

Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)



# Cisco Nexus 7000 Series NX-OS Release Notes, Release 6.0

**Date:** April 12, 2012  
**Part Number:** OL-25772-03 B0  
**Current Release:** 6.0(3)

This document describes the features, caveats, and limitations for Cisco NX-OS software for use on the Cisco Nexus 7000 Series switches. Use this document in combination with documents listed in the “[Related Documentation](#)” section on page 43.



## Note

Release notes are sometimes updated with new information about restrictions and caveats. See the following website for the most recent version of the *Cisco Nexus 7000 Series NX-OS Release Notes, Release 6.x Release Notes*:  
[http://www.cisco.com/en/US/products/ps9402/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps9402/prod_release_notes_list.html)

[Table 1](#) shows the online change history for this document.

**Table 1** Online History Change

Part Number	Revision	Date	Description
OL-25772-01	A0	October 27, 2011	Created release notes for Release 6.0(1).
	B0	November 23, 2011	Added CVR-X2-SFP10G, OneX Converter Module - X2 to SFP+ Adapter for the 8-port 10-Gigabit Ethernet I/O module XL (N7K-M108X2-12L) to <a href="#">Table 3</a> .
	C0	December 2, 2011	Added the “ <a href="#">RBAC OID Enhancement</a> ” section.



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

**[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

**Table 1 Online History Change (continued)**

Part Number	Revision	Date	Description
OL-25772-02	A0	December 22, 2011	Created release notes for Release 6.0(2).
	B0	January 11, 2012	Updated the description of the features not supported in the F2-Series hardware in the <a href="#">“Integrating F2-Series Modules Into a Cisco Nexus 7000 Series System”</a> section.
	C0	January 30, 2012	Added the “QoS Policies and ACLs” topic to the <a href="#">“Upgrade/Downgrade Caveats”</a> section.
	D0	March 15, 2012	Updated the transceiver information for the 8-port 10-Gigabit Ethernet I/O module XL (N7K-M108X2-12L) in <a href="#">Table 3</a> .
	E0	March 28, 2012	Moved CSCtu61247 to the <a href="#">“Open Caveats—Cisco NX-OS Release 6.0”</a> section.
	F0	April 3, 2012	Added CSCts11774 to the <a href="#">“Resolved Caveats—Cisco NX-OS Release 6.0(2)”</a> section.
	G0	April 4, 2012	Added CSCty21455 and CSCty23808 to the <a href="#">“Open Caveats—Cisco NX-OS Release 6.0”</a> section.
OL-25772-03	A0	April 12, 2012	Created release notes for Release 6.0(3).
	B0	May 21, 2012	Added resolved caveat CSCtz10925.

## Contents

This document includes the following sections:

- [Introduction, page 3](#)
- [System Requirements, page 3](#)
- [Upgrade/Downgrade Caveats, page 15](#)
- [CMP Images, page 17](#)
- [EPLD Images, page 17](#)
- [New Hardware Features, page 17](#)
- [New Software Features, page 17](#)
- [Licensing, page 18](#)
- [MIBs, page 19](#)
- [Limitations, page 19](#)
- [Caveats, page 19](#)
- [Related Documentation, page 43](#)
- [Obtaining Documentation and Submitting a Service Request, page 44](#)

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## Introduction

The Cisco NX-OS software for the Cisco Nexus 7000 Series switches fulfills the routing, switching, and storage networking requirements of data centers and provides an Extensible Markup Language (XML) interface and a command-line interface (CLI) similar to Cisco IOS software.

## System Requirements

This section includes the following topics:

- [Memory Requirements, page 3](#)
- [Supported Device Hardware, page 5](#)
- [Integrating F2-Series Modules Into a Cisco Nexus 7000 Series System, page 15](#)

## Memory Requirements

The Cisco NX-OS software may require 8 GB of memory, depending on the software version you use and the software features you enable.

An 8 GB supervisor memory upgrade kit, N7K-SUP1-8GBUPG=, allows for growth in the features and capabilities that can be delivered in existing Cisco Nexus 7000 Series supervisor modules. The memory upgrade kit is supported on Cisco Nexus 7000 Series systems running Cisco NX-OS Release 5.1 or later releases. Instructions for upgrading to the new memory are available in the “Upgrading Memory for Supervisor Modules” section of the *Cisco Nexus 7000 Series Hardware Installation and Reference Guide*.

The following guidelines can help you determine whether or not to upgrade an existing supervisor module:

- When the system memory usage exceeds 3 GB (75 percent of total memory), we recommend that you upgrade the memory to 8 GB. Use the **show system resources** command from any VDC context to check the system memory usage:

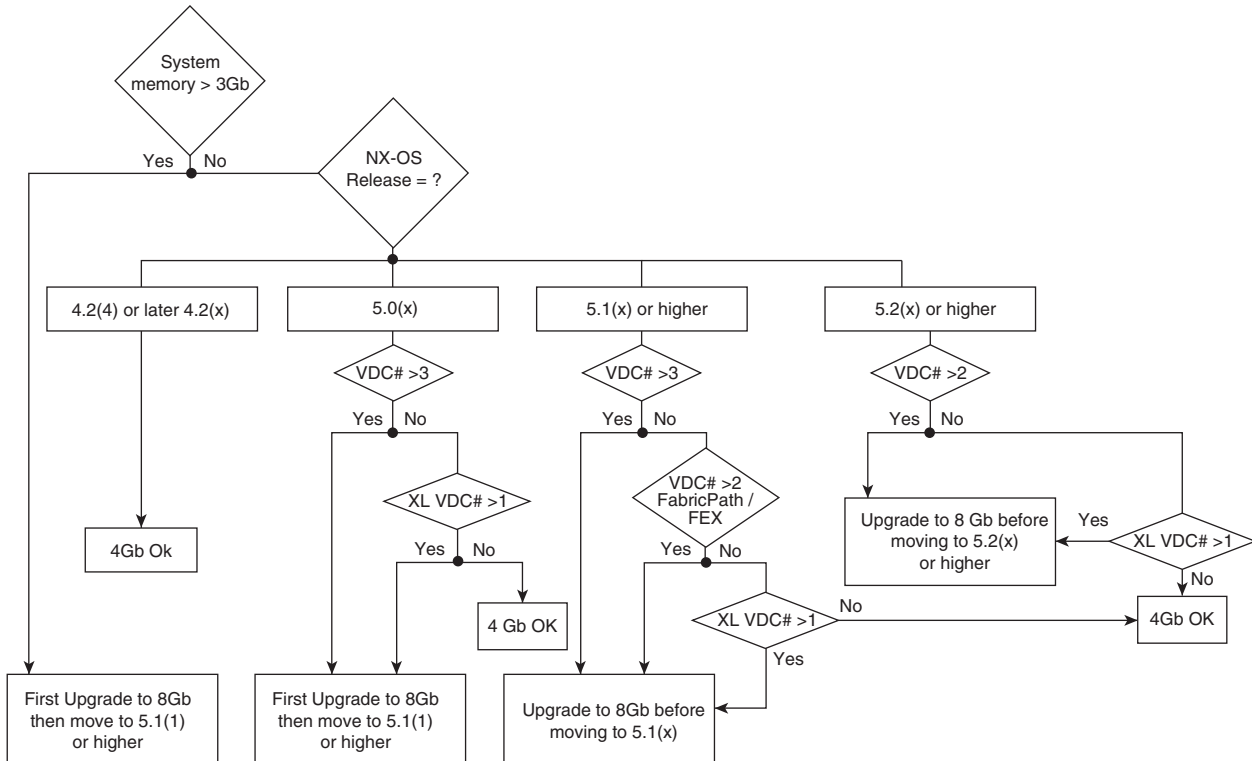
```
Nexus-7000# show system resources
Load average:  1 minute: 0.47   5 minutes: 0.24   15 minutes: 0.15
Processes   :  959 total, 1 running
CPU states  :  3.0% user,   3.5% kernel,   93.5% idle
Memory usage: 4115776K total,  2793428K used,  1322348K free <-----
```

- If you create more than one VDC with XL mode enabled, or if you have more than two VDCs, 8 GB of memory is required.

For additional guidance about whether or not to upgrade a supervisor module to 8 GB of memory, see [Figure 1](#).

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Figure 1 Supervisor Memory Upgrade Decision Flowchart



330450

When you insert a supervisor module into a Cisco Nexus 7000 Series switch running Cisco NX-OS Release 5.1(x) or a later release, be aware that one of the following syslog messages will display, depending on the software version and the amount of memory for the supervisor module:

- If you are running Cisco NX-OS Release 5.1(1) or a later release and you have an 8-GB supervisor as the active supervisor and you insert a 4-GB supervisor module as the standby, it will be powered down. A severity 2 syslog message indicates that the memory amounts should be equivalent between the active and the standby supervisor:

```
2010 Dec 3 00:05:37 switch %$ VDC-1 %$ %SYSMGR-2-SUP_POWERDOWN: Supervisor in slot 10 is running with less memory than active supervisor in slot 9
```

In this situation, you have the option to upgrade the memory in the 4-GB supervisor or shut down the system and remove the extra memory from the 8-GB supervisor.

- If you are running Cisco NX-OS Release 5.1(2) or a later release and you insert a 8-GB supervisor module as the standby, a severity 4 syslog message appears.

```
2010 Dec 1 23:32:08 switch %SYSMGR-4-ACTIVE_LOWER_MEM_THAN_STANDBY: Active supervisor in slot 5 is running with less memory than standby supervisor in slot 6.
```

In this situation, you have the option to remove the extra memory or do a switchover and upgrade the memory in the 4-GB supervisor.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## Supported Device Hardware

The Cisco NX-OS software supports the Cisco Nexus 7000 Series chassis. You can find detailed information about supported hardware in the [Cisco Nexus 7000 Series Hardware Installation and Reference Guide](#).

Table 2 shows the hardware supported by Cisco NX-OS Release, 6.x, Release 5.x and Release 4.x software.

Table 3 shows the transceiver devices supported by each release.

For a list of minimum recommended Cisco NX-OS software releases for use with Cisco Nexus 7000 Series switches, see the document [Minimum Recommended Cisco NX-OS Releases for Cisco Nexus 7000 Series Switches](#).

