Cisco Nexus 5500 Series Release Notes, Release 6.02

First Published: January 31, 2013
Date Last Modified: March 20, 2017
Current Release: NX-OS Release 6.0(2)N2(7)

This document describes the features, caveats, and limitations for the Cisco Nexus 5500 devices and the Cisco Nexus 2000 Series Fabric Extenders. Use this document in combination with documents listed in the "Related Documentation" section on page 52.

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 5500 and Cisco Nexus 2000 Series release notes:
http://www.cisco.com/en/US/docs/switches/datacenter/nexus5500/sw/release/notes/Nexus_5500_Release_Notes.html

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

Table 1 Online History Change

Date	Description
January 31, 2013	Created NX-OS Release 6.0(2)N1(1) release notes.
February 18, 2013	Added information on the maximum IP MTU in the NoteDoing a disruptive upgrade between incompatible images will result in loss of certain configurations such as unified ports, Fibre Channel (FC) ports, breakout, and FEX configurations. See CSCul22703 for details. section.
February 26, 2013	Added CSCtx42727 to the Resolved Caveats in Cisco NX-OS Release 6.0(2)N1(1)section.
February 28, 2013	Updated support for additional software features in the New Software Features in Cisco NX-OS Release 6.0(2)N1(1) section.
March 15, 2013	Created NX-OS Release 6.0(2)N1(2) release notes.

Table 1 Online History Change (continued)

Date	Description
May 1, 2013	Added link to the Cisco Nexus 6000 Series MIB Support List in the "MIB Support" section on page 52
May 22, 2013	Created NX-OS Release 6.0(2)N1(2a) release notes.
June 3, 2013	Added these items as supported hardware: QSFP-4x10G-AC7M, QSFP-4x10G-AC10M, QSFP-40G-LR4.
July 29, 2013	Created NX-OS Release 6.0(2)N2(1) release notes.
August 15, 2013	Added the following item as supported features for the NX-OS Release 6.0(2)N2(1): • iSCSI TLV Configuration Added the following items as supported features for the NX-OS Release 6.0(2)N1(2): • FEX NIF Storm Control • IP-Directed Broadcast
October 4, 2013	Created NX-OS Release 6.0(2)N2(2) release notes.
November 12, 2013	Added CSCul27686 to Open Caveats.
December 6, 2013	Created NX-OS Release 6.0(2)N2(1b) release notes.
December 20, 2013	Created NX-OS Release 6.0(2)N2(3) release notes.
December 24, 2013	Corrected ISSU path from Disruptive to Nondisruptive.
March 5, 2014	Created NX-OS Release 6.0(2)N2(4) release notes.
April 7, 2014	Added CSCug84860 to Open Caveats.
April 15, 2014	Added CSCuj36520 to Resolved Caveats.
May 6, 2014	Removed 5.0(3) from Table 5 - Supported Upgrade and Downgrade Paths.
June 30, 2014	Created NX-OS Release 6.0(2)N2(5) release notes.
July 9, 2014	Added CSCuj87061 to Open Caveats. CDC Feedback.
October 24, 2014	Created NX-OS Release 6.0(2)N2(5a) release notes.
November 26, 2014	Created NX-OS Release 6.0(2)N2(6) release notes.
April 20, 2015	Created NX-OS Release 6.0(2)N2(7) release notes.
March 15, 2017	Removed NX-OS Release 6.0(2)N2(1b) from the Supported Upgrade and Downgrade Paths 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 5500 Series device and the Cisco Nexus 2000 Series Fabric Extender (FEX) to improve the performance, scalability, and management of the product line. Cisco NX-OS Release 6.0 also supports all hardware and software supported in Cisco NX-OS Release 5.1, Cisco NX-OS Release 5.0.

Cisco Nexus Devices

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

For information about the Cisco Nexus 5500 Series, see the *Cisco Nexus 5500 Series Platform Hardware Installation Guide*.

Cisco Nexus 2000 Series Fabric Extenders

The Cisco Nexus 2000 Series Fabric Extender (FEX) is a highly scalable and flexible server networking solution that works with the Cisco Nexus 5500 Series devices 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 device, which allows zero-touch provisioning and automatic configuration. The FEX provides a single point of management that supports a large number of servers and hosts that can be configured with the same feature set as the parent Cisco Nexus 5500 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 5500 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 devices. Starting with Cisco NX-OS Release 6.0(2)N1(2), the Cisco Nexus 5010 and 5020 switches are not supported. You can find detailed information about supported hardware in the *Cisco Nexus 5500 Series Hardware Installation Guide*.

Table 2 shows the hardware supported by Cisco NX-OS Release 6.0(x) software.

Table 2 Hardware Supported by Cisco NX-OS Release 6.0(x) Software

Cisco NX-OS Release Support			
Hardware	**Part Number**	**6.0(2)N2(7) 6.0(2)N2(6) 6.0(2)N2(5a) 6.0(2)N2(5) 6.0(2)N2(4) 6.0(2)N2(3) 6.0(2)N2(1b)**	**6.0(2)N2(2) 6.0(2)N2(1) 6.0(2)N1(2) 6.0(2)N1(1)**
Cisco Nexus 5500 Series			
Cisco Nexus 5596T switch[1]	N5K-C5596T-FA	X	X
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
Cisco Nexus 5010T switch			
Cisco Nexus 2000 Series			
Cisco Nexus B22DELL FEX[2]	N2K-B22DELL-P	X	X
Cisco Nexus B22IBM FEX[3] [4]	N2K-B22IBM-P	X	X
Cisco Nexus 2248PQ FEX[5]	N2K-C2248PQ-10GE	X	X
Cisco Nexus 2232TM-E FEX[6]	N2K-C2232TM-E-10GE	X	X
Cisco Nexus B22F FEX	N2K-B22FTS-P	X	X

Table 2 Hardware Supported by Cisco NX-OS Release 6.0(x) Software (continued)

Cisco NX-OS Release Support			
Hardware	**Part Number**	**6.0(2)N2(7) 6.0(2)N2(6) 6.0(2)N2(5a) 6.0(2)N2(5) 6.0(2)N2(4) 6.0(2)N2(3) 6.0(2)N2(1b)**	**6.0(2)N2(2) 6.0(2)N2(1) 6.0(2)N1(2) 6.0(2)N1(1)**
Cisco Nexus B22HP FEX[7]	N2K-B22HP-P	X	X
Cisco Nexus 2232TM FEX	N2K-C2232TM-10GE	X	X
Cisco Nexus 2232PP FEX	N2K-C2232PP-10GE	X	X
Cisco Nexus 2248TP-E FEX	N2K-C2248TP-E-1GE	X	X
Cisco Nexus 2248TP FEX	N2K-C2248TP-1GE	X	X
Cisco Nexus 2232TP FEX			
Cisco Nexus 2232TT FEX			
Cisco Nexus 2224TP FEX	N2K-C2224TP-1GE	X	X
Cisco Nexus 2148T FEX	N2K-C2148T-1GE	—[8]	—[9]
Cisco Nexus 2020T FEX			
Expansion Modules			
4-port QSFP+ 10GBE GEM	N55-M4Q	X	X
12-port 10GBASE-T GEM[10]	N55-M12T	X	X
16-port Universal GEM	N55-M16UP(=)	X	X
N5596 Layer 3 GEM	N55-M160L3(=)	X	X
N5548 Layer 3 daughter card	N55-D160L3(=)	X	X
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

Table 2 Hardware Supported by Cisco NX-OS Release 6.0(x) Software (continued)

Cisco NX-OS Release Support			
Hardware	**Part Number**	**6.0(2)N2(7) 6.0(2)N2(6) 6.0(2)N2(5a) 6.0(2)N2(5) 6.0(2)N2(4) 6.0(2)N2(3) 6.0(2)N2(1b)**	**6.0(2)N2(2) 6.0(2)N2(1) 6.0(2)N1(2) 6.0(2)N1(1)**
8 10-Gigabit Ethernet and 8 10-Gigabit FCoE ports	N55-M8P8FP(=)	X	X
Transceivers			
Fabric Extender Transceivers			
10-Gigabit Ethernet SFP (for Cisco Nexus 2000 Series to Cisco Nexus 6000 Series connectivity)	FET-10G(=)	X	X
SFP+ Optical			
Cisco 40GBASE-LR4 QSFP+ Module for SMF	QSFP-40GE-LR4	6.0(2)N1(2) only	6.0(2)N1(2) only
4x10-Gigabit QSFP module	QSFP-4SFP10G-CU1M	X	X
4x10-Gigabit QSFP module	QSFP-4SFP10G-CU3M	X	X
4x10-Gigabit QSFP module	QSFP-4SFP10G-CU5M	X	X
4x10-Gigabit QSFP module	QSFP-4SFP10G-ACu7M	X	X
4x10-Gigabit QSFP module	QSFP-4SFP10G-ACu10M	X	X
Cisco 40GBASE-CR4 QSFP+ to 4 10GBASE-CU SFP+ direct-attach breakout 7-meter cable, active	QSFP-4X10G-AC7M	6.0(2)N1(2) only	6.0(2)N1(2) only
Cisco 40GBASE-CR4 QSFP+ to 4 10GBASE-CU SFP+ direct-attach breakout 10-meter cable, active	QSFP-4X10G-AC10M	6.0(2)N1(2) only	6.0(2)N1(2) only
Gigabit Ethernet SFP, LX transceiver[11]	GLC-LX-SMD	X	X

Table 2 Hardware Supported by Cisco NX-OS Release 6.0(x) Software (continued)

Cisco NX-OS Release Support			
Hardware	**Part Number**	**6.0(2)N2(7) 6.0(2)N2(6) 6.0(2)N2(5a) 6.0(2)N2(5) 6.0(2)N2(4) 6.0(2)N2(3) 6.0(2)N2(1b)**	**6.0(2)N2(2) 6.0(2)N2(1) 6.0(2)N1(2) 6.0(2)N1(1)**
Gigabit Ethernet SFP, EX transceiver[12]	GLC-EX-SMD	X	X
1000BASE-ZX SFP transceiver module for SMF	GLC-ZX-SM(=)	X	X
10-Gigabit Ethernet—short range SFP+ module	SFP-10G-SR(=)	X	X
10-Gigabit Ethernet—long range SFP+ module	SFP-10G-LR(=)	X	X
10-Gigabit Ethernet—extended range SFP+ module	SFP-10G-ER(=)	X	X
1000BASE-T standard	GLC-T(=)	X	X
Gigabit Ethernet SFP, LC connector SX transceiver (MMF)	GLC-SX-MM	X	X
Gigabit Ethernet SFP, LC connector SX transceiver (MMF), extended temperature range and DOM	GLC-SX-MMD	X	X
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF)	GLC-LH-SM	X	X
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF), extended temperature range and DOM	GLC-LH-SMD	X	X
SFP+ Copper			
10GBASE-CU SFP+ Cable (1 meter)	SFP-H10GB-CU1M(=)	X	X
10GBASE-CU SFP+ Cable (3 meters)	SFP-H10GB-CU3M(=)	X	X

Table 2 Hardware Supported by Cisco NX-OS Release 6.0(x) Software (continued)

