Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes,

Cisco NX-OS Release 5.1(3)N2(1c), 5.1(3)N2(1b), NX-OS Release 5.1(3)N2(1a) and NX-OS Release 5.1(3)N2(1)

Release Date: September 5, 2012
Part Number: OL-26652-03 D0
Current Release: NX-OS Release 5.1(3)N2(1c)

This document describes the features, caveats, and limitations for the Cisco Nexus 5000 Series switches and the Cisco Nexus 2000 Series Fabric Extenders. Use this document in combination with documents listed in the "Related Documentation" section on page 22.

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 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

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

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

Table 1 Online History Change

Part Number	Revision	Date	Description
OL-26652-01	A0	March 20, 2012	Created NX-OS Release 5.1(3)N2(1) release notes.
	B0	March 21, 2012	Updated the "Open Caveats" section.
	C0	March 27, 2012	Updated the "Resolved Caveats—Cisco NX-OS Release 5.1(3)N2(1a)" section.
	D0	April 3, 2012	Added CSCty92945 to a downgrade limitation in the "Limitations" section.
	E0	April 13, 2012	Added 4-Gbps CWDM SFPs to Table 2.
	F0	July 31, 2012	Updated Supported Upgrade and Downgrade Paths.
OL-26652-02	A0	June 5, 2012	Created NX-OS Release 5.1(3)N2(1a) release notes.
	B0	June 27, 2012	Added Cisco Management Interface over SSH, page 10.
	C0	June 28, 2012	Added CSCtc06276 to the "Limitations" section.
	D0	July 11, 2012	Added the Cisco Nexus B22HP FEX.
OL-26652-03	A0	September 5, 2012	Created NX-OS Release 5.1(3)N2(1b) release notes.
	B0	November 6, 2012	Updated the SFP+ Optical information in Table 2.
	C0	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.
	D0	February 19, 2013	Updated the Open Caveats, page 19 section and added the Resolved Caveats—Cisco NX-OS Release 5.1(3)N2(1c), page 19 section.

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 5.1 also supports all hardware and software supported in 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, page 4
- Online Insertion and Removal Support, page 8

Hardware Supported

The Cisco NX-OS software supports the Cisco Nexus 5000 Series. 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 5.1(x) software.

Table 2 Hardware Supported by Cisco NX-OS Release 5.1(x) Software

		Cisco NX-OS Release Support					

Hardware	**Part Number**	**5.1(3)N2(1c)
		5.1(3)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)**

Cisco Nexus 5000 Series							
Cisco Nexus 5596UP switch	N5K-C5596UP-FA	X	X	X	X	—	—
Cisco Nexus 5548UP switch	N5K-C5548UP-FA	X	X	X	X	—	—
Cisco Nexus 5548P switch	N5K-C5548P-FA	X	X	X	X	X	X
Cisco Nexus 5020P switch	N5K-C5020P-BF	X	X	X	X	X	X
Cisco Nexus 5010P switch	N5K-C5010P-BF	X	X	X	X	X	X
Cisco Nexus 2000 Series							
Cisco Nexus B22HP FEX[1]	N2K-B22HP-P	X	X	X	—	—	—
Cisco Nexus 2232TM FEX	N2K-C2232TM-10GE	X	X	X	—	—	—
Cisco Nexus 2232PP FEX	N2K-C2232PP-10GE	X	X	X	X	X	X
Cisco Nexus 2248TP E FEX	N2K-C2248TP-E-1GE	X	X	—	—	—	—
Cisco Nexus 2248TP FEX	N2K-C2248TP-1GE	X	X	X	X	X	X
Cisco Nexus 2224TP FEX	N2K-C2224TP-1GE	X	X	X	X	X	X
Cisco Nexus 2148T FEX	N2K-C2148T-1GE	X	X	X	X	X	X
Expansion Modules							
16-port Universal GEM	N55-M16UP(=)	X	X	X	X	—	—
N5596 Layer 3 GEM	N55-M160L3(=)	X	X	X	X	—	—
N5548 Layer 3 daughter card	N55-D160L3(=)	X	X	X	X	—	—