**Table 2** Hardware Supported by Cisco NX-OS Software Releases

Product ID	Hardware	Minimum Software Release
N7K-C7009	Cisco Nexus 7009 chassis	5.2(1)
N7K-C7010	Cisco Nexus 7010 chassis	4.0(1)
N7K-C7018	Cisco Nexus 7018 chassis	4.1(2)
N7K-C7010-FAN-S	System fan tray for the Cisco Nexus 7010 chassis	4.0(1)
N7K-C7010-FAN-F	Fabric fan tray for the Cisco Nexus 7010 chassis	4.0(1)
N7K-C7018-FAN	Fan tray for the Cisco Nexus 7018 chassis	4.1(2)
N7K-AC-6.0KW	6.0-kW AC power supply unit	4.0(1)
N7K-AC-7.5KW-INT	7.5-kW AC power supply unit	4.1(2)
N7K-AC-7.5KW-US		4.1(2)
N7K-DC-6.0KW	6.0-kW DC power supply unit (cable included)	5.0(2)
N7K-DC-PIU		5.0(2)
N7K-DC-CAB=		5.0(2)
	DC power interface unit	
	DC 48 V-48 V cable (spare)	
N7K-SUP1	Supervisor module	4.0(1)
N7K-SUP1-8GBUPG	Supervisor module memory kit upgrade	5.1(1)
N7K-C7009-FAB-2	Fabric module, Cisco Nexus 7000 Series 9-slot	5.2(1)
N7K-C7010-FAB-2	Fabric module, Cisco Nexus 7000 Series 10-slot	6.0(1)
N7K-C7010-FAB-1	Fabric module, Cisco Nexus 7000 Series 10-slot	4.0(1)
N7K-C7018-FAB-2	Fabric module, Cisco Nexus 7000 Series 18-slot	6.0(1)
N7K-C7018-FAB-1	Fabric module, Cisco Nexus 7000 Series 18-slot	4.1(2)

**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

**Table 2 Hardware Supported by Cisco NX-OS Software Releases (continued)**

Product ID	Hardware	Minimum Software Release
N7K-F248XP-25	48-port 1/10 Gigabit Ethernet SFP+ I/O module (F2-Series)	6.0(1)
N7K-F132XP-15	32-port 1/10 Gigabit Ethernet module (F1-Series)	5.1(1)
N7K-M108X2-12L	8-port 10-Gigabit Ethernet I/O module XL <sup>1</sup>	5.0(2)
N7K-M132XP-12	32-port 10-Gigabit Ethernet SFP+ I/O module	4.0(1)
N7K-M132XP-12L	32-port 10-Gigabit Ethernet SFP+ I/O module XL <sup>1</sup>	5.1(1)
N7K-M148GS-11	48-port 1-Gigabit Ethernet SFP I/O module	4.1(2)
N7K-M148GS-11L	48-port 1-Gigabit Ethernet I/O module XL <sup>1</sup>	5.0(2)
N7K-M148GT-11	48-port 10/100/1000 Ethernet I/O module	4.0(1)
N7K-M148GT-11L	48-port 10/100/1000 Ethernet I/O module XL <sup>1</sup>	5.1(2)
N2K-C2248TP-1GE	Cisco Nexus 2248TP Fabric Extender <sup>2</sup>	5.1(1)
N2K-C2224TP-1GE	Cisco Nexus 2224TP Fabric Extender <sup>2</sup>	5.2(1)
N2K-C2232PP-10GE	Cisco Nexus 2232PP Fabric Extender <sup>2</sup>	5.2(1)

1. Requires the Cisco Nexus 7010 Scalable Feature Package license (N7K-C7010-XL) or the Cisco Nexus 7018 Scalable Feature Package license (N7K-C7018-XL), depending on the chassis, to enable all XL-capable I/O modules to operate in XL mode.
2. Cisco Nexus Fabric Extenders (FEX) are supported on the 32-port 10-Gigabit Ethernet SFP+ I/O module (N7K-M132XP-12) and the 32-port 10-Gigabit Ethernet SF P+ I/O module XL (N7K-M132XP-12L). In addition, Cisco FEXes support the F2-Series 48-port 1/10 Gigabit Ethernet SFP+ I/O module (N7K-F248XP-25) in Cisco NX-OS Release 6.0(1) which is required for the F2-Series module. Cisco FEXes require front-to-back airflow. They use AC or DC power supplies.

**Table 3 Transceivers Supported by Cisco NX-OS Software Releases**

I/O Module	Product ID	Transceiver Type	Minimum Software Version
N7K-F248XP-25	SFP-10G-ER	10GBASE-ER SFP+	6.0(1)
	SFP-10G-LR	10GBASE-LR SFP+	6.0(1)
	SFP-10G-LRM	10GBASE-LRM SFP+	6.0(1)
	SFP-10G-SR	10GBASE-SR SFP+	6.0(1)
	FET-10G	Cisco Fabric Extender Transceiver (FET)	6.0(1)

**[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

**Table 3 Transceivers Supported by Cisco NX-OS Software Releases (continued)**

<b>I/O Module</b>	<b>Product ID</b>	<b>Transceiver Type</b>	<b>Minimum Software Version</b>
	SFP-H10GB-CUxM	SFP-H10GB-CUxM Twinax Cable Passive (1m, 3m, 5m)	6.0(1)
	SFP-H10GB-ACUxM	SFP-H10GB-ACUxM Twinax Cable Active (7m, 10m)	6.0(1)
	SFP-GE-T	1000BASE-T SFP	6.0(1)
	SFP-GE-S	1000BASE-SX SFP (DOM)	6.0(1)
	SFP-GE-L	1000BASE-LX/LH SFP (DOM)	6.0(1)
	SFP-GE-Z	1000BASE-ZX SFP (DOM)	6.0(1)
	GLC-LH-SM	1000BASE-LX/LH SFP	6.0(1)
	GLC-LH-SMD	1000BASE-LX/LH SFP	6.0(1)
	GLC-SX-MM	1000BASE-SX SFP	6.0(1)
	GLC-SX-MMD	1000BASE-SX SFP	6.0(1)
	GLC-ZX-SM	1000BASE-ZX SFP	6.0(1)
	GLC-T	1000BASE-T SFP	6.0(1)
	GLC-BX-D	1000BASE-BX10-D	6.0(1)
	GLC-BX-U	1000BASE-BX10-U	6.0(1)
	CWDM-SFP-1470	1000BASE-CWDM	6.0(1)
	CWDM-SFP-1490		6.0(1)
	CWDM-SFP-1510		6.0(1)
	CWDM-SFP-1530		6.0(1)
	CWDM-SFP-1550		6.0(1)
	CWDM-SFP-1570		6.0(1)
	CWDM-SFP-1590		6.0(1)
	CWDM-SFP-1610		6.0(1)
	DWDM-SFP-6141	1000BASE-DWDM	6.0(1)
	DWDM-SFP-6061		6.0(1)
	DWDM-SFP-5979		6.0(1)
	DWDM-SFP-5898		6.0(1)
	DWDM-SFP-5817		6.0(1)
	DWDM-SFP-5736		6.0(1)
	DWDM-SFP-5655		6.0(1)
	DWDM-SFP-5575		6.0(1)
	DWDM-SFP-5494		6.0(1)
	DWDM-SFP-5413		6.0(1)
	DWDM-SFP-5332		6.0(1)

**[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

**Table 3 Transceivers Supported by Cisco NX-OS Software Releases (continued)**

<b>I/O Module</b>	<b>Product ID</b>	<b>Transceiver Type</b>	<b>Minimum Software Version</b>
	DWDM-SFP-5252		6.0(1)
	DWDM-SFP-5172		6.0(1)
	DWDM-SFP-5092		6.0(1)
	DWDM-SFP-5012		6.0(1)
	DWDM-SFP-4931		6.0(1)
	DWDM-SFP-4851		6.0(1)
	DWDM-SFP-4772		6.0(1)
	DWDM-SFP-4692		6.0(1)
	DWDM-SFP-4612		6.0(1)
	DWDM-SFP-4532		6.0(1)
	DWDM-SFP-4453		6.0(1)
	DWDM-SFP-4373		6.0(1)
	DWDM-SFP-4294		6.0(1)
	DWDM-SFP-4214		6.0(1)
	DWDM-SFP-4134		6.0(1)
	DWDM-SFP-4056		6.0(1)
	DWDM-SFP-3977		6.0(1)
	DWDM-SFP-3898		6.0(1)
	DWDM-SFP-3819		6.0(1)
	DWDM-SFP-3739		6.0(1)
	DWDM-SFP-3661		6.0(1)
	DWDM-SFP-3582		6.0(1)
	DWDM-SFP-3504		6.0(1)
	DWDM-SFP-3425		6.0(1)
	DWDM-SFP-3346		6.0(1)
	DWDM-SFP-3268		6.0(1)
	DWDM-SFP-3190		6.0(1)
	DWDM-SFP-3112		6.0(1)
	DWDM-SFP-3033		6.0(1)
N7K-F132XP-15	SFP-10G-ER	10GBASE-ER SFP+	5.2(1)
	SFP-10G-SR	10GBASE-SR SFP+	5.1(1)
	SFP-10G-LR <sup>1</sup>	10GBASE-LR SFP+	5.1(1)
	SFP-10G-LRM	10GBASE-LRM SFP+	5.1(1)
	SFP-H10GB-CUxM	SFP-H10GB-CUxM Twinax Cable Passive (1m, 3m, 5m)	5.1(1)

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

**Table 3** Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	SFP-H10GB-ACUxM	SFP-H10GB-ACUxM Twinax Cable Active (7m, 10m)	5.1(1)
	SFP-GE-T	1000BASE-T SFP	5.1(1)
	SFP-GE-S	1000BASE-SX SFP (DOM)	5.1(1)
	SFP-GE-L	1000BASE-LX/LH SFP (DOM)	5.1(1)
	SFP-GE-Z	1000BASE-ZX SFP (DOM)	5.1(1)
	GLC-LH-SM	1000BASE-LX/LH SFP	5.1(1)
	GLC-SX-MM	1000BASE-SX SFP	5.1(1)
	GLC-ZX-SM	1000BASE-ZX SFP	5.1(1)
	GLC-T	1000BASE-T SFP	5.1(1)
	GLC-LH-SMD	1000BASE-LX/LH SFP	5.2(1)
	GLC-SX-MMD	1000BASE-SX SFP	5.2(1)
N7K-M108X2-12L	SFP-10G-LR <sup>2</sup>	10GBASE-LR SFP+	5.2(3a)
	SFP-10G-LRM <sup>2</sup>	10GBASE-LRM SFP+	5.2(3a)
	CVR-X2-SFP10G	OneX Converter Module - X2 to SFP+ Adapter	5.2(1)
	SFP-10G-SR <sup>2</sup>	10GBASE-SR SFP+	5.2(1)
	SFP-H10GB-CUxM <sup>2</sup>	SFP-H10GB-CUxM Twinax Cable Passive (1m, 3m, 5m)	5.2(1)
	X2-10GB-CX4	10GBASE-CX4 X2	5.1(1)
	X2-10GB-ZR	10GBASE-ZR X2	5.1(1)
	X2-10GB-LX4	10GBASE-LX4 X2	5.1(1)
	X2-10GB-SR	10GBASE-SR X2	5.0(2a)
	X2-10GB-LR	10GBASE-LRX2	5.0(2a)
	X2-10GB-LRM	10GBASE-LRM X2	5.0(2a)
	X2-10GB-ER	10GBASE-ERX2	5.0(2a)
	DWDM-X2-60.61=	10GBASE-DWDM X2	5.0(2a)
	DWDM-X2-59.79=		5.0(2a)
	DWDM-X2-58.98=		5.0(2a)
	DWDM-X2-58.17=		5.0(2a)
	DWDM-X2-56.55=		5.0(2a)
	DWDM-X2-55.75=		5.0(2a)
	DWDM-X2-54.94=		5.0(2a)
	DWDM-X2-54.13=		5.0(2a)
	DWDM-X2-52.52=		5.0(2a)

**[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

**Table 3 Transceivers Supported by Cisco NX-OS Software Releases (continued)**

<b>I/O Module</b>	<b>Product ID</b>	<b>Transceiver Type</b>	<b>Minimum Software Version</b>
	DWDM-X2-51.72=		5.0(2a)
	DWDM-X2-50.92=		5.0(2a)
	DWDM-X2-50.11=		5.0(2a)
	DWDM-X2-48.51=		5.0(2a)
	DWDM-X2-47.72=		5.0(2a)
	DWDM-X2-46.92=		5.0(2a)
	DWDM-X2-46.12=		5.0(2a)
	DWDM-X2-44.53=		5.0(2a)
	DWDM-X2-43.73=		5.0(2a)
	DWDM-X2-42.94=		5.0(2a)
	DWDM-X2-42.14=		5.0(2a)
	DWDM-X2-40.56=		5.0(2a)
	DWDM-X2-39.77=		5.0(2a)
	DWDM-X2-38.98=		5.0(2a)
	DWDM-X2-38.19=		5.0(2a)
	DWDM-X2-36.61=		5.0(2a)
	DWDM-X2-35.82=		5.0(2a)
	DWDM-X2-35.04=		5.0(2a)
	DWDM-X2-34.25=		5.0(2a)
	DWDM-X2-32.68=		5.0(2a)
	DWDM-X2-31.90=		5.0(2a)
	DWDM-X2-31.12=		5.0(2a)
	DWDM-X2-30.33=		5.0(2a)
N7K-M148GS-11	SFP-GE-S	1000BASE-SX	4.1(2)
	GLC-SX-MM		4.1(2)
	SFP-GE-L	1000BASE-LX	4.1(2)
	GLC-LH-SM		4.1(2)
	SFP-GE-Z	1000BASE-ZX	4.1(2)
	GLC-ZX-SM		4.1(2)
	GLC-T	1000BASE-T	4.2(1)
	SFP-GE-T		4.2(1)
	GLC-BX-D	1000BASE-BX10-D	5.2(1)
	GLC-BX-U	1000BASE-BX10-U	5.2(1)
	GLC-SX-MMD	1000BASE-SX	5.2(1)
	GLC-LH-SMD	1000BASE-LX	5.2(1)