Cisco NX-OS Release Support			
Hardware	**Part Number**	**6.0(2)N2(7) 6.0(2)N2(6) 6.0(2)N2(5a) 6.0(2)N2(5) 6.0(2)N2(4) 6.0(2)N2(3) 6.0(2)N2(1b)**	**6.0(2)N2(2) 6.0(2)N2(1) 6.0(2)N1(2) 6.0(2)N1(1)**
10GBASE-CU SFP+ Cable (5 meters)	SFP-H10GB-CU5M(=)	X	X
10GBASE-CU SFP+ Cable (7 meters)	SFP-H10GB-ACU7M(=)	X	X
10GBASE-CU SFP+ Cable (10 meters)	SFP-H10GB-ACU10M(=)	X	X
10GBASE CU SFP+ cable[13]	SFP-H10GB-CU1.5M	X	X
10GBASE CU SFP+ cable[14]	SFP-H10GB-CU2M	X	X
10GBASE CU SFP+ cable[15]	SFP-H10GB-CU2.5M	X	X
Fibre Channel			
8-Gbps Fibre Channel—short wavelength	DS-SFP-FC8G-SW(=)	X	X
8-Gbps Fibre Channel—long wavelength	DS-SFP-FC8G-LW(=)	X	X
4-Gbps Fibre Channel—short wavelength	4DS-SFP-FC4G-SW(=)	X	X
4-Gbps Fibre Channel—long wavelength	4DS-SFP-FC4G-LW(=)	X	X
4-Gbps CWDM SFP			
1470 nm CWDM 1/2/4-Gbps Fibre Channel, Gray	DS-CWDM4G1470(=)	X	X
1490 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Violet	DS-CWDM4G1490(=)	X	X
1510 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Blue	DS-CWDM4G1510(=)	X	X

Table 2 Hardware Supported by Cisco NX-OS Release 6.0(x) Software (continued)

Cisco NX-OS Release Support			
Hardware	**Part Number**	**6.0(2)N2(7) 6.0(2)N2(6) 6.0(2)N2(5a) 6.0(2)N2(5) 6.0(2)N2(4) 6.0(2)N2(3) 6.0(2)N2(1b)**	**6.0(2)N2(2) 6.0(2)N2(1) 6.0(2)N1(2) 6.0(2)N1(1)**
1530 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Green	DS-CWDM4G1530(=)	X	X
1550 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Yellow	DS-CWDM4G1550(=)	X	X
1570 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Orange	DS-CWDM4G1570(=)	X	X
1590 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Red	DS-CWDM4G1590(=)	X	X
1610 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Brown	DS-CWDM4G1610(=)	X	X
Extended Temperature Range			
1000BASE-T SFP, extended temperature range	SFP-GE-T(=)	X	X
Gigabit Ethernet SFP, LC connector SX transceiver (MMF), extended temperature range and digital optical monitoring (DOM)	SFP-GE-S(=)	X	X
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF), extended temperature range and DOM	SFP-GE-L(=)	X	X
Converged Network Adapters		X	X
Generation-1 (Pre-FIP) CNAs[16]		X	X

1. The Cisco Nexus 5596T and the 12-port 10-GBase-T GEM are supported starting with Cisco NX-OS Release 5.2(1)N1(1b).

2. The Cisco Nexus B22DELL P FEX is supported starting with Cisco NX-OS Release 5.2(1)N1(3).
3. The Cisco Nexus B22IBM FEX is supported with Cisco NX-OS Release 6.0(2)N2(1b) and later.
4. The Cisco Nexus B22IBM FEX is not supported with Cisco NX-OS Release 6.0(2)N2(2)
5. The Cisco Nexus 2248PQ FEX does not support Gen1 cables.
6. The Cisco Nexus 2232TM-E FEX is supported starting with Cisco NX-OS Release 5.2(1)N1(1a).
7. The Cisco Nexus B22HP FEX is supported starting with Cisco NX-OS Release 5.0(3)N2(2).
8. Starting with Cisco NX-OS Release 6.0(2)N1(1), 2148T FEX is not supported on Cisco Nexus 5500 series devices.
9. Starting with Cisco NX-OS Release 6.0(2)N1(1), 2148T FEX is not supported on Cisco Nexus 5500 series devices.
10. The 12 port 10-GBASE-T GEM is only supported on the Cisco Nexus 5596T starting with Cisco NX-OS Release 5.2(1)N1(1b).
11. Added support for Gibabit Ethernet SFP LX transceiver starting with Cisco NX-OS Release 6.0(2)N1(2).
12. Added support for Gibabit Ethernet SFP EX transceiver starting with Cisco NX-OS Release 6.0(2)N1(2).
13. Added support for 10GBASE CU SFP+ cable starting with Cisco NX-OS Release 6.0(2)N1(2).
14. Added support for 10GBASE CU SFP+ cable starting with Cisco NX-OS Release 6.0(2)N1(2).
15. Added support for 10GBASE CU SFP+ cable starting with Cisco NX-OS Release 6.0(2)N1(2).
16. Generation-1 (Pre-FIP) CNAs are supported on the Nexus 5000 Platform switches; however, they are not supported on the Nexus 5500 Series.

Table 3 Hardware Supported by Cisco NX-OS Release 6.0(x) Software

Cisco NX-OS Release Support							
Hardware	**Part Number**	**5.2(1)N1(5a) 5.2(1)N1(5) 5.2(1)N1(4) 5.2(1)N1(3) 5.2(1)N1(2a) 5.2(1)N1(2) 5.2(1)N1(1b) 5.2(1)N1(1a) 5.2(1)N1(1)**	**5.1(3)N2(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 5500 Series							
Cisco Nexus 5596T switch[1]	N5K-C5596T-FA	X	—	—	—	—	—
Cisco Nexus 5596UP switch	N5K-C5596UP-FA	X	X	X	X	X	—
Cisco Nexus 5548UP switch	N5K-C5548UP-FA	X	X	X	X	X	—
Cisco Nexus 5548P switch	N5K-C5548P-FA	X	X	X	X	X	X
Cisco Nexus 5010T switch					X		X

Table 3 Hardware Supported by Cisco NX-OS Release 6.0(x) Software (continued)

Cisco NX-OS Release Support							
Hardware	**Part Number**	**5.2(1)N1(5a) 5.2(1)N1(5) 5.2(1)N1(4) 5.2(1)N1(3) 5.2(1)N1(2a) 5.2(1)N1(2) 5.2(1)N1(1b) 5.2(1)N1(1a) 5.2(1)N1(1)**	**5.1(3)N2(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 2000 Series							
Cisco Nexus B22DELL FEX[2]	N2K-B22DELL-P	X	—	—	—	—	—
Cisco Nexus 2248PQ FEX[3]	N2K-C2248PQ-10GE	—	—	—	—	—	—
Cisco Nexus 2232TM-E FEX[4]	N2K-C2232TM-E-10GE	X	—	—	—	—	—
Cisco Nexus B22F FEX	N2K-B22FTS-P	X	—	—	—	—	—
Cisco Nexus B22HP FEX[5]	N2K-B22HP-P	X	X	X	X		
Cisco Nexus 2232TM FEX	N2K-C2232TM-10GE	X	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	X	—	—	—
Cisco Nexus 2248TP FEX	N2K-C2248TP-1GE	X	X	X	X	X	X
Cisco Nexus 2232TP FEX					X	X	X
Cisco Nexus 2232TT FEX					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
Cisco Nexus 2020T FEX							
Expansion Modules							
4-port QSFP+ 10GBE GEM	N55-M4Q	—	—	—	—	—	—

Table 3 Hardware Supported by Cisco NX-OS Release 6.0(x) Software (continued)

Cisco NX-OS Release Support							
Hardware	**Part Number**	**5.2(1)N1(5a) 5.2(1)N1(5) 5.2(1)N1(4) 5.2(1)N1(3) 5.2(1)N1(2a) 5.2(1)N1(2) 5.2(1)N1(1b) 5.2(1)N1(1a) 5.2(1)N1(1)**	**5.1(3)N2(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)**
12-port 10GBASE-T GEM[6]	N55-M12T	X	—	—	—	—	—
16-port Universal GEM	N55-M16UP(=)	X	X	X	X	X	—
N5596 Layer 3 GEM	N55-M160L3(=)	X	X	X	X	X	—
N5548 Layer 3 daughter card	N55-D160L3(=)	X	X	X	X	X	—
Layer 3 GEM	N55-M160L3-V2	X	X	X			
Version 2 Layer 3 daughter card	N55-D160L3-V2	X	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 6000 Series connectivity)	FET-10G(=)	X	X	X	X	X	X
SFP+ Optical							
Cisco 40GBASE-LR4 QSFP+ Module for SMF	QSFP-40GE-LR4						
4x10-Gigabit QSFP module	QSFP-4SFP10G-CU1M						
4x10-Gigabit QSFP module	QSFP-4SFP10G-CU3M						
4x10-Gigabit QSFP module	QSFP-4SFP10G-CU5M						

Table 3 Hardware Supported by Cisco NX-OS Release 6.0(x) Software (continued)

Cisco NX-OS Release Support							
Hardware	Part Number	5.2(1)N1(5a) 5.2(1)N1(5) 5.2(1)N1(4) 5.2(1)N1(3) 5.2(1)N1(2a) 5.2(1)N1(2) 5.2(1)N1(1b) 5.2(1)N1(1a) 5.2(1)N1(1)	5.1(3)N2(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)
4x10-Gigabit QSFP module	QSFP-4SFP10G-ACu7M						
4x10-Gigabit QSFP module	QSFP-4SFP10G-ACu10M						
Cisco 40GBASE-CR4 QSFP+ to 4 10GBASE-CU SFP+ direct-attach breakout 7-meter cable, active	QSFP-4X10G-AC7M						
Cisco 40GBASE-CR4 QSFP+ to 4 10GBASE-CU SFP+ direct-attach breakout 10-meter cable, active	QSFP-4X10G-AC10M						
Gigabit Ethernet SFP, LX transceiver[7]	GLC-LX-SMD						
Gigabit Ethernet SFP, EX transceiver[8]	GLC-EX-SMD						
1000BASE-ZX SFP transceiver module for SMF	GLC-ZX-SM(=)	X					
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	X			
1000BASE-T standard	GLC-T(=)	X	X	X	X	X	X
Gigabit Ethernet SFP, LC connector SX transceiver (MMF)	GLC-SX-MM	X	X	X	X	X	X

Table 3 Hardware Supported by Cisco NX-OS Release 6.0(x) Software (continued)

Cisco NX-OS Release Support							
Hardware	**Part Number**	**5.2(1)N1(5a) 5.2(1)N1(5) 5.2(1)N1(4) 5.2(1)N1(3) 5.2(1)N1(2a) 5.2(1)N1(2) 5.2(1)N1(1b) 5.2(1)N1(1a) 5.2(1)N1(1)**	**5.1(3)N2(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 SX transceiver (MMF), extended temperature range and DOM	GLC-SX-MMD	X	X	X	X	X	X
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF)	GLC-LH-SM	X	X	X	X	X	X
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF), extended temperature range and DOM	GLC-LH-SMD	X	X	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
10GBASE CU SFP+ cable[9]	SFP-H10GB-CU1.5M						
10GBASE CU SFP+ cable[10]	SFP-H10GB-CU2M						
10GBASE CU SFP+ cable[11]	SFP-H10GB-CU2.5M						
Fibre Channel							
8-Gbps Fibre Channel—short wavelength	DS-SFP-FC8G-SW(=)	X	X	X	X	X	X

Table 3 Hardware Supported by Cisco NX-OS Release 6.0(x) Software (continued)

Cisco NX-OS Release Support							
Hardware	**Part Number**	**5.2(1)N1(5a) 5.2(1)N1(5) 5.2(1)N1(4) 5.2(1)N1(3) 5.2(1)N1(2a) 5.2(1)N1(2) 5.2(1)N1(1b) 5.2(1)N1(1a) 5.2(1)N1(1)**	**5.1(3)N2(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)**
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 Channel, Gray	DS-CWDM4G1470(=)	X	X				
1490 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Violet	DS-CWDM4G1490(=)	X	X				
1510 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Blue	DS-CWDM4G1510(=)	X	X				
1530 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Green	DS-CWDM4G1530(=)	X	X				
1550 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Yellow	DS-CWDM4G1550(=)	X	X				
1570 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Orange	DS-CWDM4G1570(=)	X	X				
1590 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Red	DS-CWDM4G1590(=)	X	X				
1610 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Brown	DS-CWDM4G1610(=)	X	X				