Table 2 Hardware Supported by Cisco NX-OS Release 5.1(x) Software (continued)

		Cisco NX-OS Release Support					

Hardware	**Part Number**	**5.1(3)N2(1c)**
		5.1(3)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)**

Layer 3 GEM	N55-M160L3-V2	X	X				
Version 2 Layer 3 daughter card	N55-D160L3-V2	X	X				
16-port SFP+ Ethernet	N55-M16P(=)	X	X	X	X	X	X
8 10-Gigabit Ethernet and 8 10-Gigabit FCoE ports	N55-M8P8FP(=)	X	X	X	X	X	X
Transceivers							
Fabric Extender Transceivers							
10-Gigabit Ethernet SFP (for Cisco Nexus 2000 Series to Cisco Nexus 5000 Series connectivity)	FET-10G(=)	X	X	X	X	X	X
SFP+ Optical							
10-Gigabit Ethernet—short range SFP+ module	SFP-10G-SR(=)	X	X	X	X	X	X
10-Gigabit Ethernet—long range SFP+ module	SFP-10G-LR(=)	X	X	X	X	X	X
10-Gigabit Ethernet—extended range SFP+ module	SFP-10G-ER(=)	X	X				
1000BASE-T standard	GLC-T(=)	X	X	X	X	—	—
Gigabit Ethernet SFP, LC connector SX transceiver (MMF)	GLC-SX-MM	X	X	X	X	—	—
Gigabit Ethernet SFP, LC connector SX transceiver (MMF), extended temperature range and DOM	GLC-SX-MMD	X	X	X	X	—	—
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF)	GLC-LH-SM	X	X	X	X	—	—

Table 2 Hardware Supported by Cisco NX-OS Release 5.1(x) Software (continued)

		Cisco NX-OS Release Support					

Hardware	Part Number	5.1(3)N2(1c)
		5.1(3)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)

Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF), extended temperature range and DOM	GLC-LH-SMD	X	X	X	X	—	—
SFP+ Copper							
10GBASE-CU SFP+ Cable (1 meter)	SFP-H10GB-CU1M(=)	X	X	X	X	X	X
10GBASE-CU SFP+ Cable (3 meters)	SFP-H10GB-CU3M(=)	X	X	X	X	X	X
10GBASE-CU SFP+ Cable (5 meters)	SFP-H10GB-CU5M(=)	X	X	X	X	X	X
10GBASE-CU SFP+ Cable (7 meters)	SFP-H10GB-ACU7M(=)	X	X	X	X	X	X
10GBASE-CU SFP+ Cable (10 meters)	SFP-H10GB-ACU10M (=)	X	X	X	X	X	X
Fibre Channel							
8-Gbps Fibre Channel—short wavelength	DS-SFP-FC8G-SW(=)	X	X	X	X	X	X
8-Gbps Fibre Channel—long wavelength	DS-SFP-FC8G-LW(=)	X	X	X	X	X	X
4-Gbps Fibre Channel—short wavelength	4DS-SFP-FC4G-SW(=)	X	X	X	X	X	X
4-Gbps Fibre Channel—long wavelength	4DS-SFP-FC4G-LW(=)	X	X	X	X	X	X
4-Gbps CWDM SFP							
1470 nm CWDM 1/2/4-Gbps Fibre Channe, Gray	DS-CWDM4G1470=	X					
1490 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Violet	DS-CWDM4G1490=	X					
1510 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Blue	DS-CWDM4G1510=	X					

Table 2 Hardware Supported by Cisco NX-OS Release 5.1(x) Software (continued)

		Cisco NX-OS Release Support					

Hardware	**Part Number**	**5.1(3)N2(1c)
		5.1(3)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)**