**[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

**Table 3** *Transceivers Supported by Cisco NX-OS Software Releases (continued)*

<b>I/O Module</b>	<b>Product ID</b>	<b>Transceiver Type</b>	<b>Minimum Software Version</b>
	CWDM-SFP-1470	1000BASE-CWDM	4.2(1)
	CWDM-SFP-1490		4.2(1)
	CWDM-SFP-1510		4.2(1)
	CWDM-SFP-1530		4.2(1)
	CWDM-SFP-1550		4.2(1)
	CWDM-SFP-1570		4.2(1)
	CWDM-SFP-1590		4.2(1)
	CWDM-SFP-1610		4.2(1)
N7K-M148GS-11	DWDM-SFP-6141	1000BASE-DWDM	4.2(1)
	DWDM-SFP-6061		4.2(1)
	DWDM-SFP-5979		4.2(1)
	DWDM-SFP-5898		4.2(1)
	DWDM-SFP-5817		4.2(1)
	DWDM-SFP-5736		4.2(1)
	DWDM-SFP-5655		4.2(1)
	DWDM-SFP-5575		4.2(1)
	DWDM-SFP-5494		4.2(1)
	DWDM-SFP-5413		4.2(1)
	DWDM-SFP-5332		4.2(1)
	DWDM-SFP-5252		4.2(1)
	DWDM-SFP-5172		4.2(1)
	DWDM-SFP-5092		4.2(1)
	DWDM-SFP-5012		4.2(1)
	DWDM-SFP-4931		4.2(1)
	DWDM-SFP-4851		4.2(1)
	DWDM-SFP-4772		4.2(1)
	DWDM-SFP-4692		4.2(1)
	DWDM-SFP-4612		4.2(1)
	DWDM-SFP-4532		4.2(1)
	DWDM-SFP-4453		4.2(1)
	DWDM-SFP-4373		4.2(1)
	DWDM-SFP-4294		4.2(1)
	DWDM-SFP-4214		4.2(1)
	DWDM-SFP-4134		4.2(1)
	DWDM-SFP-4056		4.2(1)

**[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

**Table 3 Transceivers Supported by Cisco NX-OS Software Releases (continued)**

<b>I/O Module</b>	<b>Product ID</b>	<b>Transceiver Type</b>	<b>Minimum Software Version</b>	
	DWDM-SFP-3977		4.2(1)	
	DWDM-SFP-3898		4.2(1)	
	DWDM-SFP-3819		4.2(1)	
	DWDM-SFP-3739		4.2(1)	
	DWDM-SFP-3661		4.2(1)	
	DWDM-SFP-3582		4.2(1)	
	DWDM-SFP-3504		4.2(1)	
	DWDM-SFP-3425		4.2(1)	
	DWDM-SFP-3346		4.2(1)	
	DWDM-SFP-3268		4.2(1)	
	DWDM-SFP-3190		4.2(1)	
	DWDM-SFP-3112		4.2(1)	
	DWDM-SFP-3033		4.2(1)	
N7K-M148GS-11L	SFP-GE-S	1000BASE-SX	5.0(2a)	
	GLC-SX-MM		5.0(2a)	
	SFP-GE-L	1000BASE-LX	5.0(2a)	
	GLC-LH-SM		5.0(2a)	
	SFP-GE-Z	1000BASE-ZX	5.0(2a)	
	GLC-ZX-SM		5.0(2a)	
	GLC-T	1000BASE-T	5.0(2a)	
	SFP-GE-T		5.0(2a)	
	GLC-BX-D	1000BASE-BX10-D	5.2(1)	
	GLC-BX-U	1000BASE-BX10-U	5.2(1)	
	GLC-SX-MMD	1000BASE-SX	5.2(1)	
	GLC-LH-SMD	1000BASE-LX	5.2(1)	
	N7K-M148GS-11L	DWDM-SFP-6141	1000BASE-DWDM	5.0(2a)
		DWDM-SFP-6061		5.0(2a)
DWDM-SFP-5979			5.0(2a)	
DWDM-SFP-5898			5.0(2a)	
DWDM-SFP-5817			5.0(2a)	
DWDM-SFP-5736			5.0(2a)	
DWDM-SFP-5655			5.0(2a)	
DWDM-SFP-5575			5.0(2a)	
DWDM-SFP-5494			5.0(2a)	
DWDM-SFP-5413		5.0(2a)		

**[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

**Table 3** *Transceivers Supported by Cisco NX-OS Software Releases (continued)*

<b>I/O Module</b>	<b>Product ID</b>	<b>Transceiver Type</b>	<b>Minimum Software Version</b>
	DWDM-SFP-5332		5.0(2a)
	DWDM-SFP-5252		5.0(2a)
	DWDM-SFP-5172		5.0(2a)
	DWDM-SFP-5092		5.0(2a)
	DWDM-SFP-5012		5.0(2a)
	DWDM-SFP-4931		5.0(2a)
	DWDM-SFP-4851		5.0(2a)
	DWDM-SFP-4772		5.0(2a)
	DWDM-SFP-4692		5.0(2a)
	DWDM-SFP-4612		5.0(2a)
	DWDM-SFP-4532		5.0(2a)
	DWDM-SFP-4453		5.0(2a)
	DWDM-SFP-4373		5.0(2a)
	DWDM-SFP-4294		5.0(2a)
	DWDM-SFP-4214		5.0(2a)
	DWDM-SFP-4134		5.0(2a)
	DWDM-SFP-4056		5.0(2a)
	DWDM-SFP-3977		5.0(2a)
	DWDM-SFP-3898		5.0(2a)
	DWDM-SFP-3819		5.0(2a)
	DWDM-SFP-3739		5.0(2a)
	DWDM-SFP-3661		5.0(2a)
	DWDM-SFP-3582		5.0(2a)
	DWDM-SFP-3504		5.0(2a)
	DWDM-SFP-3425		5.0(2a)
	DWDM-SFP-3346		5.0(2a)
	DWDM-SFP-3268		5.0(2a)
	DWDM-SFP-3190		5.0(2a)
	DWDM-SFP-3112		5.0(2a)
	DWDM-SFP-3033		5.0(2a)

**[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

**Table 3 Transceivers Supported by Cisco NX-OS Software Releases (continued)**

I/O Module	Product ID	Transceiver Type	Minimum Software Version
N7K-M148GS-11L	CWDM-SFP-1470	1000BASE-CWDM	5.0(2a)
	CWDM-SFP-1490		5.0(2a)
	CWDM-SFP-1510		5.0(2a)
	CWDM-SFP-1530		5.0(2a)
	CWDM-SFP-1550		5.0(2a)
	CWDM-SFP-1570		5.0(2a)
	CWDM-SFP-1590		5.0(2a)
	CWDM-SFP-1610		5.0(2a)
N7K-M132XP-12	SFP-H10GB-ACUxM <sup>1</sup>	SFP-H10GB-ACUxM Twinax Cable Active (7m, 10m)	5.1(2)
	FET-10G	Cisco Fabric Extender Transceiver (FET)	5.1(1)
	SFP-10G-ER	10GBASE-ER SFP+	4.2(6)
	SFP-10G-LR	10GBASE-LR SFP+	4.0(3)
	SFP-10G-SR	10GBASE-SR SFP+	4.0(1)
N7K-M132XP-12L	FET-10G	Cisco Fabric Extender Transceiver (FET)	5.1(1)
	SFP-10G-SR	10GBASE-SR SFP+	5.1(1)
	SFP-10G-LR	10GBASE-LR SFP+	5.1(1)
	SFP-10G-ER	10GBASE-ER SFP+	5.1(1)
	SFP-10G-LRM	10GBASE-LRM SFP+	5.1(1)
	SFP-H10GB-ACUxM	SFP-H10GB-ACUxM Twinax Cable Active (7m, 10m)	5.1(1)
	SFP-H10GB-CUxM <sup>1</sup>	SFP-H10GB-CUxM Twinax Cable Passive (1m, 3m, 5m)	5.1(2)

1. Only version -02 is supported.
2. Requires CVR-X2-SFP10G, OneX Converter Module (X2 to SFP+ Adapter).

**[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

## Integrating F2-Series Modules Into a Cisco Nexus 7000 Series System

The Cisco Nexus 7000 48-port 1/10 Gigabit Ethernet SFP+ I/O module (F2-Series) module is a low-latency, high-performance, high-density module that offers most Layer 2 and Layer 3 functions of Cisco NX-OS software. When integrating the F2-Series module into a Cisco Nexus 7000 Series system, observe the following guidelines:

- An F2-Series module requires its own F2-Series module VDC. This VDC is restricted to the F2-Series module; M1 and F1 ports cannot be in the F2-Series module VDC. The default VDC can also be configured as an F2-Series module VDC.
- If you boot up an unconfigured Cisco Nexus 7000 Series switch that contains only F2-Series modules, then the default VDC is automatically configured as an F2-Series module VDC.
- Some software features are not available on the F2-Series module in Cisco NX-OS Release 6.0. These include ACL Capture, ERSPAN, FCoE, GRE tunnels, LISP, MACSEC, MPLS, Netflow, online diagnostics, OTV, PIM-BiDir, and certain counters. Many of these features will be supported in future software releases; however, the F2-Series hardware does not support LISP, MPLS, and OTV, GRE tunnels, and PIM-BiDir so these features will remain unavailable on the F2-Series module.

## Upgrade/Downgrade Caveats

This section includes caveats that relate to upgrading or downgrading Cisco NX-OS software on Cisco Nexus 7000 Series devices.



### Note

Before you upgrade or downgrade your Cisco NX-OS software, we recommend that you read the complete list of caveats in this section to understand how an upgrade or downgrade might affect your network, depending on the features that you have configured.

Do not change any configuration settings or network settings during a software upgrade. Any changes in the network settings may cause a disruptive upgrade.

Refer to [Table 4](#) for the nondisruptive upgrade (ISSU) path to, and nondisruptive downgrade (ISSD) path from Cisco NX-OS Release 6.0(x). Releases that are not listed for a particular release train do not support a direct ISSU or ISSD to the current release.

**Table 4** *ISSU and ISSD Paths to the Current Release*

Current Release	Release Train	Releases That Support ISSU to Current Release	Releases That Support ISSD from Current Release
NX-OS Release 6.0(3)	6.0	6.0(1), 6.0(2)	6.0(1), 6.0(2)
	5.2	5.2(1), 5.2(3a), 5.2(4)	5.2(1), 5.2(3a), 5.2(4)
NX-OS Release 5.2(x)	5.1	5.1(1a), 5.1(3), 5.1(4), 5.1(5), 5.1(6)	5.1(1a), 5.1(3), 5.1(4), 5.1(5), 5.1(6)
	5.0	5.0(5)	5.0(5)
	4.2	4.2(4), 4.2(6), 4.2(8)	4.2(4), 4.2(6), 4.2(8)

## Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

A nondisruptive ISSU to Cisco NX-OS Release 6.0(x) is supported only from Cisco NX-OS Release 5.2(x).



### Note

If you are running an unsupported NX-OS release, you can perform an ISSU or ISSD in multiple steps:

1. Upgrade (or downgrade) to an ISSU-compatible or ISSD-compatible release.
2. Perform additional nondisruptive upgrades (or downgrades) to the current release.