Table 3 Hardware Supported by Cisco NX-OS Release 6.0(x) Software (continued)

Cisco NX-OS Release Support							
Hardware	Part Number	5.2(1)N1(5a) 5.2(1)N1(5) 5.2(1)N1(4) 5.2(1)N1(3) 5.2(1)N1(2a) 5.2(1)N1(2) 5.2(1)N1(1b) 5.2(1)N1(1a) 5.2(1)N1(1)	5.1(3)N2(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)
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[12]		X	X	X	X	X	X

1. The Cisco Nexus 5596T and the 12-port 10-GBase-T GEM are supported starting with Cisco NX-OS Release 5.2(1)N1(1b).
2. The Cisco Nexus B22DELL P FEX is supported starting with Cisco NX-OS Release 5.2(1)N1(3).
3. The Cisco Nexus 2248PQ FEX does not support Gen1 cables.
4. The Cisco Nexus 2232TM-E FEX is supported starting with Cisco NX-OS Release 5.2(1)N1(1a).
5. The Cisco Nexus B22HP FEX is supported starting with Cisco NX-OS Release 5.0(3)N2(2).
6. The 12 port 10-GBASE-T GEM is only supported on the Cisco Nexus 5596T starting with Cisco NX-OS Release 5.2(1)N1(1b).
7. Added support for Gibabit Ethernet SFP LX transceiver starting with Cisco NX-OS Release 6.0(2)N1(2).
8. Added support for Gibabit Ethernet SFP EX transceiver starting with Cisco NX-OS Release 6.0(2)N1(2).
9. Added support for 10GBASE CU SFP+ cable starting with Cisco NX-OS Release 6.0(2)N1(2).
10. Added support for 10GBASE CU SFP+ cable starting with Cisco NX-OS Release 6.0(2)N1(2).
11. Added support for 10GBASE CU SFP+ cable starting with Cisco NX-OS Release 6.0(2)N1(2).
12. 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 4 shows the hardware and Cisco NX-OS Release 6.x software that supports online insertion and removal (OIR).

Table 4 Online Insertion and Removable Support by Cisco NX-OS Release 6.x Software

Hardware	Part Number	Cisco NX-OS Release Support						
		6.0(2)N2(7) 6.0(2)N2(6) 6.0(2)N2(5a) 6.0(2)N2(5) 6.0(2)N2(4) 6.0(2)N2(3) 6.0(2)N2(1b) 6.0(2)N2(2) 6.0(2)N2(1) 6.0(2)N1(2) 6.0(2)N1(1)	**5.2(1)N1(3), 5.2(1)N1(2a) 5.2(1)N1(2), 5.2(1)N1(1b) 5.2(1)N1(1a) 5.2(1)N1(1)**	**5.1(3)N2(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 5500 Series								
Cisco Nexus 5596UP switch	N5K-C5596UP-FA	X	X	X	X	X	—	—
Cisco Nexus 5548UP switch	N5K-C5548UP-FA	X	X	X	X	X	—	—
Cisco Nexus 5548P switch	N5K-C5548P-FA	X	X	X	X	X	X	X
Cisco Nexus 5010T switch						X	X	X
Cisco Nexus 2020T FEX								
Expansion Modules								
16-port Universal GEM	N55-M16UP(=)	X	X	X	X	X	X	—
Layer 3 GEM[1]	N55-M160L3-V2[1]	—	—	—	—	—	—	—
Version 2 Layer 3 daughter card[1]	N55-D160L3-V2[1]	—	—	—	—	—	—	—
16-port SFP+ Ethernet	N55-M16P(=)	X	X	X	X	X	X	—
8-port SFP+ Ethernet ports and 8-port SFP+ Fibre Channel ports	N55-M8P8FPL(=)	X	X	X	X	X	X	—
N5596 Layer 3 GEM[1]	N55-M160L3(=)[1]	—	—	—	—	—	—	—
N5548 Layer 3 daughter card[1]	N55-D160L3(=)[1]	—	—	—	—	—	—	—

1. Does not support online insertion and removal. You must power down the Cisco Nexus 5500 Series switch before removing or inserting a Layer 3 GEM or Version 2 Layer 3 daughter card expansion module.

New and Changed Features

This section describes the new features introduced in Cisco NX-OS Release 6.x. This section includes the following topics:

New Software Features in Cisco NX-OS Release 6.0(2)N2(7)

There are no new software features in this release.

New Software Features in Cisco NX-OS Release 6.0(2)N2(6)

There are no new software features in this release.

New Software Features in Cisco NX-OS Release 6.0(2)N2(5a)

There are no new software features in this release.

New Software Features in Cisco NX-OS Release 6.0(2)N2(5)

There are no new software features in this release.

New Software Features in Cisco NX-OS Release 6.0(2)N2(4)

There are no new software features in this release.

New Software Features in Cisco NX-OS Release 6.0(2)N2(3)

There are no new software features in this release.

New Software Features in Cisco NX-OS Release 6.0(2)N2(2)

Cisco NX-OS Release 6.0(2)N2(2) is a maintenance release that includes bug fixes and the following software features and enhancements:

- Command Addition: cts role-based batched-programming, page 19

Command Addition: cts role-based batched-programming

Enabling CTS Batch Programming by entering the **cts role-based batched-programming** command enables faster programming on SGACLs associated with large numbers of SGT,DGT pairs.

New Software Features in Cisco NX-OS Release 6.0(2)N2(1)

Cisco NX-OS Release 6.0(2)N2(1) is a maintenance release that includes bug fixes and the following software features and enhancements:

- Bidirectional Forwarding Detection, page 19
- Command Update: show lldp system -detail, page 20
- Default Interface, page 20
- Embedded Event Manager Support, page 20
- Network Time Protocol Server, page 20
- Policy Based Routing, page 20
- DHCPv4-relay and DHCPv6-relay, page 20
- FEX Host Interface Storm Control, page 20
- Scalability Enhancements, page 20
- SNMP Bridge-MIB and LLDP MIB, page 21
- vPC Shutdown, page 21
- vPC+ Routing Protocol Peering, page 21

Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast forwarding-path failure detection times for media types, encapsulations, topologies, and routing protocols. Starting with Release 6.0(2)N2(1), the Cisco Nexus 5500 supports BFD for BGP, EIGRP, OSPF, PIM, HSRP, VRRP, and static routes.

Command Update: show lldp system -detail

The **show lldp** command now includes an optional keyword for displaying system details.

Default Interface

You can use the **default interface** command to clear the existing configuration of multiple interfaces and return them to default settings. The command can be used for interfaces such as Ethernet, loopback, VLAN network, port-channel, and tunnel interfaces. You can use the **checkpoint** keyword with the command to create a copy of the interface configuration before clearing it so that you can restore it later.

Embedded Event Manager Support

The Embedded Event Manager (EEM) monitors events that occur on your device and takes action to recover from or troubleshoot these events, based on your configuration. You can use EEM to create policies that consist of a set of actions to be taken in response to a specific event. EEM can be controlled through CLI commands or Vsh scripts.

Network Time Protocol Server

A Cisco Nexus 5500 switch can use the Network Time Protocol (NTP) to synchronize the network. Other devices can be configured to use the switch as an NTP time server. In an isolated network, the switch can be configured as an authoritative NTP clock source.

An NTP server usually receives its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server, and then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of each other.

Policy Based Routing

The Cisco Nexus 5500 now supports policy-based routing (PBR). PBR allows you to configure a defined policy for IPv4 and IPv6 traffic flows, lessening reliance on routes derived from routing protocols.

DHCPv4-relay and DHCPv6-relay

Up to 32 DHCP server addresses can now be configured on an interface. Previously, the maximum number of configurable server addresses was 16.

FEX Host Interface Storm Control

HIF Storm control allows ingress traffic suppression for unknown multicast, broadcast, and unknown unicast traffic on Fabric Extender (FEX) Host Interface (HIF) ports and port channels.

Scalability Enhancements

As documented in the release specific *Verified Scalability for Cisco Nexus 5500 Series* documents, configuration limits (verified scalability) for several Layer 2 switching functions has increased. Verified and maximum limits have changed for some features, including:

- Channels/vPCs
- EtherChannels
- IGMP Snooping groups
- Logical interfaces (PVs)
- Number of FEX ports
- Number of switchports

SNMP Bridge-MIB and LLDP MIB

SNMP Bridge and LLDP MIBs have been published.

vPC Shutdown

You can use the vPC **shutdown** command to isolate a switch from the vPC complex. The switch can then be debugged, reloaded, or removed physically, without affecting the vPC traffic going through the nonisolated switch.

vPC+ Routing Protocol Peering

Added support for routing unicast and multicast protocol over vPC+.

New Software Features in Cisco NX-OS Release 6.0(2)N1(2)

Cisco NX-OS Release 6.0(2)N1(2) is a maintenance release that includes bug fixes and the following software features and enhancements:

- 802.1x Authentication, page 21
- FEX NIF Storm Control, page 21
- IP-Directed Broadcast, page 22
- iSCSI TLV Configuration, page 22
- Port Channel Minimum Links, page 22

802.1x Authentication

Support added for the IEEE 802.1X, which provides a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

FEX NIF Storm Control

The NIF Storm Control feature allows configuration on a Satellite Fabric port to all the pinned FEX HIF ports regardless of whether it is a logical or a physical HIF. In addition, a new syslog message informs the user when a switch port that has a Storm Control configuration is starting to see a storm of broadcast, multicast, or unicast when it starts dropping packets. You see another syslog message when the storm stops.

IP-Directed Broadcast

You can use an IP-directed broadcast to send a broadcast from a device that is not directly connected to the destination IP subnet. An ACL name can be specified for the broadcast. (This resolves caveat CSCuh1963.)

iSCSI TLV Configuration

As documented in the *Cisco Nexus 5500 Series NX-OS SAN Switching Configuration Guide, Release 6.x*, NICs and converged network adapters connected to a Cisco Nexus 5500 Series switch can use iSCSI as a storage protocol and can be programmed to accept the configuration values sent by the switch leveraging data center bridging exchange protocol (DCBX). DCBX negotiates configuration and settings between the switch and the adapter through a variety of type-length-values (TLV) and sub-TLVs. This process allows the switch to distribute configuration values to all attached adapters from a centralized location instead of having to manually program CoS markings on each individual server and adapter.

Port Channel Minimum Links

Added support to configure a minimum number of links for the port channel so that when a certain number of port-channel member ports go down, the host-facing interfaces are suspended.

New Software Features in Cisco NX-OS Release 6.0(2)N1(1)

Cisco NX-OS Release 6.0(2)N1(1) includes bug fixes and the following software features and enhancements:

Ingress Policing

Policing allows you to monitor the data rates for a particular class of traffic. When the data rate exceeds user-configured values, the switch drops packets immediately. Because policing does not buffer the traffic, transmission delays are not affected. When traffic exceeds the data rate, you instruct the system to drop the packets. You can define single-rate and two-color ingress policing.

Glean Throttling

When forwarding an incoming IP packet in a line card, if the Address Resolution Protocol (ARP) request for the next hop is not resolved, the line card forwards the packets to the supervisor, referred to as glean throttling. The supervisor resolves the MAC address for the next hop and programs the hardware.

The Cisco Nexus 5500 Series device hardware has glean rate limiters to protect the supervisor from the glean traffic. If the maximum number of entries is exceeded, the packets for which the ARP request is not resolved continues to be processed in the software instead of getting dropped in the hardware.

