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

Release 5.0(3)N2(2b), Release 5.0(3)N2(2a), Release 5.0(3)N2(2), Release 5.0(3)N2(1)

Release Date: December 16, 2011
Part Number: OL-25323-02 TN0
Current Release: NX-OS Release 5.0(3)N2(2b)
Current Release: NX-OS Release 5.0(3)N2(2a)
Current Release: NX-OS Release 5.0(3)N2(2)
Current Release: NX-OS Release 5.0(3)N2(1)

This document describes the features, caveats, and limitations for Cisco 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 25.

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

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

Table 1 Online History Change

Revision	Date	Description
A0	June 13, 2011	Created NX-OS Release 5.0(3)N2(1) release notes.
B0	June 16, 2011	Moved CSCtn64093 to Resolved.

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

Table 1 Online History Change

Revision	Date	Description
C0	June 22, 2011	Added Online Insertion and Removal Support. Added Auto-Negotiation Disable to New Software Features section.
D0	July 19, 2011	Added information about Cisco Nexus 2000 Series 10-Gigabit BASE-T Fabric Extenders.
E0	August 2, 2011	Updated Hardware Supported table and added information about Data Center Network Manager Release 5.2 Support.
F0	September 7, 2011	Added CSCto09813 (PSIRT) and CSCts44423. Moved CSCto23248 to Resolved. Updated Flex Links section.
G0	September 9, 2011	Created Release Notes for NX-OS Release 5.0(3)N2(2). Added Resolved Caveats—Cisco NX-OS Release 5.0(3)N2(2).
H0	September 13, 2011	Updated Supported Upgrade and Downgrade Paths.
I0	October 18, 2011	Removed the following caveats from Open Caveats: CSCti14663, CSCti19511, CSCti22121, CSCti45602, CSCti51365, , CSCtj27113, CSCtj29477, CSCtj30588, CSCtj31760, CSCtj44387, CSCtk08499, CSCtk31209, CSCtl51832, CSCtl56923, CSCtl94853, CSCtl99537, CSCtn76099, CSCtn76613, CSCtn82286, CSCtn87115. Moved the following caveats from Open Caveats to Resolved Caveats—Cisco NX-OS Release 5.0(3)N2(1): CSCtl95221, CSCtn19019, CSCtn57847, CSCtn58324, CSCto50140, CSCtl87240.
J0	October 26, 2011	Added CSCtq13290 to the Cisco NX-OS Release 5.0(3)N2(1) and Release 5.0(3)N2(2) Open Caveats.
K0	October 26, 2011	Created Release Notes for NX-OS Release 5.0(3)N2(2a). Added Resolved Caveats—Cisco NX-OS Release 5.0(3)N2(2a).
L0	December 16, 2011	Created Release Notes for NX-OS Release 5.0(3)N2(2b).
M0	July 11, 2012	Added the Cisco Nexus B22HP FEX.
N0	July 31, 2012	Updated Supported Upgrade and Downgrade Paths.

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 5.0 also supports all hardware and software supported in 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 now 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. 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 5.0(x) software.

Table 2 Hardware Supported by Cisco NX-OS Release 5.0(x) Software

		Cisco NX-OS Release Support			
Hardware	**Part Number**	**5.0(3)N2(2b) 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	—	—
Cisco Nexus 5548UP switch	N5K-C5548UP-FA	X	X	—	—
Cisco Nexus 5548P switch	N5K-C5548P-FA	X	X	X	X
Cisco Nexus 5020P switch	N5K-C5020P-BF	X	X	X	X
Cisco Nexus 5010P switch	N5K-C5010P-BF	X	X	X	X
Cisco Nexus 2000 Series					
Cisco Nexus B22HP FEX[1]	N2K-B22HP-P	X	—	—	—
Cisco Nexus 2232TM FEX	N2K-C2232TM-10GE	X	—	—	—
Cisco Nexus 2232PP FEX	N2K-C2232PP-10GE	X	X	X	X
Cisco Nexus 2248TP FEX	N2K-C2248TP-1GE	X	X	X	X
Cisco Nexus 2224TP FEX	N2K-C2224TP-1GE	X	X	X	X
Cisco Nexus 2148T FEX	N2K-C2148T-1GE	X	X	X	X
Expansion Modules					

Table 2 Hardware Supported by Cisco NX-OS Release 5.0(x) Software (continued)