For example, to upgrade from Release 4.2(3) to Release 6.0(1), perform an ISSU from Release 4.2(3) to Release 4.2(6), then perform an ISSU from Release 4.2(6) to Release 5.2(1), and then perform an ISSU from Release 5.2(1) to Release 6.0(1).

A software upgrade or downgrade can be impacted by the following features:

- QoS Policies and ACLs

Before you perform an ISSU from Cisco NX-OS Release 5.2(x) to Release 6.0(x) or perform an ISSU or ISSD between any two Cisco NX-OS 6.0(x) releases, you must first remove QoS policies and ACLs from interfaces that are in the down state. If this action is not performed, the installer process will abort the upgrade or downgrade process, and a message similar to the following will be displayed:

```
Service "ipqosmgr" : Please remove inactive policies using the command "clear
inactive-config qos" Pre-upgrade check failed. Return code 0x415E0055 (Need to clear
inactive-if-config from qos manager using the command "conf;clear inactive-config qos"
or can manually clear the config shown by the command: "show running-config ipqos
inactive-if-config").
```



### Note

The automatic **clear inactive-config qos** command that clears an inactive configuration will delete the port channel policies even if one of the ports in a port channel has inactive policies.

Guidelines for manual policy removal: during a manual removal, when the interface is part of a port channel, remove the policy map or access list from the port channel or remove the interface from the port channel before performing the ISSU or ISSD. For all other interface types, remove the policy map or access list from the interface.

- CoPP

The default Control Plane Policing (CoPP) policy does not change when you upgrade the Cisco NX-OS software.

If you downgrade from Cisco NX-OS Release 6.0(1) without using ISSD to a release earlier than NX-OS Release 5.2(1), the CoPP configuration is lost, and a CoPP policy is no longer attached to the control plane.

- Feature Support

Any features introduced in a release must be disabled before downgrading to a release that does not support those features.

- AES Password Encryption

If you enable the AES password encryption feature and a master encryption key in Cisco NX-OS Release 6.0(1), you must decrypt all type-6 passwords, disable the AES password encryption feature, and delete the master key before downgrading.

- Aggressive Failure Detection Timers

**[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

ISSU and stateful switchover (SSO) are not supported when aggressive failure detection timers are used for all Layer 3 protocols. Starting in Cisco NX-OS Release 5.2, the First Hop Redundancy Protocol (FHRP) with aggressive timers has been validated for SSO or ISSU using the extended hold timer feature. Other protocols such as OSPF have been validated with aggressive timers without SSO or ISSU support. For additional information on aggressive timer support and extended hold timers for FHRP, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*.

- BFD

BFD for static routes does not support a stateful switchover (SSO) or an ISSU. When you perform an ISSU or an SSO, a small amount of packet loss can result in flows that follow static routes that are protected by BFD.

## CMP Images

Cisco NX-OS Release 6.0(3) does not include a new image for the connectivity management processor (CMP).

Cisco NX-OS Release 6.0(1) includes a new image for the CMP. The CMP is upgraded to Release 6.0(1) on successful ISSU to Cisco NX-OS to Release 6.0(1). When the ISSU completes, you should reload the CMP image on the active and standby supervisor modules.

For additional information about the CMP, see the *Cisco Nexus 7000 Series Connectivity Management Processor Configuration Guide*.

## EPLD Images

Cisco NX-OS Release 6.0(3) does not include new EPLD images.

Cisco NX-OS Release 6.0(2) includes a new EPLD image for the Cisco Nexus 7009 chassis fan.

The new hardware introduced in Cisco NX-OS Release 6.0(1) includes new EPLD images. It is not necessary to upgrade existing EPLD images to use Cisco NX-OS Release 6.0(1). For additional information about EPLD images, see the *Cisco Nexus 7000 Series FPGA/EPLD Upgrade Release Notes, Release 6.0*.

## New Hardware Features

Cisco NX-OS Release 6.0 supports the following new hardware:

- N7K-F248XP-25, 48 port 1/10 Gigabit Ethernet SFP+ F2-series I/O module
- N7K-C7010-FAB-2, Fabric 2 module for the Cisco Nexus 7000 10-Slot Chassis (N7K-C7010)
- N7K-C7018-FAB-2, Fabric 2 module for the Cisco Nexus 7000 18-Slot Chassis (N7K-C7018)

For additional information about the F2-series module and the Fabric 2 modules, see the *Cisco Nexus 7000 Series Hardware Installation and Reference Guide*.

## New Software Features

This section describes new software features and includes the following sections:

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

- [Cisco NX-OS Release 6.0\(3\) Software Features, page 18](#)
- [Cisco NX-OS Release 6.0\(2\) Software Features, page 18](#)
- [Cisco NX-OS Release 6.0\(1\) Software Features, page 18](#)

## Cisco NX-OS Release 6.0(3) Software Features

Cisco NX-OS Release 6.0(3) is a maintenance release that includes bug fixes. It does not include new software features.

## Cisco NX-OS Release 6.0(2) Software Features

Cisco NX-OS Release 6.0(2) is a maintenance release that includes bug fixes. It does not include new software features.

## Cisco NX-OS Release 6.0(1) Software Features

Because Cisco NX-OS Release 6.0(1) is primarily a hardware release, only minor software enhancements are introduced. The following enhancements are available in Release 6.0(1):

- [BGP Load Balancing Enhancement](#)
- [RBAC OID Enhancement](#)

## BGP Load Balancing Enhancement

When Border Gateway Protocol (BGP) multipathing is enabled, BGP load balances user traffic within a single autonomous system (AS). The criteria for load balancing is that all attributes must match (weight, LP, AS path, and so on). However when a device is multi-homed to multiple autonomous systems, BGP cannot load balance traffic between the two autonomous systems by default. To enable load balancing of traffic among the multi-homed autonomous systems, use the new **bestpath as-path multipath-relax** command.

## RBAC OID Enhancement

A new role-based access control (RBAC) command is available that allows you to configure a read-only or read-and-write rule for an SNMP object identifier (OID). The **rule number {deny | permit} {read | read-write} oid snmp\_oid\_name** command lets you enter up to 32 elements for the OID. You can use this command to allow SNMP-based performance monitoring tools to poll devices but restrict their access to system-intensive branches such as the IP routing table, ARP cache, MAC address tables, specific MIBs, and so on. The deepest OID can be at the scalar level or at the table root level.

## Licensing

Cisco NX-OS Release 6.0(3), Release 6.0(2), and Release 6.0(1) do not include any new licenses.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## MIBs

Cisco NX-OS Release 6.0(1) adds support for the following MIB:

- [IP-TUNNEL-MIB](#)

## Limitations

This section describes the limitations in Cisco NX-OS Release 6.0 for the Cisco Nexus 7000 Series switches. It includes the following sections:

- [Role-Based Access Control, page 19](#)
- [Standby Supervisor Can Reset With Feature-Set Operation, page 19](#)

## Role-Based Access Control

- Beginning with Cisco NX-OS Release 5.2, you can configure role-based access control (RBAC) in the Cisco Nexus 7000 storage VDC using Cisco NX-OS CLI commands. You cannot configure RBAC in the Cisco Nexus 7000 storage VDC using Cisco DCNM. Note that RBAC in the storage VDC is RBAC for the Cisco Nexus 7000 Series switches, which is different from that for the Cisco MDS 9500 Series switches.
- RBAC CLI scripts used in Cisco MDS 9500 Series switches cannot be applied to the storage VDC configured for a Cisco Nexus 7000 Series switch.
- You cannot distribute the RBAC configuration between a Cisco MDS 9500 Series switch and the storage VDC configured for a Cisco Nexus 7000 Series switch. To prevent this distribution, make sure to assign RBAC in Cisco MDS and the Cisco Nexus 7000 storage VDC to different CFS regions.

## Standby Supervisor Can Reset With Feature-Set Operation

The standby supervisor might reload when a feature-set operation (install, uninstall, enable, or disable) is performed, if the HA state of the standby supervisor is not “HA standby” at the time of the feature-set operation. To prevent the reload, ensure that the state of the standby supervisor is “HA standby.” To check the HA state for the specific VDC where the feature-set operation is performed, enter the **show system redundancy ha status** command on the active supervisor.

A reload of the standby supervisor has no operational impact because the active supervisor is not affected.

In addition, if you perform a feature-set operation while modules are in the process of coming up, then those modules will be power cycled. Modules that are up and in the “ok” state are not power cycled when you perform a feature set operation.

## Caveats

This section includes the following topics:

- [Open Caveats—Cisco NX-OS Release 6.0, page 20](#)

## Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

- Resolved Caveats—Cisco NS-OS Release 6.0(3), page 27
- Resolved Caveats—Cisco NX-OS Release 6.0(2), page 30
- Resolved Caveats—Cisco NX-OS Release 6.0(1), page 32



### Note

Release note information is sometimes updated after the product Release Notes document is published. Use the [Cisco Bug Toolkit](#) to see the most up-to-date release note information for any caveat listed in this document.

## Open Caveats—Cisco NX-OS Release 6.0

- CSCta69220

**Symptom:** A Web Cache Control Protocol (WCCP) redirect configuration on an interface is not removed when TCAM programming fails due to an unsupported combination of features.

**Conditions:** This symptom might be seen when Bank Chaining (Hardware Resource Pooling) is enabled and a WCCP configuration is applied after a RACL configuration. This issue might result in a SBADDFAIL syslog that indicates an unsupported feature combination. The WCCP configuration on the interface is not removed when the error occurs and the WCCP redirect is not programmed in the TCAM.

**Workaround:** Remove the WCCP redirect from the interface. When this operation is done, the SBDELFAIL syslog will appear. Ignore the syslog message and remove the RACL configuration from the interface and reapply the WCCP redirect on the interface. TCAM programming should go through.

- CSCtg90667

**Symptom:** If the netstack process fails, existing BGP sessions might flap and routes might be relearned, which could cause traffic loss.

**Conditions:** This symptom might be seen only when the netstack process fails or terminates ungracefully.

**Workaround:** None.

- CSCtl18412

**Symptom:** Policies such as ACL, QoS, and PBR for FEX interfaces are not cleaned from connecting modules when the FEX fabric ports are moved to another VDC. If those ports are moved back later to the same VDC and configured as a fabric port, or some other ports in same module are configured to be fabric ports, the FEX module might not come online (using those ports), or the relevant policies might not be enforced.

**Conditions:** This symptom might be seen when FEX fabric ports are moved to any other VDC.

**Workaround:** Unconfigure the FEX fabric ports from the fabric port channel before moving them to any other VDC. If this issue occurs, power down the FEX module, remove all FEX configurations, and reconfigure the FEX module again.

- CSCtn27064

**Symptom:** Applying a large egress ACL to an interface might cause BFD flaps.

**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

**Conditions:** This symptom might be seen when a large egress ACL is applied to, or removed from an unrelated Layer 3 physical interface or SVI.

**Workaround:** None.

- CSCto84731

**Symptom:** The linkUp trap is not generated for the management interface.

**Conditions:** This symptom might be seen if the trap is sent out from the management interface.

**Workaround:** None.

- CSCtq41235

**Symptom:** Slow STP convergence occurs after the **shut** and **no shut** commands are entered on a range of interfaces.

**Conditions:** When you enter the **shut** command followed by the **no shut** command on a large range of interfaces, bringing up the interfaces is delayed due to the pacing of the interfaces.

**Workaround:** Specify a smaller range of interfaces when you enter the **shut** and **no shut** commands.

- CSCtq48316

**Symptom:** SNMP fails when `cfcRequestEntryStatus` is set to active.

**Condition:** This symptom might be seen when the `cfcRequestEntryStatus` field in a table in the CISCO-FTP-CLIENT-MIB is set to a value of one.

**Workaround:** None.

- CSCtq65756

**Symptom:** Reloading a switch with many BFD sessions can leave a few port-channel member ports in an error-disabled state on the connected switches.