When an ARP request is sent, the software adds a /32 drop adjacency in the hardware to prevent the packets to the same next-hop IP address from being forwarded to the supervisor. When the ARP entry is resolved, the hardware entry is updated with the correct MAC address. If the ARP entry is not resolved before a timeout period, the entry is removed from the hardware.

ACL Logging

The ACL logging feature allows the logging of packets that hit the IPv4 ACLs. The log messages are displayed on a flow basis. The flow is identified using a combination of the IP source address, destination address, L4 protocol, and the L4 source/destination ports on an interface. The log message is generated under the following conditions:

- INFO message—When a new flow is created
- WARNING message—When the packet threshold is reached for a flow
- Configurable INFO message—At the end of a periodic interval containing information on the number of packets to hit the flow. The interval default is 5 minutes.

The log keyword is not supported with any permit statement for PACL or RACL. The log keyword is supported only with deny statements.

Table 5 ACL Logging Support Table

Nexus 5500		**Nexus 5600/6000**		
	Logging Support		Logging Support	
PACL	Yes	Drop only	Yes	Drop only
Ingress RACL			Yes	Drop only
Egress RACL	Yes	Drop only	Yes	Drop only
VACL	Yes (action Drop log also supported)	Drop only	Yes	Drop only
RBACL	Yes (SW logging)	Permit/Drop	N/A	
vty ACL	Yes	Permit/Drop	Yes	Permit/Drop
Ingress RACL on mgmt 0	Yes	Permit/Drop	Yes	Permit/Drop

Note When the number of flows exceed a threshold in the given interval, a warning message is logged, and that flow is not added to the logging cache.

POAP Enhancement

POAP enhancements include hostname- and MAC address-based configuration file selection, TCL or Python script logging, and a remote syslog facility.

BGP Enhancement

BGP enhancements include BGP Allow-AS-in, local-AS, prefix-peering, AS-path relax, and remove-private-AS.

VRF Route Leaking

Support for VRF route leaking enables the sharing of routes that were previously visible and available only in segmented networks.

FCoE over 10GBASE-T

FCoE configuration is supported over 10GBASE-T using Cat6a and Cat7 cables up to a distance of 30 m.

Open Management Infrastructure

The Open Management Infrastructure (OMI) agent is a web server that runs on the Cisco Nexus switch. It is based on the Common Infrastructure Model (CIM) standard, which is an open standard that defines a schema for representing managed resources (for example, CPUs, disks, networks, processes, and so on.). The OMI agent enables you to perform the following operations:

New Hardware Features in Cisco NX-OS Release 6.0(2)N2(7)

No new hardware features have been introduced with this release.

New Hardware Features in Cisco NX-OS Release 6.0(2)N2(6)

No new hardware features have been introduced with this release.

New Hardware Features in Cisco NX-OS Release 6.0(2)N2(5a)

No new hardware features have been introduced with this release.

New Hardware Features in Cisco NX-OS Release 6.0(2)N2(5)

Cisco NX-OS Release 6.0(2)N2(5) supports the following new hardware:

- QSA Optics with 10G SR

New Hardware Features in Cisco NX-OS Release 6.0(2)N2(1b)

Cisco NX-OS Release 6.0(2)N2(1b) supports the following new hardware:

- N2K-B22IBM-P—Cisco Nexus B22 Fabric Extender for IBM

New Hardware Features in Cisco NX-OS Release 6.0(2)N2(1)

No new hardware features have been introduced with this release.

New Hardware Features in Cisco NX-OS Release 6.0(2)N1(2)

Cisco NX-OS Release 6.0(2)N1(2) supports the following new hardware:

- 4-port QSFP+ Nexus N55-M4Q GEM
- New power supplies for Cisco Nexus 5596T and Cisco Nexus 5596UP switches:
  - Cisco Nexus 1100 W AC front-to-back power supply (PID: NXA-PAC-1100W)
  - Cisco Nexus 1100 W AC back-to-front power supply (PID: NXA-PAC-1100W-B)
  - Cisco Nexus 1100 W DC front-to-back power supply (PID: N55-PDC-1100W)
- New transceivers:
  - QSFP-4X10G-AC7M
  - QSFP-4X10G-AC10M
  - QSFP-40G-LR4
  - SFP-H10GB-CU1.5M
  - SFP-H10GB-CU2M
  - SFP-H10GB-CU2.5M
  - GLC-LH-SMD
  - GLC-EX-SMD

New Hardware Features in Cisco NX-OS Release 6.0(2)N1(1)

Cisco NX-OS Release 6.0(2)N1(1) supports the following new hardware:

- Cisco Nexus 2248PQ 10-Gigabit FEX

New Hardware Features

This section describes the following new hardware:

- Cisco Nexus 2248TP-E Fabric Extender, page 25
- Cisco Nexus 5000 Series Expansion Modules, page 26
- ER Optics Support, page 26

Cisco Nexus 2248TP-E Fabric Extender

The new Cisco Nexus 2248TP-E Fabric Extender is a 1-RU, general purpose 100-Mb/1-G FEX that is optimized for specialized data center workloads such as data, distributed storage, distributed computing, market data, and video editing. The Cisco Nexus 2248TP-E FEX has 48x1 Gigabit Ethernet host ports and 4x10 Gigabit Ethernet uplinks. It supports all of the existing features and topologies as the Cisco

Nexus 2248 and the Cisco Nexus 2148 support. In addition, the Cisco Nexus 2248TP-E offers rich counters for troubleshooting and capacity monitoring. It has a user-configurable shared buffer, and it has a per-port ingress and egress queue limit.

For detailed information about the Cisco Nexus 2248TP-E FEX, see the *Cisco Nexus 2000 Series Hardware Installation Guide.*

Cisco Nexus 5000 Series Expansion Modules

Two new Generic Expansion Modules (GEM) are being released:

- Layer 3 GEM, N55-M160L3-V2
- Layer 3 I/O Module, N55-D160L3-V2

ER Optics Support

The 10-Gigabit Ethernet, extended range SFP+ module (SFP-10G-ER) supports a link length of up to 40 kilometers on standard single-mode fiber (SMF, G.652). All Cisco Nexus 5500 switches and all Cisco FEX models support the new SFP-10G-ER optic.

Note Cisco Nexus 2232 FEX does not support the SFP+ module on the HIF port.

New Software Features—Cisco Nexus 5500 Switch

Cisco NX-OS Release 5.1(3)N1(1) supports the following new software features only on the Cisco Nexus 5500 switch:

- Cisco FabricPath, page 26
- Cisco TrustSec, page 27
- Adapter FEX, page 28
- VM-FEX, page 28
- Support for FCoE on a Dual Homed FEX, page 29
- CoPP, page 29
- Enhanced vPC Support, page 30
- IP ARP Synchronization, page 30
- Management SVI, page 30

Cisco FabricPath

Cisco FabricPath is a set of multipath Ethernet technologies that combine the reliability and scalability benefits of Layer 3 routing with the flexibility of Layer 2 networks, which enables it to build scalable data centers. Cisco FabricPath offers a topology-based Layer 2 routing mechanism that provides an equal-cost multipath (ECMP) forwarding model. Cisco NX-OS Release 5.1(3)N1(1) supports one FabricPath topology.

The FabricPath feature provides the following:

- Allows Layer 2 multipathing in the FabricPath network.

- Provides built-in loop prevention and mitigation with no need to use the Spanning Tree Protocol (STP).
- Provides a single control plane for unknown unicast, unicast, broadcast, and multicast traffic.
- Enhances mobility and virtualization in the FabricPath network.

The FabricPath network uses the Layer 2 Intermediate System-to-Intermediate System (IS-IS) protocol to forward traffic in the network using the FabricPath headers. Layer 2 IS-IS is different than Layer 3 IS-IS; the two protocols work independently. Layer 2 IS-IS requires no configuration and becomes operational when you enable FabricPath on the device. The frames carry the same FTag that is assigned at ingress throughout the FabricPath network, and Layer 2 IS-IS allows all devices to have the same view of all the trees built by the system. Known unicast traffic uses the Equal Cost Multipath Protocol (ECMP) to forward traffic throughout the network. The system automatically load balances traffic throughout the FabricPath network by using ECMP and the trees.

Cisco FabricPath is supported on all Cisco Nexus 5500 switches (N5K-C5596UP-FA, N5K-C5548UP-FA, and N5K-C5548P-FA). The switch must be running Cisco NX-OS Release 5.1(3)N1(1). In addition, Cisco FabricPath requires the Enhanced Layer 2 license. For licensing information, see the *License and Copyright Information for Cisco NX-OS Software* document.

For detailed information about Cisco FabricPath, see the *Cisco Nexus 5000 Series NX-OS FabricPath Configuration Guide.*

Cisco TrustSec

The Cisco TrustSec security architecture builds secure networks by establishing clouds of trusted network devices. Cisco TrustSec also uses the device information acquired during authentication for classifying, or coloring, the packets as they enter the network. This packet classification is maintained by tagging packets on ingress to the Cisco TrustSec network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path. The tag, also called the security group tag (SGT), allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT to filter traffic.

For more information about Cisco TrustSec, see the *Cisco Nexus 5000 Series NX-OS Security Configuration Guide.*

IEEE 1588 Time Synchronization

IEEE 1588 or Precision Time Protocol (PTP) is a time synchronization protocol for nodes distributed across a network. Its hardware timestamp feature provides greater accuracy than other time synchronization protocols such as Network Time Protocol (NTP).

A PTP system can consist of a combination of PTP and non-PTP devices. PTP devices include ordinary clocks, boundary clocks, and transparent clocks. Non-PTP devices include ordinary network switches, routers, and other infrastructure devices.

PTP is a distributed protocol that specifies how real-time PTP clocks in the system synchronize with each other. These clocks are organized into a master-member synchronization hierarchy with the grandmaster clock, the clock at the top of the hierarchy, determining the reference time for the entire system. Synchronization is achieved by exchanging PTP timing messages, with the members using the timing information to adjust their clocks to the time of their master in the hierarchy. PTP operates within a logical scope called a PTP domain.

Adapter FEX

Cisco is introducing Adapter-FEX support on the Cisco Nexus 5500 platform and on Cisco Nexus 2200 FEXes that are connected to a Cisco Nexus 5500 parent switch. The Cisco NX-OS Adapter-FEX feature provides the advantages of the FEX Link architecture with that of server I/O virtualization to create multiple virtual interfaces over a single Ethernet interface. This allows the deployment of a dual port NIC on the server and the ability to configure more than two virtual interfaces that the server sees as a regular Ethernet interface. The advantage of this approach is a reduction of power and cooling requirements and a reduction of the number of network ports.

The Adapter-FEX implementation is designed to work on a variety of FEX-capable adapters including the Cisco adapter for Cisco UCS C-Series Platform (UCS P81E VIC) and third-party adapters that implement VNTag technology. For additional, see Cisco UCS C-Series documentation.

Adapter-FEX supports FCoE when a VIC-enabled adapter is attached to a Cisco Nexus 2000 FEX or directly to a Cisco Nexus 5000 Series switch.

Adapter-FEX at the access layer needs a FEX-enabled adapter in a server that connects to a parent switch that supports Adapter-FEX functionality. There are two adapters that support Adapter-FEX functionality:

- Cisco UCS P81E Virtual Interface Card
- Broadcom NIV Adapter

Note Adapter FEX does not support SPAN and cannot be used as a SPAN source.