		Cisco NX-OS Release Support			
Hardware	**Part Number**	**5.0(3)N2(2b) 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)**
16-port Universal GEM	N55K-M16UP(=)	X	X	—	—
N5596 Layer 3 GEM	N55K-M160L3(=)	X	X	—	—
N5548 Layer 3 daughter card	N55-D160L3(=)	X	X	—	—
16-port SFP+ Ethernet	N55-M16P(=)	X	X	X	X
8- 10 Gigabit Ethernet and 8- 10 Gigabit FCoE ports	N55-M8P8FP(=)	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
SFP+ Optical					
10-Gigabit Ethernet—short range	SFP-10G-SR(=)	X	X	X	X
10-Gigabit Ethernet—long range	SFP-10G-LR(=)	X	X	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 LX/LH transceiver (SMF)	GLC-LH-SM(=)	X	X	X	X
SFP+ Copper					
10GBASE-CU SFP+ Cable (1 meters)	SFP-H10GB-CU1M(=)	X	X	X	X
10GBASE-CU SFP+ Cable (3 meters)	SFP-H10GB-CU3M(=)	X	X	X	X
10GBASE-CU SFP+ Cable (5 meters)	SFP-H10GB-CU5M(=)	X	X	X	X
10GBASE-CU SFP+ Cable (7 meters)	SFP-H10GB-ACU7M(=)	X	X	X	X
10GBASE-CU SFP+ Cable (10 meters)	SFP-H10GB-ACU10M(=)	X	X	X	X
Fibre Channel					

Table 2 Hardware Supported by Cisco NX-OS Release 5.0(x) Software (continued)

		Cisco NX-OS Release Support			
Hardware	**Part Number**	**5.0(3)N2(2b) 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)**
8-Gbps Fibre Channel—short wavelength	DS-SFP-FC8G-SW(=)	X	X	X	X
8-Gbps Fibre Channel—long wavelength	DS-SFP-FC8G-LW(=)	X	X	X	X
4-Gbps Fibre Channel—short wavelength	4DS-SFP-FC4G-SW(=)	X	X	X	X
4-Gbps Fibre Channel—long wavelength	4DS-SFP-FC4G-LW(=)	X	X	X	X
Extended Temperature Range					
1000BASE-T SFP, extended temperature range	SFP-GE-T(=)	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
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF), extended temperature range and DOM	SFP-GE-L(=)	X	X	X	X
Converged Network Adapters		X	X	X	X
Generation-1 (Pre-FIP) CNAs[2]		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 5.0(x) software that supports online insertion and removal (OIR).

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

Hardware	Part Number	Cisco NX-OS Release Support			
		5.0(3)N2(2b) 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	—	—	—
Cisco Nexus 5548UP switch	N5K-C5548UP-FA	X	—	—	—
Cisco Nexus 5548P switch	N5K-C5548P-FA	X	X	X	—
Expansion Modules					
16-port Universal GEM	N55K-M16UP(=)	X	—	—	—
16-port SFP+ Ethernet	N55-M16P(=)	X	X	—	—
8-port SFP+ Ethernet Ports and 8-port SFP+ Fibre Channel Ports	N55-M8P8FPL(=)	X	X	—	—
N5596 Layer 3 GEM	N55K-M160L3(=)	—	—	—	—
N5548 Layer 3 daughter card	N55-D160L3(=)	—	—	—	—

New and Changed Features

This section describes the new features introduced in Cisco NX-OS Release 5.0(3)N2(1). This section includes the following topics:

New Hardware Features

This section describes the following new hardware:

Cisco Nexus 2000 Series 10-Gigabit BASE-T Fabric Extenders

The new Cisco Nexus 2000 Series 10GBASE-T Fabric Extenders (N2K-C2232TM-10GE and N2K-C2232TF-10GE) are the first 10GBASE-T platform switches in the Cisco Nexus product family.

The new Cisco Nexus 2232TM FEX and Nexus 2232TF FEX offer the following benefits:

- 32 1- and 10-Gigabit BASE-T ports.
- 8 10-Gigabit Ethernet ports (The Nexus 2232TM FEX requires SFP+ transceivers and the Nexus 2232TF includes 16 FEX transceivers.)
- Category 6, Category 6a, and Category 7 cabling support.

- 1 Uplink module that supports 8 10-Gigabit Ethernet fabric interfaces.
- 2 Power supplies (AC or DC power supplies).
- 1 Fan module with a choice of standard or reversed airflow.

Cisco Nexus B22 Blade Fabric Extender for HP (Cisco Nexus B22HP)

Starting with Cisco NX-OS Release 5.0(3)N2(2), the Cisco Nexus® B22 Blade Fabric Extender for HP (Cisco Nexus B22HP) provides an extension of the Cisco Nexus switch fabric to the HP server edge.

