 5.2(1)N1(9a) 5.2(1)N1(9) 5.2(1)N1(8b) 5.2(1)N1(8a) 5.2(1)N1(8) 5.2(1)N1(7) 5.2(1)N1(6) 5.2(1)N1(5) 5.2(1)N1(4) 5.2(1)N1(3) 5.2(1)N1(2a) 5.2(1)N1(2) 5.2(1)N1(1b) 5.2(1)N1(1a) 5.2(1)N1(1)**	**5.1(3)N2(1c) 5.1(3)N2(1b) 5.1(3)N2(1a) 5.1(3)N2(1)**	**5.1(3)N1(1b) 5.1(3)N1(1a) 5.1(3)N1(1)**	**5.0(3)N2(2a) 5.0(3)N2(2) 5.0(3)N2(1)**	**5.0(3) N1(1)**	**5.0(2) N2(1)**	**5.0(2) N1(1)**
10GBASE-CU SFP+ Cable (3 meters)	SFP-H10GB-CU3M(=)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
10GBASE-CU SFP+ Cable (5 meters)	SFP-H10GB-CU5M(=)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
10GBASE-CU SFP+ Cable (7 meters)	SFP-H10GB-ACU7M(=)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
10GBASE-CU SFP+ Cable (10 meters)	SFP-H10GB-ACU10M(=)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Fibre Channel								
8-Gbps Fibre Channel—short wavelength	DS-SFP-FC8G-SW(=)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
8-Gbps Fibre Channel—long wavelength	DS-SFP-FC8G-LW(=)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4-Gbps Fibre Channel—short wavelength	4DS-SFP-FC4G-SW(=)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4-Gbps Fibre Channel—long wavelength	4DS-SFP-FC4G-LW(=)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4-Gbps CWDM SFP								
1470 nm CWDM 1/2/4-Gbps Fibre Channel, Gray	DS-CWDM4G1470(=)	Yes	Yes					
1490 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Violet	DS-CWDM4G1490(=)	Yes	Yes					

Table 2 Hardware Supported by Cisco NX-OS Release 5.2(x) Software (continued)

Cisco NX-OS Release Support								
Hardware	**Part Number**	**5.2(1)N1(9b) 5.2(1)N1(9a) 5.2(1)N1(9) 5.2(1)N1(8b) 5.2(1)N1(8a) 5.2(1)N1(8) 5.2(1)N1(7) 5.2(1)N1(6) 5.2(1)N1(5) 5.2(1)N1(4) 5.2(1)N1(3) 5.2(1)N1(2a) 5.2(1)N1(2) 5.2(1)N1(1b) 5.2(1)N1(1a) 5.2(1)N1(1)**	**5.1(3)N2(1c) 5.1(3)N2(1b) 5.1(3)N2(1a) 5.1(3)N2(1)**	**5.1(3)N1(1b) 5.1(3)N1(1a) 5.1(3)N1(1)**	**5.0(3)N2(2a) 5.0(3)N2(2) 5.0(3)N2(1)**	**5.0(3) N1(1)**	**5.0(2) N2(1)**	**5.0(2) N1(1)**
1510 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Blue	DS-CWDM4G1510(=)	Yes	Yes					
1530 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Green	DS-CWDM4G1530(=)	Yes	Yes					
1550 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Yellow	DS-CWDM4G1550(=)	Yes	Yes					
1570 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Orange	DS-CWDM4G1570(=)	Yes	Yes					
1590 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Red	DS-CWDM4G1590(=)	Yes	Yes					
1610 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Brown	DS-CWDM4G1610(=)	Yes	Yes					
Extended Temperature Range								
1000BASE-T SFP, extended temperature range	SFP-GE-T(=)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Gigabit Ethernet SFP, LC connector SX transceiver (MMF), extended temperature range and digital optical monitoring (DOM)	SFP-GE-S(=)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 2 Hardware Supported by Cisco NX-OS Release 5.2(x) Software (continued)

Cisco NX-OS Release Support								
Hardware	**Part Number**	**5.2(1)N1(9b) 5.2(1)N1(9a) 5.2(1)N1(9) 5.2(1)N1(8b) 5.2(1)N1(8a) 5.2(1)N1(8) 5.2(1)N1(7) 5.2(1)N1(6) 5.2(1)N1(5) 5.2(1)N1(4) 5.2(1)N1(3) 5.2(1)N1(2a) 5.2(1)N1(2) 5.2(1)N1(1b) 5.2(1)N1(1a) 5.2(1)N1(1)**	**5.1(3)N2(1c) 5.1(3)N2(1b) 5.1(3)N2(1a) 5.1(3)N2(1)**	**5.1(3)N1(1b) 5.1(3)N1(1a) 5.1(3)N1(1)**	**5.0(3)N2(2a) 5.0(3)N2(2) 5.0(3)N2(1)**	**5.0(3) N1(1)**	**5.0(2) N2(1)**	**5.0(2) N1(1)**
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF), extended temperature range and DOM	SFP-GE-L(=)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Converged Network Adapters								
Generation-1 (Pre-FIP) CNAs[6]		Yes	Yes	Yes	Yes	Yes	Yes	Yes

1. The Cisco Nexus 5596T and the 12-port 10-GBase-T GEM are supported starting with Cisco NX-OS Release 5.2(1)N1(1b).
2. The Cisco Nexus B22DELL P FEX is supported starting with Cisco NX-OS Release 5.2(1)N1(3).
3. The Cisco Nexus 2232TM-E FEX is supported starting with Cisco NX-OS Release 5.2(1)N1(1a).
4. The Cisco Nexus B22HP FEX is supported starting with Cisco NX-OS Release 5.0(3)N2(2).
5. The 12 port 10-GBASE-T GEM is only supported on the Cisco Nexus 5596T starting with Cisco NX-OS Release 5.2(1)N1(1b).
6. Generation-1 (Pre-FIP) CNAs are supported on the Nexus 5000 Platform switches; however, they are not supported on the Nexus 5500 Series.

Online Insertion and Removal Support

Table 3 shows the hardware and Cisco NX-OS Release 5.x software that supports online insertion and removal (OIR).

Table 3 Online Insertion and Removable Support by Cisco NX-OS Release 5.x Software

Hardware	Part Number	Cisco NX-OS Release Support						
		5.2(1)N1(9b) 5.2(1)N1(9a) 5.2(1)N1(9) 5.2(1)N1(8b) 5.2(1)N1(8a) 5.2(1)N1(8) 5.2(1)N1(7) 5.2(1)N1(6) 5.2(1)N1(5) 5.2(1)N1(4) 5.2(1)N1(3) 5.2(1)N1(2a) 5.2(1)N1(2), 5.2(1)N1(1b) 5.2(1)N1(1a) 5.2(1)N1(1)	5.2(1)N2(1c) 5.2(1)N2(1b) 5.1(3)N2(1a) 5.1(3)N2(1)	5.1(3)N1(1a) 5.1(3)N1(1)	5.0(3)N2(2a) 5.0(3)N2(2) 5.0(3)N2(1)	5.0(3) N1(1)	5.0(2) N2(1)	5.0(2)N1 (1) and earlier
Cisco Nexus 5000 Series								
Cisco Nexus 5596T switch	N5K-C5596T-FA	Yes	No	No	No	No	No	No
Cisco Nexus 5596UP switch	N5K-C5596UP-FA	Yes	Yes	Yes	Yes	No	No	No
Cisco Nexus 5548UP switch	N5K-C5548UP-FA	Yes	Yes	Yes	Yes	No	No	No
Cisco Nexus 5548P switch	N5K-C5548P-FA	Yes	Yes	Yes	Yes	Yes	X	No
Expansion Modules								
12-port CU GEM	N55-M12T	Yes	No	No	No	No	No	No
16-port Universal GEM	N55-M16UP(=)	Yes	Yes	Yes	Yes	Yes	No	No
Layer 3 GEM[1]	N55-M160L3-V2[1]	No	No	No	No	No	No	No
Version 2 Layer 3 daughter card[1]	N55-D160L3-V2[1]	No	No	No	No	No	No	No
16-port SFP+ Ethernet	N55-M16P(=)	Yes	Yes	Yes	Yes	Yes	No	No
8-port SFP+ Ethernet ports and 8-port SFP+ Fibre Channel ports	N55-M8P8FPL(=)	Yes	Yes	Yes	Yes	Yes	No	No
N5596 Layer 3 GEM[1]	N55-M160L3(=)[1]	No	No	No	No	No	No	No
N5548 Layer 3 daughter card[1]	N55-D160L3(=)[1]	No	No	No	No	No	No	No

1. Does not support online insertion and removal. You must power down the Cisco Nexus 5000 Series switch before removing or inserting a Layer 3 GEM or Version 2 Layer 3 daughter card expansion module.

New and Changed Software Features

This section describes the new software features introduced in Cisco NX-OS Release 5.2(1)N1(x). This section includes the following topics:

New Software Features in Cisco NX-OS Release 5.2(1)N1(9b)

Cisco NX-OS Release 5.2(1)N1(9b) is a maintenance release that includes bug fixes. This release does not include new software.

New Software Features in Cisco NX-OS Release 5.2(1)N1(9a)

Cisco NX-OS Release 5.2(1)N1(9a) is a maintenance release that includes bug fixes. This release does not include new software.

New Software Features in Cisco NX-OS Release 5.2(1)N1(9)

Cisco NX-OS Release 5.2(1)N1(9) does not include new software.

New Software Features in Cisco NX-OS Release 5.2(1)N1(8b)

Cisco NX-OS Release 5.2(1)N1(8b) does not include new software.

New Software Features in Cisco NX-OS Release 5.2(1)N1(8a)

Cisco NX-OS Release 5.2(1)N1(8a) does not include new software.

New Software Features in Cisco NX-OS Release 5.2(1)N1(8)

Cisco NX-OS Release 5.2(1)N1(8) does not include new software.

New Software Features in Cisco NX-OS Release 5.2(1)N1(7)

Cisco NX-OS Release 5.2(1)N1(7) does not include new software.

New Software Features in Cisco NX-OS Release 5.2(1)N1(6)

Cisco NX-OS Release 5.2(1)N1(6) is a maintenance release that includes bug fixes and introduces this new feature:

- You can now configure static DHCP bindings and port security features simultaneously on the same interface.