1530 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Green	DS-CWDM4G1530=	X					
1550 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Yellow	DS-CWDM4G1550=	X					
1570 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Orange	DS-CWDM4G1570=	X					
1590 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Red	DS-CWDM4G1590=	X					
1610 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Brown	DS-CWDM4G1610=	X					
Extended Temperature Range							
1000BASE-T SFP, extended temperature range	SFP-GE-T(=)	X	X	X	X	X	X
Gigabit Ethernet SFP, LC connector SX transceiver (MMF), extended temperature range and digital optical monitoring (DOM)	SFP-GE-S(=)	X	X	X	X	X	X
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF), extended temperature range and DOM	SFP-GE-L(=)	X	X	X	X	X	X
Converged Network Adapters							
Generation-1 (Pre-FIP) CNAs[2]		X	X	X	X	X	X

[1] The Cisco Nexus B22HP FEX is supported starting with Cisco NX-OS Release 5.0(3)N2(2).

[2] 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 5.1(x) and Release 5.0(x) software that supports online insertion and removal (OIR).

Table 3 Online Insertion and Removable Support by Cisco NX-OS Release 5.1(x) and Release 5.0(x) Software

		Cisco NX-OS Release Support					

Hardware	**Part Number**	**5.1(3)N2(1c)
		5.1(3)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 releases**

Cisco Nexus 5000 Series							
Cisco Nexus 5596UP switch	N5K-C5596UP-FA	X	X	X	—	—	—
Cisco Nexus 5548UP switch	N5K-C5548UP-FA	X	X	X	—	—	—
Cisco Nexus 5548P switch	N5K-C5548P-FA	X	X	X	X	X	—
Expansion Modules							
16-port Universal GEM	N55-M16UP(=)	X	X	X	X	—	—
Layer 3 GEM	N55-M160L3-V2[1]	—	—	—	—	—	—
Version 2 Layer 3 daughter card	N55-D160L3-V2[1]	—	—	—	—	—	—
16-port SFP+ Ethernet	N55-M16P(=)	X	X	X	X	—	—
8-port SFP+ Ethernet ports and 8-port SFP+ Fibre Channel ports	N55-M8P8FPL(=)	X	X	X	X	—	—
N5596 Layer 3 GEM	N55-M160L3(=)	—	—	—	—	—	—
N5548 Layer 3 daughter card	N55-D160L3(=)	—	—	—	—	—	—

[1] Does not support online insertion and removal.

New and Changed Features

This section describes the new features introduced in Cisco NX-OS Release 5.1(3)N2(1c), 5.1(3)N2(1b), Cisco NX-OS Release 5.1(3)N2(1a) and Cisco NX-OS Release 5.1(3)N2(1). This section includes the following topics:

- New Features in Cisco NX-OS Release 5.1(3)N2(1c), page 9
- New Features in Cisco NX-OS Release 5.1(3)N2(1c), page 9
- New Features in Cisco NX-OS Release 5.1(3)N2(1a), page 9
- New Software Features in Cisco NX-OS Release 5.1(3)N2(1), page 9
- New Hardware Features in Cisco NX-OS Release 5.1(3)N2(1), page 10

New Features in Cisco NX-OS Release 5.1(3)N2(1c)

Cisco NX-OS Release 5.1(3)N2(1c) is a patch release that provides bug fixes. It does not include new software or hardware features.

New Features in Cisco NX-OS Release 5.1(3)N2(1b)

Cisco NX-OS Release 5.1(3)N2(1b) is a patch release that provides bug fixes. It does not include new software or hardware features.

New Features in Cisco NX-OS Release 5.1(3)N2(1a)

Cisco NX-OS Release 5.1(3)N2(1a) is a patch release that provides bug fixes. It does not include new software or hardware features.