**Conditions:** This symptom might be seen when there is a heavy BFD and ACL Manager interaction, with many sessions going up or down, and the ACL manager process on the supervisor module can get busy processing BFD-related ACL requests. At the same time, if one or more port-channel members are trying to come up, they fail to be part of that port channel and potentially leave them in a suspended state on the local and remote end.

**Workaround:** Enter the **shut** and **no shut** commands on the member ports of the suspended port-channel members to bring them back up.

- CSCtq73420

**Symptom:** On the 32-port 1/10 Gigabit Ethernet module (N7K-F132XP-15), an ACL policy might be rejected with an atomic failure.

**Conditions:** This symptom might be seen on the 32-port 1/10 Gigabit Ethernet module when an atomic update is configured and policies which need slightly less than 512 TCAM entries are rejected with an atomic failure.

**Workaround:** Configure a nonatomic update if needed.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

- CSCtq84651  
**Symptom:** OSPFv3 advertises the local prefix even though the address is a duplicate in the network.  
**Conditions:** This symptom might be seen when OSPFv3 forms an IPv6 neighbor, even though the local address is a duplicate in the network. This can result in a black hole of traffic to the local IPv6 address.  
**Workaround:** Reconfigure the local address with a unique IPv6 address.
- CSCtq95695  
**Symptom:** DHCP clients fail to get an IP address when they are connected to a FEX Layer 3 port where a DHCP relay is configured.  
**Conditions:** This issue might be seen when feature dhcp is enabled after the FEX module is online.  
**Workaround:** To avoid this issue, enable feature dhcp before you bring up the FEX module. If you experience the issue, take the FEX module offline, and then bring it back online to recover the state.
- CSCtr34219  
**Symptom:** GRE tunnel counters do not increment even though there is valid traffic using the GRE tunnel. Because OTV overlay counters rely on GRE tunnel counters, they also do not increment.  
**Conditions:** This symptom might be seen when the adjacency used by the tunnel adjacency comes from a nonstatistics region, which breaks the tunnel statistics.  
**Workaround:** None.
- CSCtr40010  
**Symptom:** The FEX state is stuck in the Registered state.  
**Conditions:** This symptom might be seen in rare situations when a port is being flapped with the **shut** and **no shut** commands.  
**Workaround:** Enter the **shut** command on the port, reload the FEX module, and then enter the **no shut** command on the port.
- CSCtr45128  
**Symptom:** The **no default val** command on table maps does not remove the default table map value.  
**Conditions:** This symptom might be seen when the **no default val** command is executed for user-defined table map names. System default table maps do not exhibit this behavior.  
**Workaround:** Enter the **default copy** command to the table map to remove the default value.
- CSCtr45329  
**Symptom:** The FEX fabric port is error-disabled with the message “fex: Port is not a port-channel member.”  
**Conditions:** This symptom might be seen when a port that is not a port-channel member is brought up or a port is changed to “switchport mode fex-fabric” while it is up.  
**Workaround:** Enter the **shut** and **no shut** commands on the port after adding the port to a port channel.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

- CSCtr49395

**Symptom:** The running configuration contains lines of a configuration that is no longer valid because they pertain to a feature that was active at some point but has since been disabled. If you try to execute the configuration, you receive syntax errors for those lines. The lines of the configuration in question are these:

**[no] snmp-server enable traps bfd session-up**

**[no] snmp-server enable traps bfd session-down**

**Conditions:** This symptom might be seen anytime the feature BFD is disabled after being enabled.

**Workaround:** None.
- CSCtr58022

**Symptom:** Memory usage of the system manager goes up by approximately 100 KB upon a VDC reload.

**Conditions:** The symptom is not seen with every VDC reload and the triggers for it are unknown.

**Workaround:** None.
- CSCtr63848

**Symptom:** An snmpwalk on the entitySensorMIB for SFP entities does not return entries.

**Conditions:** This symptom might be seen when a module is powered down. If a module is powered down, the entitySensorMIB entries for all modules in the next slots are not returned.

**Workaround:** Keep the modules powered on if the snmpwalk output is needed for entitySensorMIB entries for SFPs.
- CSCtr66076

**Symptom:** An SNMP walk for the BFD MIB timed out during an ISSU.

**Conditions:** This symptom might be seen during an ISSU. The BFD MIB requests may time out.

**Workaround:** Wait for the ISSU to complete, then try the SNMP request again.
- CSCtr67670

**Symptom:** The pixm service displays a critical syslog message that the ltl programming fails for the standby supervisor.

**Conditions:** This symptom might be seen when an EPLD upgrade is performed on the standby supervisor. As part of the EPLD upgrade, the standby supervisor is reloaded. The syslog message from the pixm service is a side-effect of the standby supervisor reload.

**Workaround:** None. There is no operational impact caused by this issue.
- CSCtr70912

**Symptom:** OTV overlay adjacencies might flap when there is a node switchover.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

**Conditions:** This symptom might be seen when the physical node has a large number of VDCs or a large configuration. In such a case, it takes time during the switchover for the OTV-IS-IS process to get its configuration. During that time, neighbors can time out the node that is undergoing the switchover.

**Workaround:** Increase the hello timers to larger than the default values.

- CSCtr76181

**Symptom:** The snmpd process dumps core if you set the managementDomainName with zero-length string in the CISCO-VTP-MIB.

**Conditions:** This symptom might be seen because the value in the SNMP SET operation is set to a zero-length string. If you set the managementDomainName to a non-zero-length value, that works correctly.

**Workaround:** None.

- CSCtr76708

**Symptom:** The aclqos process occasionally fails after a successful ISSD from Cisco NX-OS Release 5.2(1) to Cisco NX-OS Release 5.1(x).

**Conditions:** This symptom might be seen if the COPP policy that is in use in Cisco NX-OS Release 5.2(1) has a class map that refers to “match protocol mpls router-alert.”

**Workaround:** Before performing an ISSD from Cisco NX-OS Release 5.2(1) to Cisco NX-OS Release 5.1(x), remove “match protocol mpls router-alert” from the referring class map and add it back to the same class map after the ISSD completes.

- CSCts64738

**Symptom:** Unicast MAC addresses are learned in FabricPath core switches during a broadcast ARP on a setup with an F2-Series module.

**Conditions:** This symptom might be seen on an F2-Series module when unicast MAC addresses are learned from a broadcast ARP that results in MAC addresses being learned suboptimally in the MAC address table. Further unicast re-ARP messages should take care of MAC addresses being removed on FabricPath core switches. This issue only occurs in switches with F2-Series modules.

**Workaround:** None.

- CSCtt00148

**Symptom:** Memory leaks occur when port-security dynamic MAC addresses are aged out and then relearned.

**Conditions:** This symptom might be seen only for port-security dynamic MAC addresses. (It is not seen with static and sticky MAC addresses.) There are two types of aging: absolute and inactive. For the absolute timer, the MAC addresses are aged out after the specified number of minutes (aging time). For the inactivity timer, the MAC addresses are aged out if they are inactive for the specified aging time. If there is still traffic after the MAC addresses are aged out, then they are relearned. In this case, memory leaks occur.

**Workaround:** None.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

- CSCtt18403

**Symptom:** An OSPFv3 instance has some interfaces that remain in the down state after the **copy file running-configuration** command is executed.

**Conditions:** This symptom might be seen when there are no IPv4 addresses configured on the switch. As a result, OSPFv3 cannot pick a router ID from the system.

**Workaround:** Unconfigure the router ID and then reconfigure it in router OSPFv3 mode.
- CSCtt97386

**Symptom:** If Unicast Reverse Path Forwarding (uRPF) is enabled on a Layer 3 interface and the mode of the port is changed to switchport and then changed back to Layer 3 interface, then the uRPF configuration is still present on the interface. On configuring Layer 3 again on the port, there is no uRPF configuration on the port and no configuration should be there in the hardware too.

**Condition:** This symptom might be seen when the stale configuration is present in the hardware only when the transition of the ports is as described in the Symptom.

**Workaround:** Enable and disable uRPF again on the interface.
- CSCtu61247

**Symptom:** When an F2 Series module port is configured to operate at 1G port rate, changing the CoS to queue mapping on an oversubscribed port might cause the ports to go to a hardware failure state.

**Conditions:** This symptom might be seen when the CoS to queue mapping on an oversubscribed port with both credited (known Unicast traffic) and uncredited traffic (multicast, broadcast, or unknown unicast traffic) is changed. The result can be a fatal exception and ports are marked as a hardware failure.

**Workaround:** Stop all user traffic on the port or ensure that the port is not oversubscribed when performing CoS to queue mapping change.
- CSCtw81313

**Symptom:** The SNMP process leaks memory during an SNMP get operation on the lldpStatsTxPortTable or lldpStatsRxPortTable objects.

**Condition:** This symptom might be seen when you perform a **getone** or **getnext** operation on the LLDP MIB objects.

**Workaround:** None. Reduce the frequency of accessing these MIB objects so that the memory leak is slower.
- CSCtw88289

**Symptom:** A module upgrade fails during an ISSU from Cisco NX-OS Release 6.0(1) to Release 6.0(2).

**Conditions:** This symptom might be seen when there is a large ACL or QoS policy configuration. An ISSU from Cisco NX-OS Release 6.0(1) to Release 6.0(2) might fail due to a aclqos process timeout on the module.

**Workaround:** Retry the ISSU. Alternatively, reload the modules after the failure.

**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

- CSCtw93199

**Symptom:** Some of the dynamically learned MAC addresses might point to the wrong interface.

**Conditions:** This symptom might be seen in an unstable Layer 2 topology that could be caused by a Layer 2 loop or any event where a peer link can drop traffic which results in a mac-sync across a vPC peer to be out of sync.

**Workaround:** Enter the **clear mac address dynamic** command for a specific MAC address or VLAN where the issue is seen. This command clears the MAC address and correctly relearns the MAC address across peers.
- CSCtw93913

**Symptom:** Flooded traffic may not reach all FabricPath switches in a network where FabricPath is deployed.

**Conditions:** This symptom might be seen if FabricPath is included in the flood outgoing interfaces list and it is moved to a port channel.

**Workaround:** Enter the **shut** command on the FabricPath member port and ensure that it is not a member of an outgoing flood list before adding it to a port channel. Enter the **show l2 mroute flood vlan *vlan-id*** command to verify that the member port is not a part of the flood outgoing interface list.
- CSCtw95584

**Symptom:** There are insufficient TCAM entries in a bank.

**Conditions:** This symptom might be seen only when bank chaining is enabled. When very large policies that belong to multiple classes (such as IPv4, IPv6 and so on) are applied on the same interface, they fill up the entire TCAM part of a single session, which exposes this issue.

**Workaround:** Do not apply policies belonging to multiple classes in the same session. If they are applied in different sessions, this issue is not seen.
- CSCtw95999

**Symptom:** Flowcontrol cannot be configured on a port-channel interface after an ISSU. The following error can be seen:

```
switch(config)# interface port-channel 5
switch(config-if)# flowcontrol receive on
ERROR: port-channel5: no such pss key
```

**Conditions:** This symptom might be seen following an ISSU from Cisco NX-OS Release 6.0(1) to Release 6.0(2).

**Workaround:** Remove the port channel and create it again.
- CSCtw98942

**Symptom:** IGMP has the state for a route on a particular interface, but that interface is not listed in the fanout of the route in hardware or in the Multicast Routing Information BASE (MRIB).

**Conditions:** This symptom is extremely rare. If the Protocol Independent Multicast (PIM) expires the route and if at the same time IGMP has MRIB informs about an interface for the same route, a PIM delete can silently remove this interface from the route in the MRIB.

**Workaround:** Enter the **clear ip mroute group** command to address this issue.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

- CSCtw99546
 

**Symptom:** When you enter the **limit-resource module-type** command to change support from F1 to M1, the command might take 10 minutes to run. After that time, the command succeeds and there are no further issues.