For detailed information about Adapter-FEX, see the *Cisco Nexus 5000 Series NX-OS Adapter-FEX Configuration Guide.*

VM-FEX

The VM-FEX is an extension of the FEX that extends to the VIC virtual interface card (VIC) in the server. It simulates ports and enables a high-speed link between the switch and the server. The VM-FEX consolidates the virtual and physical network. Each VM gets a dedicated port on the switch. In addition, the VM-FEX provides for vCenter management of Adapter-FEX interfaces.

The VM-FEX solution provides the following benefits:

- Policy-based VM connectivity
- Mobility of network and security properties
- A nondisruptive operation model

VM-FEX does not support SPAN and cannot be used as a SPAN source.

VM-FEX does not support FCoE in NPV mode. Support for this feature will be available when CSCts09434 is resolved, which is expected in the next maintenance release of VMware ESX 5.0.

For more information about VM-FEX, see the *Cisco Nexus 5000 Series NX-OS Layer2 Switching Configuration Guide.*

Support for FCoE on a Dual Homed FEX

The Cisco Adapter FEX with FCoE feature allows you to create an FCoE connection to a Cisco Nexus 2000 Series Fabric Extender (FEX), which can then establish an FCoE connection to a server with a virtual interface card (VIC) adapter. The switch connects to the FEX through a virtual port channel (vPC) while the FEX connects to the server using a standard FCoE link between the FEX and the VIC adapter.

If you are using Enhanced vPC, the FEX can be associated with one and only one Cisco Nexus 5000 fabric for FCoE forwarding.

If you are using FabricPath, you must use a dedicated link for FCoE traffic.

If you are using a Cisco UCS C-Series Rack-Mount Server with a Cisco UCS P81E Virtual Interface Card (VIC):

- The VIC must be configured in Network Interface Virtualization (NIV) mode, which makes the two unified ports appear to the system as virtual host bus adapters (vHBAs).
- The VIC cannot be connected to the FEX through a VNP port. If this type of connection is used, NIV mode cannot be enabled on the VIC.
- The NIC mode on the Cisco UCS C-Series Rack-Mount Server must be set to active-standby.
- If you deploy FCoE over Adapter FEX on a server with a Cisco UCS P81E Virtual Interface Card (VIC) and that is running Windows 2008, you must install new versions of software drivers.

For more information about support for FCoE on Dual Homed FEX, see the *Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide.*

CoPP

Control Plane Policing (CoPP) provides QoS-based prioritization and protection of control plane traffic that arrives at the switch in the data plane, which ensures network stability, reachability, and packet delivery.

Cisco NX-OS Release 5.1(3)N1(1) provides several predefined CoPP policies that administrators can deploy for different environments. In these predefined CoPP policies, the classification of flows is predetermined and the policing rates for the flows is fixed. In addition, there is one flexible CoPP policy for cases where predefined policies do not address the needs of the deployment.

The CoPP implementation on Cisco Nexus 5500 Series switches provides three predefined COPP policies for different deployment environments.

- Default
- Scaled-Layer 2
- Scaled-Layer 3
- Customized Policy

The CoPP policies can be changed at run time like any other QoS configuration. Classification of flows is predetermined and cannot be modified. Policing rates for the flows is fixed and cannot be modified.

For additional information about CoPP, see the *Cisco Nexus 5000 Series NX-OS Security Configuration Guide.*

Enhanced vPC Support

Enhanced vPC (EvPC) provides a uniform access layer for any server to any FEX in hybrid deployments. In addition, EvPC provides data, control plane, and management plane redundancy. A new vPC option allows port channel connectivity to dual-homed FEXes.

The Cisco Nexus 2000 Series Fabric Extender (FEX) that contains the port assigned to the vPC must be associated with the Cisco Nexus switch.

The CNA must be attached to the Cisco Nexus 2000 Series FEX rather than directly to the Cisco Nexus 5000 Series switch.

If you want to ensure backward compatibility for all previous configurations and supported topologies, you must configure the FEX in a straight-through FEX topology that does not use Enhanced vPC.

Note Enhanced vPC does not support SPAN and cannot be used as a SPAN source.

For more information about EvPC, see the *Cisco Nexus 5000 Layer 2 Switching Configuration Guide.*

IP ARP Synchronization

Cisco NX-OS Release 5.1(3)N1(1) introduces the **ip arp synchronize** command.When this command is enabled, faster convergence of address tables between the vPC peers is possible. This convergence is designed to overcome the delay involved in ARP table restoration when the peer-link port channel flaps or when a vPC peer comes back online.

Enabling ARP synchronization improves convergence times during the restart of a vPC peer when a Cisco Nexus 5000 Series switch acts as a default gateway. By default, ARP synchronization is not enabled.

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

Management SVI

A switch virtual interface (SVI) is a VLAN of switch ports represented by one interface to a routing or bridging system. The SVI can be configured for routing, in which case it supports Layer 3 protocols for processing packets from all switch ports associated with the VLAN, or for in-band management of the switch.

Starting with Release 5.1(3)N1(1), the NX-OS switch has specific support for management SVIs. Having different SVIs for routing and management separates data traffic from management traffic, which can reduce competition for routing resources. If you are using an SVI for management purposes, we recommend that you specifically configure your SVI for management using the **management** command so that you can take advantage of this added functionality.

With this change, there are new guidelines and limitations for routed SVIs:

- Although the CLI does not prevent you from configuring routing protocols on a management SVI, we recommend that you do not configure them on management SVIs.
- Routed SVIs that are being used for management (that is, routed SVIs that have not been specifically configured for management using the **management** command) can still be used for management as long as the Layer 3 license is not installed.
- Management SVIs do not support configuration synchronization mode (config-sync). Configuration synchronization is performed using the mgmt 0 interface.

- RACL is not supported. Use VACL to filter the management traffic.

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

New Software Features—Cisco Nexus 5000 Series Switches

Cisco NX-OS Release 5.1(3)N1(1) supports the following new software features on all Cisco Nexus 5000 Series switches:

ERSPAN

Encapsulated Remote Switched Port Analyzer (ERSPAN) introduces an additional level of flexibility to the powerful network monitoring capabilities of SPAN and RSPAN. ERSPAN allows the analyzer to be placed on one location and multiple switches can send mirrored traffic to this analyzer. Traffic from any port on the network on any remote switch can be analyzed without physically moving the analyzer tool.

- ERSPAN encapsulates SPAN traffic to IP-GRE frame format and allows remote monitoring traffic over an IP network.
- All Cisco Nexus 5000 Series switches, including Cisco Nexus 5500 switches, support ERSPAN.
- Cisco NX-OS Release 5.1(3)N1(1) supports an ERSPAN source session only; there is no support for an ERSPAN destination session. The Cisco Nexus 5000 Series switch hardware cannot deencapsulate an ERSPAN frame.
- ERSPN does not require a Layer 3 module and Layer 3 license.
- The Cisco Nexus 5010 and Nexus 5020 switches support two active ERSPAN sessions. The Cisco Nexus 5548P, Nexus 5548UP, and Nexus 5596UP switch support four active ERSPAN sessions.

For more information about ERSPAN, see the *Cisco Nexus 5000 Series NX-OS System Management Configuration Guide.*

Multicast VLAN Registration

Multicast VLAN Registration (MVR) allows a Layer 2 switch to deliver a multicast packet received from one VLAN to multiple receivers that reside in different VLANs, without Layer 3 replication.

MVR offers the following advantages:

- It reduces the overhead of Layer 3 multicast replication on a multicast router.
- It reduces the bandwidth consumption for the link between the Layer 2 switch and the multicast router.
- It reduces the multicast forwarding table size on the Layer 2 switch.

All models of Cisco Nexus 5000 Series switches support MVR.

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

Port Security

Port security is a simple Ethernet MAC-based security feature that can restrict input to an interface by limiting and identifying MAC addresses of the end host that are allowed to access the port. Cisco NX-OS Release 5.1(3)N1(1) adds port security to the Cisco Nexus 5000 Series and Cisco Nexus 2000 Series, and it is available on both Cisco Nexus 5000 and Nexus 5500 switches. Port security supports the following features:

- It supports both physical ports and port channels.
- It supports vPC ports for the first time in Cisco NX-OS, and only in the Cisco Nexus 5000 Series. (Port security support for vPC ports is not available in the Cisco Nexus 7000 Series, although the port security feature itself is supported on that platform.)
- It supports EvPC ports.
- It does not support NIV ports.

A device maximum of 8192 secure MAC addresses in addition to one MAC address per port is supported. The interface maximum is 1025 MAC addresses per interface.

For additional information about the port security feature, see the *Cisco Nexus 5000 NX-OS Security Configuration Guide.*

FCoE Over Enhanced vPC

Beginning with the Cisco NXOS Release 5.1(3)N1(1) release, Cisco Nexus 5000 switches support FCoE on Enhanced vPC (eVPC). In a topology that uses FCoE with eVPC, the SAN fabrics must remain isolated. Therefore, each Cisco Nexus 2000 Fabric Extender in the system must be associated with one and only one Cisco Nexus 5000 Series switch. This guarantees that every time a Fabric Extender forwards FCoE traffic, it forwards it to the same Nexus 5000 switch.

For more information about FCoE over Enhanced vPC, see the *Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide.*

Boot from SAN with vPC

Cisco Nexus Series 5000 switches support SAN boot with vPC. A VFC interface must be bound to a vPC member physical interface (and not to the vPC port-channel interface itself) for a SAN boot to occur.

For more information about SAN boot with vPC, see the *Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide.*

Config-Sync Enhancements

Config-sync allows you to synchronize the configuration between a pair of vPC switches. It eliminates downtime due to vPC inconsistencies, simplifies vPC operations, and reduces administrative overhead.

The enhancements to config-sync in Cisco NX-OS Release 5.1(3)N1(1) remove the port channel configuration restriction that previously existed. All port channels and member interfaces should be configured inside a switch profile.

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

SNMP over IPv6

Cisco NX-OS Release 5.1(3)N1(1) supports SNMP over IPv6.

For more information, see the *Cisco Nexus 5000 Series NX-OS System Management Configuration Guide.*

Support for Eight Syslog Servers

In Cisco NX-OS Release 5.1(3)N1(1), you can configure up to eight syslog servers. You use the Cisco Fabric Services (CFS) to distribute the syslog server configuration; however, CFS distribution of the syslog server configuration is limited to three servers.

For more information, see the *Cisco Nexus 5000 Series NX-OS System Management Configuration Guide.*

Upgrading or Downgrading to a New Release

This section describes the upgrade and downgrade paths that are supported for Cisco NX-OS Release 6.0(2)N2(7) on the Cisco Nexus device.

The section includes the following topics:

Upgrade and Downgrade Guidelines

The following guidelines apply to Cisco NX-OS Release 6.0(2)N2(7) for Cisco Nexus devices:

- If host interface (HIF) port channels or EvPCs are configured in the system, and if the system was already upgraded to NX-OS Release 5.1(3)N1(1) or Release 5.1(3)N1(1a) from any release earlier than Release 5.1(3)N1(1), ensure that the system was reloaded at least once before you upgrade to Release 5.1(3)N2(1a) or Release 5.1(3)N2(1). If the switch was not previously reloaded, reload it and upgrade to Release 5.1(3)N2(1a) or Release 5.1(3)N2(1).
- When a Layer 3 license is installed, the Cisco Nexus 5500 Platform does not support an ISSU. Hot swapping a Layer 3 module, for example, the Layer-3 GEM (N55-M160L3-V2) or Version 2 Layer 3 daughter card (N55-D160L3-V2), is not supported. You must power down the Cisco Nexus device before removing or inserting a Layer-3 expansion module.
- In a vPC topology STP disputes occur in upstream devices when:

  - you upgrade one node of the Cisco Nexus 5500/6000 series device from Cisco NX-OS Release 6.0 or earlier release versions to Cisco NX-OS Release 7.0 versions
  - the other node still runs Cisco NX-OS Release 6.0 or earlier release versions
  - vPC primary switch is upgraded first to Cisco NX-OS Release 7.0 versions

  It is recommended that you upgrade both the nodes to Cisco NX-OS Release 7.0 version to

overcome this known issue. This issue is seen only when there is a NX-OS mismatch in the vPC pair of Cisco Nexus 5500/6000 series devices. This issue is resolved in Cisco NX-OS Release 7.0(6)N1(1). See CSCuo74024 for details.