New Software Features in Cisco NX-OS Release 5.2(1)N1(5)

Cisco NX-OS Release 5.2(1)N1(5) is a maintenance release that includes bug fixes and introduces this new feature:

- CLI for controlling digital optical monitoring (DOM) on a Switchport. By default, DOM polling is disabled. The new CLI commands allow you to turn polling on and off and monitor status.

  Table 4 summarizes DOM polling availability for Cisco NX-OS Release 5.2(1)N1(5) and previous 5.2(1)N1(x) releases.

Table 4 DOM Polling Capability by Cisco NX-OS Release

DOM Polling Feature	Cisco NX-OS Release 5.2(1)N1(5)	Cisco NX-OS Release 5.2(1)N1(4)	Cisco NX-OS Release 5.2(1)N1(3) and Earlier
Switchport DOM Polling	Supported, disabled by default CLI available to enable/disable.	Supported Enabled by default	Not supported
HIF DOM Polling	Not supported Not configurable	Not supported	Not supported

New Software Features in Cisco NX-OS Release 5.2(1)N1(4)

Cisco NX-OS Release 5.2(1)N1(4) is a maintenance release that includes bug fixes and introduced this new feature:

- Switchport digital optical monitoring (DOM) is available and enabled by default.

New Software Features in Cisco NX-OS Release 5.2(1)N1(3)

Cisco NX-OS Release 5.2(1)N1(3) is a maintenance release that includes bug fixes and the following software feature:

- Support for Cisco Nexus B22 Fabric Extender for Dell (N2K-B22DELL-P).

New Software Features in Cisco NX-OS Release 5.2(1)N1(2a)

Cisco NX-OS Release 5.2(1)N1(2a) is a patch release that provides bug fixes. It does not include new software features.

New Software Features in Cisco NX-OS Release 5.2(1)N1(2)

Cisco NX-OS Release 5.2(1)N1(2) is a maintenance release that includes bug fixes and the following software feature:

- NIF Storm Control

NIF Storm Control

You can configure traffic storm control on a Fabric Extender (FEX) port. Storm control configured on a FEX port applies to the aggregate traffic coming in on all the ports on that FEX, however, the storm control configuration is not inherited down to the host interface (HIF) ports.

New Software Features in Cisco NX-OS Release 5.2(1)N1(1b)

Cisco NX-OS Release 5.2(1)N1(1b) is a patch release that provides bug fixes. It does not include new software features.

New Software Features in Cisco NX-OS Release 5.2(1)N1(1a)

Cisco NX-OS Release 5.2(1)N1(1a) is a patch release that provides bug fixes. It does not include new software features.

New Software Features in Cisco NX-OS Release 5.2(1)N1(1)

Cisco NX-OS Release 5.2(1)N1(1) includes bug fixes and the following software features and enhancements:

- Cisco Management Interface over SSH, page 16
- IPv6 Support for Additional Features, page 16
- PTP Support, page 17
- Open Shortest Path First (OSPFv3), page 17
- Configuration Synchronization Enhancements, page 17

Cisco Management Interface over SSH

Beginning with Cisco NX-OS Release 5.1(3)N2(1), you can configure the following devices using the XML management interface:

- Cisco Nexus 5548UP Switch
- Cisco Nexus 5596UP Switch
- Cisco Nexus 5548P Switch

The interface uses the XML-based Network Configuration Protocol (NETCONF) that allows you to manage devices and communicate over the interface with an XML management tool or a program. The Cisco NX-OS implementation of NETCONF requires you to use a Secure Shell (SSH) session for communication with the device.

NETCONF is implemented with an XML Schema (XSD) that allows you to enclose device configuration elements within a remote procedure call (RPC) message. From within an RPC message, you select one of the NETCONF operations that matches the type of command that you want the device to execute. You can configure the entire set of CLI commands on the device with NETCONF. To download the Cisco NX-OS XML Schema Definition, go to the following URL and select one of the supported devices: http://www.cisco.com/cisco/software/navigator.html.

For more information, see the *Cisco Nexus XML Interface User Guide*.

IPv6 Support for Additional Features

IPv6 support has been added for the following features:

- IPv6 unicast forwarding
- IPv6 addressing (including routed interfaces, subinterfaces, switch virtual interfaces (SVI), and port-channel interfaces)
- IPv6 support for Neighbor Discovery (ND) or Address Resolution Protocol (ARP)
- IPv6 support for Internet Control Message Protocol (ICMP)
- IPv6 support for router ACLs
- IPv6 support for Control Plane Policing (CoPP)
- IPv6 support for QoS packet classification and marking
- IPv6 support for SNMP

- STATICv6 routing protocol
- BGPv6 routing protocol
- EIGRPv6 routing protocol

PTP Support

With the Precision Time Protocol (PTP) feature, IEEE 1588 is supported. 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).

Open Shortest Path First (OSPFv3)

You can configure the following basic and advanced Open Shortest Path First version 3 (OSPFv3) features for IPv6 networks:

- OSPF3 instance
- OSPFv3 authentication
- Filter lists
- Virtual links
- Stub route
- Route redistribution

Configuration Synchronization Enhancements

Configuration synchronization improvements for deleting and restoring switch profile configuration were added to the **no switch-profile name** command.

Predefined SAN Admin User Role

The new SAN admin (san-admin) user role is a noneditable, predefined user role that provides separation between LAN and SAN administrative tasks. Users that have been assigned the SAN admin user role do not have read or write access for Ethernet features unless it is assigned to them through another user role.

Multicast Scaling

You can use the **hardware profile multicast max-limit** command to set the maximum number of entries in the multicast routing table. The range is from 0 to 8000. In Cisco NX-OS Release 5.2(1)N1(1) only a max-limit of 8000 is supported.

Note A max-limit value above 4096 for this command is valid only on the N55-M160L3-V2 module and N55-D160L3-V2 daughter card.

Dynamic System Reserved VLAN Range

You can change the range of the system-reserved VLANs to any other 80 contiguous VLAN range. Reserving a range frees the range of VLANs that were allocated for internal use by default, and all of those VLANs are available for user configuration except for VLAN 4094. These commands were added:

- **system vlan** {*start-vlan*} **reserve**
- **no system vlan** {*start-vlan*} **reserve**
- **show system vlan reserved**

Increased Host Route Support

For the Generation 2 Layer 3 module, Cisco NX-OS 5.2(1)N1(X) will:

- Increase IPv4 host routes to 16,000.
- Increase IPv6 host routes to 8,000.

IGMP Snoop Limits

You can use the **hardware multicast snooping group-limit** command to configure the number of groups learned through IGMP Snooping. The range is from 100 to 8000.

Virtual Port Channel Peer Switch

The Virtual Port Channel (vPC) peer switch feature addresses performance concerns around STP convergence. This feature allows a pair of Cisco Nexus 5000 Series devices to appear as a single STP root in the Layer 2 topology. This feature eliminates the need to pin the STP root to the vPC primary switch and improves vPC convergence if the vPC primary switch fails.

To avoid loops, the vPC peer link is excluded from the STP computation. In vPC peer switch mode, STP BPDUs are sent from both vPC peer devices to avoid issues related to STP BPDU timeout on the downstream switches, which can cause traffic disruption.

This feature can be used with the pure peer switch topology in which the devices all belong to the vPC.

Object Tracking Enhancements

The object tracking feature now includes vPC support.

Fabric Path Multiple Topologies

The Cisco Nexus 5000 Series switches support two topologies: the default or base topology (topology 0) and the local VLAN topology (topology 1).

ACL Logging over Management Interface

Access-control list (ACL) logging provides hardware support for ACL logging so that the CPU is not impacted by ACL logging. ACL logging is supported for entries on the mgmt0 interface.

Python Scripting APIs

Python Application Programming Interface (API) support is available on Cisco Nexus 5000 Series switches.

POAP with Python Scripts

Python scripting is fully integrated with Power-On Auto Provisioning (POAP).

New and Changed Hardware Features

This section describes the new hardware features introduced in Cisco NX-OS Release 5.2(1)N1(x). This section includes the following topics:

New Hardware Features in Cisco NX-OS Release 5.2(1)N1(9b)

Cisco NX-OS Release 5.2(1)N1(9b) does not include new hardware.

New Hardware Features in Cisco NX-OS Release 5.2(1)N1(9a)

Cisco NX-OS Release 5.2(1)N1(9a) does not include new hardware.

New Hardware Features in Cisco NX-OS Release 5.2(1)N1(9)

Cisco NX-OS Release 5.2(1)N1(9) does not include new hardware.

New Hardware Features in Cisco NX-OS Release 5.2(1)N1(8b)

Cisco NX-OS Release 5.2(1)N1(8b) does not include new hardware.

New Hardware Features in Cisco NX-OS Release 5.2(1)N1(8a)

Cisco NX-OS Release 5.2(1)N1(8a) does not include new hardware.

New Hardware Features in Cisco NX-OS Release 5.2(1)N1(8)

Cisco NX-OS Release 5.2(1)N1(8) does not include new hardware.

New Hardware Features in Cisco NX-OS Release 5.2(1)N1(7)

Cisco NX-OS Release 5.2(1)N1(7) does not include new hardware.

New Hardware Features in Cisco NX-OS Release 5.2(1)N1(6)

Cisco NX-OS Release 5.2(1)N1(6) does not include new hardware.

New Hardware Features in Cisco NX-OS Release 5.2(1)N1(5)

Cisco NX-OS Release 5.2(1)N1(5) does not include new hardware.

New Hardware Features in Cisco NX-OS Release 5.2(1)N1(4)

Cisco NX-OS Release 5.2(1)N1(4) now supports the following hardware:

- New power supplies for Cisco Nexus 5596T switches:
- Cisco Nexus 1100 Watt AC front-to-back power supply (PID: NXA-PAC-1100W)
- Cisco Nexus 1100 Watts AC back-to-front power supply (PID: NXA-PAC-1100W-B)
- Cisco Nexus 1100 Watt DC front-to-back power supply (PID: N55-PDC-1100W)

New Hardware Features in Cisco NX-OS Release 5.2(1)N1(3)

Cisco NX-OS Release 5.2(1)N1(3) supports the following new hardware:

- Cisco Nexus B22 Fabric Extender for Dell (N2K-B22DELL-P)
- New power supplies for Cisco Nexus 5596UP switches:
  - Cisco Nexus 1100 Watt DC front-to-back power supply (PID: N55-PDC-1100W)

New Hardware Features in Cisco NX-OS Release 5.2(1)N1(2a)

Cisco NX-OS Release 5.2(1)N1(2a) does not include new hardware.