**Conditions:** This symptom might be seen when you enter the **limit-resource module-type m1** command on a VDC that previously supported the F1 module type.

**Workaround:** None.
- CSCtx02315
 

**Symptom:** A vPC fails and comes back up.

**Conditions:** This symptom might be seen in a rare race condition when a role priority is changed and the peer link is flapped. There is no functional impact however, because the running configuration is restored and traffic flow continues as expected.

**Workaround:** None.

## Resolved Caveats—Cisco NS-OS Release 6.0(3)

- CSCtn64672
 

**Symptom:** Too many MAC address moves over a vPC peer link can cause the l2fm process to fail or the chassis to reload. The output of the **show system reset-reason** command indicates that the reload reason is caused by a l2fm hap reset.

**Conditions:** This symptom might be seen under normal operating conditions of a Cisco Nexus 7000 Series switch.

**Workaround:** This issue is resolved.
- CSCts55243
 

**Symptom:** A MAC address is in VLAN 4042 instead of in another VLAN, which also prevents the static MAC address from being added to that VLAN.

**Conditions:** This symptom might be seen following an ISSU from Cisco NX-OS Release 5.1(x) to Release 5.2(1).

**Workaround:** This issue is resolved.
- CSCtw65614
 

**Symptom:** During an ISSU, a module with a FEX connected to it fails to upgrade from Cisco NX-OS Release 5.1(3) to Release 5.2(3a), or from Release 5.1(3) to Release 5.2(1) to Release 6.0.

The following output might be seen:

```
Module 1: Non-disruptive upgrading.
[#          ] 0
<snip>
[#          ] 0% -- FAIL.
Return code 0x401D002D (Module Manager initiated failure routine after a timeout
occurred).
```

## Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

**Conditions:** This symptom might be seen on a 32-port, 10-Gigabit Ethernet SFP+ I/O module (N7K-M132XP-12) with a FEX module connected to it, and an ISSU from Cisco NX-OS Release 5.1(3) to Release 5.2(3a) is performed.

**Workaround:** This issue is resolved.

- CSCtw90418

**Symptom:** The Cisco PROCESS MIB times out during an snmpwalk when SNMPv3 is used.

**Conditions:** This symptom might be seen when the Cisco PROCESS MIB library tries to create a file and write the information for all the services on the switch into that file before sending a response back to the front end SNMP that handles the SNMP requests.

**Workaround:** This issue is resolved.

- CSCty02134

**Symptom:** When bringing up new SVI interfaces, the following message appears on the switch:

```
%IFTMC-SLOT4-2-IFTMC_RES_ALLOC_FAIL: IFTMC resource allocation failure: No. of ASIC LIF left 0, total 4040.
```

**Conditions:** This symptom might be seen when you do the following:

- Create VLANs
- Create the SVI and IP address
- Assign the VLAN to the allowed VLAN list of the peer link

The message is seen in the context of creating VLAN SVI 2100.

**Workaround:** This issue is resolved.

- CSCty21455

**Symptom:** Routing protocols might flap on a switch that is running Cisco NX-OS Release 6.0(1) or Release 6.0(2) when the neighbors are attached through a Layer 3 interface or a Layer 2 access port.

**Conditions:** This symptom might be seen when there is heavy inband congestion for extensive periods of time.

**Workaround:** This issue is resolved.

- CSCty23808

**Symptom:** A Cisco Nexus 7000 Series switch that is running Cisco NX-OS Release 6.0(2) with F2 series modules might exhibit an issue when traffic hits a null0 route in hardware. The F2 SoC will leak the traffic that hits the null0 route to inband through a hardware rate-limiter when the ingress port is a Layer 3 port that has the **ip redirects** command enabled.

**Conditions:** This symptom might be seen when the following conditions are met:

- Traffic has to come into the Cisco Nexus 7000 Series switch on an F2 series module.
- The port has to have the **ip redirects** command enabled.
- The route lookup for the destination must point to null0, such as ip route 10.0.0.0/8 null0

**Workaround:** This issue is resolved.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

- CSCty33791

**Symptom:** IGMPv3 packets are looped if they arrive on a vPC. It does not matter if you have one port or multiple ports in vPC.

**Conditions:** This symptom might be seen when a packet arrives on a vPC port channel. The vPC can have one port or multiple ports.

**Workaround:** This issue is resolved.
  
- CSCty61797

**Symptom:** A vPC with policy-based routing (PBR) breaks the IPv6 neighbor discovery process.

**Conditions:** This symptom might be seen when you have peer gateway and PBR enabled.

**Workaround:** This issue is resolved.
  
- CSCtz01464

**Symptom:** A server that is connected to two Cisco Nexus 2232PP Fabric Extenders that are connected to two Cisco Nexus 7000 Series switches with a F2 Series module must download an image via PXE boot. During this time it cannot send LACP PDU and therefore the **no lacp suspend-individual** command must be configured to prevent the Cisco Nexus 7000 Series switch or the Cisco Nexus 2232PP FEX from suspending host interface links towards the server. After this was configured, links were still suspended and the server failed to download its image.

**Conditions:** This symptom might be seen when a server that is connected to two Cisco Nexus 2232PP Fabric Extenders that are connected to two Cisco Nexus 7000 Series switches with a F2 Series module must download an image via PXE boot.

**Workaround:** This issue is resolved
  
- CSCtz01813

**Symptom:** Any port that connects any Fabric Extender (FEX) device that is terminated on the 48-port, 1/10 Gigabit Ethernet SFP+ I/O F2-Series module (N7K-F248XP-25) in a Cisco Nexus 7000 Series chassis might become error disabled and possibly cause the FEX to go offline.

**Conditions:** This symptom might be seen only on ports of the 48-port 1/10 Gigabit Ethernet SFP+ I/O F2-Series module.

**Workaround:** This issue is resolved.
  
- CSCtz10290

**Symptom:** When a Cisco Nexus 7000 Series switch is a rendezvous point (RP) and a Cisco IOS device such as a Catalyst 4900M is a first-hop and last-hop router, the Cisco Nexus 7000 Series device does not return a registration stop when it receives a multicast source registration and PIM (S,G,R) prune message back-to-back. As a result, the S,G route gets stuck in registration mode on the IOS router and it has to software switch the multicast packets, which causes high CPU utilization.

**Conditions:** This symptom might be seen in a topology where a Cisco Nexus 7000 Series switch is a rendezvous point (RP) and a Cisco IOS device such as a Catalyst 4900M is a first hop and last hop router.

**[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

**Workaround:** This issue is resolved.

- CSCtz10925

**Symptom:** Ports on an F2-Series module fail with the error  
CLP\_PS\_INT\_ERR\_FLD\_EG\_PKT\_PNUM\_ER.

**Conditions:** This symptom might be seen when ASIC interrupts occur for packets with random packet headers. These interrupts should be ignored.

**Workaround:** This issue is resolved.

## Resolved Caveats—Cisco NX-OS Release 6.0(2)

- CSCtr95031

**Symptom:** When you enable LDP, the following message appears:

```
TRANSPORT_SERVICES_PKG license not installed. ldp feature will be shut down after
grace period of approximately x day(s).
```

**Conditions:** This symptom might be seen when you enable LDP.

**Workaround:** This issue is resolved.

- CSCts11774

**Symptom:** Shutting down the SVI caused the ipfib process to fail.

**Conditions:** This symptom might be seen on a Cisco Nexus 7000 Series switch that is running NX-OS Release 5.1(3).

**Workaround:** This issue is resolved.

- CSCtt12365

**Symptom:** Multicast Listener Discovery (MLD) groups are not added back to the IPv6 multicast routing table (M6RIB) after a module reload.

**Conditions:** This symptom might be seen following a module reload.

**Workaround:** This issue is resolved.

- CSCtt35503

**Symptom:** When a Cisco Nexus 7000 Series switch receives giant packets with CRC errors on an F2-Series module, they are not counted as giant packet counters.

**Conditions:** This symptom might be seen on an F2-Series module. When an interface MTU is set to a value smaller than 9216 and packets that are larger than the MTU value are received, they are counted as Jumbo packets.

**Workaround:** This issue is resolved.

- CSCtt44718

**Symptom:** Precision Time Protocol (PTP) does not work on port channel members.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

**Conditions:** This symptom might be seen in Cisco NX-OS Release 6.0(1) under normal operating conditions.

**Workaround:** This issue is resolved.

- CSCtt46089

**Symptom:** Ftag-1 is not set on a port channel after a FabricPath port channel is changed to trunk and then changed back to FabricPath.

**Conditions:** This symptom might be seen when it is triggered by a manual intervention, when a FabricPath core port is moved to CE mode and back to FabricPath mode.

**Workaround:** This issue is resolved.

- CSCtt69008

**Symptom:** A SWID is not programmed in an F2-Series module after an ISSU from Cisco NX-OS Release 5.2(1) to Release 6.0(1).

**Conditions:** This symptom occurs only if an F2-Series module is brought up in Release 6.0(1) in a VDC that existed in Release 5.2(1) and was converted to a F2-Series module VDC.

**Workaround:** This issue is resolved.

- CSCtt97142

**Symptom:** If an ISSU aborts during an upgrade of any of the modules in the switch, multicast packets are not copied at the first hop router and S,G states are not created on other modules in the system.

**Conditions:** This symptom might be seen when a module upgrade is aborted.

**Workaround:** This issue is resolved.

- CSCtt97357

**Symptom:** If you have IPv4 or IPv6 static routes with Equal Cost Multiple Paths (ECMP), the adjacency for the next hop for certain paths might not be resolved which can affect hardware packet forwarding.

**Conditions:** This symptom might be seen only with IPv4 or IPv6 Static ECMP routes.

**Workaround:** This issue is resolved.

- CSCtt98508

**Symptom:** Packet loss can happen when Layer 3 FEX subinterfaces and Layer 2 Trunk FEX interfaces on the same fabric interface share the VLAN number space.

**Conditions:** This symptom might be seen when the FEX interfaces belong to the same fabric interface. The Layer 3 FEX subinterface.1q tag and Layer 2 FEX trunk VLAN space clash and can cause packet loss.

**Workaround:** This issue is resolved.

- CSCtw88133

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

**Symptom:** Starting with Cisco NX-OS Release 6.0, empty vPC+ links should have a reserved Service Set Identifier (SSID). Prior to Cisco NX-OS Release 6.0, empty vPC links have a valid SSID (11-254).

Upon an ISSU to NX-OS Release 6.0, empty vPC+ links might end up with a valid Service Set Identifier (SSID) (11-254). Upon ISSU from NX-OS Release 6.0, empty vPC+ links might end up with the reserved SSID (1).

**Conditions:** This symptom might be seen if there are empty vPC+ links when you perform an ISSU to Cisco NX-OS Release 6.0 or an ISSU from Cisco NX-OS Release 6.0.

**Workaround:** This issue is resolved.

## Resolved Caveats—Cisco NX-OS Release 6.0(1)

- CSCsw24739

**Symptom:** The `ipv6_next_hop` value is missing in the captured NetFlow packets.

**Conditions:** This symptom might be seen when exporting packets at a high rate.

**Workaround:** This issue is resolved.

- CSCtc82869

**Symptom:** When there is a vPC configured between two Cisco Nexus 7000 Series switches that are connected by a port channel and the **shut** and **no shut** commands are entered on the peer link on the primary vPC, there is a system failure and a core dump is generated.

**Conditions:** This symptom might be seen when the vPC is configured between the two Cisco Nexus 7000 Series switches and the interface port channel is bounced.

**Workaround:** This issue is resolved.

- CSCtj44206

**Symptom:** The internal queue overflowed after the **copy running-config startup-config** command was entered. A syslog can be seen in the output of the **show logging** command on the supervisor module.

```
%KERN-2-SYSTEM_MSG: Utaker overflowed. Size -40/5242880 - kernel
```

**Conditions:** This symptom might be seen when a large number of processes exit or fail.

**Workaround:** This issue is resolved.

- CSCtq03187

**Symptom:** The subswitch ID for a vPC on the secondary switch is incorrectly programmed in the hardware as 1 (reserved) even though it has the correct SSID, as can be seen in the output of the **show vpc brief** command.