New Software Features

Cisco NX-OS Release 5.0(3)N2(1) includes the following new or changed software features:

- Fibre Channel over Ethernet N-Port Virtualization, page 8
- Flex Links, page 8
- Configurable Hash Polynomial, page 9
- Orphan Port Shutdown, page 9
- Auto-Negotiation Disable, page 9
- Licensing, page 9
- Data Center Network Manager Release 5.2 Support, page 10

Fibre Channel over Ethernet N-Port Virtualization

Beginning with Cisco NX-OS Release 5.0(3)N2(1), Fibre Channel over Ethernet N-Port Virtualization (FCoE NPV) is supported on the Cisco Nexus 5000 Series switches. The FCoE NPV feature is an enhanced form of FIP snooping that provides a secure method to connect FCoE-capable hosts to an FCoE-capable FCoE forwarder (FCF) switch. The FCoE NPV feature provides the following benefits:

- FCoE NPV does not have the management and troubleshooting issues that are inherent to managing hosts remotely at the FCF.
- FCoE NPV implements FIP snooping as an extension to the NPV function while retaining the traffic-engineering, VSAN-management, administration and trouble-shooting aspects of NPV.
- FCoE NPV and NPV together allow communication through FC and FCoE ports at the same time. This provides a smooth transition when moving from FC to FCoE topologies.

For more information, see the *Cisco Nexus 5000 Series NX-OS SAN Switching Configuration Guide, Release 5.0(3)N2(1)*.

Flex Links

Beginning with Cisco NX-OS Release 5.0(3)N2(1), Flex Links are supported on Cisco Nexus 5000 Series switches. Flex Links are a pair of a Layer 2 interfaces (switchports or port channels), where one interface is configured to act as a backup to the other. Flex Links are typically configured in service-provider or enterprise networks where customers do not want to run STP. Flex Links provide link-level redundancy that is an alternative to Spanning Tree Protocol (STP). STP is automatically disabled on Flex Links interfaces.

Note To configure flex links, you must remove the LAN_ENTERPRISE_SERVICES_PKG, LAN_BASE_SERVICES_PKG and then reload the switch.

For more information, see the *Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.0(3)N2(1)*.

Configurable Hash Polynomial

Beginning with Cisco NX-OS Release 5.0(3)N2(1), the Cisco Nexus 5500 Platform switches support 8 hash polynomials that can be used for compression on the hash-parameters. Depending on variations in the hash parameters for egress traffic flows from a port channel, different polynomials could provide improved load distribution results.

For more information, see the *Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.0(3)N2(1)*.

Orphan Port Shutdown

Beginning with Cisco NX-OS Release 5.0(3)N2(1), you can suspend a non-virtual port channel (vPC) port when a vPC secondary peer link goes down. A non-vPC port, also known as an orphaned port, is a port that is not part of a vPC.

For more information, see the *Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.0(3)N2(1)*.

Auto-Negotiation Disable

Beginning with Cisco NX-OS Release 5.0(3)N2(1), you can disable auto-negotiation on a switch port. This feature allows you to connect devices that do not support auto-negotiation (for example, certain DWDM multiplexers) to a Cisco Nexus 5000 Series switch.

Licensing

The Cisco NX-OS licensing feature allows you to access premium features on the device after you install the appropriate license for that feature. Any feature not included in a license package is bundled with the Cisco NX-OS software and is provided to you at no extra charge.

You must purchase and install a license for each device.

Note You can enable most features without installing a license. The Cisco NX-OS software provides a grace period for most features during which time you can try out a feature before purchasing its license. The Layer 3 features do not have a grace period and require an installed Layer 3 Base license to use the routing features.

Beginning with Cisco NX-OS Release 5.0(3)N2(1), the FCoE NPV license (FCOE_NPV_PKG) is available to use the FCoE NPV feature.

For more information on licensing, see the *Cisco NX-OS Licensing Guide*.

Data Center Network Manager Release 5.2 Support

Cisco DCNM is advanced management software that provides comprehensive life cycle management for the data center LAN and SAN.

Cisco DCNM Release 5.2 combines Cisco Fabric Manager, which previously managed SANs, and Cisco DCNM, which previously managed only LANs, into a unified product that can manage a converged data center fabric. As a part of the product merger in Cisco DCNM Release 5.2, the name Cisco DCNM for SAN replaces the name Cisco Fabric Manager. The name Cisco Fabric Manager still applies to Cisco Fabric Manager Release 5.0(x) and all earlier versions.

Cisco DCNM Release 5.2 supports the Cisco Nexus product family including the Cisco Nexus 5000 Series, Cisco MDS 9000 product family, Catalyst 6500 Series, and the Cisco UCS product family.

For information about new DCNM features for the Cisco Nexus 5000 Series switch, see the *Cisco DCNM Release Notes, Release 5.2*. For Cisco Nexus 5000 Series and DCNM compatibility information, see the *Cisco DCNM Release Compatibility Matrix*.

Upgrading or Downgrading to a New Release

This section describes the upgrade and downgrade paths that are supported for Cisco NX-OS Release 5.0(3)N2(1) on the Cisco Nexus 5000 Series switch.