- In a vPC topology STP disputes occur in upstream devices when:

  - the upgraded switch is operating as vPC primary
  - you upgrade from Cisco NX-OS Release 5.2 version to Cisco NX-OS Release 7.0 version
  - STP BPDU packets are sent from the root towards vPC secondary node, and then synced across peer-link to vPC primary
  - vPC secondary is already upgraded to the Cisco NX-OS Release 7.0 version
  - you perform non-disruptive ISSU upgrade

  This is a known issue. It is recommended that you try performing a disruptive upgrade to overcome this issue. See CSCuo74024 for details.

Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 6.0(2)N2(7)

Table 6 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 6.0(2)N2(7). For more information, see the *Cisco Nexus 5500 Series NX-OS Software Upgrade and Downgrade Guide, Release 6.0(2)N2(7)*.

For other 6.0 releases, see the *Cisco Nexus 5500 Series NX-OS Software Upgrade and Downgrade Guide* specific for that release at: http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-guides-list.html.

Table 6 Supported Upgrade and Downgrade Paths for Cisco NX-OS Release 6.0(2)N2(7)

Current Cisco NX-OS Release	Upgrade to NX-OS Release 6.0(2)N2(7)	Downgrade from NX-OS Release 6.0(2)N2(7)
6.0(2)N2(6) 6.0(2)N2(5a) 6.0(2)N2(5) 6.0(2)N2(4) 6.0(2)N2(3) 6.0(2)N2(2) 6.0(2)N2(1) 6.0(2)N1(2a) 6.0(2)N1(2) 6.0(2)N1(1a) 6.0(2)N1(1)	Nondisruptive upgrade (ISSU)	Disruptive downgrade
5.2(1)N1(9b) 5.2(1)N1(9a) 5.2(1)N1(9) 5.2(1)N1(8b) 5.2(1)N1(8a) 5.2(1)N1(7) 5.2(1)N1(6) 5.2(1)N1(5) 5.2(1)N1(4)	Nondisruptive upgrade (ISSU)	Disruptive downgrade

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

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

Note An upgrade from Cisco NX-OS release 5.2(1)N1(7) to 6.0(2)N2(3) or 6.0(2)N2(4) is disruptive and not supported. It is recommended to upgrade from Cisco NX-OS release 5.2(1)N1(6) to 6.0(2)N2(3) or 6.0(2)N2(4).

Note If you want to upgrade from a release, that is not listed in the "Current Cisco NX-OS Release" column of Table 6 to the latest Cisco NX-OS release version, then you must first upgrade to a release that is listed in the "Current Cisco NX-OS Release" column and then to the latest release version.

Limitations

This section describes the limitations for Cisco NX-OS Release 6.0(2)N1(7).

- Ingress inter-VLAN-routed Layer3 multicast packets are treated as "unknown multicast" by the storm-control feature. This is due to the Layer 3 forwarding design in the Cisco Nexus 5500 Series switch. For details, see CSCuh34068.
- When performing an ISSU from Cisco NX-OS Release 5.1(3)N1(1) or Cisco NX-OS Release 5.1(3)N2(1) to Cisco NX-OS Release 5.2(1)N1(1), a Forwarding Manager (FWM) core can occur, which causes the system to reset. This situation occurs when network interface virtualization (NIV) is enabled. To work around this issue, use the **force** option in the **install** command to perform a disruptive upgrade. For details, see CSCty92117.
- Starting from Cisco Release 6.0(2)N2(6), the **ip igmp join-group** command does not work any longer. The OIL will not be programmed in the hardware. You can now verify the null OIL using the **show forwarding multicast route source x.x.x.x group y.y.y.y**.
- The SAN admin user role (san-admin) is a new predefined user role in Cisco NX-OS Release 5.2(1)N1(1). If you have an existing user role with the name san-admin in Cisco NX-OS Release 5.1(3)N1(1) or Cisco NX-OS Release 5.1(3)N2(1), the new system-defined role is removed when you upgrade. To resolve this issue, downgrade to the previous release, rename the user role, and perform the upgrade. For details, see CSCua21425.
- Bridge and STP traps are displayed in the downgrade incompatibility list when you downgrade from Cisco NX-OS Release 5.2(1)N1(1) to Cisco NX-OS Release 5.0(3)N1(1c). To resolve this issue, reset the STP/Bridge trap configuration to the default settings by entering the **no snmp-server enable traps bridge**, the **no snmp-server enable traps stpx** command, and then the **copy running-config startup-config** command. For details, see CSCua75907.
- The Server Virtualization Switch (SVS) connection is not deleted during a rollback when NIV is enabled. To resolve this issue, delete the current SVS connection and reapply the original SVS connection. For details, see CSCts17033.

- If SPAN traffic is rate-limited by entering the switchport monitor rate-limit 1G command, then a maximum transmission unit (MTU) truncation size cannot be used to truncate SPAN packets. For details, see CSCua05799.
- When an FC SPAN destination port is changed from SD to F mode and back to SD mode on an 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 an 802.3x pause.