**Conditions:** This symptom might be seen in the following situation:

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

- Configure a vPC port channel on a secondary switch (for example, vPC 1 and port channel 1) and make sure that from the access switch's perspective (that is, port channel 1), only the links going to the secondary switch are up. (If the port channel 1 links from the access switch to primary switch are also up, then this problem will not occur.)
- Configure the corresponding vPC on the primary switch.

**Workaround:** This issue is resolved.

- CSCtq33715

**Symptom:** The DTFM services fails four times and the 32-port 1/10 Gigabit Ethernet module (F1-Series) goes into failure mode.

**Conditions:** This symptom might be seen when more than 4000 VLANs are created on the 32-port 1/10 Gigabit Ethernet module. Internally the failure occurs because of the corresponding SVI creation for those VLANs. The failure happens when the module is supporting more than 1 VDC and the total VLAN count across all VDCs is greater than 4000. Such VLAN scale numbers are not currently supported taking into account the total Layer 2 group features supported on Cisco Nexus 7000 Series switches.

**Workaround:** This issue is resolved.

- CSCtq34950

**Symptom:** Ports randomly lose connectivity and the following error message can be seen:

```
%MODULE-2-MOD_SOMEPORTS_FAILED: Module 2 (serial: XXXXXXXX) reported failure on ports
2/36-2/36 (Ethernet) due to R2D2 : Speed patch failed - no frames transmitted in device
143 (error <error-code>)
```

**Conditions:** This symptom might be seen with the Cisco Nexus 7000 48-port 10/100/1000 Ethernet I/O module (N7K-M148GT-11).

**Workaround:** This issue is resolved.

- CSCtq57444

**Symptom:** Spanning Tree Protocol (STP) shows a VLAN in PVID\_Inc state on the trunk port between two Cisco Nexus 7010 switches with a 32-port 10-Gigabit Ethernet SFP+ I/O module (N7K-M132XP-12).

**Conditions:** This symptom might be seen after one port in EtherChannel (E1/9) is bounced to recover from a Unidirectional Link Detection (UDLD) error disabled state.

**Workaround:** This issue is resolved.

- CSCtq58558

**Symptom:** SSO routes might be deleted on a EIGRP peer in a scale setup.

**Conditions:** When there are a large number of routes that are redistributed into EIGRP and the source protocol takes longer to converge than EIGRP does, routes are deleted from the EIGRP peer on SSO.

**Workaround:** This issue is resolved.

- CSCtr07544

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

**Symptom:** In a network where FabricPath is deployed, packets can loop until the Time to Live (TTL) on the packet expires.

**Condition:** This symptom might be seen in a FabricPath topology with M1 series modules on the edge for ingress flows and two or more non-port-channel parallel links between the FabricPath core switches.

**Workaround:** This issue is resolved.

- CSCtr17002

**Symptom:** When a parent interface goes down, allocated VLANs are created in the owner VDC.

**Workaround:** This issue is resolved.

- CSCStr11036

**Symptom:** CDP discovery does not occur when ports are Layer 2 to Layer 3 with a native VLAN on a Layer 2 VLAN 1.

**Conditions:** This symptom might be seen when a Layer 2 trunk port on a Catalyst 6000 switch with native a VLAN other than 1 is connected to a Layer 3 port on a Cisco Nexus 7000 Series switch that does not have a subinterface with VLAN 1. In this configuration, CDP neighbors are not seen. The symptom is not seen if the Layer 2 trunk port is configured with native VLAN 1.

**Workaround:** This issue is resolved.

- CSCtr21843

**Symptom:** Local MDT routes are not present in the BRIB.

**Conditions:** This symptom might be seen in the router BGP mode, if the following events occurred:

- address-family ipv4 mds was not configured under router BGP mode.
- address-family ipv4 mdt was configured and then it was removed if BGP is restarted, or if the device is reloaded with this configuration (where there is no MDT AF in the router bgp mode).

The local MDT routes gets removed from BRIB.

**Workaround:** This issue is resolved.

- CSCtr25965

**Symptom:** In some scalability setups, where there are a lot of FEX modules and lot of HIF vPCs, a reload of all the fabric modules (which in turn causes a reload of all the FEX modules), can cause some satellite interfaces (FEX ports) to become error-disabled after the reload. Syslog messages are also generated with more details on specific ports that are error-disabled.

**Conditions:** This symptom might be seen in scale setups when all the fabric modules that are connected to all the FEX modules are reloaded.

**Workaround:** This issue is resolved.

- CSCtr33173

**Symptom:** A Cisco Nexus 7000 Series switch repeatedly has ACLQOS service failures followed by module resets:

## Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

```
%SYSMGR-SLOT3-2-SERVICE_CRASHED: Service "aclqos" (PID 27249) hasn't caught signal 6
(core will be saved).
%SYSMGR-SLOT3-2-SERVICE_CRASHED: Service "aclqos" (PID 18426) hasn't caught signal 11
(core will be saved).
%IPQOSMGR-4-QOSMGR_LC_SESSION_ERROR_MSG: Linecard 2 returned the following error for
statistics session: Operation timed out.
%IPQOSMGR-4-QOSMGR_LC_SESSION_ERROR_MSG: Linecard 3 returned the following error for
statistics session: Operation timed out.
%IPQOSMGR-4-QOSMGR_LC_SESSION_ERROR_MSG: Linecard 1 returned the following error for
statistics session: Operation timed out.
%SYSMGR-SLOT3-2-SERVICE_CRASHED: Service "aclqos" (PID 18605) hasn't caught signal 11
(core will be saved).
%ETHPORT-5-IF_SEQ_ERROR: Error ("sequence timeout") communicating with MTS_SAP_SPM
for opcode MTS_OPC_ETHPM_PORT_LOGICAL_CLEANUP (RID_PORT: Ethernet<mod/port>)
%MODULE-2-MOD_DIAG_FAIL: Module 3 (serial: JXXXXXXXX) reported failure due to Service
on linecard had a hap-reset in device 134 (device error 0x16e)
```

**Conditions:** This issue might be seen on a Cisco Nexus 7000 Series switch that is running Cisco NX-OS Release 5.1(3). The issue persists after a switch reload

**Workaround:** This issue is resolved.

- CSCtr33544

**Symptom:** The **copy running-config startup-config** command aborts.

**Conditions:** This symptom might be seen when there are repeated **copy running-config startup-config** commands.

**Workaround:** Reset the standby supervisor.

- CSCtr36566

**Symptom:** On a Cisco Nexus 7000 Series switch, any change to the summer-time configuration (daylight saving time) is not correctly updated in the RPM.

**Conditions:** This symptom might be seen if you enter the clock summer-time command and attempt to make changes to the summer-time configuration. Even though the output of the show clock detail command will show the correct summer-time settings, the changes are not updated in the RPM which can affect other components, such as key chains, that rely on timing.

**Workaround:** This issue is resolved.

- CSCtr42896

**Symptom:** The output of the **show running config** command shows type-7 secrets with encryption services enabled instead of type-6.

**Conditions:** This issue might be seen only in a dual-supervisor system following a supervisor switchover. The issue occurs in the following situation:

- Applications such as RADIUS or TACACS have type-7 secrets configured.
- Encryption service is enabled.
- The **encryption reencrypt** command is entered.
- A supervisor switchover is performed.

## Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

The **show running config** command displays type-7 secrets instead of the expected type-6 secrets. The same issue can occur with the **encryption delete** command and the **encryption decrypt** command.

**Workaround:** This issue is resolved.

- CSCtr52593

**Symptom:** Two protocols add the same route: OSPF and RIP. The admin distance of RIP is configured to be the same as OSPF. If the metric for the RIP route is better than the OSPF route, the RIP route is selected (which is incorrect behavior).

**Conditions:** This symptom might be seen when two protocols are configured to have the same admin distance. If RIP and OSPF are configured to have the same admin distance, the software chooses the route with the lower metric. Because metrics do not have any meaning across protocols and only within a protocol, this selection does not make sense. The route found by the protocol with the lower default admin distance should be selected.

**Workaround:** This issue is resolved.

- CSCtr54250

**Symptom:** A module might get reloaded more than once before it comes up. In rare cases, the ports in the module might be up before the module is reloaded once. When the module is reloaded slightly after the ports are brought up, an adjacent switch might see a port flap.

**Conditions:** This symptom might be seen if the FCoE feature set is installed on a storage VDC upon a cold boot of the switch, but this is an extremely rare occurrence.

**Workaround:** This issue is resolved.

- CSCtr60525

**Symptom:** A VLAN specific configuration may fail when you try to roll back to the previous checkpoint after configuring a new reserved VLAN range.

**Conditions:** This symptom might be seen once you configure the system reserved VLAN range. All the VLAN configurations for the new range get deleted from the running configuration and any checkpoint that has a VLAN configuration in the new range also become obsolete.

At this point in time, if you roll back to an earlier checkpoint, the rollback fails for the VLAN configuration in the new reserved range.

**Workaround:** This issue is resolved.

- CSCtr65510

**Symptom:** Some of the **wccp show** commands do not display the output completely. The following **show** commands are affected:

- **show ip wccp service\_group number mask**
- **show ip wccp service\_group number detail**
- **show ip wccp service\_group number internal**
- **show ip wccp**
- **show system internal wccp config-dump**

## Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

**Conditions:** This symptom might be seen when the mask value is 64 or greater or when there are many service groups (roughly greater than 20). The output is not displayed completely because the TLVs used to send the information to the frontend are not big enough to store all the necessary information.

**Workaround:** This issue is resolved.

- CSCtr66043

**Symptom:** The RESOURCE\_UNAVAILABLE\_ERROR was received when walking mplsLabelStackTable.

**Conditions:** This symptom might be seen when walking the LSR MIB on a scaled topology with 75,000 or more local labels in use.

**Workaround:** This issue is resolved.

- CSCtr72438

**Symptom:** VRRP groups become master-master, with text authentication enabled. The following syslog messages are displayed:

```
Jul 26 23:01:06.870 IST: %VRRP-4-BADAUTH: Bad authentication from 100.100.199.2,
group 3, type 1
```

**Conditions:** This issue might be seen if VRRP groups form peers with devices other than Cisco Nexus 7000 Series switches, authentication is enabled, and the password configured is less than eight characters.

**Workaround:** This issue is resolved.

- CSCtr75627

**Symptom:** If a port-channel member is removed and readded back to a dce-core port-channel, in some cases it is possible that traffic might not flow on that member.

**Conditions:** This symptom might be seen because the CBL is set to blocked.

**Workaround:** This issue is resolved.

- CSCtr79772

**Symptom:** Traffic loss occurs after a BGP restart in a 1 DPS scale setup.

**Conditions:** This symptom might be seen when you do the following:

- Configure 1000 VRFs and pump 300,000 routes in per-prefix label mode in a specific topology.
- Send traffic from remote to local devices.
- Perform a BGP restart.

The issue occurs in the following setups:

Non-VDC:

- 1000 VRFs and 300,000 routes in per-prefix mode
- 1000 VRFs and 500,000 routes in per-vrf mode

3 VDCs:

- 1000 VRFs and 300,000 routes in per-prefix mode

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

- 1000 VRFs and 500,000 routes in per-vrf mode

**Workaround:** This issue is resolved.

- CSCtr79988

**Symptom:** After an ISSU, the following error messages can be seen when the vPC peer link flaps:

```
%ETH_PORT_CHANNEL-3-PCM_HWCFG_FAIL_ERROR: Port-channel:port-channel1
mbr:Ethernet1/5 SAP 176 returned error Unknown error 1088421890 for opc
MTS_OPC_PIXM_MOD_MEMB_LTL; if lacp port-channel please collect <show
tech-support lacp all> or please collect <show tech-suppor
```

**Conditions:** This symptom might be seen when the following conditions are met:

- A vPC is configured.
- Only the peer link is affected (not the vPC members).
- A vPC needs to be configured and removed again before the ISSU.
- An ISSU is performed.
- The peer link need to be flapped (it can go down for any reason).