New Hardware Features in Cisco NX-OS Release 5.2(1)N1(2)

Cisco NX-OS Release 5.2(1)N1(2) did not introduce new hardware.

New Hardware Features in Cisco NX-OS Release 5.2(1)N1(1b)

Cisco NX-OS Release 5.2(1)N1(1b) supports the following new hardware:

- Cisco Nexus 5596T (N5K-C5596T-FA)

New Hardware Features in Cisco NX-OS Release 5.2(1)N1(1a)

Cisco NX-OS Release 5.2(1)N1(1a) supports the following new hardware:

- Cisco Nexus 2232TM-E FEX (N2K-C2232TM-E-10GE)

New Hardware Features in Cisco NX-OS Release 5.2(1)N1(1)

Cisco NX-OS Release 5.2(1)N1(1) supports the following new hardware:

- 1000BASE-ZX SFP transceiver module for SMF (GLC-ZX-SM)
- Cisco Nexus B22 Fabric Extender for Fujitsu (N2K-B22FTS-P)

Upgrading or Downgrading to a New Release

This section describes the upgrade and downgrade paths that are supported for Cisco NX-OS Release 5.2(1)N1(1) on the Cisco Nexus 5000 Series switch.

This section includes the following topics:

Upgrade and Downgrade Guidelines

- If host interface (HIF) port channels or EvPCs are configured in the system and if the system was already upgraded to NX-OS Release 5.1(3)N1(1) or Release 5.1(3)N1(1a) from any release earlier than Release 5.1(3)N1(1), ensure that the system was reloaded at least once before you upgrade to Release 5.1(3)N2(1a) or Release 5.1(3)N2(1). If the switch was not previously reloaded, reload it and upgrade to Release 5.1(3)N2(1a) or Release 5.1(3)N2(1).
- When a Layer 3 license is installed, the Cisco Nexus 5500 Platform does not support an ISSU. Hot swapping a Layer 3 module, for example, the Layer 3 GEM (N55-M160L3-V2) or Version 2 Layer 3 daughter card (N55-D160L3-V2), is not supported. You must power down the Cisco Nexus 5000 Series switch before removing or inserting a Layer 3 expansion module.
- Doing an ISSU from any release prior to Cisco NX-OS Release 5.2(1)N1(1b) may fail. See CSCua34584 for more details.

Supported Upgrade and Downgrade Paths

Table 5 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 5.2(1)N1(9b). For more information, see the *Cisco Nexus 5000 Series NX-OS Software Upgrade and Downgrade Guide, Release 5.2(1)N1(9b)*.

For other 5.2 releases, see the *Cisco Nexus 5000 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 5 Cisco NX-OS Release 5.2(1)N1(9b) Supported Upgrade and Downgrade Paths

Current Cisco NX-OS Release	Upgrade to NX-OS Release 5.2(1)N1(9b)	Downgrade from NX-OS Release 5.2(1)N1(9b)
5.2(1)N1(9a)	Non-disruptive upgrade (ISSU)	Disruptive downgrade
5.2(1)N1(9)	Non-disruptive upgrade (ISSU)	Disruptive downgrade
5.2(1)N1(8b)	Non-disruptive upgrade (ISSU)	Disruptive downgrade
5.2(1)N1(8a)	Non-disruptive upgrade (ISSU)	Disruptive downgrade
5.2(1)N1(8)	Non-disruptive upgrade (ISSU)	Disruptive downgrade
5.2(1)N1(7)	Non-disruptive upgrade (ISSU)	Disruptive downgrade
5.2(1)N1(6)	Non-disruptive upgrade (ISSU)	Disruptive downgrade
5.2(1)N1(5)	Non-disruptive upgrade (ISSU)	Disruptive downgrade
5.2(1)N1(4)	Non-disruptive upgrade (ISSU)	Disruptive downgrade
5.2(1)N1(3)	Non-disruptive upgrade (ISSU)	Disruptive downgrade
5.2(1)N1(1b)—5.2(1)N1(2a)	No support for direct non-disruptive upgrade (ISSU)[1]	Disruptive downgrade
5.1(3)N2(1c) 5.1(3)N2(1b)[2] 5.1(3)N2(1a) 5.1(3)N2(1)	Non-disruptive upgrade (ISSU)	Disruptive downgrade
5.0(3)N2(2b) 5.0(3)N2(2a) 5.0(3)N2(2) 5.0(3)N2(1) 5.0(3)N1(1c)	Non-disruptive upgrade (ISSU)	Disruptive downgrade

1. To upgrade to Cisco NX-OS Release 5.2(1)N1(9b), from Cisco Nexus releases 5.2(1)N1(1b), 5.2(1)N1(2) and 5.2(1)N1(2a), you must first upgrade to Cisco NX-OS Release 5.2(1)N1(9) and then to 5.2(1)N1(9b).

2. Upgrading and downgrading are both disruptive between releases 5.1(3)N2(1b) and 5.2(1)N1(2) only.

Note Doing a disruptive upgrade between incompatible images will result in loss of certain configurations such as unified ports, Fibre Channel (FC), breakout, and FEX configurations. See CSCul22703 for details.

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 If you want to upgrade from a release not listed in the “Current Cisco NX-OS Release” column of Table 5 to 5.2(1)N1(9b), then you must first upgrade to a release that is listed in the “Current Cisco NX-OS Release" column and then to 5.2(1)N1(9b).

Note If you want to upgrade from a release, that is not listed in the “Current Cisco NX-OS Release” column of Table 5 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.

Limitations

This section describes the limitations for Cisco NX-OS Release 5.2x.

- If you are upgrading from an earlier release version to Cisco NX-OS Release 5.2.x and later, make sure you do not have **feature fcoe-npv** enabled with native fibre channel ports provisioned as uplinks in Cisco NX-OS Release 5.1.x; this will result in incompatible configuration and will cause the fcoe-npv uplinks to no longer function.
- When performing an ISSU from Cisco NX-OS Release 5.1(3)N1(1) or Cisco NX-OS Release 5.1(3)N2(1) to Cisco NX-OS Release 5.2(1)N1(1), a Forwarding Manager (FWM) core can occur which causes the system to reset. This situation occurs when network interface virtualization (NIV) is enabled. To work around this issue, use the **force** option in the **install** command to perform a disruptive upgrade. For details, see CSCty92117.
- The SAN admin user role (san-admin) is a new predefined user role in Cisco NX-OS Release 5.2(1)N1(1). If you have an existing user role with the name san-admin in Cisco NX-OS Release 5.1(3)N1(1) or Cisco NX-OS Release 5.1(3)N2(1), the new system defined role is removed when you upgrade. To resolve this issue, downgrade to the previous release, rename the user role, and perform the upgrade. For details, see CSCua21425.
- Bridge and STP traps are displayed in the downgrade incompatibility list when you downgrade from Cisco NX-OS Release 5.2(1)N1(1) to Cisco NX-OS Release 5.0(3)N1(1c). To resolve this issue, reset the STP/Bridge trap configuration to the default settings by entering the **no snmp-server enable traps bridge**, the **no snmp-server enable traps stpx** command, and then the **copy running-config startup-config** command. For details, see CSCua75907.
- 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. For details, see CSCts17033.

- If SPAN traffic is rate-limited by entering the switchport monitor rate-limit 1G command, then a maximum transmission unit (MTU) truncation size cannot be used to truncate SPAN packets. For details, see CSCua05799.
- SPAN incompatibility is displayed in the downgrade incompatibility list when you perform a disruptive downgrade from Cisco NX-OS Release 5.2(1)N1(8) to Cisco NX-OS Release 4.2(1)N2(1b). See Supported Upgrade and Downgrade Paths, page 23 for the recommended downgrade path. To work around this issue, remove and add the SPAN configuration. For details, see CSCtz39192.
- Disruptive upgrades from Cisco NX-OS Release 4.2(1)N2(1b) to Cisco NX-OS Release 5.2(1)N1(8) are not supported and result in FC source interfaces from the SPAN sessions being removed. See Supported Upgrade and Downgrade Paths, page 23 for the recommended upgrade path. For details, see CSCtz65395.
- When upgrading from Cisco NX-OS Release 4.2(1)N1(1) and earlier releases to any release, the policy description is lost. This problem does not occur when upgrading from Cisco NX-OS Release 4.2(1)N1(1) and later releases. After an upgrade, we recommend that you reconfigure the policy description. For details, see CSCth14225.
- Starting with Cisco NX-OS Release 4.2(1)N2(1), LACP fast timers are supported. If you downgrade to an earlier release that does not support this feature, entering the **install all** command displays the following warning:

  ```
  "Configuration not supported - Lacp fast rate is enabled",
    "Use \"lacp rate normal\" on those interfaces"
  ```

  Before downgrading to an earlier release, change the LACP rate to normal. If you ignore the warning and force the installation, then it is possible that the leftover LACP rate fast configuration would still be active with previous releases of software but the behavior would be unpredictable and link flap might occur. We recommend that you change the LACP rate setting to normal. For details, see CSCth93787.
- When an FC SPAN destination port is changed from SD to F mode and back to SD mode on a NPV switch, the port goes into an error-disabled state. Perform a shut/no-shut after the mode change recovers the port. This issue occurs only in NPV mode. For details, see CSCtf87701.
- 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 a 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.
- Given the implementation of a single CPU ISSU, the STP root on the PVST region with switches on an MST region is not supported. The PVST simulation on the boundary ports go into a PVST SIM inconsistent blocked state that breaks the STP active path. To work around this issue, move all STP roots to the MST region. However, the workaround causes a non-disruptive ISSU to fail because non-edge designated forwarding ports are not allowed for an ISSU. For additional information, see CSCtf51577. For information topologies that a non-disruptive upgrade is supported, see to the *Cisco Nexus 5000 Series NX-OS Upgrade and Downgrade Guide*.
- IGMP queries sent in CSCtf94558 are group-specific queries that are sent with the destination IP/MAC address as the group's address.