New Software Features in Cisco NX-OS Release 5.1(3)N2(1)

Cisco NX-OS Release 5.1(3)N2(1) is a maintenance release that includes bug fixes and the following software features and enhancements:

- Power On Auto-Provisioning, page 9
- VLAN QoS, page 9
- PVLAN On FEX Trunk Ports, page 10
- Increased Buffer-to-Buffer Credit Range, page 10
- SPAN and Enhanced vPC, page 10
- SPAN and Adapter FEX, page 10
- Cisco Management Interface over SSH, page 10

Power On Auto-Provisioning

Power On Auto Provisioning (POAP) automates the process of upgrading software images and installing configuration files on Nexus switches that are being deployed in the network for the first time. For more information, see the *Cisco Nexus 5000 Series NX-OS Fundamentals Configuration Guide*.

VLAN QoS

On Cisco Nexus 5500 Series devices, you can configure quality of service (QoS) policies for classification and marking on VLANs. The policies that you apply to a VLAN are applied to the traffic on the VLAN's Layer 2 and switch virtual interface (SVI) ports. For more information, see the *Cisco Nexus 5000 NX-OS Quality of Service Configuration Guide*.

PVLAN On FEX Trunk Ports

You can enable or disable a private VLAN (PVLAN) on FEX trunk ports. FEX trunk ports extend the PVLAN domain to all the hosts connected to it and when configured, globally affects all FEX ports connected to the Cisco NX-OS 5000 Series switch.

You must disable all the FEX isolated trunk ports before configuring PVLANs on the FEX trunk ports. If the FEX isolated trunk ports and the FEX trunk ports are both enabled, unwanted network traffic might occur.

For more information, see the *Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide.*

Increased Buffer-to-Buffer Credit Range

The buffer-to-buffer credit range has increased to 240. For more information, see the *Cisco Nexus 5000 Series NX-OS SAN Switching Guide.*

SPAN and Enhanced vPC

Cisco NX-OS Release 5.1(3)N2(1) supports SPAN with an enhanced vPC (EvPC)as the source.

SPAN and Adapter FEX

Cisco NX-OS Release 5.1(3)N2(1) supports SPAN with an adapter FEX as the ingress source.

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 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*.

New Hardware Features in Cisco NX-OS Release 5.1(3)N2(1)

Cisco NX-OS Release 5.1(3)N2(1) supports the following new hardware:

- Cisco Nexus 5596UP switch,1100 Watts AC Reverse Air Flow Power Supply (N55-PAC-1100W-B)

- Cisco Nexus 5596UP switch, Reverse Air Flow Fan Tray (N5596UP-FAN-B)
- Cisco Nexus 22xx FEX, 350 Watts DC Reversed Air Flow Power Supply (N2200-PDC-350W-B)

Upgrading or Downgrading to a New Release

This section describes the upgrade and downgrade paths that are supported for Cisco NX-OS Release 5.1(3)N2(1c), 5.1(3)N2(1b), Cisco NX-OS Release 5.1(3)N2(1a), and Cisco NX-OS Release 5.1(3)N2(1) on the Cisco Nexus 5000 Series switch.

This section includes the following topics:

- Upgrade and Downgrade Guidelines, page 11
- Supported Upgrade and Downgrade Paths, page 11

Upgrade and Downgrade Guidelines

The following guidelines apply to Cisco NX-OS Release 5.1(3)N2(1c), Cisco NX-OS Release 5.1(3)N2(1b),Cisco NX-OS Release 5.1(3)N2(1a) and Cisco NX-OS Release 5.1(3)N2(1) for the Cisco Nexus 5000 Series switches:

- 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(1b), 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(1b), 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 is not supported.

Supported Upgrade and Downgrade Paths

Table 4 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 5.1(3)N2(1c), Cisco NX-OS Release 5.1(3)N2(1b), Cisco NX-OS Release 5.1(3)N2(1a) and NX-OS Release 5.1(3)N2(1).