**Workaround:** This issue is resolved.

- CSCtr88786

**Symptom:** Reloading an OTV VDC causes an OTV adjacency to immediately come up, but the **show otv isis adjacency** command shows that the neighbor name is not resolved and no IS-IS LSP is received from the neighbor until 8 to10 minutes later.

**Conditions:** This symptom might be seen when you reload the OTV VDC.

**Workaround:** This issue is resolved.

- CSCtr88815

**Symptom:** Following a reload of a Cisco Nexus 7000 Series switch that has a core VDC and an OTV VDC, the other site ED cannot establish an OTV adjacency with the VDC on the reloaded switch. The other site ED has \*,G for the OTV core multicast group and s,g for the other ED, but no s,g for the reloaded ED.

**Conditions:** This symptom might be seen when you reload a Cisco Nexus 7000 Series switch.

**Workaround:** This issue is resolved.

- CSCtr92742

**Symptom:** When the ACL manager stops responding, access-group commands cannot be removed from a bound interface.

**Conditions:** This symptom might be seen in very rare cases under continuous test cycles when a large ACL (40,000+ lines) is added to a running configuration.

**Workaround:** This issue is resolved.

- CSCtr97385

## Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

**Symptom:** SNMP can fail when the config-copy MIB is used.

**Conditions:** This symptom might be seen when there are missed heartbeats.

**Workaround:** This issue is resolved.

- CSCts00210

**Symptom:** A type-3 default gateway summary route is sent to Area 0 from an Area Border Router (ABR).

**Conditions:** This symptom can be seen only if stub areas are configured and there is a type-5 default route in the database. If both of these conditions are not met, the symptom cannot occur.

This issue can be triggered by an interface flap of OSPF neighbors, a module reload, or the **clear ip ospf neighbor** command. The probability of this issue occurring is higher if many neighbors flap at the same time, but it does not occur at each flap.

**Workaround:** This issue is resolved.

- CSCts08764

**Symptom:** After supervisors fail over in a Cisco Nexus 7000 Series switch, a VDC may show as failed in the output of the **show vdc** command:

```
switch# show vdc
N7K# show vdc
vdc_id  vdc_name      state    mac                lc
-----  -
<snip>
2       VDC2            failed   <mac-address>     m1 f1 m1x1
<snip>
```

**Conditions:** This symptom might be seen immediately after a forced switchover between supervisors.

**Workaround:** This issue is resolved.

- CSCts27542

**Symptom:** You cannot enter the **system startup-config unlock x** command when *x* is greater than 65536.

**Conditions:** This symptom might be seen under normal operating conditions for a Cisco Nexus 7000 Series switch.

**Workaround:** This issue is resolved.

- CSCts29458

**Symptom:** A memory leak occurs during a MIB walk of the CISCO-STP-EXTENSIONS-MIB.

**Conditions:** This symptom might be seen on a switch running Cisco NX-OS Release 5.2(1) when there is a MIB walk of the CISCO-STP-EXTENSIONS-MIB.

**Workaround:** This issue is resolved.

**[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

- CSCts35587

**Symptom:** A supervisor failover occurs on a Cisco Nexus 7000 Series switch when the **show diff rollback-patch running-config startup-config** command is entered while a module is booting up.

```
2011 Aug 23 04:06:09 Nexus7K %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service
"ethpm" (PID 5223) hasn't caught signal 11 (core will be saved).
2011 Aug 23 04:06:09 Nexus7K %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service
"ethpm" (PID 30011) hasn't caught signal 11 (core will be saved).
2011 Aug 23 04:06:10 Nexus7K %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service
"ethpm" (PID 30013) hasn't caught signal 11 (core will be saved).
```

```
switch# show cores vdc-all
```

VDC	Module	Instance	Process-name	PID	Date(Year-Month-Day Time)
1	6	1	ethpm	30013	2011-08-23 04:23:33
1	6	1	ethpm	5223	2011-08-23 04:23:35

**Conditions:** This symptom might be seen on a Cisco Nexus 7000 Series switch running Cisco NX-OS Release 5.1(1) that has modules booting up while a CLI command is executing.

**Workaround:** This issue is resolved.

- CSCts45337

**Symptom:** When an ISSU from Cisco NX-OS Release 5.1(3) to Release 5.2(1) is performed on a Cisco Nexus 7000 Series switch, the MTU on the Layer 3 port channel interfaces that have a jumbo MTU configured will be misprogrammed in hardware which will result in traffic being switched incorrectly in software and will cause poor performance.

**Conditions:** This symptom might be seen when you perform an ISSU upgrade to Cisco NX-OS Release 5.2(1) on a Cisco Nexus 7000 Series switch that is running Cisco NX-OS Release 5.1(3).

**Workaround:** This issue is resolved.

- CSCts50402

**Symptom:** On a Cisco Nexus 7000 Series switch that is running Cisco NX-OS Release 5.1(2), DHCP offers with a client MAC address of 0000.0000.0000 are dropped and are not forwarded to the client.

**Conditions:** This symptom might be seen specifically with devices that use a client MAC address of all zeroes in the Bootp portion of the packet.

**Workaround:** This issue is resolved.

- CSCts53540

**Symptom:** A Cisco Nexus 7000 Series switch that is running Cisco NX-OS Release 5.2(1) is not serving NTP to NTP clients that are not directly connected.

**Conditions:** This symptom might be seen when the NTP server for a Cisco Nexus 7000 Series switch responds only to directly connected NTP clients.

**Workaround:** This issue is resolved.

**[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

- CSCts55243

**Symptom:** A MAC address shows up in VLAN 4042 instead of in another VLAN, which also prevents the static MAC from being added to that VLAN.

**Conditions:** This symptom might be seen following an ISSU from Cisco NX-OS Release 5.1(x) to Release 5.2(1).

**Workaround:** This issue is resolved.
  
- CSCts68444

**Symptom:** A connectivity issue occurs on an existing port channel when a new port channel is brought up or an existing port channel is flapped.

**Conditions:** This symptom might be seen in a port channel with more than one member that goes from a FEX to the end hosts.

**Workaround:** This issue is resolved.
  
- CSCts73997

**Symptom:** The eth\_port\_channel service might fail and display the following syslog message:  
"SYSMGR-2-SERVICE\_CRASHED: Service "eth\_port\_channel" (PID 28252) hasn't caught signal 6 (core will be saved)."

**Conditions:** This symptom might be seen if you enter the **show running** command or the **show startup** command many times. A memory leak occurs in the service eth\_port\_channel when handling this operation.

**Workaround:** This issue is resolved.
  
- CSCts771340

**Symptom:** An ISSU from Cisco NX-OS Release 4.2(4) to Release 5.1(3) can cause an internal process to fail. In addition, the ISSU might be incomplete which can cause a few modules to remain on Release 4.2(4).

**Conditions:** This symptom might be seen when an ISSU from Cisco NX-OS Release 4.2(4) is performed.

**Workaround:** This issue is resolved.
  
- CSCts77257

**Symptom:** The summary route is missing from the RIB, but the LSA that corresponds to the prefix is present in the OSPF database.

**Conditions:** This symptom might be seen under the following conditions:

  - A **summary-address** command is configured on a router.
  - The summary address has no component routes to advertise that fall in that summary.
  - The router receives a LSA from another router for a component route that falls in that summary.

Under these conditions, when an incremental summary SPF runs, the route might be missing from the RIB.

**[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

**Workaround:** This issue is resolved.

- CSCttl6348

**Symptom:** A module resets because the ori\_fwd process fails.

**Conditions:** This issue can occur at approximately 150 days OR when the number of interrupts in the system (due to topology, traffic flow, and so on) is very high.

**Workaround:** This issue is resolved.

- CSCtt43115

**Symptoms:** An M-1 Series module resets following the configuration of a new VLAN. The following errors appear:

```
%MODULE-2-MOD_DIAG_FAIL: Module X (serial: <serial#>) reported failure on ports
X/1-X/48 (Ethernet) due to Octopus internal error in device 78 (device error
<ErrCode>)
```

**Conditions:** This symptom might be seen when a Cisco Nexus 7000 Series switch is a mixed chassis, with both M-1 and F1- Series modules, and there is a TX SPAN session configured with the destination port as a trunk port. The SPAN destination port can be in either the M-1 or F1- Series module. The switch is running Cisco NX-OS Release 5.2(1).

**Workaround:** This issue is resolved.

- CSCtt97355

**Symptom:** Creation of new multicast groups with FEX interfaces as members fails with this error:

```
"Multicast resource (DVIF) unavailable"
```

**Conditions:** This symptom might be seen if there are any topology changes during an ISSU, such as multicast join or leave, or link flaps of the FEX ports. The issue can cause some resource leaks and an MTS buffer leak in the vntag\_mgr process. The issue might appear a long time after the ISSU.

**Workaround:** This issue is resolved.

- CSCtt98939

**Symptom:** During a switch reload, modules that are attached to a Cisco FEX module do not always come up at the same time as modules that are not attached to a Cisco FEX module.

**Conditions:** This symptom might be seen when a switch with multiple modules is reloaded and some of the modules that are attached to Cisco FEX modules do not come up.

**Workaround:** This issue is resolved.

**[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

## Related Documentation

Cisco NX-OS documentation is available at the following URL:

[http://www.cisco.com/en/US/products/ps9372/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html)

The Release Notes for upgrading the FPGA/EPLD is available at the following URL:

[http://www.cisco.com/en/US/docs/switches/datacenter/sw/4\\_1/epld/epld\\_rn.html](http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_1/epld/epld_rn.html)

Cisco NX-OS includes the following documents:

### Release Notes

*Cisco Nexus 7000 Series NX-OS Release Notes, Release 6.x*

### NX-OS Configuration Guides

*Cisco Nexus 7000 Series NX-OS Virtual Device Context Quick Start*

*Cisco Nexus 7000 Series OTV Quick Start Guide*

*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x*

*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*

*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 6.x*

*Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide, Release 6.x*

*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x*

*Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 6.x*

*Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide, Release 6.x*

*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x*

*Cisco Nexus 7000 Series NX-OS OTV Configuration Guide*

*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 6.x*

*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*

*Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 6.x*

*Cisco Nexus 7000 Series NX-OS LISP Configuration Guide*

*Cisco NX-OS Licensing Guide*

*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*

*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x*

*Cisco NX-OS FCoE Configuration Guide*

*Configuring the Cisco Nexus 2000 Series Fabric Extender*

*Cisco NX-OS XML Management Interface User Guide*

*Cisco NX-OS System Messages Reference*

*Cisco Nexus 7000 Series NX-OS MIB Quick Reference*

### NX-OS Command References

*Cisco Nexus 7000 Series NX-OS Command Reference Master Index*

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

*Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference*  
*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*  
*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*  
*Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*  
*Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference*  
*Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference*  
*Cisco Nexus 7000 Series NX-OS MPLS Command Reference*  
*Cisco Nexus 7000 Series NX-OS Security Command Reference*  
*Cisco Nexus 7000 Series NX-OS OTV Command Reference*  
*Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference*  
*Cisco Nexus 7000 Series NX-OS FabricPath Command Reference*  
*Cisco Nexus 7000 Series NX-OS System Management Command Reference*  
*Cisco Nexus 7000 Series NX-OS LISP Command Reference*  
*Cisco NX-OS FCoE Command Reference*

#### **Other Software Document**

*Cisco Nexus 7000 Series NX-OS Troubleshooting Guide*

## **Obtaining Documentation and Submitting a Service Request**

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

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

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

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

Cisco Nexus 7000 Series NX-OS Release Notes, Release 6.0

© 2012 Cisco Systems, Inc. All rights reserved.