GS queries are sent for IP address: 224.1.14.1 to 224.1.14.100 [0100.5E01.0E01 to 0100.5E01.0E64]

These are not link-local addresses. By default, they are not flooded by the hardware into the VLAN. They are sent only to the ports that have joined this group.

This is expected behavior during an ISSU.

In another scenario, the IGMP global queries [dest IP 224.0.0.1] get flooded correctly in the VLAN.

Group-specific queries are not forwarded to ports other than the one that joined the group during ISSU. The reason to forward group-specific queries toward hosts is to avoid having them leave the group. However, if a port has not joined the group, then this is not an issue. If there is an interface that has joined the group, then the queries are expected to make it to the host. While the behavior is different when ISSU is not occurring, it is sufficient and works as expected and there is no impact to traffic. For details, see CSCtf94558.

- The meaning of an MTU configuration has changed in Cisco NX-OS Release 4.2(1)N1(1) and earlier releases. In releases earlier than Cisco NX-OS Release 4.2(1)N1(1), the configured MTU included the Ethernet payload and Ethernet headers. In Cisco NX-OS Release 4.2(1)N1(1), the configured MTU includes only the Ethernet payload and not the Ethernet headers. When upgrading or downgrading between Cisco NX-OS Release 4.2(1)N1(1) and earlier releases, Cisco NX-OS automatically converts the configuration to address this semantic change by adding or subtracting 38 to the MTU to address the Ethernet header size.

  In a vPC configuration, the MTU per class needs to be consistent on both switches in the vPC domain for the vPC peer link to come up. When upgrading/downgrading a working vPC setup between pre-4.2(1)N1(1) and 4.2(1)N1(1) releases, the MTU is adjusted to make sure that the MCT peer-link always comes up.

  However if you add a peer-link between two switches in a vPC domain that are identically configured (MTU in particular) with one switch running Cisco NX-OS Release 4.2(1)N1(1) and another switch running an earlier release, then the vPC peer link does not come up because the MTU is inconsistent between the two switches.

  This is not an issue when upgrading or downgrading peer switches in a vPC domain; this is only an issue when adding a peer link between two switches running Cisco NX-OS Release 4.2(1)N1(1) and earlier releases that were not previously in the same vPC domain.

  To resolve this issue, upgrade or downgrade one switch to match the version on the other switch and reconfigure the MTU to be consistent on both sides. For details, see CSCtg27538.

- The channel-group configuration is not applied to the Cisco Nexus 2000 Series downlink interface after downgrading to the Cisco NX-OS Release 4.1(3)N1(1) software. This issue occurs if the **speed 1000** command is present under the context of the port channel. To work around this issue, reconfigure the **channel-group** command after the system comes up and reapply the configuration from the saved configuration in the bootflash. For details, see CSCtc06276.
- 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 5000 Series switch, and all host-facing ports are connected and each host-facing interface has a large configuration (that supports the maximum permissible ACEs per interface).
- Egress scheduling is not supported across the drop/no-drop class. Each Fabric Extender host port does not support simultaneous drop and no drop traffic. Each Fabric Extender host port can support drop or no drop traffic.

- 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 remove an expansion module with Fibre Channel ports, and the cable is still attached, the following FCP_ERRFCP_PORT errors are displayed:

  ```
  2008 May 14 15:55:43 switch %KERN-3-SYSTEM_MSG: FCP_ERRFCP_PORT:
  gat_fcp_isr_ip_fcmac_sync_intr@424, jiffies = 0x7add9a:Unknown intr src_id 42 - kernel
  2008 May 14 15:55:43 switch %KERN-3-SYSTEM_MSG: FCP_ERRFCP_PORT:
  gat_fcp_isr_ip_fcmac_sync_intr@424, jiffies = 0x7add9a:Unknown intr src_id 41 - kernel
  ```

  These messages are informational only, and result in no loss of functionality.
- If you configure Multiple Spanning Tree (MST) on a Cisco Nexus 5000 Series switch, we do not recommend that you partition the network into a large number of regions.
- A downgrade from Cisco NX-OS Release 5.1(3)N1(1) to any 5.0(3)N1(x) image can cause the Cisco Nexus 5000 Series switch to fail. For details, see CSCty92945.
- If you upgrade a vPC peer switch from Cisco NX-OS Release 5.0(3)N2(1) to Cisco NX-OS Release 5.1(3)N2(1) or Cisco NX-OS Release 5.2(1)N1(1), and feature-set FabricPath is enabled on the upgraded switch, the vPC Peer-Link enters STP Bridge Assurance Inconsistency which affects all VLANs except VLAN 1 and affects traffic forwarding for vPC ports.

  To avoid this issue, upgrade the peer switch that is running Cisco NX-OS Release 5.0(3)N2(1) switch also to Cisco NX-OS Release 5.1(3)N2(1) or higher and then enable feature-set FabricPath on the switch or switches. If you accidentally enable feature-set FabricPath in Cisco NX-OS Release 5.1(3)N2(1) when the peer vPC switch is running Cisco NX-OS Release 5.0(3)N2(1), disable the feature-set FabricPath and the vPC will resume STP forwarding state for all VLANs.
- By design, vEth interfaces do not share the underlying behavior of a vPC port. As a result, a VLAN does not get 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 is up as it is an active VLAN on the secondary switch.
- RBACL policy enforcement is performed on VLANs on which CTS enforcement is not configured. This situation occurs when there is at least one VLAN in the switch where CTS is enforced. On a VLAN where CTS is not enforced, RBACL policy lookup occurs for ingress packets and the packet is denied or permitted according to the policies in the system. To work around this issue, make sure that all VLANs on which SGT tagged packets ingress enforce CTS.
- 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. This situation can occur whenever the MTU value that is configured in an ERSPAN or SPAN session is smaller than the SPAN packet, such as when the packet is truncated. The IP GRE packet is truncated to a value that differs by -2 to 10 bytes from the expected MTU.

- When you configure a Layer 3 interface as an ERSPAN source, and configure the ERSPAN termination on a Catalyst 6000 switch or a Cisco Nexus 7000 Series switch, you cannot terminate the Layer 3 interface ERSPAN source on the Cisco Nexus 7000 Series switch or the Catalyst 6000 switch. To work around this issue, configure VLAN 1 to 512 on the Cisco Nexus 7000 Series switch or the Catalyst 6000 switch.
- 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 5000 Series switch increments the interface counter based on the outer FabricPath header. As a result, multicast counters are incremented. In the case of a Cisco Nexus 7000 Series switch, Unicast counters are incremented as they are based on an inner Ethernet header. There is no workaround for this issue.
- If you configure a speed of 1 G on a base or GEM port and then check for compatibility with a Cisco NX-OS Release 5.0(2) image, no incompatibility is shown. However, because 1 G was not supported in the Cisco NX-OS Release 5.0(2), an incompatibility should be shown. To work around this issue, manually remove the 1 G configuration from the ports before downgrading to Cisco NX-OS Release 5.0(2) or an earlier release.
- In an emulated switch setup, 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 CE VLAN.
  - Add the management keyword to the corresponding SVI so that the failure of a Layer 3 module will not bring down the SVI interface.
  - 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.
- Fabricpath requires 802.1q tagging of inner Ethernet header of the packet. Native VLAN packets that are sent by a Cisco Nexus 7000 Series switch are not tagged. As a result, a Cisco Nexus 5000 Series switch drops packets due to packet parsing errors. To work around this issue, enable **vlan dot1q tag native** on the Cisco Nexus 7000 Series switch to force 802.1q tagging of native VLAN packets.
- SPAN traffic is rate-limited on Cisco Nexus 5500 Series switches platforms to prevent impact to production traffic:
  - SPAN is rate-limited to 5 Gbps per ASIC (every 8 ports share one ASIC).
  - SPAN is rate-limited to 0.71 Gbps per monitor source port when the RX traffic on the port exceeds 5 Gbps.

  For details, see CSCti94902.
- Cisco Nexus 5548UP and Cisco Nexus 5598UP switches with a Fibre Channel connection to HP Virtual Connect modules experience link destabilization and packet loss when the speed is set to 8 GB. To work around this issue for the HP VC FlexFabric 10-Gbps 24-port module, upgrade to VC-FF 3.70 or higher firmware. To work around this issue for the HP VC 8-Gbps 24-port Fibre Channel module, upgrade to VC-FC2 1.04 or higher. In the autonegotiation mode, the speed will drop to 4 Gb. The workaround is to manually set the speed to higher than 4 GB. For the HP VC 8-Gbps 20-port Fibre Channel module, leave the speed at 4 GB. For details, see CSCtx52991.

Limitations on the Cisco Nexus 5010 and Cisco Nexus 5020

The limitations on the Cisco Nexus 5010 switch and the Cisco Nexus 5020 switch are as follows:

- Traffic going out the Ethernet SPAN destination is always tagged. The SPAN destination can be in the access or trunk mode and frames on the SPAN source port can be tagged or untagged. Frames are always tagged internally as they travel through the system. Information about whether the frame was originally tagged or untagged, as it appeared in the SPAN source, is not preserved in the SPAN destination. The spanned traffic exiting the SPAN destination port always has the VLAN tag on it. The correct VLAN tag is applied on the frame as it goes out the SPAN destination. The only exception is if frames ingress on a SPAN source port on an invalid VLAN. In this case, **vlan 0** is applied on a spanned frame.
- Spanned FCoE frames do not preserve original SMAC and DMAC fields. The Ethernet header gets modified as the frame is spanned to the destination. The modified header fields are displayed when monitored on the SPAN destination.
- The CoS value in spanned FCoE frames on the Ethernet SPAN destination port does not match with the CoS value in the SPAN FCoE source frame. The CoS value on the captured SPAN FCoE frame should be ignored.
- The class-fcoe cannot be removed even if Fibre Channel is not enabled on a switch.
- If a port drains traffic at a rate less than 100 Kbps, it is error-disabled in 10 seconds to avoid buffer exhaustion. However, if the drain rate is larger than 100 Kbps, the port might not be consistently error-disabled within 10 seconds which exhaust ingress buffers and discard frames. Use the **shut** command to disable the slow-draining port.
- The multicast storm control functionality in the Cisco Nexus 5000 Series does not distinguish between IP, non-IP, registered, or unregistered multicast traffic. All multicast traffic is subject to a single-multicast storm control policer when configured.