Table 4 Cisco NX-OS Release 5.1(3)N2(1) Supported Upgrade and Downgrade Paths

Current Cisco NX-OS Release	Upgrade to NX-OS Release 5.1(3)N2(1c), NX-OS Release 5.1(3)N2(1b), NX-OS Release 5.1(3)N2(1a), or NX-OS Release 5.1(3)N2(1)	Downgrade from NX-OS Release 5.1(3)N2(1c), NX-OS Release 5.1(3)N2(1b), NX-OS Release 5.1(3)N2(1a) or NX-OS Release 5.1(3)N2(1)

5.1(3)N1(1c)
5.1(3)N1(1b)
5.1(3)N1(1a)
5.1(3)N1(1)
	Nondisruptive upgrade (ISSU)[1]	Disruptive downgrade

5.0(3)N2(2b)
5.0(3)N2(2a)
5.0(3)N2(2)
5.0(3)N2(1)
	Nondisruptive upgrade (ISSU)	Disruptive downgrade

5.0(3)N1(1c)	Nondisruptive upgrade (ISSU)	Disruptive downgrade
5.0(2)N2(1)	Nondisruptive upgrade (ISSU)	Disruptive downgrade
5.0(2)N1(1)	Nondisruptive upgrade (ISSU)	Disruptive downgrade

[1] If HIF port channels or EvPCs are configured in the switch, see CSCtz42084 for additional details.

Limitations

This section describes the limitations for Cisco NX-OS Release 5.1(3)N2(1c), Cisco NX-OS Release 5.1(3)N2(1b), Cisco NX-OS Release 5.1(3)N2(1a) and Cisco NX-OS Release 5.1(3)N2(1).

- 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 nondisruptive 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 nondisruptive 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 may 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 Release5.1(3)N2(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.

Configuration Synchronization Limitation

When you remove a switch profile using the **no switch-profile** *name* **[all-config | local-config]** command, the configuration in the switch profile is not immediately removed from the running configuration. The following warning message appears:

```
WARNING: Deleting switch-profile will remove all commands configured under
switch-profile. Are you sure you want to delete all switch-profile commands from the
system ?
Are you sure? (y/n)  [n]
```

For current information about this issue, refer to CSCtl87260.

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 may 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.

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 may 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.

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 throught 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, page 19
- Resolved Caveats—Cisco NX-OS Release 5.1(3)N2(1c), page 19
- Resolved Caveats—Cisco NX-OS Release 5.1(3)N2(1c), page 19
- Resolved Caveats—Cisco NX-OS Release 5.1(3)N2(1a), page 21
- Resolved Caveats—Cisco NX-OS Release 5.1(3)N2(1), page 21

Open Caveats

Table 5 lists descriptions of open caveats in Cisco NX-OS Release 5.1(3)N2(1c), Cisco NX-OS Release 5.1(3)N2(1b), Cisco NX-OS Release 5.1(3)N2(1a) and Cisco NX-OS Release 5.1(3)N2(1).

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

Table 5 Cisco NX-OS Release 5.1(3)N2(1) Open Caveats

Record Number	Open Caveat Headline
Open Caveats	
CSCtx84752	The MVR receiver-port output for an AA FEX port displays ACTIVE after a switchover.
CSCtx99080	The FEX temperature does not reflect the correct value.

Resolved Caveats—Cisco NX-OS Release 5.1(3)N2(1c)

Table 8 lists the caveats that are resolved in Cisco NX-OS Release 5.1(3)N2(1c) . The caveats may be open in previous Cisco NX-OS releases.

Table 6 Cisco NX-OS Release 5.1(3)N2(1c) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCts27757	vPC delay restore is configured for 30 seconds and is the default.
CSCtt10736	With auto-recovery configured on a pair of Cisco Nexus 5000 Series switches in a vPC pair, the traffic coming from the peer link might get dropped if the secondary switch is reloaded with the peer-keepalive link disconnected and then restored after bootup.
CSCtx69677	In certain topologies where vPC peer-keepalive packets egress the Cisco Nexus 5000 Series device via the mgmt interface and then ingress the Cisco Nexus 5000 Series device peer via a port (vPC or not vPC), the device will drop the packets.
CSCtx79241	ISSU on a Cisco Nexus 5000 Series device can fail if the logging level on any process is above 5 during the code upgrade. Running an ISSU impact pre-install checks will still indicate a non-disruptive upgrade.
CSCty56134	After upgrading the Cisco Nexus 5000 Series device to Cisco NX-OS Release 5.1(3)N1(1a) or later, the VTY IPv4 access-class is converted to IPv6 access-class.
CSCty83755	The Cisco Nexus 5000 switch reloads due to the service eth_port_sec crashing.
CSCtz02038	MAC address is learnt on the vPC peer-link intermittently instead of a regular vPC link.