This section includes the following topics:

Upgrade and Downgrade Guidelines

The following guidelines apply to Cisco NX-OS Release 5.0(3)N2(2b), Cisco NX-OS Release 5.0(3)N2(2a), Release 5.0(3)N2(2), and Release 5.0(3)N2(1) for the Cisco Nexus 5000 Series switches:

- Do not change any configuration settings or network settings during the upgrade. Any changes in the network settings may cause a disruptive upgrade.
- Cisco NX-OS Release 5.0(3)N2(2b), Release 5.0(3)N2(2a), Release 5.0(3)N2(2), and Release 5.0(3)N2(1) are ISSU-compatible with NX-OS Release 4.2(1)N1(1) and later releases.
- Downgrading from NX-OS Release 5.0(2) to NX-OS Release 4.2(1) is disruptive.
- Upgrading from NX-OS Release 4.2(1) to NX-OS Release 5.0(2) is a nondisruptive upgrade (ISSU).
- Upgrading from a Cisco NX-OS Release 4.2(1)-based release to Cisco NX-OS Release 5.0(3)N2(2a), Release 5.0(3)N2(2), or Release 5.0(3)N2(1)is nondisruptive.
- Downgrading from Cisco NX-OS Release 5.0(3)N2(2a), Release 5.0(3)N2(2), or Release 5.0(3)N2(1) to a previous release is disruptive.
- 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 5.0(3)N2(2b), Release 5.0(3)N2(2a), Release 5.0(3)N2(2a), Release 5.0(3)N2(2), and Release 5.0(3)N2(1):

Upgrading from NX-OS Release 5.0(3)N2(1) to Release 5.0(3)N2(2), Release 5.0(3)N2(2a), or Release 5.0(3)N2(2b) is nondisruptive.

Downgrading from Cisco NX-OS Release 5.0(3)N2(2b), NX-OS Release 5.0(3)N2(2a) or NX-OS Release 5.0(3)N2(2) to NX-OS Release 5.0(3)N2(1) is disruptive.

Table 4 Cisco NX-OS Release 5.0(3)N2(x) Supported Upgrades and Downgrades

Current Cisco NX-OS Release	Upgrade to NX-OS Release 5.0(3)N2(2b), Relese 5.0(3)N2(2a), Release 5.0(3)N2(2), or Release 5.0(3)N2(1)	Downgrade from NX-OS Release 5.0(3)N2(2b), Release 5.0(3)N2(2a), Release 5.0(3)N2(2), or Release 5.0(3)N2(1)
5.0(3)N1(1c) 5.0(3)N1(1b)	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
4.2(1)N2(1a) 4.2(1)N2(1) 4.2(1)N1(1)	Nondisruptive upgrade (ISSU)	Disruptive downgrade

Limitations

This section describes the limitations for Cisco NX-OS Release 5.0(3)N2(2b), Release 5.0(3)N2(2a), Release 5.0(3)N2(1) and Release 5.0(3)N2(2).

- 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, autonegotiation does not occur, which is 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 on the MST region. However, the work around causes a nondisruptive ISSU to fail because Non-Edge Designated Forwarding Ports are required 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 group 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 work around.
- 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).
- The Cisco Nexus 2000 Fabric Extender does not support PVLANs over VLAN trunks used to connect to another switch. The PVLAN trunks are used only on inter-switch links but the FEX ports are only meant to connect to servers. Because it is not a valid configuration to have an isolated secondary VLAN as part of a Fabric Extender port configured as a VLAN trunk, all frames on isolated secondary VLANs are pruned from going out to a FEX.
- 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 dot1p 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.

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 immediately removed from the running configuration. This disrupts the configurations that were present in the switch profile. For example, port channel and vPC configurations are disrupted. For current information about this issue, refer to CSCtl87240 and 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 errdisabled in 10 seconds to avoid buffer exhaustion. However, if the drain rate is larger than 100 Kbps, the port may not be consistently errdisabled 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 then 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 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, then 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, then a 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.

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 SVIs are shutdown.

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 5.0(3)N1(1b) or NX-OS Release 5.0(3)N1(1c) 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 9 lists descriptions of open caveats in Cisco NX-OS Release 5.0(3)N2(1) and Release 5.0(3)N2(2).