IGMP Snooping Limitation

On the Cisco Nexus 5010 switch and the Cisco Nexus 5020 switch with a Cisco Nexus 2000 Series Fabric Extender (FEX) installed, unregistered IP multicast packets on one VLAN are forwarded to other VLANs where IGMP snooping is disabled. We recommend that you do not disable IGMP snooping on the Cisco Nexus 5010 switch and the Cisco Nexus 5020 switch. A static IGMP join can be configured for devices intended to receive IP multicast traffic but not to send IGMP join requests. This limitation applies to the Cisco Nexus 5010 switch and the Cisco Nexus 5020 switch only.

Beginning with NX-OS release 5.2(1)N1(5), IGMP general queries received on FEX interfaces are dropped thereby preventing a FEX interface from becoming an mrouter port.

SPAN Limitations on Fabric Extender Ports

The SPAN limitations on Fabric Extender ports are as follows:

- On a Cisco Nexus 5000 Series switch, if the SPAN source is a FEX port, the frames will always be tagged when leaving the SPAN destination.
- On a Cisco Nexus 5010 switch or a Nexus 5020 switch, if the SPAN source is an access port on a switch port or FEX port, the spanned frames at the SPAN destination will be tagged.
- On a Cisco Nexus 5500 Platform 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 4.0(1a)N2(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 the following error is displayed:

```
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 on all VLANs for which the tx-source port is a member, is spanned. 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, the broadcast, non-IGMP Layer-2 multicast, and 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.
- A FEX port cannot be configured as a SPAN destination. Only a switch port can be configured and used as a SPAN destination.
- Cisco NX-OS Release 5.1(3)N2(1) does not support SPAN on a VM FEX.

Checkpoint and Configuration Rollback Limitation

When FCoE is enabled, the checkpoint and configuration rollback functionality is disabled.

Upgrading and Downgrading Limitations

When upgrading and downgrading between Release 5.1(3)N2(1), Release 5.2(1)N1(8a), and Release 5.2(1)N1(1a), you might see the following issues in switch profile mode:

- **switchport** command configuration issues

If you previously used the **switchport access vlan** command, the **switchport trunk allowed vlan** command, or the **switchport trunk native vlan** command to configure the switch profile mode, the configurations you created are not visible.

Note This problem is a configuration display issue only, and there is no traffic disruption.

Table 6 lists the situations where you might experience **switchport** command configuration issues and the workarounds.

Table 6 Switchport Command Configuration Upgrade and Downgrade Issues

Path	Workaround
Upgrade from 5.1(3)N2(1) to 5.2(1)N1(1)	Perform the following tasks for all port channels where the configurations you created using the **switchport** commands are missing from the switch profile mode. **Note** Each affected **switchport** command configuration must be entered separately. The example uses the **switchport trunk allowed vlan** command. 1. Enter the following commands from the switch profile mode: switch(config-sync-sp)# **interface port-channel** *channel-number* switch(config-sync-sp)# **switchport trunk allowed vlan** *vlan-list* switch(config-sync-sp)# **commit** 2. If you receive a mutual exclusion error, import the command as follows: switch(config-sync-sp)# **import interface port-channel** *channel-number* switch(config-sync-sp-import)# **commit**
Downgrade from 5.2(1)N1(1) to 5.1(3)N2(1)	Same as upgrade from 5.1(3)N2(1) to 5.2(1)N1(1).
Upgrade from 5.1(3)N2(1) to 5.2(1)N1(1a)	Not applicable.
Downgrade from 5.2(1)N1(1a) to 5.1(3)N2(1)	Not applicable.
Upgrade from 5.2(1)N1(1) to 5.2(1)N1(1a)	Same as upgrade from 5.1(3)N2(1) to 5.2(1)N1(1).
Downgrade from 5.2(1)N1(1a) to 5.2(1)N1(1)	Same as upgrade from 5.1(3)N2(1) to 5.2(1)N1(1).

- **fex associate** command issues

  When in switch profile mode, the following commands are not visible:

  – **fex associate**

  Table 7 lists the situations where you might experience **fex associate** command issues and the workarounds.

Table 7 Fex Associate Command Upgrade and Downgrade Issues

Path	Workaround
Upgrade from 5.1(3)N2(1) to 5.2(1)N1(1)	In Release 5.1(3)N2(1), the **fex associate** command is rarely entered in configuration synchronization mode. If you plan to enter the **fex associate** command from the configuration synchronization mode, you must remove the command from the config-sync switch profile mode, and add the command from the configure terminal mode before you upgrade. For example: switch# **configure terminal** switch(config)# **interface ethernet** switch(config-if)# **interface port-channel** *channel-number* switch(config-if)# **switchport mode fex-fabric** switch(config-if)# **fex associate** *chassis_ID* **Note** If you did not add the **fex associate** command before the upgrade, you must import the command manually.
Downgrade from 5.2(1)N1(1) to 5.1(3)N2(1)	If you plan to enter the **fex associate** command from the configuration synchronization mode, you must remove the command from the config-sync switch profile mode, and add the command from the configure terminal mode before you downgrade. For example: switch# **configure terminal** switch(config)# **interface ethernet** switch(config-if)# **interface port-channel** *channel-number* switch(config-if)# **switchport mode fex-fabric** switch(config-if)# **fex associate** *chassis_ID* **Note** If you did not add the **fex associate** command before the downgrade, you must import the command manually.
Upgrade from 5.1(3)N2(1) to 5.2(1)N1(1a)	Same as upgrade from 5.1(3)N2(1) to 5.2(1)N1(1).
Downgrade from 5.2(1)N1(1a) to 5.1(3)N2(1)	Same as downgrade from 5.2(1)N1(1) to 5.1(3)N2(1).
Upgrade from 5.2(1)N1(1) to 5.2(1)N1(1a)	Not applicable.
Downgrade from 5.2(1)N1(1a) to 5.2(1)N1(1)	Not applicable.
Upgrade from 5.2(1)N1(3) to 5.2(1)N1(4)	--
Upgrade from 5.2(1)N1(4) to 5.2(1)N1(5)	--

Layer 3 Limitations

Asymmetric Configuration

In a vPC topology, two Cisco Nexus 5000 switches configured as vPC peer switches need to be configured symmetrically for Layer 3 configurations such as SVIs, Peer Gateway, routing protocol and policies, and RACLs.

Note vPC consistency check does not include Layer 3 parameters.

SVI

When a Layer 3 module goes offline, all non-management SVIs are shut down. An SVI can be configured as a management SVI using the **interface vlan** command and configuring *management*. This configuration allows traffic to the management SVIs to not go through the Layer 3 module which maintains connectivity in case of a Layer 3 module failure.

Upgrading and Downgrading

When a Layer 3 license is installed, the Cisco Nexus 5500 platform does not support an ISSU. Layer 3 module hot swaps are not supported.

Cisco Nexus 5548P Daughter Card (N55-D160L3)

Before installing a Layer 3 daughter card (N55-D160L3) into a Cisco Nexus 5548P switch, you must upgrade to Cisco NX-OS Release NX-OS Release 5.0(3)N1(1c) or a later release, and then install the card into the chassis.

Caveats

This section includes the open and resolved caveat record numbers for this release. Links are provided to the Bug Toolkit where you can find details about each caveat.

This section includes the following topics:

Open Caveats

Table 8 lists descriptions of open caveats in Cisco NX-OS Release 5.2(1)N1(x).

The record ID links to the Cisco Bug Toolkit where you can find details about the caveat.

Table 8 Cisco NX-OS Release 5.2x Open Caveats

Record Number	Open Caveat Headline
CSCun66310	Nexus 5596: System fails to boot after a power cycle.
CSCty43038	ethpm allowed vlan list and fwm fwd vlans are wrong after rollback
CSCuj10676	Static port-security macs on vpc primary change
CSCtz78363	hsrp vmac learned with primary switch-id instead of ES sw-id
CSCtx99080	fex temp does not reflect the correct value
CSCul78738	N2K-B22HP-P: HIF stays down when Blade Server moved into new slot.
CSCuc23124	750 W AC PS in O2-96T: warning syslog or shutdown system
CSCua27097	'no feature private-vlan' does not remove the complete config
CSCuc27069	DUT reads uninit value into "sh int count" after "clear count"+link flap

Resolved Caveats in Cisco NX-OS Release 5.2(1)N1(9b)

Table 9 lists the caveats that are resolved in Cisco NX-OS Release 5.2(1)N1(9b). The caveats might be open in previous Cisco NX-OS releases.

Table 9 Cisco NX-OS Release 5.2(1)N1(9b)

Record Number	Resolved Caveat Headline
CSCuo10554	Cisco Nexus 5000 Message of the Day (MOTD) Telnet Login Vulnerability
CSCvb88927	Evaluation of Nexus-5000-all for CVE-2016-5195 (DIRTY CoW)
CSCvc85845	Leap second update triggers watchdog crash
CSCuz44147	Evaluation of N9k/N7k/N5k/N3k/MDS for NTP April 2016 CVEs
CSCuz92661	Evaluation of N9k/N7k/N5k/N3k/MDS for NTP June 2016 CVEs
CSCvc23468	Evaluation of N9k/N7k/N5k/N3k/MDS for NTP November 2016
CSCuv08448	Cisco Nexus 5000 VDC Authenticated Privilege Escalation Vulnerability

Table 9 Cisco NX-OS Release 5.2(1)N1(9b)

Record Number	Resolved Caveat Headline
CSCuy54496	Evaluation of nexus-5000-all for OpenSSL March 2016
CSCuz52401	Evaluation of nexus-5000-all for OpenSSL May 2016
CSCvb48573	Evaluation of nexus-5000-all for Openssl September 2016