Table 6 Cisco NX-OS Release 5.1(3)N2(1c) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtz12883	The Cisco Nexus 5000 switch gets into a reboot loop after upgrading to Cisco NX-OS Release 5.1(3) due to the ipqosmgr process crashing.
CSCtz84683	A FEX may report that its power supplies are failing, although there is no perceived issue.
CSCua13558	The IGMP snooping process on a Cisco Nexus 5500 switch crashes when more than 50 IGMP snooping mrouter ports are detected. This is followed by a High-Availability Policy crash.
CSCua16219	The vPC peers reload one after the other continually.
CSCua23762	The Cisco Nexus 5500 Monitor session prevents FCoE hosts from completing logins.
CSCua58514	The Cisco Nexus 5000 Series device can not ping between SVIs across a peer-link after a bridging loop.
CSCub38011	Cisco Nexus 5000 Series device may boot to a bash prompt after a reload.
CSCub66124	FTS FEX "satctrl" core is observed but the core is not saved.
CSCuc81916	The OSPF process caused the Cisco Nexus 5548 switch to crash and the core dumped.
CSCud51284	Ipqosmgr crashed when doing a "show tech" on the HSRP active switch.

Resolved Caveats—Cisco NX-OS Release 5.1(3)N2(1b)

Table 8 lists the caveats that are resolved in Cisco NX-OS Release 5.1(3)N2(1b) . The caveats may be open in previous Cisco NX-OS releases.

Table 7 Cisco NX-OS Release 5.1(3)N2(1b) Resolved Caveats

Record Number	Resolved Caveat Headline
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.
CSCua88180	The vic_proxy process crashes after multiple fex reloads.
CSCub02109	Cisco Nexus 5000 Series switch vlan manager crashes due to memory leak caused by SNMP polling.
CSCub09466	The value of "dot1dTpFdbStatus" is always shown as "0".
CSCub14399	“Error disabled” error occurs with Cisco Nexus 7000 Series switch connected to Cisco Nexus 5000 Series switch.
CSCub19606	FCoE control plane traffic is impacted after upgrade.
CSCub31212	Cisco Nexus 5000 Series switches restart with “ipfib hap reset” error.
CSCub44542	When FCoE targets connected to Cisco Nexus 5000 Series switch go offline, the host experiences IO errors that take approximately 2 minutes to clear.
CSCub48265	Cisco Nexus B22HP FEX 10GB host interface port autonegotiates to 1GB during initial server bootup.
CSCub69862	A Cisco Nexus 5000 Series switch might restart due to netstack hap reset.

Resolved Caveats—Cisco NX-OS Release 5.1(3)N2(1a)

Table 8 lists the caveats that are resolved in Cisco NX-OS Release 5.1(3)N2(1a) . The caveats may be open in previous Cisco NX-OS releases.