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

Table 5 Cisco NX-OS Release 5.0(3)N2(1) and Release 5.0(3)N2(2) Open Caveats

Record Number	Open Caveat Headline
New Open Caveats in NX-OS Release 5.0(3)N2(1)	
CSCtn00893	The undebug all command does not turn off CDP debugging logs.
CSCtn66859	A Cisco Nexus 5548P switch reboots after copying files from the bootlfash to USB flash.
CSCtn99894	When DHCP snooping is disabled globally but enabled in a VLAN, the boot-request packet is looped on the MCT in certain cases.
CSCtq13290	VPC PO goes to FWD after ISSU with MST multiple regions configured
CSCtq14143	If you enable Layer 3 routing after an ISSU upgrade, Layer 3 routing protocols do not come up until the switch reloads.
CSCtq79377	IGMP reports are going to the supervisor when IGMP is disabled on an SVI-enabled VLAN.
Open Caveats	
CSCtj94130	The Layer 3 traffic over an MCT link has dropped.
CSCtk84182	The **show incompatibilities** command does not display an incompatible configuration.
CSCtl09648	The interface from the static IGMP group cannot be removed if it is part of a range.
CSCtl45495	After the license has been reinstalled, the Layer 3 DC remains offline until the switch is rebooted.
CSCtl46093	OSPF does not come up with a Layer 3 interface MTU of 9000 because the supervisor MTU is 2000.
CSCtl51447	All Layer 3 features remain enabled after you remove the Layer 3 license.
CSCtl53720	The service does not respond when you delete the Layer 3 port channel and SVI interfaces.
CSCtl66943	DHCP validation errors have occurred in the PVLAN setup.
CSCtl87598	The QoS Type-2 inconsistency is not displayed in the show vpc command.
CSCtl87649	A commit failed when copying a configuration to the running configuration twice as per the recommended procedure.
CSCtl88086	On a host interface port in a straight-through topology, the channel-grp command displays an error due to "Slot in vpc A-A mode"
CSCtl94228	No IP load-sharing not reset to default mode
CSCtl95401	The FIB does not synchronize with the RIB after the FIB hit the hardware limit and the entries aged out.
CSCtl99388	A syntax error occurred after parsing the router-id and applying the saved configuration.
CSCtn19504	The HIF port is stuck in the vpc-peer-link-down state during a switchover test.
CSCtn27125	Traffic leaking on SVI ACL during switch bootup
CSCtn31018	On a host interface port in a straight-through topology, the **channel-grp** command displays an error message indicating “Slot in vpc A-A mode".
CSCtn40301	The syslog is consistently using more than 95% CPU after a switch upgrade.

Table 5 Cisco NX-OS Release 5.0(3)N2(1) and Release 5.0(3)N2(2) Open Caveats (continued)

Record Number	Open Caveat Headline
CSCtn40667	A FEX does not recover after a failed hitless upgrade during an ISSU.
CSCtn50937	The (s,g) mroutes do not expire if the source stopped and (*,g) is still joined.
CSCtn51223	Pre-provisioning and port profile configurations are not supported on Layer 3 interfaces.
CSCtn52446	A problem occurs when adding routes in VRF.
CSCto63412	In a Cisco Nexus 5548 switch with a Layer 3 module running Cisco NX-OS Release 5.0(3)N1(1b), due to address aliasing, groups in the range of [225-239].0.0.x cannot be used.
Platform, Infrastructure	
CSCso01268	VDC-related syslog message appears when a module is hot-swapped.
CSCsv95478	On a FEX, the **fex pinn redist** command does not wait for a user prompt with a y/n.
CSCti11823	When upgrading from NX-OS Release 4.2(1)N1(1) to NX-OS Release 4.2(1)N2(1), the 1-Gb HIF LED blinks amber after an ISSU.
CSCtj22747	On a failing type_check, GEMs do not recover from that state
Configuration Synchronization	
CSCti19892	Pressing Ctrl + Z does not interrupt a switch-profile deletion.
CSCti40833	Long failure detection times occur for the verify and commit (commands or actions?) in certain cases.
CSCti63620	An import has failed verification for channel-group member interfaces.
CSCti68764	Some spanning-tree commands are not supported in the switch profile.
CSCtj10460	A failure has occurred while deleting a switch profile.
CSCtj26673	A configuration synchronization import has failed for an implicitly generated QoS configuration.
CSCtl87260	A switch profile has been removed so as not to impact the running configuration.
Layer 2 Switching	
CSCso25966	The Catalyst 6500 Series LACP ports go to the err disable state when a peer Cisco Nexus 5000 Series switch PC has a configuration mismatch.
CSCso27446	The management port does not bring down/up a link when you enter the **shut/no shut** commands.
CSCso84269	An unsaved configuration warning appears even when there was no configuration change after a reload.
CSCsq35527	When doing IGMP snooping, the ip-mcast might take longer to converge on an STP top change.
CSCsr36661	Static IGMP groups with PVLAN host ports are not restored after a reload.
CSCsv56881	Inconsistent behavior occurs when duplicate IPv4/IPv6 addresses are configured.
CSCsv81694	A flap occurs when the dynamically learned port removes the auto-learn static mac entry.

