Cisco Nexus 7000 Series NX-OS Release Notes, Release 5.1

Published: February 7, 2012
Part Number: OL-23608-07 E0
Current Release: 5.1(6)
Deferred Release: 5.1(2)

This document describes the features, caveats, and limitations for the 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 77.

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 5.x* Release Notes:
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-23608-01	A0	October 25, 2010	Created release notes for Release 5.1(1).
	B0	October 26, 2010	• Added open Caveat CSCtj62597. • Added open Caveat CSCtj69423.
	C0	October 29, 2010	Added a QoS limitation for FEX host interfaces to the Limitations section.

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

Table 1 Online History Change (continued)

Part Number	Revision	Date	Description
OL-23608-02	A0	November 05, 2010	Created release notes for Release 5.1(1a).
	B0	November 10, 2010	Removed SFP-H10GB-ACUxM Twinax Cable Active (7m, 10m), SFP-H10GB-ACUxM from Table 3.
	C0	November 24, 2010	• Added the N7K-M132XP-12L module to Table 2. • Added the optics supported by the N7K-M132XP-12L module to Table 3.
	D0	December 03, 2010	• Added SFP-10G-LR Rev. 2 for N7K-F132XP-15 to Table 3. • Corrected the EPLD upgrade information for the Cisco Nexus 2248TP Fabric Extender in the "EPLD Images" section.
OL-23608-03	A0	December 21, 2010	Created release notes for Release 5.1(2).
	B0	December 23, 2010	• Added open caveat CSCtl08798. • Added open caveat CSCtl10832.
	C0	January 6, 2011	Clarified the Note in the "Disabling BFD Prior to a Software Upgrade or Downgrade" section to better explain when a software upgrade or downgrade is required.
	D0	January 28, 2011	Added open caveat CSCtl11424.
	E0	February 7, 2011	• Added open caveat CSCtl81882. • Added open caveat CSCtl94248. • Added a limitation that QoS policies should not be configured on fabric port channels to the"FEX Module Software Limitations" section and to the "QoS Limitations"section.

Table 1 Online History Change (continued)

Part Number	Revision	Date	Description
OL-23608-04	A0	March 12, 2011	Created release notes for Release 5.1(3).
	B0	March 15, 2011	• Added resolved caveat CSCtn27760. • Updated the "Disabling BFD Prior to a Software Upgrade or Downgrade" section to include information about disabling BFD prior to upgrading to, or downgrading from Cisco NX-OS Release 5.1(3).
	C0	March 16, 2011	Added open caveat CSCtn91507.
	D0	May 16, 2011	Added resolved caveat CSCtj44206.
	E0	May 24, 2011	Added open caveat CSCtq29575.
	F0	May 25, 2011	Added SFP-H10GB-ACUxM Twinax Cable Active (7m, 10m) support for N7K-M132XP-12 in Table 3.
	G0	May 31, 2011	Updated the Upgrade/Downgrade Caveats section and the Limitations sections to indicate that ISSU is not supported when a vPC goes across multiple VDCs.
	H0	June 1, 2011	Added a footnote to Table 3 about the need to reload module N7K-M132XP-12L following an ISSU to Cisco NX-OS Release 5.1(2) when using the SFP-H10GB-CUxM optic.
OL-23608-05	A0	June 29, 2011	Created release notes for Release 5.1(4).
	B0	July 2, 2011	Moved CSCto54463 to the "Resolved Caveats—Cisco NX-OS Release 5.1(4)" section.
	C0	August 2, 2011	Updated Table 3.
	D0	August 26, 2011	Updated the Conditions for caveat CSCtq62339.
OL-23608-06	A0	September 19, 2011	Created release notes for Release 5.1(5).
	B0	October 6, 2011	Added Table 4, which lists the ISSU and ISSD paths to the current release.
OL-23608-07	A0	February 7, 2012	Created release notes for Release 5.1(6).
	B0	February 29, 2012	Moved CSCtt37768 to the "Resolved Caveats—Cisco NX-OS Release 5.1(6)" section.
	C0	March 5, 2012	Added a caveat about AAA configuration commands to the "Upgrade/Downgrade Caveats" section.
	D0	November 12, 2012	Added a caveat about removing the IP ARP synchronization configuration prior to an ISSU to the "Upgrade/Downgrade Caveats" section.
	E0	June 21, 2013	Added "GARP Behavior Changed" as a new feature to the "Cisco NX-OS Release 5.1(1)"section.

Contents

This document includes the following sections:

- Introduction, page 4
- System Requirements, page 4
- Upgrade/Downgrade Caveats, page 14
- CMP Images, page 16
- EPLD Images, page 16
- Cisco DCNM, page 17
- New Software Features, page 17
- Licensing, page 23
- MIBS, page 23
- Limitations, page 24
- Caveats, page 29
- Related Documentation, page 77
- Obtaining Documentation and Submitting a Service Request, page 78

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 4
- Supported Device Hardware, page 6

Memory Requirements

The Cisco NX-OS software requires 4 GB of memory or 8 GB of memory, depending on the software version you use and the software features you enable.

As of Cisco NX-OS Release 5.1(2), a supervisor module memory upgrade kit is available. The 8 GB 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(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:

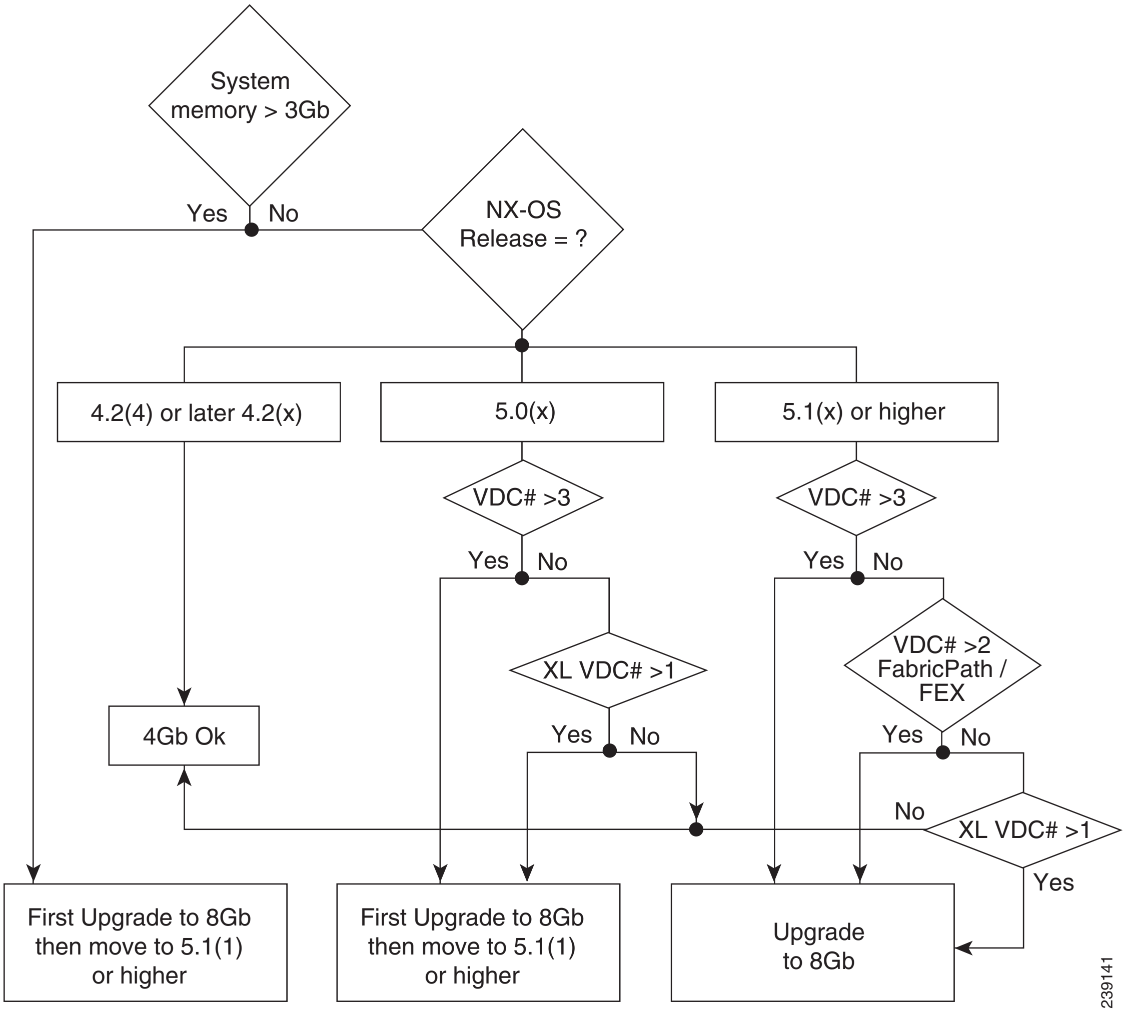
- When the system memory usage exceeds 3 GB (75 percent of total memory), we recommend that you upgrade the memory to 8 GB. Use the **show system resources** command from any VDC context to check the system memory usage:

```
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 are running Cisco NX-OS Release 5.1(x) and you have created more than three VDCs, or if XL mode is enabled in more than one VDC, then you must upgrade the memory to 8 GB.
- If you are running Cisco NX-OS Release 5.1(x), 8 GB of memory is required if the number of VDCs is greater than two, and FabricPath or FEX features are enabled.

See for additional guidance about whether or not to upgrade a supervisor module to 8 GB of memory, see Figure 1.

Figure 1 Supervisor Memory Upgrade Decision Flowchart



When you insert a supervisor module into a Cisco Nexus 7000 Series switch running Cisco NX-OS Release 5.1(x), 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) 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) 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.

Supported Device Hardware

Cisco NX-OS Release 4.2(1) and later releases support management and monitoring of the Cisco Nexus 7010 switch and Cisco Nexus 7018 switch. Although you can use Cisco NX-OS Release 4.0 to manage a Cisco Nexus 7010 switch, you must use Cisco NX-OS Release 4.1(2) or later releases to manage a Cisco Nexus 7018 switch, the 7.5-kW AC power supply unit, and the 48-port 1-Gigabit SFP I/O module (N7K-M148GS-11).

Cisco NX-OS Release 5.0 introduces support for the 6.0-kW DC power supply and the DC power interface unit. The 6.0-kW DC power supply requires Cisco Nexus Release 5.0(2a) or later releases.

Cisco NX-OS Release 5.0(2a) is required to manage the 8-port 10-Gigabit Ethernet XL I/O module (N7K-M108X2-12L) and the 48-port Gigabit Ethernet XL I/O module (N7K-M148GS-11L). The default behavior of the XL modules is the same as it is for the non-XL modules. Depending on the chassis, the Cisco Nexus 7010 Scalable Feature Package license (N7K-C7010-XL) or the Cisco Nexus 7018 Scalable Feature Package license (N7K-C7018-XL) is required to enable all XL-capable I/O modules to operate in XL mode.

Cisco NX-OS Release 5.1(1) or later is required to manage the 32-port1/10-Gigabit Ethernet module (F1-Series) (N7K-F132XP-15) and the 32-port 10-Gigabit Ethernet SFP+ I/O module XL (N7KM132XP-12L).

Cisco NX-OS Release 5.1(2) or later is required to manage the 48-port 10/100/1000 Ethernet I/O module XL (N7K-M148GT-11L).

Table 2 shows the hardware supported by Cisco NX-OS Release 5.x and Cisco NX-OS 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-C7010	Cisco Nexus 7010 chassis	4.0(1)
N7K-C7018	Cisco Nexus 7018 chassis	4.1(2)
N7K-SUP1	Supervisor module	4.0(1)
N7K-SUP1-8GBUPG	Supervisor module memory kit upgrade	5.1(1)
N7K-C7010-FAB-1	Fabric module, Cisco Nexus 7000 Series 10-slot	4.0(1)
N7K-C7018-FAB-1	Fabric module, Cisco Nexus 7000 Series 18-slot	4.1(2)
N7K-M108X2-12L	8-port 10-Gigabit Ethernet I/O module XL[1]	5.0(2)
N7K-M132XP-12L	32-port 10-Gigabit Ethernet SFP+ I/O module XL[1]	5.1(1)
N7K-F132XP-15	32-port 1/10 Gigabit Ethernet module (F1-Series)	5.1(1)
N7K-M148GS-11L	48-port 1-Gigabit Ethernet I/O module XL[1]	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[1]	5.1(2)
N7K-M148GS-11	48-port 1-Gigabit Ethernet SFP I/O module	4.1(2)
N7K-M132XP-12	32-port 10-Gigabit Ethernet SFP+ I/O module	4.0(1)
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 N7K-AC-7.5KW-US	7.5-kW AC power supply unit	4.1(2) 4.1(2)
N7K-DC-6.0KW N7K-DC-PIU N7K-DC-CAB=	6.0-kW DC power supply unit (cable included) DC power interface unit DC 48 V-48 V cable (spare)	5.0(2) 5.0(2) 5.0(2)
N2K-C2248TP-1GE	Cisco Nexus 2248TP Fabric Extender	5.1(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.

Table 3 Transceivers Supported by Cisco NX-OS Software Releases

I/O Module	Product ID	Transceiver Type	Minimum Software Version
N7K-F132XP-15	SFP-10G-SR	10GBASE-SR SFP+	5.1(1)
	SFP-10G-LR[1]	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)
	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)
N7K-M108X2-12L	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)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	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)
	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)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
N7K-M148GS-11	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)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
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)
	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)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
	DWDM-SFP-3190		4.2(1)
	DWDM-SFP-3112		4.2(1)
	DWDM-SFP-3033		4.2(1)
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)
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)

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

I/O Module	Product ID	Transceiver Type	Minimum Software Version
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)
	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)

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[1]	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[1]	SFP-H10GB-CUxM Twinax Cable Passive (1m, 3m, 5m)	5.1(2)[2]

[1] Only version -02 or later is supported.

[2] Requires a module reload if you perform an ISSU to Cisco NX-OS Release 5.1(2) from an earlier release.

Upgrade/Downgrade Caveats

The following caveats apply to the Cisco NX-OS Release 5.1(1) or later releases for the Cisco Nexus 7000 Series devices:

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

Refer toTable 4 for the nondisruptive upgrade (ISSU) path to, and nondisruptive downgrade (ISSD) path from Cisco NX-OS Release 5.1(6). 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 5.1(6)	5.1	5.1(1a), 5.1(3), 5.1(4), 5.1(5)	5.1(1a), 5.1(3), 5.1(4), 5.1(5)
	5.0	5.0(5)	5.0(5)
	4.2	4.2(6), 4.2(8)	4.2(6), 4.2(8)

Cisco NX-OS Release 5.1(6) is not ISSU-compatible with NX-OS Release 5.1(2), which is a deferred release.

Cisco NX-OS Release 5.1(6) or later releases are not ISSU-compatible with Release 4.1(x) and Release 4.0(x). Similarly, a downgrade to Release 4.1(x) or Release 4.0(x) is disruptive.

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

1. Upgrade (or downgrade) to an ISSU-compatible or ISSD-compatible release.
2. Perform a second nondisruptive upgrade (or downgrade) to the current release.

- FEX Host Interface

  When you upgrade Cisco NX-OS software by changing boot variables and reloading the device, make sure to save the FEX HIF configuration to the startup configuration, as well as another location (such as bootflash or an external server). Once the upgrade to a new release is complete, and the FEX is fully online and associated, reapply the FEX HIF configuration.

- If you have the Bidirectional Forwarding Detection (BFD) feature enabled, you should disable it before you upgrade from Cisco NX-OS Release 5.0(x) to Cisco NX-OS Release 5.1(1), or before you upgrade from Cisco NX-OS Release 5.1(1) to Cisco NX-OS Release 5.1(3). You can reenable BFD after the upgrade completes. Similarly, if you have BFD enabled and you downgrade from Cisco NX-OS Release 5.1(3) to Cisco NX-OS Release 5.1(1), or from Cisco NX-OS Release 5.1(1) to a Cisco NX-OS Release 5.0(x), you should disable BFD before the downgrade and then reenable it after the downgrade completes. For more information, see the "Disabling BFD Prior to a Software Upgrade or Downgrade" section on page 24.

- CoPP MAC policies are supported in Cisco NX-OS Release 5.1, and default policies are installed upon execution of the initial setup script. However, if you use ISSU to upgrade to Cisco NX-OS Release 5.1, the default CoPP policies for the following features must be manually configured: FabricPath, OTV, L2PT, LLDP, DHCP, and DOT1X. For more information on the default CoPP policies, see the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 5.x.*

- You cannot nondisruptively downgrade from Cisco NX-OS Release 5.1(3) or Release 5.1(2) to Cisco NX-OS Release 5.1(1) when both F1 series and M1 series modules are online in the switch. You are prevented from a nondisruptive downgrade in this situation because of the increased number of Layer-3 forwarders that are present in Cisco NX-OS Release 5.1(3) and Release 5.1(2.). If you power down the modules to ensure that there are only M1 series or only F1 series modules in the system, then you can downgrade.

- If you are using the 32-port 10 Gigabit Ethernet M series XL module (N7K-M132XP-12L) in your Cisco Nexus 7000 Series switch and you perform an ISSU from Cisco NX-OS Release 5.1(1) to NX-OS Release 5.1(2) or Release 5.1(3), be aware that the module will have to be reloaded for the CX1 optics to work correctly. During the ISSU, internal microcode that is installed on part of the optical transceiver has an earlier date than the microcode that the CX1 optics support. When the module is reloaded, the newer microcode is installed.

  CX1 support is available for microcode that has the date code 2010-1004-1634. You can verify the date of the microcode by attaching to the module and entering the **show hardware internal edc info** command.
- If you have the vPC peer-gateway feature enabled with a peer link on an F1 series module, you must upgrade both switches in the vPC to Cisco NX-OS Release 5.1(3) for normal operations of the vPC peer-gateway feature to resume.
- A nondisruptive software upgrade or downgrade is not supported when vPC peers are on a single physical switch, but they run across VDCs.
- If you are running Cisco NX-OS Release 5.1(1a) or Release 5.1(2) and you have the vPC peer-gateway feature enabled, you must upgrade both vPC peers to 5.1(4); otherwise the upgrade will be disruptive.
- A nondisruptive software downgrade to Cisco NX-OS Release 5.1(1) is supported only from Cisco NX-OS Release 5.1(2) or later releases if you have the same type of modules in the switch, either F1 series or M1 series.
- If you downgrade a Cisco Nexus 7000 Series device from Cisco NX-OS Release 5.2(x) or Release 5.1(x) to Cisco NX-OS Release 5.0(x) or Release 4.2(x), AAA configuration commands might fail. The workaround is to write-erase the startup configuration and reboot the device.
- If you have IP ARP synchronization configured in a vPC, you should remove the configuration prior to a nondisruptive software upgrade from Cisco NX-OS Release 4.2(6) or Release 4.2(8) to Cisco NX-OS Release 5.1(x). You can reapply the configuration after the ISSU completes. Follow these steps:
  - Enter the **no ip arp synchronize** command to remove IP ARP synchronization from the configuration.
  - Perform the ISSU.
  - After the ISSU completes successfully, enter the **ip arp synchronize** command to configure IP ARP synchronization.

CMP Images

Cisco NX-OS Release 5.1(6), 5.1(5), 5.1(4), 5.1(3), and Release 5.1(2) use the CMP image for Cisco NX-OS Release 5.1(1).

Cisco NX-OS Release 5.1(1) includes a new image for the CMP. The CMP is upgraded to Release 5.1(1) on a successful ISSU of Cisco NX-OS to Release 5.1(1). When the ISSU completes, you should reload the CMP image on the active and standby supervisor modules. For additional information, see the *Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 5.x*.

EPLD Images

Cisco NX-OS Release 5.1(x) software uses the EPLD images for Cisco NX-OS Release 5.1(1).

All I/O modules that connect to the Cisco Nexus 2248TP Fabric Extender must have their EPLD images upgraded to Cisco NX-OS Release 5.1(1). If the EPLD images on the I/O modules are not upgraded, none of the ports on the modules can be configured with the **switchport mode fex** command. Use the **show interface ethernet** *slot/port* **capabilities** command to determine if a port is FEX capable. If the EPLD images have not been upgraded on the module, the output of this command is FEX Fabric: no.

Cisco NX-OS Release 5.0(3) and Release 5.0(2a) uses the Release 5.0(2) EPLD images. Many of the EPLD images were upgraded for Cisco NX-OS Release 5.0(2).

To determine whether you need to upgrade the EPLD images on your Cisco Nexus 7000 Series switch, see the *Cisco Nexus 7000 Series FPGA/EPLD Upgrade Release Notes, Release 5.0.*

Cisco DCNM

Cisco Data Center Network Manager (DCNM) Release 5.1(2) supports Cisco NX-OS 5 Release 5.1(6) and other software release versions depending on the Cisco Nexus platform. See the *Cisco DCNM Release Notes, Release 5.1(1)* for specific information about the Cisco Nexus platforms and software release versions that Cisco DCNM supports.

New Software Features

This section briefly describes the new features introduced in Cisco NX-OS Release 5.1 for the Cisco Nexus 7000 Series switches. For detailed information about the features listed, see the documents listed in the "Related Documentation" section on page 77. The "New and Changed Information" section in each of these books provides a detailed list of all new features and includes links to the feature description or new command.

This section includes the following topics:

- Cisco NX-OS Release 5.1(6), page 17
- Cisco NX-OS Release 5.1(5), page 17
- Cisco NX-OS Release 5.1(4), page 18
- Cisco NX-OS Release 5.1(3), page 18
- Cisco NX-OS Release 5.1(2), page 18
- Cisco NX-OS Release 5.1(1a), page 19
- Cisco NX-OS Release 5.1(1), page 19

Cisco NX-OS Release 5.1(6)

Cisco NX-OS Release 5.1(6) is a maintenance release. There are no new features in Cisco NX-OS Release 5.1(6).

Cisco NX-OS Release 5.1(5)

Cisco NX-OS Release 5.1(5) is a maintenance release. There are no new features in Cisco NX-OS Release 5.1(5).

Cisco NX-OS Release 5.1(4)

Cisco NX-OS Release 5.1(4) is a maintenance release. There are no new features in Cisco NX-OS Release 5.1(4).

Cisco NX-OS Release 5.1(3)