CSCuy11847	TACACS Daemon Hap Reset When Adding an SSH Key

Resolved Caveats in Cisco NX-OS Release 5.2(1)N1(9a)

Table 10 lists the caveats that are resolved in Cisco NX-OS Release 5.2(1)N1(9a). The caveats might be open in previous Cisco NX-OS releases.

Table 10 Cisco NX-OS Release 5.2(1)N1(9a)

Record Number	Resolved Caveat Headline
CSCux78120	Upgrade failure due to FEX file transfer error.
CSCuq75453	Nexus 50x0 - vPC peer is not reachable between 5.0(3) and 5.2(1)N1(8)
CSCui84039	ascii-cfg core and n6k reload observed no feature-set fabricpath
CSCup70139	N5K fwm hap reset
CSCup49604	Multiple hwclock zombie processes triggered by ntp
CSCus92726	N5K link flaps with HP StoreEasy x5530
CSCuw48559	Nexus 5K: Change fan detection logic
CSCux17060	N5K xmlma hap reset

Resolved Caveats in Cisco NX-OS Release 5.2(1)N1(9)

Table 11 lists the caveats that are resolved in Cisco NX-OS Release 5.2(1)N1(9). The caveats might be open in previous Cisco NX-OS releases.

Table 11 Cisco NX-OS Release 5.2(1)N1(9)

Record Number	Resolved Caveat Headline
CSCua39096	TACACS+ missing header length check.
CSCua39159	Command injection with CA functionality.
CSCub38654	N5K: Switch hang/lock up may occur due to Leap second update.
CSCus26870	December 2014 ntpd CVEs for Nexus 5k/6k/7k/MDS.
CSCus68591	Assess GHOST vulnerability for Nexus 5k (CVE-2015-0235).
CSCut77411	Assess April 2015 NTPd vulnerabilities for N5k/N6k/N7k.
CSCut45896	Nexus 5k/6k - MARCH 2015 OpenSSL Vulnerabilities.
CSCus42980	JANUARY 2015 OpenSSL Vulnerabilities.
CSCur31350	Multiple Vulnerabilities in OpenSSL - August 2014

Table 11 Cisco NX-OS Release 5.2(1)N1(9) (continued)

Record Number	Resolved Caveat Headline
CSCub38654	N5K: Switch hang/lock up may occur due to Leap second update.
CSCuq18021	SNMPset to community strings with special characters cause hap reset
CSCur30631	Nexus 6000: FWM crash with not enough core files saved
CSCuo34379	N5K/6K:NXOS upgrade by changing bootvariables & reload isn't recommended
CSCup85771	Nexus 6000 resets SSH intermittently
CSCut08809	Bug CSCuj56227 gets carried over ISSU upgrade.
CSCut09166	fwm hap reset on vlan delete
CSCur39582	vlan_mgr unresponsive on creating or deleting VLAN
CSCus77310	vpc hap reset vpc process crashed
CSCus78102	N6K crashed due to "kernel panic" @ stale pointer
CSCut25576	When deleting a profile, VRF param list are left over
CSCuq98419	N5K crash due to kernel panic during ISSU 5.2(1)N1(7)
CSCut22554	Workaround for CSCuo46284: Nexus 5500 showing SFP uC: Module 1: v0.0.0.0
CSCup36515	N5k/N6k SSH process may crash during authentication process.
CSCut81357	PTP Leap Second : n5k ptp off clock off by 35 seconds.

Resolved Caveats in Cisco NX-OS Release 5.2(1)N1(8b)

Table 12 lists the caveats that are resolved in Cisco NX-OS Release 5.2(1)N1(8b). The caveats might be open in previous Cisco NX-OS releases.

Table 12 Cisco NX-OS Release 5.2(1)N1(8b)

Record Number	Resolved Caveat Headline
CSCup53176	ethpm service crash on both VPC peers
CSCup31952	N5K: Nexus crash at eth_port_sec hap reset
CSCue62640	N5K/6K: TCP ports 21, 512-514 are opened after enabling FCoE
CSCup22663	Multiple Vulnerabilities in OpenSSL - June 2014
CSCur05017	N5K/N6K evaluation for CVE-2014-6271 and CVE-2014-7169
CSCuo14888	Zone hap reset after device-alias rename

Resolved Caveats in Cisco NX-OS Release 5.2(1)N1(8a)

Table 13 lists the caveats that are resolved in Cisco NX-OS Release 5.2(1)N1(8a). The caveats might be open in previous Cisco NX-OS releases.

Table 13 Cisco NX-OS Release 5.2(1)N1(8a)

Record Number	Resolved Caveat Headline
CSCup74690	Complete fix of CSCuj46069:DHCP offers might not get relayed in FP topos
CSCup74438	N5K: ISSU upgrade from 5.2(1)N1(8) to 6.0(2)N2(5) and 7.x is disruptive

Resolved Caveats in Cisco NX-OS Release 5.2(1)N1(8)

Table 14 lists the caveats that are resolved in Cisco NX-OS Release 5.2(1)N1(8). The caveats might be open in previous Cisco NX-OS releases.

Table 14 Cisco NX-OS Release 5.2(1)N1(8)

Record Number	Resolved Caveat Headline
CSCue31348	tacacsd process crash during authentication/authorization
CSCug20090	N5K/N6K: Switch reload to afm process hap reset
CSCtn64914	Proper error message to be shown for valid arp cases with proxy arp
CSCua71549	CLI file redirection read vulnerability
CSCul19656	Nexus 5000 switch reloaded due to evmc hap reset
CSCuo01637	Nexus5k: Network-operator role can view sensitive configuration
CSCuf56076	config-sync allowed vlan list moved to global-db after reload
CSCue40117	N5K may experience unexpectedly reboot when issuing show tech (tac-pac)
CSCun37493	Dynamic ARP Inspection and Port Security are not compatible with vPC
CSCui96694	N5k DHCP relay not working due to TCAM entry missing.
CSCuo86400	Memory leak causing the DRAP service to crash
CSCuf82423	Nexus 5596 ethpm hap reset
CSCuo16822	Port-Sec and DAI config should not depend on vPC role
CSCum62719	fcoe_mgr crash with "show platform software fcoe_mgr info global"
CSCud07967	Sysmgr service "fcoe_mgr" crashed
CSCuh57927	FEX hardware type changed after ISSU/ISSD
CSCue80077	FEX: Port flap request from SAP: MTS_SAP_SATMGR
CSCul90150	FWM HAP Reset causing both switches in vPC to crash
CSCuc88331	igmp snooping flooded on stp blocking after stp change
CSCuo10325	igmp snooping flooded on stp blocking after stp change
CSCul52253	VPC+ allocates ftag-1 and ftag-2 as active
CSCun67627	LACP Hap Reset while executing "show lacp interface"
CSCug49968	Nexus 5K/6K: Memory leak in LACP process leading up to switch reset
CSCuc61695	port-channel members error disabled due to eltm seq timeout
CSCud61168	SNMPWalk fallback on ifHCInOctets for FEX interfaces
CSCum35498	N5K kernel panic crash usd_mts_kthread

Table 14 Cisco NX-OS Release 5.2(1)N1(8) (continued)

Record Number	Resolved Caveat Headline
CSCub49964	The default route inject route table when next hop unreachable
CSCuo41201	Netstack buffer leaking with IPv6 feature running
CSCuh56328	netstack panic when closing the socket with sbuff lock acquired
CSCum47367	Cisco NX-OS Software TACACS+ Command Authorization Vulnerability
CSCul69860	FEX reset due to watchdog timeout
CSCul19908	False positive transceiver warnings on Nexus 5000
CSCuj03704	False transceiver alarm error messages on FC interfaces of nexus 5000
CSCuj35879	n5k kernel panic with process stats_client at skb_dequeue
CSCum13332	N5K: Changes to input voltage logging
CSCuc26047	Nexus 5000 reset due to Kernel Panic
CSCue71612	Nexus 5548P/5548UP: Silent Reload with i2c code 0x0100
CSCui50776	OpenSSH LoginGraceTime Denial of Service Vulnerability
CSCuj82699	Power-sequencer may need to be upgraded separetely
CSCug54317	N5k: Port-profile crash after configuring trunk allowed vlan <long list>
CSCuj36520	Nexus: reload due to PIM process crash
CSCuh97833	Cannot get IF-MIB counters for SVI
CSCuh42629	CSCuh42629SNMPd crashed in idle state
CSCub73781	Device stops responding to SNMP when incorrect use-acl is removed
CSCuf77936	Issue with entPhysicalContainedIn position for Nexus device
CSCui67164	Nexus Switch Crash in SNMPd w/ RMON Traps Configured
CSCtz91917	SNMPD core at snmp_add_delete_acl_policy while trying to remove communit
CSCuj33075	Slower response time when polling the if-table for FEX host interfaces
CSCuh97833	Cannot get IF-MIB counters for SVI
CSCuh42629	CSCuh42629SNMPd crashed in idle state
CSCub73781	Device stops responding to SNMP when incorrect use-acl is removed
CSCuf77936	Issue with entPhysicalContainedIn position for Nexus device
CSCui67164	Nexus Switch Crash in SNMPd w/ RMON Traps Configured
CSCtz91917	SNMPD core at snmp_add_delete_acl_policy while trying to remove communit

Resolved Caveats in Cisco NX-OS Release 5.2(1)N1(7)

Table 15 lists the caveats that are resolved in Cisco NX-OS Release 5.2(1)N1(7). The caveats might be open in previous Cisco NX-OS releases.

Table 15 Cisco NX-OS Release 5.2(1)N1(7)

Record Number	Resolved Caveat Headline
CSCuj90123	N5K: aclmgr crash during sh tech
CSCul27686	Nexus 55xx P Devices: After Upgrade Interface Down & Unrecoverable
CSCul27511	eth_port_channel crash on Nexus 5K
CSCui47367	"shut/no shut" for vfc crashed device due to FWM hap reset
CSCug96074	MAC unsync between vPC peers when vpc port down and recovered
CSCum29958	An N5K configured for ip directed-broadcast causes duplicate packets
CSCuj32483	N5K:LACP member ports stuck in I state
CSCth76201	DOM info is not correctly retrieved for Cisco-Finisar SFP
CSCuj86736	Need to optimize DFE tuning in 55xxUP series switches - RX CRC Errors
CSCuj84269	Nexus 5000 switch reloaded due to gatosusd hap reset
CSCue02576	N5K / N6K: port-profile service crash after VLAN changes
CSCul80812	Port inheritance disappears from int config if large number of VLAN used
CSCts72361	Inbound and output ICMP frames on different ports when L3 is enabled
CSCum44722	N5K/N6K snmpd crash
CSCuh33604	optimize dot1d snmp for fex stats
CSCui44640	N5k SNMP memory leak - libport_mgr.so
CSCul30680	N5k restart due to monitor process crash when a VLAN is added/removed
CSCud45836	Error disabled/STP set port state failure after vlan removed by VTP
CSCty86291	MTS buffer exhaustion with sequential add of large vlans.
CSCuj59439	vPC hap reset after peer-keepalive link comes up

Resolved Caveats in Cisco NX-OS Release 5.2(1)N1(6)

Table 16 lists the caveats that are resolved in Cisco NX-OS Release 5.2(1)N1(6). The caveats might be open in previous Cisco NX-OS releases.