Table 5 Cisco NX-OS Release 5.0(3)N2(1) and Release 5.0(3)N2(2) Open Caveats (continued)

Record Number	Open Caveat Headline
CSCsv93922	If the modulos operator "(%)" is used in a FEX description, the show command will not display information correctly.
CSCsx35870	If the modulos operator "(%)" is used in a FEX description, the show command will not display information correctly.
CSCta77490	When you quickly toggle the primary VLAN type, a failure of the type change occurs.
CSCtb58641	Entering the **clear mac-address** command did not delete a MAC address.
CSCtc04213	The VLAN configuration doesn't get applied on a range of interfaces.
CSCtc36397	A vPC role switchover does not occur when the vPC role is a primary operational role.
CSCtc44231	When a VLAN is deleted from the switch, the LACP port channels that have that VLAN set as a native VLAN fail to come-up.
CSCtd31131	This caveat was superseded by CSCtb70565.
CSCtf79253	Multiple alternate ports results in a root port failover and transient loops in a vPC topology.
CSCtg33706	Debug LACP is not available on FEX ports.
CSCth69160	An SVI over a secondary PVLAN is not working.
CSCti86007	When a peer-link comes up and vPC ports are in the process of coming up, if a peer switch reboots, there is a small window where vPC ports don't come up due to the peer-link down status.
CSCtj27113	When configuring the LACP fast rate, an MCT member port went to the UDLD empty echo state.
CSCtj85867	Entering the **show run** command is not displaying the switchport trunk VLAN list when a port profile is inherited.
SAN Switching	
CSCso46345	The i10K interop 4 mode is not supported.
CSCsq35728	When creating a SAN port channel, a MAP_PARAM_FROM_CHANNEL syslog message is displayed.
CSCsr28868	When you disable FCoE, the untagged Ethernet packet type 0000 shows CRC errors.
CSCsv19979	The speed should be configured manually for Fibre Channel ports in SD mode.
CSCsx80279	Addresses are not learned when egress interfaces are only FEX-facing ports.
CSCsy02439	An FC port error message displays occasionally.
CSCsy99816	The wrong FEX serial number does not show as an Identity-Mismatch in the output of the **show interface fex** command.
CSCtb61197	There are inconsistent SAN-port member states in the output of the **show interface** and **show san-port** commands.
CSCth98138	The command output for the **show fc-port-security** command for some virtual Fibre Channel interfaces is wrong.
CSCti99872	Superceded by CSCtr66343.

Table 5 Cisco NX-OS Release 5.0(3)N2(1) and Release 5.0(3)N2(2) Open Caveats (continued)

Record Number	Open Caveat Headline
CSCtj19861	Shutting down nontrunking SAN port channel members takes more than 30 seconds.
FCoE	
CSCtc77180	When you enable FCoE, ports are error-disabled.
CSCti87913	When you upgrade from NX-OS Release 4.2(1)N to NX-OS Release 5.0(2)N1(1), FLOGI fails after an ISSU.
Installation/Upgrade/Downgrade	
CSCtd15304	A successful reset occurred during the upgrade of Release 4.1(3)N1(1) to Release 4.1(3)N2(1) using Fabric Manager.
CSCtd70554	The fc-port-security configuration did not get converted when downgrading from NX-OS Release 4.1(3)N2(1) to NX-OS Release 4.1(3)N1(1).
CSCtf98638	During an ISSU, the following message appears: %SYSMGR-5-SUBPROC_KILLED "System Manager (core-client)"
Pre-Provisioning	
CSCti84186	The output of the **show run all** command shows an inconsistent configuration for the pre-provisioned interface.
Security	
CSCsl21529	The command-line interface has been enhanced to display the per-class maximum transmission unit (MTU).
CSCsq64251	A directed request does not work with TACACS+.
CSCsr20499	During a configuration restore to the running configuration from a configuration file using the **copy <file> running-config** command, the aclmgr may leak memory.
CSCsu77946	You cannot unconfigure statistics from an ACL in a configuration session.
CSCsv39939	Incorrect values are displayed for the interface capabilities for ports on a Cisco Nexus 2000 Series Fabric Extender connected to a Cisco Nexus 5000 Series switch.
CSCsz82199	When priority-flow-control is disabled between two Cisco Nexus 5000 Series switches, std.pause (interface flowcontrol) configuration does not take affect.
CSCtc62994	When combining RBAC roles (multiple roles assigned to the same user account), interface policies in those roles aren't working on a per-role basis.
CSCti15226	On Cisco Nexus 5500 platform switches, no error is identified when you configure an ACL-based qos policy for class-fcoe.
CSCti34155	The output for the **show run ipqos all** command does not show the default queuing class map.
CSCti61513	The **match ip rtp** command is not supported in the match-all class.
Configuration Rollback	

Table 5 Cisco NX-OS Release 5.0(3)N2(1) and Release 5.0(3)N2(2) Open Caveats (continued)