  speed 100—Does not autonegotiate; pause cannot be advertised. The peer must be set to not autonegotiate and to 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 goes 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 nonedge designated forwarding ports are not allowed for an ISSU. For additional information, see CSCtf51577. For information about topologies that support a nondisruptive upgrade, see the *Cisco Nexus 5500 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, 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 the traffic. For details, see CSCtf94558.
- When a private VLAN port is configured as a TX (egress) SPAN source, the traffic seen at the SPAN destination port is marked with the VLAN of the ingressed frame. There is no workaround.
- In large-scale configurations, some Cisco Nexus 2000 Series Fabric Extenders might take up to 3 minutes to appear online after entering the **reload** command. A configuration can be termed large-scale when the maximum permissible Cisco Nexus 2000 Series Fabric Extenders are connected to a Cisco Nexus device, 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 appear:

  ```
  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 device, we recommend that you avoid partitioning 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 device to fail. For details, see CSCty92945.
- If you upgrade a vPC peer switch from Cisco NX-OS Release 5.0(3)N2(1) to Cisco NX-OS Release 5.1(3)N2(1) or Cisco NX-OS Release 5.2(1)N1(1), and feature-set FabricPath is enabled on the upgraded switch, the vPC Peer-Link enters STP Bridge Assurance Inconsistency, which affects all VLANs except VLAN 1 and affects traffic forwarding for vPC ports.

  To avoid this issue, upgrade the peer switch that is running Cisco NX-OS Release 5.0(3)N2(1) to Cisco NX-OS Release 5.1(3)N2(1) or later release 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 the 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 because it is an active VLAN on the secondary switch.
- Rol-based Access Control List (RBACL) policy enforcement is performed on VLANs on which Cisco Trusted Security (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 5500 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 5500 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 device 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 switch virtual interface (SVI) when a switch is in FabricPath mode:
  - Use a dedicated front panel port as a vPC+ keepalive. The port should be in CE mode.
  - Use a dedicated VLAN to carry the keepalive interface. The VLAN should be a CE VLAN.
  - 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 the 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 device drops packets due to packet parsing errors. To work around this issue, enter the **vlan dot1q tag native** command 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 devices 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 devices 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, leave the speed set to 4 GB. For details, see CSCtx52991.
- A nondisruptive ISSU is not supported when ingress policing is configured.
- The maximum IP MTU that can be set on Layer 3 interfaces on which Layer 3 protocols are running is 9196, because of the internal header used inside the switch. The network-qos policy must be set to 9216.

Limitations on the Cisco Nexus Device

The limitations on the Cisco Nexus device 5500 Series devices are as follows:

SPAN Limitations on Fabric Extender Ports

The SPAN limitations on Fabric Extender ports are as follows:

- On a Cisco Nexus device, if the SPAN source is a FEX port, the frames will always be tagged when leaving the SPAN destination.
- On a Cisco Nexus 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 following error appears:

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

- When a FEX port is configured as a tx-source, the multicast traffic 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), that multicast traffic goes out on FEX ports 100/1/3–12, but not on 100/1/1–2.

  If you configure SPAN Tx on port 100/1/1, although the multicast traffic does not egress out of port 100/1/1, the SPAN destination does receive that multicast traffic, which is due to a design limitation.
- When a FEX port is configured as both SPAN rx-source and tx-source, the broadcast, non-IGMP Layer-2 multicast, and unknown unicast frames originating from that port might be seen twice on the SPAN destination: once on the ingress and once on the egress path. On the egress path, the frames are filtered by the FEX to prevent them from going out on the same port on which they were received. For example, if FEX port 100/1/1 is configured on VLAN 11 and is also configured as SPAN rx-source and tx-source and a broadcast frame is received on that port, the SPAN destination recognizes two copies of the frame, even though the frame is not sent back on port 100/1/1.

- A FEX port cannot be configured as a SPAN destination. Only a switch port can be configured and used as a SPAN destination.
- Cisco NX-OS Release 5.1(3)N2(1) does not support SPAN on a VM FEX.

Checkpoint and Configuration Rollback Limitation

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

Upgrading and Downgrading Limitations

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

- **switchport** command configuration issues

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

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

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

Table 7 Switchport Command Configuration Upgrade and Downgrade Issues

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

Table 7 Switchport Command Configuration Upgrade and Downgrade Issues

Path	Workaround
Upgrade from 5.2(1)N1(1) to 5.2(1)N1(1a)	Same as upgrade from 5.1(3)N2(1) to 5.2(1)N1(1).
Downgrade from 5.2(1)N1(1a) to 5.2(1)N1(1)	Same as upgrade from 5.1(3)N2(1) to 5.2(1)N1(1).

- **fex associate** command issues

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

  – **fex associate**

  Table 8 lists the situations where you might experience **fex associate** command issues and the workarounds.

Table 8 Fex Associate Command Upgrade and Downgrade Issues

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

Table 8 Fex Associate Command Upgrade and Downgrade Issues

Path	Workaround
Upgrade from 5.2(1)N1(1) to 5.2(1)N1(1a)	Not applicable.
Downgrade from 5.2(1)N1(1a) to 5.2(1)N1(1)	Not applicable.

Layer 3 Limitations

Asymmetric Configuration

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

Note The 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 by entering the **interface vlan** command and configuring *management*. This configuration allows traffic to the management SVIs to not go through the Layer 3 module which maintains connectivity in case of a Layer 3 module failure.

Upgrading and Downgrading

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

Cisco Nexus 5548P Daughter Card (N55-D160L3)

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

Caveats

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

This section includes the following topics:

Open Caveats

Table 9 lists descriptions of open caveats in Cisco NX-OS Release 6.x.

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

Table 9 Cisco NX-OS Release 6.0x Open Caveats

Record Number	Open Caveat Headline
CSCun66310	Nexus 5596: System fails to boot after a power cycle.
CSCuu59941	FC ports error disabled with non-Cisco SFPs after upgrade to 6.x/7.x
CSCul27686	Nexus 55xx P Devices: After Upgrade Interface Down & Unrecoverable
CSCty43038	ethpm allowed vlan list and fwm fwd vlans are wrong after rollback
CSCue22038	Unable to poweron the module after poweroff the module
CSCuj87061	Unified fc interfaces come up as Ethernet after disruptive upgrades
CSCtz78363	hsrp vmac learned with primary switch-id instead of ES sw-id
CSCud48710	Unshut NIF PO L2 Mcast loss for 1-2 mins for groups of mixed v2/v3 recvr
CSCuq56923	Logging level virtual-service reverts to default after a NX-OS upgrade..
CSCuc43503	feature-set virtualization with IGMP VPC optimization is not supported
CSCtx99080	fex temp does not reflect the correct value
CSCua27097	'no feature private-vlan' does not remove the complete config
CSCuc25187	Config-sync: unable to remove VLAN QOS policy and offset configuration

Resolved Caveats in Cisco NX-OS Release 6.0(2)N2(7)

Table 10 Cisco NX-OS Release 6.0(2)N2(7) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCua39096	TACACS+ missing header length check.
CSCua39159	Command injection with CA functionality.
CSCus26870	December 2014 ntpd CVEs for Nexus 5k/6k/7k/MDS.
CSCus68591	Assess GHOST vulnerability for Nexus 5k (CVE-2015-0235).
CSCut77411	Assess April 2015 NTPd vulnerabilities for N5k/N6k/N7k.
CSCut45896	Nexus 5k/6k - MARCH 2015 OpenSSL Vulnerabilities.

Table 10 Cisco NX-OS Release 6.0(2)N2(7) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCus42980	JANUARY 2015 OpenSSL Vulnerabilities.
CSCur31350	Multiple Vulnerabilities in OpenSSL - August 2014
CSCus28101	N5K/6K: Inband TACACS traffic matched against exception-class in CoPP
CSCuo34512	fwm hap reset with traffic running over the weekend
CSCuo34379	N5K/6K:NXOS upgrade by changing bootvariables & reload isn't recommended
CSCus04851	N5k/6k -FP BCAST/MCAST broken on VPC edge ports after remote root change
CSCur01470	N5K/6K fails to respond to unicast ARP request and may loop it back
CSCup85771	Nexus 6000 resets SSH intermittently
CSCut08809	Bug CSCuj56227 gets carried over ISSU upgrade.
CSCus15505	clk_mgr process crash due to a memory leak
CSCus70491	N6004 bigsurusd hap reset
CSCur76751	N6K/5K: Need knob to configure mgmt0 interface to operate at auto 10/100
CSCus39651	N6k:CRC errors on random 40gig port after reload
CSCut09166	fwm hap reset on vlan delete
CSCur39582	vlan_mgr unresponsive on creating or deleting VLAN
CSCus77310	vpc hap reset vpc process crashed
CSCul25239	N-96: qd hap reset while performing manual swap of 16UPLEM with CR LEM
CSCus78102	N6K crashed due to "kernel panic" @ stale pointer
CSCut25576	When deleting a profile, VRF param list are left over
CSCut29175	bzero() cause buffer overflow
CSCup36515	N5k/N6k SSH process may crash during authentication process.
CSCut22554	Workaround for CSCuo46284: Nexus 5500 showing SFP uC: Module 1: v0.0.0.0
CSCut81357	PTP Leap Second : n5k ptp off clock off by 35 seconds.

Resolved Caveats in Cisco NX-OS Release 6.0(2)N2(6)

Table 11 Cisco NX-OS Release 6.0(2)N2(6) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCue31348	tacacsd process crash during authentication/authorization
CSCub20644	cdp core dump in 5.0.3
CSCup87395	Config-sync failures with no cdp enable and pre-provisioning
CSCup77720	cts manual command not allowed with fex pre provisioning
CSCup79805	lldp mts buffer leak with continous port-flapping

Table 11 Cisco NX-OS Release 6.0(2)N2(6) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCup74690	Complete fix of CSCuj46069:DHCP offers might not get relayed in FP topos
CSCuo20517	Unexpected reboot on Nexus after enabling ipv6 dhcp relay
CSCuo86400	Memory leak causing the DRAP service to crash
CSCup82567	Config stuck after interface down during vPC bringup.
CSCup53176	ethpm service crash on both VPC peers
CSCuf82423	Nexus 5596 ethpm hap reset
CSCup31952	N5K: Nexus crash at eth_port_sec hap reset
CSCuq61301	FEX FCOE FCNS FC4-TYPE:FEATURE incomplete, empty.
CSCue62640	N5K/6K: TCP ports 21, 512-514 are opened after enabling FCoE
CSCup78930	'fex' process crash after switches in fabric-path are reset
CSCul02903	Enh: U2rib timesout on response from DCEFIB causing delayed ftag update
CSCur30631	Nexus 6000: FWM crash with not enough core files saved
CSCui32648	Reboot/core when issuing "clear forwarding cumulative counter all" cmd
CSCuo10325	igmp snooping flooded on stp blocking after stp change
CSCup78930	'fex' process crash after switches in fabric-path are reset
CSCul02903	Enh: U2rib timesout on response from DCEFIB causing delayed ftag update
CSCur30631	Nexus 6000: FWM crash with not enough core files saved
CSCui32648	Reboot/core when issuing "clear forwarding cumulative counter all" cmd
CSCuo10325	igmp snooping flooded on stp blocking after stp change
CSCup85771	Nexus 6000 resets SSH intermittently
CSCun06675	ISSU upgrade might fail due to FWM hap reset
CSCun10615	N6k - Software MAC learning of SVI MAC in HW table
CSCuh56328	netstack panic when closing the socket with sbuff lock acquired
CSCul78738	N2K-B22HP-P: HIF stays down when Blade Server moved into new slot.
CSCuq71362	Kernel panic in snmpd
CSCum13332	N5K: Changes to input voltage logging
CSCuj86736	Need to optimize DFE tuning in 55xxUP series switches - RX CRC Errors
CSCuc26047	Nexus 5000 reset due to Kernel Panic
CSCuq13396	Nexus 5500 ethpc hap reset - SYSMGR_DEATH_REASON_FAILURE_HEARTBEAT
CSCuh44248	Nexus 6000: Need to map "reload power-cycle" option to regular reload
CSCuo44979	Nexus 6004: Bios corrupt during reload/power cycle
CSCup46036	Nexus 6004: FAN OIR issues
CSCuo99149	NXOS Kernel Panic - Process fport_svr
CSCuq66628	VDC-MGR crash on N5k
CSCuq37768	'qd' Segfault at qd_bigsur_print_voq_asic_stats

Table 11 Cisco NX-OS Release 6.0(2)N2(6) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCua67460	Memory Leak in "ipqosmgr" -- FU_MEM_fu_hashtable_node_t
CSCuh97833	Cannot get IF-MIB counters for SVI
CSCui67164	Nexus Switch Crash in SNMPd w/ RMON Traps Configured
CSCul19949	snmpd crash when polling cpkiTrustPointTable with smart call home certs
CSCul30680	N5k restart due to monitor process crash when a VLAN is added/removed
CSCur54642	N5K with ERSPAN enabled may face a slow leak in 'monitor' process
CSCuq18021	SNMPset to community strings with special characters cause hap reset
CSCup22663	Multiple Vulnerabilities in OpenSSL - June 2014
CSCur05017	N5K/N6K evaluation for CVE-2014-6271 and CVE-2014-7169
CSCum40651	Tacacs+ per CLI authorization failure upon entering CLI > 64 char
CSCun10691	VLAN_MGR-2-CRITICAL_MSG VLAN Create Failed lacking necessary information
CSCup74458	few seconds of packet loss on vpc secondary link bringup
CSCup69347	Traffic loss when bringing up pre-existing vPC member port
CSCug11795	vlans error disabled over Peer-link
CSCuo63150	VPC hap reset on primary during secondary ISSU
CSCuo14888	Zone hap reset after device-alias rename