Table 16 Cisco NX-OS Release 5.2(1)N1(6)

Record Number	Resolved Caveat Headline
CSCuc98155	MAC address table not sync in peers' vPC ports
CSCtq32794	"tacacs source-interface" failed to be parsed after copy cfg 2 run
CSCuh67647	Lot of Tacacsd zombie processes can be seen on N7k.
CSCue20224	Nexus VSH crashes when prompted for "enable" password
CSCuh97211	removing and re-enalbing device alias can result in fabric waiting
CSCuc43023	N5K: Unknown unicast forwarding block CLI exposed.
CSCui79701	Config Sync / Verify Failed / Lock already taken by another session
CSCtj26673	config-sync import fails for certain implicitly generated qos config

Table 16 Cisco NX-OS Release 5.2(1)N1(6)

Record Number	Resolved Caveat Headline
CSCug97032	N5K COPP - ARP Traffic not classified when arriving on PeerLink
CSCuj24129	DHCP offers with unicast bootp flag not relayed.
CSCue65973	Nexus 2248TP: HIF speed not showing the actual link bandwidth
CSCua02062	Ethpm causes high cpu; MTS buffers stuck
CSCty44132	N7k: peer is not reachable through fabricpath
CSCuc24181	output discards are seen in vfc interface
CSCub80303	FEX Crash When Running Command "phystats" In Command Shell
CSCuh57927	FEX hardware type changed after ISSU/ISSD
CSCuj56227	IGMP proxy reports may loop on the network
CSCtt26423	error message when configure DNS related command under management VRF
CSCtz67585	Service VPC may crash when no MTS buffers are available.
CSCtw96661	N5K not able to suppress Sev5 syslog messages related with connected FEX
CSCuh27818	dcos-xinetd core due to segmentation fault in 6.2.2 during netstack reg
CSCug26811	Kernel Panic, process hap reset caused by excessive traffic on mgmt port
CSCui34757	Nexus 5k acting as an NTP Client does not sync with an NTP server
CSCtx52217	ntp crashed when left idle
CSCug29190	'ethpc' hap reset tied to SFP diagnostics
CSCub52503	Need Warning in Syslog for 750W PS when input Voltage exceeds
CSCui28946	Nexus 5596T fails to boot
CSCub08667	Some mibs N5K responds with next object in tree and not with next index.
CSCuh66598	Private-vlan hap reset after 'default switchport private-vlan mapping'
CSCug79384	PVLAN with port-security and static mac-address disappear
CSCtx89902	able to match more than one cos for default class-fcoe
CSCui40707	TACACSd and RADIUSd Writing Uncompressed Cores to var/sysmgr/work
CSCui22907	6.0(2)N1(2) - generating TCAM fib full syslog when not FIB is not full
CSCug38697	OSPF LSA Injection Vulnerability
CSCui08344	multicast convergence improvements
CSCuj07601	"Error: OID not increasing" with SNMPwalk on ciscoStpExtensionsMIB
CSCub66817	RMON event config with large desc causes SNMPD crashes and HAP reset
CSCuf30186	snmpd service crash due to error table filled with messages
CSCue74597	N7K: Stale SSH sessions are seen if client is not sending close ack.
CSCth31107	not all process cores are managed by sysmgr causing disk space to leak
CSCtr97385	SNMP crash due in config-copy MIB due to missed heartbeats
CSCty33679	Crash w/ show interface eth1/7 transceiver details / mping
CSCui52144	Nexus 5k - Uncompressed Cores Filling Up /var/sysmgr/work
CSCub50434	VTP packets looping on vpc

Resolved Caveats in Cisco NX-OS Release 5.2(1)N1(5)

Table 17 lists the caveats that are resolved in Cisco NX-OS Release 5.2(1)N1(5). The caveats might be open in previous Cisco NX-OS releases.

Table 17 Cisco NX-OS Release 5.2(1)N1(5) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCud02139	Access to nexus7k via vty may get lost at random times with tacacs+
CSCue85990	AUTHPRIV-2-SYSTEM_MSG pam_unix(login:auth): auth could not identify
CSCuc62084	CSCuc62084 Sh accounting log / show log output is missing initial
CSCtx52991	Nexus 5500 is not compliant with FC-PI-4 at 8G FC speed
CSCub77319	port-profile in Config sync mode missing Description command
CSCua82034	FabricPath Switch ID not populating correctly
CSCug84290	False transceiver alarm error messages on nexus 5000
CSCuc54623	Show Port Channel command fails
CSCuf57043	("sequence timeout") communicating with MTS_SAP_ETH_PORT_SEC
CSCug90571	Service "fcdomain" crashed
CSCuh07302	mis-programmed hw adj entry causing device alias distribution to fail
CSCug95929	Multiple FEX can go offline at the same time .
CSCug69534	Memory leak in the FWM process at FWM_MEM_fwm_mac_t
CSCue24735	N5K has incorrect virtual-mac-address entries in HSRP state transition
CSCug80833	N5K: Connectivity issues after MAC fails over
CSCud08015	N5K / PTP multicast packets punted and dropped instead of forwarded
CSCug39029	Igmp report floods back to same hif port on which it was received
CSCud41492	IGMP not in sync with peer VPC switch after simultaneous leaves and join
CSCuc88331	igmp snooping flooded on stp blocking after stp change
CSCtz80915	TACACS service crash on nexus running 6.0.2
CSCuf08921	N5K fabricpath MAC address not re learnt on GARP
CSCuf51541	VPC/VPC+ HSRP VMAC removed on HSRP standby
CSCua42827	Nexus 5548: mroutes not created for sources connected across vpc
CSCts39876	CSCts39876 - NTP authentication key showing in clear text
CSCtr46317	ntp crashed after ISSU from 5.1.3 to 5.2.1.S69
CSCub90520	CLI threads not exited if 'sh tech <routing_protocol>' is interrupted
CSCuc39303	satctrl heartbeat miss when polling fex interfaces with solarwinds
CSCua52926	5548UP interface flaps on reload w/ passive twinax
CSCue81832	HW clock out of Sync , could result in ISSU failure .
CSCty01353	MAC learning issue after expansion module goes into hung state
CSCuf48422	N5K miss "-" sign for Tx/Rx power on `sh int transceiver detail`
CSCtx21891	Nexus 5000/5500 control plane failure not bringing links down

Table 17 Cisco NX-OS Release 5.2(1)N1(5) Resolved Caveats (continued)

Record Number	Resolved Caveat Headline
CSCue71612	Nexus 5548P/5548UP: Silent Reload with i2c code 0x0100
CSCub80935	Running "tac-pac" from non-admin username prompts for the password
CSCug07482	Memory leak at ppm with switch profile configured
CSCuh20770	N5k keep reboot with fabric path, vpc+ and fex configured
CSCud26463	Preprovision dynamic string changes + support for large commands
CSCue36960	FabricPath ISIS hello dropped if non-disruptive ISSU performed
CSCug42375	N5k - Same "match cos" value shared between class-fcoe and another class
CSCue02015	telnet to non-management SVI broken after reload
CSCug24976	N5k/6k: Need to expose knob "ip pim register-until-stop"
CSCtu34118	OSPF router link not advertised in Type 1 LSA on interface up
CSCuf61304	NX-OS : RPF on mroute incorrectly pointing to the RP for (S,G)
CSCue79881	SNMP crashes on SNMP bulk get query
CSCub15147	snmp memory leak on nexus 5000.
CSCug19662	MemLimit missing from show processes memory command on the Nexus 5K/2K
CSCtz32293	%TACACS-3-TACACS_ERROR_MESSAGE: All servers failed to respond
CSCua39287	System reloads due to TACACS+ process crash
CSCub16539	SNMP MTS Buffer Leak on VLAN MIBs - dot1d bridge, vlan membership, smon
CSCuf21318	N5k: Secondary VPC flaps VPC port-channels after peer-link is down
CSCub92274	PO127,PO128 appear on the output of "show vpc orphan-ports"
CSCua50255	ARP entry not learned over vPC link between N5K
CSCtz32233	Memory leak in the vPC process on a Nexus switch

Resolved Caveats in Cisco NX-OS Release 5.2(1)N1(4)

Table 18 lists the caveats that are resolved in Cisco NX-OS Release 5.2(1)N1(4). The caveats might be open in previous Cisco NX-OS releases.

Table 18 Cisco NX-OS Release 5.2(1)N1(4) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtz04737	"feature fcoe-npv" allows native FC ports to be provisioned
CSCty56134	N5k: VTY IPv4 access-class changed to IPv6 access-class after ISSU
CSCtg20592	callhome message doesn't use correct timezone configured on the device
CSCth06584	Need a command for resetting interface config to default
CSCub88489	Nexus 5000 XML process crash when running XML scripts
CSCue03528	Session Database / Config Sync / CFS locked on one side without a commit
CSCud33616	DHCPack for DHCPinform destined to 0.0.0.0
CSCub47702	Nexus 5000 does not print out logs for low/high power alarms.

Table 18 Cisco NX-OS Release 5.2(1)N1(4) Resolved Caveats (continued)

Record Number	Resolved Caveat Headline
CSCud64935	FCtrace missing from 5.2
CSCtz40390	Switch allows host unrestricted access to fabric information
CSCue25885	Feature Manager restart
CSCue35880	intermittent link up delay on fex ports
CSCue19686	Nexus 5000: Incorrect learn_bypass after ISSU
CSCua55506	IPv6 ND fails for v6 address which were on SVI but moved to hosts
CSCua58514	Nexus 5000: Cannot ping between SVIs across peer-link after loop
CSCud22845	Nexus 5548up forwarding IGMP Report frame out incorrect interface
CSCtx79241	Nexus 5k ISSU disruptive due to logging level above 5
CSCud72948	Fabricpath: BPDUs not sent out vPC secondary upon link failure
CSCuc97283	After reboot downstream Po moves to forwading while VPC is down
CSCue33958	Nexus 55xx: Traffic received on bind-vrf VLAN not routed to receiver
CSCtl73025	Failed to allocate shared memory while creating m4route
CSCtt00190	N7K: vsh process crashes while executing show/copy commands
CSCtu05113	Nexus 55xx core in fcpc -- heartbeat failure
CSCub38011	Nexus 5k might boot to bash prompt
CSCuc71921	Mem leak at ppm on removing and adding PO interface for 60 iterations
CSCtz12883	after upgrade N5k reboot loop due to ipqosmgr process crashing