Record Number	Open Caveat Headline
CSCti77835	A rollback fails to revert to the earlier VLAN configuration.
CSCti87532	A rollback fails when changes are made in the buffer-size for class-fcoe.
CSCti97003	A rollback fails and the output of the **show rollback log exec** command displays "Deletion of switch profile failed".
CSCtj16996	A rollback fails when the switch profile configuration involves a conditional feature.
System Management	
CSCsm03765	You cannot assign an IP address on the mgmt0 interface using Device Manager.
CSCso74872	When two SNMP walks are started simultaneously, one of them may fail with the following error - 'OID not increasing'.
CSCsq57558	The software does not support an EISL encapsulation on an SD port (VFT cannot be preserved).
CSCsq76688	A CDP neighbor is not removed immediately after the port is shut down.
CSCsq90423	In NPV mode, EISL encapsulation for an SD port is not supported.
CSCsr68690	When egress SPAN is configured on a port that is transmitting jumbo or large frames, the spanned frames are truncated to 2384 bytes.
CSCsx40562	When using a FEX, the ACL drop traffic is not reaching the SPAN destination in certain configuration cases.
CSCsx59489	When the switch and FEX bootup after entering the **reload all** command, the time of event for any environment call home event, such as temperature alarm, power supply or fan alarms, is set to 1970.
CSCsz81365	Even after private-vlan mapping is removed on a trunk port using the **no switchport private-vlan mapping trunk** command, traffic received over the VLAN continues to be SPANed.
CSCtb53820	The monitor session goes to the error state with VSAN as a source after a reload.
CSCtb84512	In a mixed SPAN mode where Ethernet port channels, vFCs, and FC ports are span sources and an Ethernet interface is a SPAN destination, a vFC flap causes the traffic coming in on the Ethernet port channel not to be spanned.
CSCtb94310	Removing or adding a SAN port member causes a monitor session to go into an error state.
CSCtf32340	An error occurs while changing the VSAN and Interface scope of an existing role name.
CSCti10941	The destination port is wrong in the **show interface brief** command output.
CSCtj53287	Traffic received over Fibre Channel ports cannot be monitored on SPAN.
CFS	
CSCsl73766	RADIUS configuration distribution via CFS is unsupported.
CSCsm16222	Roles configuration distribution via CFS is unsupported.
CSCsr35452	CFS-based distribution of the NTP peer configuration does not work.

Table 5 Cisco NX-OS Release 5.0(3)N2(1) and Release 5.0(3)N2(2) Open Caveats (continued)

Record Number	Open Caveat Headline
CSCtb34546	Peer switches gets stuck in CFS discovery when you enter the **deny all ip pkts mgmt0** command.
Fabric Extender	
CSCsv15775	The priority-tagged frames on FEX ports get dropped.
CSCsv93263	FEX port configurations are lost when a configuration restore is done after a write erase and reload.
CSCsx68778	Flowcontrol configuration on the FEX ports may fail when the **range** command is used with interfaces that are spread across FEXs.
CSCta04383	The FEX should automatically revert to an older image if a second switch boots with the same version.
Transceiver	
CSCsv00989	Transceiver details are read as zeros even on DOM-capable 1G SFPs.
CSCsv02866	The **show interface ethernet transceiver details** command may show "invalid calibration" for DOM supported 1G SFPs.

Resolved Caveats—Cisco NX-OS Release 5.0(3)N2(2b)

Table 7 lists the caveats that are resolved in Cisco NX-OS Release 5.0(3)N2(2b). The caveats may be open in previous Cisco NX-OS releases.

Table 6 Cisco NX-OS 5.0(3)N2(2b) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtr72576	Upgrade to Release 5.0(3)N2(1) VFC initializing on FEX 2232 ports.
CSCtu06674	Following a shut of vPC PL, a VLAN interface on a secondary Nexus 5000 switch remains up.
CSCtu31915	Multicast and broadcast traffic stops forwarding on a FEX port after a vPC primary reloads.
CSCtv00468	Improve logging mechanisms for vpc keep-alive errors.
CSCtw62559	Do not print vPC peer keepalive failure messages during a peer switch ISSU.

Resolved Caveats—Cisco NX-OS Release 5.0(3)N2(2a)

Table 7 lists the caveats that are resolved in Cisco NX-OS Release 5.0(3)N2(2a). The caveats may be open in previous Cisco NX-OS releases.

Table 7 Cisco NX-OS 5.0(3)N2(2a) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtq13290	VPC PO goes to FWD after ISSU with MST multiple regions configured
CSCtr55489	The ipForwarding MIB OID returns 1 (enabled) for 55xx without L3 card
CSCtr64821	The sh env power command does not detect loss of power -> N5596
CSCts72469	FEX Power Supply showing absent
CSCtt12524	There is an ISSU failure and the FEX reloaded
CSCtt20801	Rec in non-vpc vlan are not receiving mcast trfc received over bind-vrf

Resolved Caveats—Cisco NX-OS Release 5.0(3)N2(2)

Table 8 lists the caveats that are resolved in Cisco NX-OS Release 5.0(3)N2(2). The caveats may be open in previous Cisco NX-OS releases.