CSCup22663	Multiple Vulnerabilities in OpenSSL - June 2014
CSCur05017	N5K/N6K evaluation for CVE-2014-6271 and CVE-2014-7169
CSCum40651	Tacacs+ per CLI authorization failure upon entering CLI > 64 char
CSCun10691	VLAN_MGR-2-CRITICAL_MSG VLAN Create Failed lacking necessary information
CSCup74458	few seconds of packet loss on vpc secondary link bringup
CSCup69347	Traffic loss when bringing up pre-existing vPC member port
CSCug11795	vlans error disabled over Peer-link
CSCuo63150	VPC hap reset on primary during secondary ISSU
CSCuo14888	Zone hap reset after device-alias rename

Resolved Caveats in Cisco NX-OS Release 6.0(2)N2(5a)

Table 12 Cisco NX-OS Release 6.0(2)N2(5a) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCur05017	N5K/N6K evaluation for CVE-2014-6271 and CVE-2014-7169

Resolved Caveats in Cisco NX-OS Release 6.0(2)N2(5)

Table 13 Cisco NX-OS Release 6.0(2)N2(5) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCum79187	Core due to AAA process hap reset
CSCuj90123	N5K: aclmgr crash during sh tech
CSCun97052	RBACL policies not correctly programmed in TCAM
CSCuo01637	Nexus5k : Network-operator role can view sensitive configuration
CSCuo18604	CTS change of any-any policy not effective after the first download
CSCue40117	N5K may experience unexpectedly reboot when issuing show tech (tac-pac)
CSCuo10550	Nexus 55xx DCBX negotiating to CIN mode
CSCuj46069	DHCP offers might not get relayed in Fabricpath topologies
CSCuo20517	Unexpected reboot on Nexus after enabling ipv6 dhcp relay
CSCuf82423	Nexus 5596 ethpm hap reset
CSCud07967	Sysmgr service "fcoe_mgr" crashed
CSCue80077	FEX: Port flap request from SAP: MTS_SAP_SATMGR
CSCul52253	VPC+ allocates ftag-1 and ftag-2 as active
CSCum90179	N6K: Fabricpath ECMP issue with packet forwarding
CSCun67627	LACP Hap Reset while executing "show lacp interface"
CSCtw96661	N5K not able to suppress Sev5 syslog messages related with connected FEX
CSCuh27818	dcos-xinetd core due to segmentation fault in 6.2.2 during netstack reg
CSCum35498	N5K kernel panic crash usd_mts_kthread
CSCuo41201	Netstack buffer leaking with IPv6 feature running
CSCuh56328	netstack panic when closing the socket with sbuff lock acquired
CSCum47367	Cisco NX-OS Software TACACS+ Command Authorization Vulnerability
CSCul78738	N2K-B22HP-P: HIF stays down when Blade Server moved into new slot.
CSCul19908	False positive transceiver warnings on Nexus 5000
CSCum13332	N5K: Changes to input voltage logging
CSCue71612	Nexus 5548P/5548UP: Silent Reload with i2c code 0x0100
CSCum81287	Not able to pass traffic over Eth ports with FC and Fabricpath config
CSCui50776	OpenSSH LoginGraceTime Denial of Service Vulnerability
CSCun38423	Nexus 6000: Packets discarded on ingress
CSCuh97833	Cannot get IF-MIB counters for SVI
CSCui67164	Nexus Switch Crash in SNMPd w/ RMON Traps Configured
CSCuj32684	Snmpwalk : stpxRSTPPortRoleValue in the CISCO-STP-EXTENSIONS MIB broken
CSCui46891	N7K - mts recv_q SNMP Response SAP - stp+dot1dBridge+qBridge
CSCum57545	Peer-link STP inconsistency due to corrupt BPDU does not clear

Table 13 Cisco NX-OS Release 6.0(2)N2(5) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCum09342	Multiple tacacsd processes running causing authentication failures
CSCum40651	Tacacs+ per CLI authorization failure upon entering CLI > 64 char
CSCun71906	N5k VPC Incorrect SVI Type-2 inconsistency syslog
CSCuj42061	Vlan in suspended mode after adding them to fabric path
CSCun54561	Zone hap reset

Resolved Caveats in Cisco NX-OS Release 6.0(2)N2(4)

Table 14 Cisco NX-OS Release 6.0(2)N2(4) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCuh67647	Lot of Tacacsd zombie processes can be seen on N7k.
CSCul62250	N55xx link debounce time not working as expected
CSCul89905	L2 control packets dropped on CTS links with SGT encapsulation
CSCum62719	fcoe_mgr crash with "show platform software fcoe_mgr info global"
CSCul90150	FWM HAP Reset causing both switches in vPC to crash
CSCuj85007	vPC+: After Reload FEX MAC is not Synced Resulting in Traffic Black-Hole
CSCue76773	"ip routing multicast software-replicate" Support for N5K/N6k platform
CSCue55816	ppm core file size should be set properly to avoid truncation
CSCuj36520	Nexus: reload due to PIM process crash
CSCud45836	Error disabled/STP set port state failure after vlan removed by VTP
CSCum29831	VSHD_SYSLOG_EOL_ERR with "show version"

Resolved Caveats in Cisco NX-OS Release 6.0(2)N2(3)

Table 15 Cisco NX-OS Release 6.0(2)N2(3) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCuj92481	N5K: ISSU 6.0.2.N1.1 to 6.0.2.N2.2 free space below threshold
CSCul27686	Nexus 55xx P Devices: After Upgrade Interface Down & Unrecoverable
CSCui79701	Config Sync / Verify Failed / Lock already taken by another session
CSCuj40011	Nexus switch unexpectedly reloaded due to dhcp_snoop hap reset
CSCui47367	"shut/no shut" for vfc crashed device due to FWM hap reset
CSCuj56227	IGMP proxy reports may loop on the network
CSCuj32483	N5K:LACP member ports stuck in I state
CSCul20086	'snmpd' process crash on Nexus tied to user permissions
CSCuh33604	optimize dot1d snmp for fex stats

Table 15 Cisco NX-OS Release 6.0(2)N2(3) Resolved Caveats

CSCuf90644	STP BPDUs sent with different MAC with peer-switch after upgrade
CSCuj59439	vPC hap reset after peer-keepalive link comes up

Resolved Caveats in Cisco NX-OS Release 6.0(2)N2(2)

Table 16 Cisco NX-OS Release 6.0(2)N2(2) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCue65973	Nexus 2248TP: HIF speed not showing the actual link bandwidth
CSCuh57927	FEX hardware type changed after ISSU/ISSD
CSCuh31035	IP-MIB returns length of ipaddress as part of snmp instance.
CSCug79384	PVLAN with port-security and static mac-address disappear
CSCui08344	multicast convergence improvements
CSCty33679	Crash w/ show interface eth1/7 transceiver details / mping

Resolved Caveats in Cisco NX-OS Release 6.0(2)N2(1)

Table 17 Cisco NX-OS Release 6.0(2)N2(1)

Record Number	Resolved Caveat Headline
CSCug90187	SFP and QSFP support for FEX.
CSCuc62084	CSCuc62084 Sh accounting log / show log output is missing initial
CSCua50422	Call Home indicates successfully sent message when no message is sent
CSCtx62151	Accounting logs modification for config sync message logging
CSCud87482	Allowed VLAN list might not be applied on port-profile changes
CSCub77319	port-profile in Config sync mode missing Description command
CSCug97032	N5K COPP - ARP Traffic not classified when arriving on PeerLink
CSCub48506	Channel-group passive/active does not change the config
CSCug90571	Service "fcdomain" crashed
CSCuc91171	copy run starts fails: Service "fcns" failed to save its configuration
CSCub80303	FEX Crash When Running Command "phystats" In Command Shell
CSCug95929	Multiple FEX can go offline at the same time .
CSCua23418	Nexus 5000 does not update serial number of FEX PS
CSCug69534	Memory leak in the FWM process at FWM_MEM_fwm_mac_t
CSCue24735	N5K has incorrect virtual-mac-address entries in HSRP state transition
CSCug80833	N5K: Connectivity issues after MAC fails over
CSCud08015	N5K / PTP multicast packets punted and dropped instead of forwarded

Table 17 Cisco NX-OS Release 6.0(2)N2(1)

Record Number	Resolved Caveat Headline
CSCuc23163	IGMP general queries getting suppress for prolong time
CSCud90103	Multicast source address inverted by N7K in received igmpv3 message.
CSCug39029	Igmp report floods back to same hif port on which it was received
CSCud41492	IGMP not in sync with peer VPC switch after simultaneous leaves and join
CSCuh00696	N5k/L2MP - IGMP reports not forwarded out of non-Core Mrouter ports
CSCua32166	Optimized multicast flooding(OMF) shows up as disabled in show command
CSCuc16550	memory leak in ipqosmgr
CSCuf08921	N5K fabricpath MAC address not re learnt on GARP
CSCuf77723	license grace-period does not work for BGP for Nexus 5k
CSCuf51541	VPC/VPC+ HSRP VMAC removed on HSRP standby
CSCue21399	MC-lag failover does not work on virtual Port Channels (vPC)
CSCua69620	vpc+:peer-link down doesnt trigger mac delete notification on vpc peer
CSCua42827	Nexus 5548: mroutes not created for sources connected across vpc
CSCud61168	SNMPWalk fallback on ifHCInOctets for FEX interfaces
CSCuc72018	Static routes added while VRF is shutdown fails to install in RIB
CSCug32189	BGP process fail due to constant Socket (43/-1) accept: Bad file descrip
CSCtz70343	CLI process crashes when line length greater than 471 characters
CSCua22284	SNMP walk doesnt display PS Type for the FEX.
CSCuc39303	satctrl heartbeat miss when polling fex interfaces with solarwinds
CSCue81832	HW clock out of Sync , could result in ISSU failure .
CSCtx21891	Nexus 5000/5500 control plane failure not bringing links down
CSCub48277	Flooding while switch is in POAP mode
CSCud26463	Preprovision dynamic string changes + support for large commands
CSCug42375	N5k - Same "match cos" value shared between class-fcoe and another class
CSCue02015	telnet to non-management SVI broken after reload
CSCuc92186	BGP -When a Peer-Template is modified , BGP adjacency remains iddle
CSCuc84457	BGP Password doesn't enforce or disable without Process Restart
CSCub73193	BGP routes stuck in delete state blocked by ulib flow control
CSCuc56790	Invalid path in 2 VRFs constantly triggers bestpath selection
CSCuc92190	N7k Default Originate Not working when redistributing Static into Bgp
CSCuc94629	N7K eBGP adjacency bounces after creating a new interface
CSCuc93084	N7K:BGP error log %BGP-3-RPM_LIB_INT_ERROR rpm_get_next_action_by_type()
CSCub55990	No BGP prefixes after "default address-family" command under neighbor
CSCuc97808	NX-OS: Set BGP Community/extended community on Redistribution is Broken
CSCuc55910	N7K EIGRP memory leak

Table 17 Cisco NX-OS Release 6.0(2)N2(1)

Record Number	Resolved Caveat Headline
CSCug24976	N5k/6k: Need to expose knob "ip pim register-until-stop"
CSCuc04285	"show ip ospf" shows incorrect no. of stubs/nssa areas after HA trigger.
CSCud59785	Intra-area Summary Route not re-advertised if a Summary Route exists
CSCto98401	N7K cannot flush OSPF non area type compatible LSA
CSCud69928	N7K: Received Duplicate DBD packets cause 7K to increase sequence number
CSCuc73943	NX-OS / OSPF not installing all ECMP paths in RIB
CSCud25824	OSPF dead-timer not applied on reload
CSCua97463	OSPF default-information originate behave inconsistantly
CSCud00524	More specific PIM ASM RP config not overriding bidir RP config
CSCuf61304	NX-OS : RPF on mroute incorrectly pointing to the RP for (S,G)
CSCub99717	"Redistribute static route-map" redistribute the defaullt route
CSCud03634	RIP keep advertising route even though original route source is down
CSCua94509	FEX: no fex id fails after moving fabric ports across different fpc
CSCug77133	Nexus 5k incorrectly programs the SPAN source port
CSCuc20817	N7K: Trunk port allowing system reserved VLANs after ISSU upgrade.
CSCuc84599	Fex port-channel links suspend after config sync change
CSCuf21318	N5k: Secondary VPC flaps VPC port-channels after peer-link is down
CSCuc26101	Wrong warning message when changing default auto-recovery timer
CSCub50434	VTP packets looping on vpc
CSCuc35483	%ZONE-2-ZS_CHANGE_SFC_FAILED INVALID_ZSET_FORMAT
CSCuc17458	active zoneset of enhance vsan with interop 1 de-activated after ISSU

Resolved Caveats in Cisco NX-OS Release 6.0(2)N1(2a)

Table 18 lists the caveats that are resolved in Cisco NX-OS Release 6.0(2)N1(2a). The caveats might be open in previous Cisco NX-OS releases.

Table 18 Cisco NX-OS Release 6.0(2)N1(2a) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCug46504	DHCP Relay does not work when the Bootp flag is set (Broadcast)
CSCud08015	N5K / PTP multicast packets punted and dropped instead of forwarded
CSCug07482	Memory leak at ppm with switch profile configured
CSCuf61304	NX-OS : RPF on mroute incorrectly pointing to the RP for (S,G)
CSCtw72949	Slow drain of udp sock mts buffers for some bulk requests in bridge-mib
CSCue79881	SNMP crashes on SNMP bulk get query
CSCuf17575	N64P: /32 host route via routing prtcol gets programed with all ecmp nh

Resolved Caveats in Cisco NX-OS Release 6.0(2)N1(2)

Table 19 lists the caveats that are resolved in Cisco NX-OS Release 6.0(2)N1(2). The caveats might be open in previous Cisco NX-OS releases.

Table 19 Cisco NX-OS Release 6.0(2)N1(2) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtu05113	Nexus 55xx core in fcpc -- heartbeat failure.
CSCue03528	Session Database / Config Sync / CFS locked on one side without a commit
CSCue22023	EMC-ENTRANCE:fcoe_mgr core due to memory leak.
CSCue35880	intermittent link up delay on fex ports
CSCtz62596	dom read failed err messages
CSCue39246	Need to remove N5K protocol headers from Ethanalyzer detail output
CSCue03528	Session Database / Config Sync / CFS locked on one side without a commit

Resolved Caveats in Cisco NX-OS Release 6.0(2)N1(1)

Table 20 lists the caveats that are resolved in Cisco NX-OS Release 6.0(2)N1(1). The caveats might be open in previous Cisco NX-OS releases.

Table 20 Cisco NX-OS Release 6.0(2)N1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtx75226	HSRP state fluctuating between active/speak/standby for ver v1.
CSCua23762	Nexus 5500 Monitor session prevents FCoE hosts from completing login
CSCtt10736	Traffic from peer-link dropped after secondary reload and pka reconnect

MIB Support

The Cisco Management Information Base (MIB) list includes Cisco proprietary MIBs and many other Internet Engineering Task Force (IETF) standard MIBs. These standard MIBs are defined in Requests for Comments (RFCs). To find specific MIB information, you must examine the Cisco proprietary MIB structure and related IETF-standard MIBs supported by the Cisco Nexus 5500 Series switch.

The MIB Support List is available at the following FTP site:

ftp://ftp.cisco.com/pub/mibs/supportlists/nexus5000/Nexus5000MIBSupportList.html

Related Documentation

Documentation for Cisco Nexus 5500 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 documentation set includes the following types of documents:

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

Documentation Feedback

To provide technical feedback on this document or to report an error or ommission, please send your comments to nexus5k-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

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

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