CSCud51284	Ipqosmgr crashes when doing a show tech on the HSRP active switch
CSCty80885	To handle the memory allocation failure cases in ascii-cfg library
CSCty92420	BGP in vrf malloc errors and can not insert bgp routes in RIB
CSCud16740	Dynamic neighbor fails to re-establish after config change
CSCuc66439	Inbound soft reconfiguration not working on Nexus5k 5.2(1)N1(1a)
CSCty93371	dot1dBasePortIfIndex support in MST scenario - Bridge MIB
CSCue24258	Nexus 5000 returns 0 when SNMP Manager tries to get "ifOutErrors" MIB
CSCtw72949	Slow drain of udp sock mts buffers for some bulk requests in bridge-mib
CSCue14043	Dual-homed FEX goes offline after type-1 inconsistency recovering
CSCud54427	Norcal: Tracking object config lost after Reload- vPC Object Tracking
CSCtt10736	Traffic from peer-link dropped after secondary reload and pka reconnect

Resolved Caveats in Cisco NX-OS Release 5.2(1)N1(3)

Table 19 lists the caveats that are resolved in Cisco NX-OS Release 5.2(1)N1(3). The caveats might be open in previous Cisco NX-OS releases.

Table 19 Cisco NX-OS Release 5.2(1)N1(3) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtx69526	After a non-disruptive ISSU upgrade from release 5.0(3)N1(1c) or earlier, VTP pruning may get enabled on the Nexus 5000 series if it is enabled on other parts of the network.
CSCtx74521	There is a high CPU found on a vPC pair due to a PIM assert storm. A vPC domain source check is needed.
CSCua65570	Nexus 5596UP and 5548UP switches discovery over UDP from FM or DCMN fails.
CSCub41054	Sending an ARP request on invalid interface loopback0.
CSCub66225	The interlace physical MAC address returns inconsistent values.
CSCub68625	There **switch-profile config-sync** command does not function correctly after upgrading from the NX-OS release 5.2(1)N1(1) to the 5.2(1)N1(1b) patch release.
CSCuc13077	Any Nexus 5000 series switch without the layer 3 module drop fragmented packets when it pings the SVI.
CSCuc51083	After ISSU upgrade from 5.1(3)N2(1a) to 5.2(1)N1(1b), interfaces on the N2K-C2232TM-10GE which were down before the upgrade do not come until the FEX is reloaded.
CSCuc54814	Cisco Nexus 5000 Series switches configured with vPC+ and peer-gateway enabled, switched packets are sent over the peer-link.
CSCuc73895	HSRP standby learns VIP MAC addresses for the end host in a vPC peer with local proxy ARP configured which breaks connectivity to the host.
CSCuc84658	For the Nexus 5000 series switches there is an incorrect adjacency for the next hop IPv4 and IPv6 address causing traffic to be misrouted.
CSCuc87195	The N5548UP and N5596UP with reversible air fan and power supply report low fan speed errors after NX-OS 5.1(3) N1(1) upgrade and higher.
CSCuc92455	FEX Fabric port integrity improvement on the N2248TP.
CSCuc96551	FWM process cores sub-interface configuration.

CSCub02794 Many FLOGI and FCNs states are not cleared after the neighbors are disconnected.

Resolved Caveats in Cisco NX-OS Release 5.2(1)N1(2a)

Table 20 lists the caveats that are resolved in Cisco NX-OS Release 5.2(1)N1(2a). The caveats might be open in previous Cisco NX-OS releases.

Table 20 Cisco NX-OS Release 5.2(1)N1(2a) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCuc80263	ISSU from 5.1(3)N2(1b) to 5.2(1)N1(2) is disruptive.

Resolved Caveats in Cisco NX-OS Release 5.2(1)N1(2)

Table 21 lists the caveats that are resolved in Cisco NX-OS Release 5.2(1)N1(2). The caveats might be open in previous Cisco NX-OS releases.

Table 21 Cisco NX-OS Release 5.2(1)N1(2) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtr62922	Using FEX preprovisioning and configuring a vPC, the vPC number configuration in the two-layer port channel is accepted.
CSCtx88231	A switch reloads occurs when subinterfaces are configured on more than 10 Layer 3 interfaces.
CSCty00140	Internal vPC numbering needs to be optimized on the dual-homed FEX.
CSCtz00583	EIGRP MIBs are missing in Cisco NX-OS release 5.2(1)N1(x).
CSCua06312	The switch does not respond to unicast ARP requests received through the peer link.
CSCua86006	On a Version 2 Layer 3 daughter card (N55-D160L3-V2), when the maximum number of entries in the multicast routing table is greater than 4096, the multicast route programming can exceed the configured hardware limit and impact the allocated space for unicast host routes.
CSCua55155	Following an ISSU, the mode fabricpath VLAN configuration was lost.
CSCua74057	A "Warning: Failed saving command: (Command Parsing Failed)" error displays after a VLAN is added or removed on a trunk.
CSCua93951	Following an ISSU in a vPC setup, an internal failure can occur if a FEX has a PVLAN isolated trunk port.
CSCub01130	In a FabricPath configuration, when GSTP SWID = 0 and the peer switch reloads, no MAC address is flushed upon TCN.
CSCub09466	The value of "dot1dTpFdbStatus" is always shown as 0 in the BRIDGE-MIB.
CSCub56954	The Cisco Nexus 2248TPE FEX reports a power-on self test (POST) failure.
CSCub63985	Unicast ARP requests are dropped by the HSRP active after a session flap.
CSCub77357	The output of the **show running switch-profile** command does not show the allowed VLAN list.
CSCub82742	DCBX convergence occurs when PFC is set to off.
CSCub99364	A Cisco Nexus 5596 switch with a Layer 3 module and PVLAN configured drops packets on the internal port 15.
CSCub46846	A replacement Cisco Nexus 5000 Switch causes the FEX interfaces to flap.
CSCuc37057	VLAN membership is incorrect after an upgrade to Cisco NX-OS Release 5.2(x).
CSCuc37925	The **show environment** command displays incorrect PID information for fan modules.

Resolved Caveats in Cisco NX-OS Release 5.2(1)N1(1b)

Table 22 lists the caveats that are resolved in Cisco NX-OS Release 5.2(1)N1(1b). The caveats might be open in previous Cisco NX-OS releases.

Table 22 Cisco NX-OS Release 5.2(1)N1(1b) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtw82571	After a NX-OS upgrade of a Cisco Nexus 5010 or 5020 switch to release 5.1(3)N1(1), the switch does not forward traffic on certain vlans. If the switch uses FCoE, then vFCs fails to come up.
CSCua23762	The Cisco Nexus 5500 monitor session prevents FCoE hosts from completing logins.
CSCua54088	When a new member port from a new ASIC is added to a SAN port channel or the last member from any ASIC of a SAN port channel is flapped, the ingress FC frames are dropped at that member port due to the layer 3 logical interface (LIF) VLAN membership check failure.
CSCub19606	FCoE control plane traffic is impacted after upgrade.
CSCub48265	Cisco Nexus B22HP FEX 10GB host interface port autonegotiates to 1GB during initial server bootup.
CSCub69862	Cisco Nexus 5000 switch may reload due to a netstack crash.
CSCub73455	PVLAN cloned MAC addresses are deleted when a packet with a learned MAC address on a promiscuous port with a primary VLAN gets reflected on a secondary port.
CSCub79135	When checking the config-sync state of the peer using the command **show switch-profile peer detail**, a crash of the port-profile manager is displayed.
CSCub96331	FC credits up to a value above 64 can not be configured.

Resolved Caveats in Cisco NX-OS Release 5.2(1)N1(1a)

Table 23 lists the caveats that are resolved in Cisco NX-OS Release 5.2(1)N1(1a). The caveats might be open in previous Cisco NX-OS releases.

Table 23 Cisco NX-OS Release 5.2(1)N1(1a) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCua86602	The **update license** command is no longer hidden.
CSCua17122	Two Cisco Nexus 5000 switches running Cisco NX-OS Release 5.1(3)N1(1a) reloaded unexpectedly. The reason was "port-profile hap reset".
CSCua34584	An ISSU from Cisco NX-OS Release 5.0(3)N1(1) to Cisco NX-OS Release 5.2(1)N1(1) failed with "Maximum downtime exceeded" error.
CSCub38911	IGMP groups that are learned using IGMP snooping on FEX interfaces fail to synchronize when the fabric port fails or is shut down.
CSCua41448	A MAC violation occurs when a virtual MAC address moves from a vPC peer link to a secured port.
CSCua92618	Input/CRC errors are seen on FEX host interfaces on the Cisco Nexus 2232TM Fabric Extender.

Resolved Caveats in Cisco NX-OS Release 5.2(1)N1(1)

Table 24 lists the caveats that are resolved in Cisco NX-OS Release 5.2(1)N1(1). The caveats might be open in previous Cisco NX-OS releases.

Table 24 Cisco NX-OS Release 5.2(1)N1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtl56428	Solution for vPC failover when all data ports are down and mgmt0 is up.
CSCtl87260	Removing a switch-profile impacts the running configuration.
CSCua51385	An ISSU from Cisco NX-OS Release 5.1(3)N2(1a) to Cisco NX-OS Release 5.2(1)N1(1) causes the Fibre Channel link to go down.

Related Documentation

Documentation for Cisco Nexus 5000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders 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 includes the following types of documents:

- Licensing Information Guide
- Release Notes
- Installation and Upgrade Guides
- Configuration Guides
- Configuration Examples and TechNotes
- Programming Guides
- Operations Guides
- Error and System Message Guides
- Field Notices
- Security Advisories, Responses and Notices
- Troubleshooting Guide
- Command References
- MIB Reference Guide

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, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.