Table 8 Cisco NX-OS 5.0(3)N2(2) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtq60360	A remote user name with "@" in the username field, fails authentication.
CSCtq60920	Fabric interfaces sdp timeout occurs on a reload with a new reserved VLAN.
CSCtq86334	Traffic is not load-balanced on port channel links on a Nexus 2248 Fabric Extender and on a Nexus 5548 switch.
CSCtr10164	On Nexus 5000 Series switches, an ospfv2 memory leak may occur when receiving specific malformed packets.
CSCtr17962	Turning on SVI on an access switch causes data forwarding that bypasses the flexlink blocked link.
CSCtr37490	Switch use different bridge ID for STP convergion and BPDU
CSCtr59635	Multihop FCoE: Any \"Storm-control brodcast level\" hanging LUN access
CSCtr65682	An SNMP memory leak associated with libcmd() may ocurr.
CSCtr76417	A memory leak in a port profile (ppm) process associated with libavl() may occur.
CSCts26382	Broadcasts received on peer links are not forwarded on some vPCs.
CSCts36169	If an ARP request is sent over a vPC peer link, then the response is sent as a broadcast.

Resolved Caveats—Cisco NX-OS Release 5.0(3)N2(1)

Table 9 lists the caveats that are resolved in Cisco NX-OS Release 5.0(3)N2(1). The caveats may be open in previous Cisco NX-OS releases.

Table 9 Cisco NX-OS 5.0(3)N2(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtj54918	On a Cisco Nexus 2000 Fabric Extender, the VLANs on a private VLAN host-port error after a vPC peer-link flap.
CSCtl87240	A switch profile has been removed to display a warning message prior to execution.
CSCtl95221	On the Cisco Nexus 5010 switch, an error message is displayed after you issue the **wrr cos queue** command.
CSCtn01449	When a Cisco Nexus 5548 switch is connected to a N7K-M132XP-12L module on a Nexus 7000 Series device using twinax cables (any version), the connected port goes into an error disabled state due to excessive link flaps.
CSCtn19019	Sometimes, the configuration does not synchronize when the switch is rebooted.
CSCtn24930	Messages are not sent to the syslog server (there no file or director).
CSCtn57847	An NPV switch has dropped FCoE after an ISSU and an OIR GEM.
CSCtn58324	Packets are not forwarded when an IPSG-enabled access port is made into a trunk.
CSCtn62877	During a software upgrade on a Cisco Nexus 5000 Series or Nexus 5500 Platform switch, the switch might reload with an fwm process crash.
CSCtn64093	The **no ip igmp snooping mrouter vpc-peer-link** command is not supported with FEX in a dual-homed topology.
CSCtn76099	A gratuitous ARP broadcast storm occurs when multiple vPCs are configured between Cisco Nexus 7000 Series devices and Cisco Nexus 5000 Series switches.
CSCtn89709	The BPDU loop guard is triggered when a vPC peer link is shut down.
CSCto09813	A vulnerability exists in Cisco Nexus 5000 and 3000 Series Switches that may allow traffic to bypass deny statements in access control lists (ACLs) that are configured on the device. Cisco has released free software updates that address this vulnerability. A workaround is available to mitigate this vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110907-nexus.shtml.
CSCto23248	When arp entry for peer-gateway doesn't exist, DHCP relay drops DHCP reply frames to a vPC peer.
CSCto47633	On a Cisco Nexus 5000Series switch running Cisco NX-OS Release 5.0(3)N1(1a), the CPU spikes in the PID wwn.
CSCto50140	A vPC crash occurs when configuring a value of 9216 in a range of interfaces. This is followed by a reboot on both Nexus 5000 Series peer switches.
CSCto68011	On Cisco Nexus 5000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders running in FC switching mode, an SNMP get request causes the fcdomain service to fail.
CSCto69352	On a Cisco Nexus 5596UP switch, the show tech-support command causes a service failure and the switch reboots.
CSCto75330	Unsupported FEXs are listed in the FEX-type configuration.
CSCto81320	A Cisco Nexus 2232 Fabric Extender fan module (N2K-C2232-FAN) is misidentified as N2K-C2232-FAN-B.

Table 9 Cisco NX-OS 5.0(3)N2(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtq00855	After a nondisruptive ISSU, the FCoE manager process may fail.
CSCtq03687	A Cisco Nexus 5000 Series or Nexus 5500 Platform switch running NX-OS Release 5.0(3)N1(1), NX-OS Release 5.0(3)N1(1a), or NX-OS Release 5.0(3)N1(1b) might crash when you enter the **show queuing interface** command on a FEX fabric interface which is administratively down.
CSCts44423	SFPs are not recognized after an ISSU to NX-OS Release 5.0(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 5.0(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, Release 4.2(1)N1(1)

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

©2011 Cisco Systems, Inc. All rights reserved.