Table 8 Cisco NX-OS Release 5.1(3)N2(1a) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCty07729	Custom Perl scripts can cause the Cisco Nexus 5000 Series switch to fail with kernel panic.
CSCty59143	After switch restore from reload, the port-channel status is down even though the members are up.
CSCty83483	Traffic traversing the peer-link on a Cisco Nexus 5000 Series switch may be dropped.
CSCty86545	Private VLAN isolated trunk mode to a Cisco Nexus 5000 Series switch does not work after upgrade.
CSCtz00790	After reloading a Nexus 55xx UP switch, eight consecutive ports may start dropping all ingress traffic.
CSCtz13307	A Cisco Nexus 5500 Series switch running NX-OS 5.1(3)N1(1) might reload with kernel panic.
CSCtz15346	The directory /mnt/pss grows too large and has no free space.
CSCtz33023	ISSU from 5.1(3)N1(1a) to N2(1) performed with CSCty59143 causes the port-channels to go down.
CSCtz42084	SNMPWalk entPhysicalName for Cisco Nexus 5000 Series switch temperature sensor returns incomplete value.
CSCtz89173	Whenever the **type N2248TP-E** command is entered under FEX, it is displayed as N2348GTP.
CSCua21174	Priority Flow Control (PFC) stops working after upgrade.

Resolved Caveats—Cisco NX-OS Release 5.1(3)N2(1)

Table 9 lists the caveats that are resolved in Cisco NX-OS Release 5.1(3)N2(1). The caveats may be open in previous Cisco NX-OS releases.

Table 9 Cisco NX-OS Release 5.1(3)N2(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCti10941	SPAN destination port shows wrongly in the **show int brief** command.
CSCtl87260	The switch profile removal option should not impact the running configuration.
CSCtl94228	No IP load sharing not reset to default mode.
CSCtn31018	On an ST host interface port, the **channel-grp** command gets an error due to “slot in vPC A-A mode.”
CSCtr73654	Peer ports go to UDLD error disabled when a module is powered off.
CSCtu14476	The insert-before option in a COPP customized policy should be removed.
CSCtu25289	RACLs on a subinterface are not applied following the **copy startup-config running-config** command.

Table 9 Cisco NX-OS Release 5.1(3)N2(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtu81489	Configuring a Layer 3 port with no license followed by a hot removal of a GEM causes the switch to fail.
CSCtw65587	Fabric ports go to hardware failure when a Layer 2 vPC is configured as a SPAN source.
CSCty61539	FWM core @fu_cb_restore_pss_data - ISSU from Release 5.0(3)N2(1) to Release 5.1(3)N2(1).

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/en/US/products/ps9670/tsd_products_support_series_home.html

The following are related Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Fabric Extender documents:

Release Notes

Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes

Cisco Nexus 5000 Series Switch Release Notes

Configuration Guides

Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 5.1(3)

Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 5.0(2)N1(1)

Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 4.2(1)N1(1) and Release 4.2(1)N2(1)

Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide

Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide

Cisco Nexus 5000 Series NX-OS Multicast Routing Configuration Guide

Cisco Nexus 5000 Series NX-OS Quality of Service Configuration Guide

Cisco Nexus 5000 Series NX-OS SAN Switching Configuration Guide

Cisco Nexus 5000 Series NX-OS Security Configuration Guide

Cisco Nexus 5000 Series NX-OS System Management Configuration Guide

Cisco Nexus 5000 Series NX-OS Unicast Routing Configuration Guide

Cisco Nexus 5000 Series Switch NX-OS Software Configuration Guide

Cisco Nexus 5000 Series Fabric Manager Configuration Guide, Release 3.4(1a)

Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.2

Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide

Maintain and Operate Guides

Cisco Nexus 5000 Series NX-OS Operations Guide

Installation and Upgrade Guides

Cisco Nexus 5000 Series and Cisco Nexus 5500 Platform Hardware Installation Guide

Cisco Nexus 2000 Series Hardware Installation Guide

Cisco Nexus 5000 Series NX-OS Software Upgrade and Downgrade Guide

Regulatory Compliance and Safety Information for the Cisco Nexus 5000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders

Licensing Guide

Cisco NX-OS Licensing Guide

Command References

Cisco Nexus 5000 Series Command Reference

Technical References

Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Fabric Extender MIBs Reference

Error and System Messages

Cisco NX-OS System Messages Reference

Troubleshooting Guide

Cisco Nexus 5000 Troubleshooting Guide

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.