Cisco NX-OS Release 5.1(3) is a maintenance release that includes the following enhancement to the vPC peer-gateway feature:

- Layer 3 Backup Routing VLAN, page 18

Layer 3 Backup Routing VLAN

Cisco NX-OS Release 5.1(3) includes the new **vpc peer-gateway exclude** *vlan* command that enables a vPC switch to behave as a gateway for its peer switch.

Use this command to configure a Layer 3 backup routing VLAN whenever you use the vPC peer-gateway feature.

- If the vPC peer link is configured on a Cisco Nexus 32-port 1/10 Gigabit Ethernet (F1-Series) module (N7K-F132XP-15), then you *must* include the Layer 3 backup routing VLAN in the VLAN list specified by the **vpc peer-gateway exclude** *vlan* command.
- If the vPC peer link is configured on an M1 series module, then you should include the Layer 3 backup routing VLAN in the VLAN list specified by the **vpc peer-gateway exclude** *vlan* command, but it is not required.

The peer-gateway functionality is *not* enabled for those VLANs specified in the exclude VLAN list. If the no exclude VLAN list is specified, then this functionality is enabled for all VLANs.

The latest occurrence of this configuration overwrites all previous configurations. This command also disables IP redirects on all VLANs. The **no vpc peer-gateway exclude** *vlan* command disables the peer-gateway functionality for all VLANs.

For additional information about this feature, see the “Configuring vPCs” section of the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide.*

Cisco NX-OS Release 5.1(2)

Cisco NX-OS Release 5.1(2) includes the following enhancements:

- Increased Number of Layer-3 Forwarders, page 18
- ARP Syncing in a vPC, page 19
- Snake Loopback Diagnostic Test for F1 Series Modules, page 19

Increased Number of Layer-3 Forwarders

Starting with Cisco NX-OS Release 5.1(2), the maximum possible number of proxy forwarders that can be used to proxy Layer 3 traffic that ingresses from an F1-series module has increased from 16 to 128. The output of the **show hardware proxy layer-3 detail** command displays up to 128 Layer-3 forwarders.

The increased number of Layer-3 Forwarders prevent a downgrade to NX-OS Release 5.1(1) when both F1 series and M1 series modules are online in the switch. If you power down the modules to ensure that there are only M1 series or only F1 series modules in the system, then you can downgrade.

ARP Syncing in a vPC

This feature addresses table synchronization across vPC peers using the reliable transport mechanism of the Cisco Fabric Service over Ethernet (CFSoE) protocol. It enables the exchange of ARP/ND tables between VPC peers which results in faster network convergence after failures.

Snake Loopback Diagnostic Test for F1 Series Modules

The Snake Loopback test is a new health monitoring diagnostic test that performs a nondisruptive loopback on all ports, even those ports that are not in the shut state. The ports are formed into a snake during module bootup, and the supervisor periodically checks the snake connectivity. Only F1 series modules support the Snake Loopback test.

Cisco NX-OS Release 5.1(1a)

Cisco NX-OS Release 5.1(1a) includes software fixes for two caveats related to Federal Information Processing Standard (FIPS). There are no new features in Cisco NX-OS Release 5.1(1a).

Cisco NX-OS Release 5.1(1)

This section briefly describes the new features introduced in Cisco NX-OS Release 5.1(1) for the Cisco Nexus 7000 Series switches and includes the following topics:

- Cisco FabricPath, page 20
- VLAN Trunking Protocol Enhancements, page 20
- ERSPAN, page 20
- ACL on Virtual Terminal, page 21
- Port Channel Minimum and Maximum Links, page 21
- DHCP Snooping in a vPC Environment, page 21
- Default Interface Command, page 21
- WCCP Enhancements, page 21
- Cisco IOS EEM Enhancement, page 21
- Support for Cisco Nexus 2248TP Gigabit Ethernet Fabric Extenders, page 22
- CoPP Enhancements, page 22
- Data Center Bridging Exchange Protocol, page 22
- FIPS, page 22
- Rate Limit Enhancements, page 22
- SCP and SFTP Servers, page 22

- SPAN Enhancement, page 23
- User Role Enhancements, page 23
- VDCs, page 23
- TCL Scripting, page 23
- GARP Behavior Changed, page 23

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(1) supports one FabricPath topology.

Cisco FabricPath implements an enhancement called conversational learning that solves the MAC address table scalability problem of switched Layer 2 networks. Cisco FabricPath supports vPC+, a technology that is similar to vPC that allows redundant interconnection of the existing Ethernet infrastructure to Cisco FabricPath without using the Spanning Tree Protocol. vPC+ is available starting in Cisco NX-OS Release 5.1(1).

VLAN Trunking Protocol Enhancements

The VLAN Trunking Protocol (VTP) helps to reduce the administrative and provisioning tasks in data center switched networks. When a VLAN is configured on a switch in VTP server mode, the VLAN is distributed automatically through all the switches in the same domain, which removes the need to configure the VLAN everywhere.

VTP can be configured in one of the following modes:

- Server—In this mode, VLANs can be created, deleted, modified for the entire domain, or advertised to the other switches for synchronization. Support for server mode is added in Cisco NX-OS Release 5.1(1).
- Client—In this mode, switches receive the VLAN advertisements from the server and synchronize the configuration. Support for client mode is added in Cisco NX-OS Release 5.1(1).
- Transparent—In this mode, the switches do not participate in VTP. This function is already available on the Cisco Nexus 7000 Series starting from Cisco NX-OS Software Release 4.1.

VTP pruning allows to prune the support of unneeded VLANs from trunk links to optimize flood traffic.

ERSPAN

The Cisco Nexus 7000 Series already provides powerful network traffic monitoring functions through SPAN and RSPAN. The Encapsulated Remote Switched Port Analyzer (ERSPAN) introduces an additional level of flexibility to the monitoring capability, because it allows the source and destination ports of the monitored data to be in different locations of the routed or switched network. ERSPAN offers this feature by encapsulating the mirrored traffic within a Layer 3 routable generic routing encapsulation (GRE) tunnel.

An extension to this feature, ERSPAN ACL, is also supported. ERSPAN ACL uses an ACL to filter out only the traffic that you want to be spanned before sending it into the GRE tunnel.

ACL on Virtual Terminal

This feature allows you to configure inband access control for the switch for a virtual terminal (VTY), regardless of where the connection is established.

Port Channel Minimum and Maximum Links

This feature improves the operation and management of port-channel interfaces. Currently, the first or last port to be bundled or unbundled in the port channel makes this logical interface usable or unusable with link up or down.

The minimum-link (min-link) feature is used to change this behavior so that the port channel is usable or unusable when a configurable number of ports (minimum links) are available, which helps to ensure a certain bandwidth availability. This feature offers a number of benefits:

- Prevents a low-bandwidth Link Aggregation Control Protocol (LACP) port channel from becoming active.
- Causes an LACP port channel to become inactive if there are too few active members ports to supply the required minimum bandwidth.

The maximum-link (max-link) parameter defines the maximum number of bundled ports allowed in an LACP port channel.

DHCP Snooping in a vPC Environment

This enhancement helps to ensure the proper behavior of Dynamic Host Configuration Protocol (DHCP) snooping in a virtual port channel (vPC) environment. The correct DHCP binding on the peer switches allows the correct behavior of associated features, such as Dynamic ARP Inspection (DAI) and IP source guard.

Default Interface Command

This feature allows you to revert a given interface configuration to the default configuration through a command or API.

WCCP Enhancements

Cisco NX-OS Release 5.1(1) includes the following Web Cache Communications Protocol (WCCP) enhancements:

- Support for the **show ip interface** command
- Configurable timers for service groups
- Improved scalability for large numbers of interfaces

Cisco IOS EEM Enhancement

This feature allows Cisco IOS Embedded Event Manager (EEM) actions to be triggered by the generation of specific syslog messages that a user configures in the Cisco IOS EEM policies. Specific or wildcard patterns in syslogs can be matched to trigger a configured Cisco IOS EEM action.

Support for Cisco Nexus 2248TP Gigabit Ethernet Fabric Extenders

Cisco Nexus 7000 Series switches that run Cisco NX-OS Release 5.1(1) and use the Cisco Nexus 2248TP Gigabit Ethernet Fabric Extender (N2K-C2248TP-1GE) support the following features:

- 100/1000 BASE-T support
- NIC Teaming
- Switch port
- Layer 2 STP Edge Port (portfast)
- Layer 3 support on a switch virtual interface (SVI)
- Port ACL
- VLAN ACL
- Port security
- VDC on a per Cisco Nexus 2248TP GE Fabric Extender basis
- QoS marking
- Up to 32 Cisco Nexus 2248TP GE Fabric Extender scale per Cisco Nexus 7000 Series switch
- Unlimited Cisco Nexus 2248TP GE Fabric Extender per module

CoPP Enhancements

These enhancements add support for non-IP traffic classes and control plane policing (CoPP) MAC policies, update the default policies with 802.1Q class of service (cos) values, and add the ability to specify the threshold value for dropped packets.

Data Center Bridging Exchange Protocol

The Data Center Bridging Exchange Protocol (DCBXP) is an extension of the Link Layer Discovery Protocol (LLDP). It announces, exchanges, and negotiates node parameters between peers.

FIPS

The Federal Information Processing Standards (FIPS) mode can be configured on Cisco NX-OS devices. FIPS specifies certain cryptographic algorithms as secure, and it identifies which algorithms should be used if a cryptographic module is to be called FIPS compliant.

Rate Limit Enhancements

Cisco NX-OS Release 5.1(1) adds the ability to configure rate limits for packets that reach the supervisor module, to log a system message if the limit is exceeded, to disable rate limits, and to configure rate limits for a specific module and port range.

SCP and SFTP Servers

SCP and SFTP servers can be configured on the switch to support the copy of files to and from a remote device.

SPAN Enhancement

The number of supported Ethernet switched port analyzer (SPAN) sessions has increased from 18 to 48.

User Role Enhancements

The ability to display the syntax of the commands that the network-admin and network-operator roles can use has been added.

VDCs

A virtual device context (VDC) can now be limited to one type of line card.

TCL Scripting

Cisco NX-OS Release 5.1 supports TCL scripting.

GARP Behavior Changed

Starting with Cisco NX-OS Release 5.1, HSRP failover GARP uses a VDC MAC address instead of the virtual MAC (VMAC) address as the source MAC address.

Licensing

Cisco NX-OS Release 5.1(1)includes one new license that is described in the following section:

- Enhanced Layer 2 License, page 23

Enhanced Layer 2 License

The Enhanced Layer 2 license is required to use the Cisco FabricPath feature that is a part of Cisco NX-OS Release 5.1(1).

MIBS

The following MIBs are supported:

- IP MIB (RFC 4293)
- Cisco VTP MIB
- TCP MIB (RFC 4022)
- MSDP MIB (RFC 4624)

Limitations

This section describes the limitations in Cisco NX-OS Release 5.1(x) for the Cisco Nexus 7000 Series switches.

This section includes the following topics:

- ISSU is Not Supported When a vPC Goes Across VDCs, page 24
- Disabling BFD Prior to a Software Upgrade or Downgrade, page 24
- ERSPAN Behavior Following a Supervisor Switchover, page 25
- Software Limitations for the 32-port 10-Gigabit Ethernet F Series Module, page 26
- FEX Module Software Limitations, page 26
- vPCs, page 26
- XML Management Interface, page 26
- QoS Limitations, page 26
- Rollback, page 27
- Port Profiles, page 27
- GOLD, page 27
- Multicast over Tunnel Interfaces, page 27
- Syslog Message Indicates SAP Failure, page 27
- vPC Peer Link Inconsistency Messages, page 28
- VDC Snapshot Files are Saved in bootflash, page 28
- SXP Connections Exceed the Limit, page 28
- Stale V6 Adjacencies Are Recovered Following an ISSU, page 28
- Old Switch Name Appears Following Write Erase, page 28
- A Version Mismatch Syslog Message Displays Following an ISSD, page 28
- NTP Errors Display During a Switchover, page 29
- Packet Forwarding in a vPC with a HSRP V6 Group, page 29

ISSU is Not Supported When a vPC Goes Across VDCs

A nondisruptive software upgrade or downgrade is not supported when vPC peers are on a single physical switch, but they run across VDCs. If you attempt the software upgrade or downgrade, it will fail at the end of the process due to a vPC configuration lock.

Disabling BFD Prior to a Software Upgrade or Downgrade

The Bidirectional Forwarding Detection (BFD) uses ACLs to redirect its packets to the CPU of a Cisco Nexus 7000 Series module. ACL resource allocation is changed to provide BFD improved interoperability with other features that use ACLs. Because of this change, disabling BFD is required when you upgrade from a release that uses the old ACL resource allocation scheme to a release that uses the new ACL resource allocation scheme; likewise, disabling BFD is required when you downgrade from a release that uses the new ACL resource allocation scheme to a release that uses the old ACL resource allocation scheme.

If you run a configuration check or attempt to perform a nondisruptive software upgrade (ISSU) without first disabling BFD, you should see a message like the following:

```
switch# sh incompatibility-all system bootflash:n7000-s1-dk9.5.0.3.bin
Checking incompatible configuration(s) for vdc 'n7k5':
-----------------------------------------------------
The following configurations on active are incompatible with  the system image
1) Service : bfd , Capability : CAP_FEATURE_BFD_V2
Description : Feature bfd is enabled.
Capability requirement : STRICT
Disable command : Disable bfd using"no feature bfd"
Checking incompatible configuration(s) for vdc 'blue':
-----------------------------------------------------
The following configurations on active are incompatible with  the system image
1) Service : bfd , Capability : CAP_FEATURE_BFD_V2
Description : Feature bfd is enabled.
Capability requirement : STRICT
         Disable command : Disable bfd using"no feature bfd"
============================= END =======================
```

Note

- Before you disable BFD, make sure that you understand the implications of doing so for your network.
- 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.
- Disabling BFD is required in the following situations:
  - If you upgrade from any Cisco NX-OS Release 5.1(x) earlier than 5.1(3) to Cisco NX-OS Release 5.1(3) or a later release
  - If you upgrade from any Cisco NX-OS Release 5.0(x) to any Cisco NX-OS Release 5.1(x)
  - If you downgrade from Cisco NX-OS Release 5.1(3) or a later release to any Cisco NX-OS Release 5.1(x) earlier than 5.1(3)
  - If you downgrade from any Cisco NX-OS Release 5.1(x) to any Cisco NX-OS Release 5.0(x)

ERSPAN Behavior Following a Supervisor Switchover

Following a switchover from the standby supervisor to the active supervisor, you may observe intermittent packet loss at the ERSPAN destination switch. Although ERSPAN encapsulation and decapsulation may function normally prior to the switchover, when the standby supervisor comes up, an internal policy map resets on the active supervisor. As a result, ERSPAN decapsulation does not fully complete and packet loss might be observed at the ERSPAN destination switch.

Software Limitations for the 32-port 10-Gigabit Ethernet F Series Module

The 32-port 10-Gigabit Ethernet F Series module (N7K-F132XL-15) has the following software limitations:

- VLAN counters are not supported on this module.
- Port security cannot be enabled on a port when DHCP snooping is enabled.
- The ACL for a bridge protocol data unit (BPDU) MAC address does not take effect when a static match on the BPDU MAC address is enabled.
- When FabricPath is configured:
  - DHCP will not learn binding entries on ports in FabricPath mode.
  - IP Source Guard (IPSG) cannot be enabled on FabricPath ports.

FEX Module Software Limitations

The following software limitation is associated with the Cisco Nexus 2248TP Fabric Extender (N2K-C2248TP-1GE) module.

- If you simultaneously reload all I/O modules that are connected to a Cisco Nexus 2248TP Fabric Extender (FEX) module, sometimes the FEX module might remain offline, even after all I/O modules are back online. You can enter a **shut** command followed by a **no shut** command on the fabric port channel to bring the FEX module online.
- QoS policies cannot be configured on fabric port channels. If QoS policies are configured, you might lose connectivity to the FEX module.

vPCs

Cisco NX-OS Release 5.1(1) for Cisco Nexus 7000 Series switches supports up to 256 vPCs per device.

The Cisco NX-OS software for Cisco Nexus 7000 Series switches does not support PIM SSM or BIDIR on vPCs; PIM ASM is fully supported.

XML Management Interface

You must enable the Secure Shell (SSH) server on the device to use the XML management interface because this is a mandatory requirement of the NETCONF Configuration Protocol (RFC 4741).

QoS Limitations

The following software limitations exist with the Quality of Service (QoS) feature:

- The Cisco NX-OS software does not support QoS policing on Layer 2 interfaces in the egress direction, only ingress.
- Type queuing policies cannot be configured for FEX host interfaces.
- Type QoS policies that refer to classes matching on an ACL (access-group) cannot be configured for FEX host interfaces.

- QoS policies cannot be configured on fabric port channels. If QoS policies are configured, you might lose connectivity to the FEX module.

Rollback

In Cisco NX-OS Release 4.1(4) and later releases, if you configure the Cisco NX-OS device while an atomic rollback is in progress, the rollback operation fails.

Port Profiles

Port profiles do not support Layer 3 (routing and routing protocol) commands or CTS commands.

A maximum of 512 interfaces can inherit a single port profile.

The system allows only one level of inheritance for all commands for the following functions:

- **switchport private-vlan mapping**
- **private-vlan mapping**

To inherit port profiles, you must have the same configuration settings for the following:

- **switchport**
- **medium p2p**

GOLD

In Cisco NX-OS Release 4.2(1), the PortLoopback test is deprecated on the N7K-M148GS-11 module.

Multicast over Tunnel Interfaces

A tunnel interface cannot be an OIF for multicast. Tunnel interfaces do not support PIM or IGMP.

Syslog Message Indicates SAP Failure

During a Service Access Point (SAP) negotiation on a port that is shut, the following syslog message might display:

```
CTS_SAP_REKEY_FAILED: SAP exchange failed on interface Ethernet8/8. (Reason:  CTS
hardware programming failure (for action: number))
```

This message might be triggered when the port is in an Auth Pending state or an SAP rekey is occurring on the port. There is no impact to the functionality associated with this message. Enter the **no shut** command if you see this message and all operations continue normally.

This limitation is associated with CSCtg45647.

vPC Peer Link Inconsistency Messages

In a large scale vPC configuration, operations triggered by the **shut** command and **no shut** command on a peer link, or the reload of secondary switch may cause peer link inconsistency messages to be displayed. The messages appear for a transient period until convergence is achieved. No action is required if you see these messages because the system converges automatically.

This limitation is associated with CSCtf06688.

VDC Snapshot Files are Saved in bootflash

When you create a VDC, a snapshot file is saved in bootflash and remains there even after the VDC is deleted. You can manually delete the snapshot file if it is not needed.

This limitation is associated with CSCte20405.

SXP Connections Exceed the Limit

If you have more than 984 SXP connections configured, your system may get extremely busy and nonresponsive. If this situation occurs, remove some of the SXP connections to get the number of connections under 984. The system does not support more than 984 SXP connections.

This limitation is associated with CSCtf20811.

Stale V6 Adjacencies Are Recovered Following an ISSU

If you perform an ISSU to Cisco NX-OS Release 5.0(2a) from NX-OS Release 4.2(4), any stale V6 adjacencies that exist in persistent storage service (PSS) are recovered. You can enter the **clear ip adjacency** command to clear these adjacencies.

This limitation is associated with CSCtg51017.

Old Switch Name Appears Following Write Erase

If you boot the kickstart image on a switch, do a write erase, and then load the ISAN image without reloading the switch, the switch comes up with the old switch name. If this situation occurs, you should reload the switch following the write erase; otherwise, after you load the ISAN image, you can enter the **switchname** command to change the switch name.

This limitation is associated with CSCsz99964.

A Version Mismatch Syslog Message Displays Following an ISSD

If you perform a nondisruptive software downgrade (ISSD) from Cisco NX-OS Release 5.0(2a) to any version lower than Cisco NX-OS Release 4.2(2), a syslog message displays that indicates a PSS1 version mismatch. This message is harmless and does not affect the functionality. Any version lower than Cisco NX-OS Release 4.2(1) detects this situation and fixes it without user intervention. Cisco NX-OS Release 4.2(2) detect the situation and fixes it, but does not display a syslog message.

This limitation is associated with CSCtd82864.

NTP Errors Display During a Switchover

During a switchover, the following message displays when the NTP daemon comes up:

```
2010 Apr  9 13:10:32 qadc3-ind18 %$ VDC-1 %$ ntpd[5251]: ntp:getconfig: Couldn't open
</etc/ntp.conf>
```

This message is informational. Traditionally, the NTP configuration is provided by etc/ntp.conf, but this file is not present on the system. On a Cisco Nexus 7000 Series switch, the NTP configuration is provided through the CLI.

This limitation is associated with CSCtg33335.

Packet Forwarding in a vPC with a HSRP V6 Group

In a vPC, packets that are forwarded through an HSRP virtual IP address (VIP) or virtual MAC address (VMAC) might fail. This situation can occur if a VLAN that is in a vPC has a HSRP V6 group and has the use-bia option enabled on an interface. Layer 3 traffic will be disrupted and packets might not reach the VIP. Removing the use-bia option from the interface in the vPC should correct this issue.

Caveats

This section includes the following topics

- Open Caveats—Cisco NX-OS Release 5.1, page 29
- Known Issues—Cisco NX-OS Release 5.1(6), page 39
- Resolved Caveats—Cisco NX-OS Release 5.1(6), page 41
- Resolved Caveats—Cisco NX-OS Release 5.1(5), page 44
- Resolved Caveats—Cisco NX-OS Release 5.1(4), page 49
- Resolved Caveats—Cisco NX-OS Release 5.1(3), page 55
- Resolved Caveats—Cisco NX-OS Release 5.1(2), page 65
- Resolved Caveats—Cisco NX-OS Release 5.1(1a), page 68
- Resolved Caveats—Cisco NX-OS Release 5.1(1), page 69

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 5.1

This section includes the following open caveats:

- CSCsm22329

  Symptom: QoS statistics require a policing action to allow marking actions to produce statistics.

  Conditions: When you define a QoS service policy with only marking actions, the statistics do not work. The statistics feature works only when the service policy has a policing action defined also.

Workaround: You can get statistics for a marking-only policy by applying a dummy policing action to the policies. For example, in addition to the marking actions, you should define a policing action that permits 100 percent traffic. Configure the violate and conform action as transmit.

- CSCta65195

  Symptom: The **ping** command to a First Hop Redundancy Protocol (FHRP) virtual IP address from an external device may fail.

  Conditions: This problem occurs when you enable Strict Unicast reverse path forwarding (RPF) on FHRP interfaces, and the response from the **ping** command is forced to take the path using a standby/listen or backup router. To confirm if this symptom exists in your system, enter the **ping** command to a virtual IP address from the same source with Unicast RPF disabled on FHRP-enabled interfaces; check if the **ping** command succeeds.

  Workaround: Disable the Unicast RPF on the interfaces where FHRP is enabled, or change RPF to loose RPF.

- CSCte73854

  Symptom: Layer 2 Protocol Tunneling (L2PT) does not work for Spanning Tree Protocol (STP), VLAN Trunking Protocol (VTP), or Cisco Discovery Protocol (CDP) packets coming in on a Cisco Trusted Security (CTS) link to 802.1Q tunnel ports.

  Conditions: Enable L2PT on a 802.1Q tunnel port for all supported protocols. Connect the 802.1Q tunnel port onto a trunk port (customer side) that has CTS enabled. L2PT drops all the STP/CDP/VTP frames coming in on the 802.1Q tunnel port because the bridge protocol data units (BPDUs) are encrypted.

  Workaround: None. CTS encrypts the payload of the BPDUs (including LLC or SNAP information) which makes it difficult to identify the BPDU type in order to perform L2PT. Dot1AE encryption with SAP negotiation is not compatible with Q-in-Q tunnels.

- CSCtg92420

  Symptom: When you enter the **show interface** command on the Cisco Nexus 7000 32-port, 10-Gigabit Ethernet SFP+ I/O module, the output incorrectly displays storm suppression in packets rather than in bytes.

  Conditions: You might see this symptom only on the Cisco Nexus 7000 32-port, 10-Gigabit Ethernet SFP+ I/O module.

  Workaround: Interpret storm suppression packets as storm suppression in bytes on the Cisco Nexus 7000 32-port, 10-Gigabit Ethernet SFP+ I/O module.

- CSCtj29688

  Symptom: Peer-link ports may become error disabled on the primary switch.

  Conditions: This symptom might be seen if you enter the **shut** command followed by the **no shut** command on the peer-link port when there are a large number of vPCs (250 or more).

  Workaround: To work around this issue, follow these steps:

  1. Shut down the vPCs on the secondary switch before you enter the **shut** command and the **no shut** command on the peer-link port.
  2. After the peer-link comes up, enter the **no shut** command on the VPCs on the secondary switch.

- CSCtj36639

  Symptom: IP switched flows in a VLAN are not reported.

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

  - If a VLAN has been disabled by the **no vlan** command and is reenabled later.
  - If VLAN Trunking Protocol (VTP) is enabled and configured for client mode, this issue might occur if the VLAN is deleted and readded at the VTP server node.

  Workaround: To work around this issue, follow these steps:

  1. Enter the **vlan configuration** *x* command and copy the configuration.
  2. Enter the **no vlan configuration** *x* command.
  3. Enter the **vlan configuration** *x* command to reapply the configuration.

- CSCtj62597

  Symptom: (S,G) mroutes are not created on the aggregation router, which is a last-hop/first-hop router, after you disable and reenable the Protocol Independent Multicast (PIM) feature on the router. This issue may cause traffic from source S for the group G to be dropped.

  Conditions: This symptom might be seen when you enter commands in the following sequence to disable and reenable the PIM feature configuration:

  - **copy run** *pim-cfg-file*
  - **no feature pim**
  - **copy** *pim-cfg-file* **run**

  Workaround: Enter a **clear ip mroute** *group-addr source-addr* command for the missing (S,G) mroute to resolve this issue and ensure the (S,G) mroute is immediately recreated.

- CSCtj66382

  Symptom: Initial packet loss occurs for multicast traffic because of a delay between internal commands.

  Conditions: This symptom might be seen at the beginning of a stream during state creation.

  Workaround: None.

- CSCtk36830

  Symptom: SNMP stops responding after the following message started appearing on the console:

  ```
  KERNEL-2-SYSTEM-MSG
  ```

  Conditions: This symptom might be seen when there is a long-lived TCP connection from NMS to the Cisco Nexus 7000 Series switch. The netstack TCP buffer gets full and the following send() call gets stuck if it is a BLOCKING call. As a result, SNMP fails due to missing a heartbeat.

  Workaround: None. SNMP will fail and restart statefully.

- CSCtk55946

Symptom: After MAC addresses are moved multiple times, the MAC addresses do not appear when you enter the **show mac address-table** command on the supervisor module.

Conditions: This symptom might be seen when a MAC address move is initiated due to a topology change by STP. The MAC addresses that are missing in the output of the **show mac address-table** command do not have active traffic coming from them.

Workaround: This issue has no functional impact because it is a display issue only. The MAC addresses are present in the line card, but are missing on the supervisor module. Any active traffic that has the source MAC address as the missing MAC addresses will bring back the MAC address in the supervisor **show mac address-table** command output. Enter the **clear mac address-table dynamic** command to fix the display issue.

- CSCtk60746

  Symptom: Occasionally you might see the following error message in the syslog file:

  ```
  Failure communicating with MTS_SAP_SPM for opcode MTS_OPC_ETHPM_BUNDLE_MEMBER_BRINGUP.
  ```

  Conditions: This message is seen when the port channel interface comes online or goes offline with a Web Cache Control Protocol (WCCP) policy applied to it. The message is seen only in Cisco NX-OS Release 5.1(1) and NX-OS Release 5.1(2).

  Workaround: Add the WCCP policy after the port channel interface is up, and then remove the WCCP policy before bringing the port channel interface down.

- CSCtk63052

  Symptom: Upon extending multiple ranges of VLANs, the output of the **show running-config** command displays an inconsistent and distorted output.

  Conditions: This symptom might be seen in Cisco NX-OS Release 5.1(2) and Release 5.1(3).

  Workaround: Reduce the number of arguments in the extended VLANs list.

- CSCtl42628

  Symptom: Following a switchover or a switch reload on a switch with multiple VDCs in a vPC environment with a large number of VLANs and vPCs, a l2fm process fails or there is a slow drain of Messages and Transactional Services (MTS) buffers with many flush related MTS messages in the l2fm process MTS queue.

  Condition: This symptom might be seen when there are multiple VDCs and there is at least one VDC with 3000 VLANs and 20 to 30 vPCs that carry most of the VLANs. This issue affects only NX-OS Release 5.1(x). It does not occur in NX-OS Release 4.x software.

  Workaround: None.

- CSCtn21586

  Symptom: A policy-based routing (PBR) policy on Layer 3 interfaces does not redirect traffic. As a result, the traffic takes the normal route.

  Conditions: This symptom might be seen if the same PBR policy is applied on multiple interfaces before the next hop adjacencies are resolved. It does not redirect the traffic correctly on some interfaces.

  Workaround: To work around this issue, do one of the following:

  - Apply the PBR policy after the next hop adjacencies are resolved.
  - If PBR traffic issues already exist, delete the route-map configuration present in the interface configuration and then reapply the same route-map configuration after the adjacencies are resolved.

- CSCtn41987

  Symptom: After you enter the **shut** command followed by the **no shut** command on a vPC+ peer link, you might see that Address Resolution Protocol (ARP) entries are not resolved or that some adjacencies point to null:

  ```
  <ip-addr>        <time>   <mac-addr>   <vlan>           (null)
  ```

  Conditions: This symptom might be seen in a vPC+ configuration after you enter the **shut** command followed by the **no shut** command on a vPC+ peer link.

  Workaround: Enter the **clear ip arp** *entry/vlan/interface* **force-delete** command to correct this issue. You can also enter the **clear mac address-tbl dynamic address** *mac-address* command or the **clear mac address-tbl dynamic vlan** *vlan-id* command to fully resolve this issue.

- CSCtn61023

  Symptom: After a DWDM-X2 SFP is inserted, a port or link does not come up.

  Conditions: This symptom might be seen when a DWDM-X2 SFP is repeatedly inserted and removed. The issue is not specific to any particular DWDM-X2 SFP.

  Workaround: Remove the DWDM-X2 SFP and insert it again.

- CSCtn78549

  Symptom: FabricPath forwarding engines (FEs) do not populate remote MAC addresses according to port-channel membership in a chassis with both M1 series modules and F1 series modules.

  Conditions: This symptom might be seen when two members of the same FE (x and y) belong to the same FabricPath port channel (that contains any number of port-channel members) and one of the members (x or y) is brought down. This symptom occurs only on switches where FabricPath is enabled.

  Workaround: After you bring down one of the members of the port channel, enter the **shut** command followed by the **no shut** command on the port channel to restore normal operations.

- CSCtn79375

  Symptom: When you enter the **default interface** *interface* command, a trunk allowed list for that interface does not go back to the default state. The trunk allowed list becomes “none” (empty).

  Conditions: This symptom might be seen when the port is in trunk mode with some allowed VLANs.

  Workaround: Enter the **switchport trunk allowed vlan all** command for the interface after you enter the **default interface** *interface* command.

- CSCtn81880

  Symptom: When a peer link comes up on an F1 series module, the following level 2 syslog message displays, even when the peer-gateway is not configured:

```
VPC_ADD_L3_BKUP_VLAN_TO_PEER_GW_EXCLUDE_LIST
```

Conditions: This symptom might be seen on an F1 series module when a peer link comes up, but the peer-gateway is not configured.

Workaround: None.

- CSCtn91507

  Symptom: The GOLD snake loopback test fails on an F1 series module and displays the following syslog message:

  ```
  2011 Mar  9 15:00:39 n7k01 %$ VDC-1 %$ %DIAG_PORT_LB-2-SNAKE_TEST_LOOPBACK_TEST_FAIL: 
  Module:8 Test:SnakeLoopback failed 10 consecutive times. Faulty module:Module 8 
  affected ports:affected ports:10  Error:Error in Fabric recieve for  Forwarding Asic 
  module
  2011 Mar  9 15:00:39 n7k01 %$ VDC-1 %$ %MODULE-4-MOD_WARNING: Module 8 (serial: 
  JAF1423ASRA) reported warning on ports 8/10-8/10 (Ethernet) due to Error in Fabric 
  recieve for  Forwarding Asic module in device 136 (device error 0x41830059)
  ```

  Conditions: This symptom might be seen when a private VLAN (PVLAN) is configured on ports on an F1 series module.

  Workaround: Disable the snake loopback test on the F1 series module where the PVLAN is configured.

- CSCtn93738

  Symptom: A CFS sessionless commit can cause TACACS to fail.

  Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch that is running Cisco NX-OS Release 5.1(4) or an earlier release, if TACACS or RADIUS CFS is enabled and a CFS sessionless commit occurs.

  Workaround: There are two ways to work around this issue:

  – If possible, avoid using CFS for TACACS or RADIUS CFS.

  – If CFS is enabled, do not use sessionless commit.

- CSCtn96236

  Symptom: A Cisco Nexus 7000 Series switch sends register packets until it has created an entry in the hardware. This enhancement will cause the First Hop Router (FHR) to send register packets until a Register stop is received per RFC 4601.

  Conditions: The symptom might be seen for the PIM sparse mode registration process at the FHR.

  Workaround: None.

- CSCtn79238

  Symptom: Multicast traffic loss occurs 4 minutes and 11 seconds after a switchover completes.

  Conditions: This issue is only seen if a switchover occurs on both vPC peers.

  Workaround: Do not do a switchover on both peers at the same time.

- CSCto31791

Symptom: ERSPAN destination ports do not receive the copied traffic from ERSPAN sources. ERSPAN GRE encapsulated traffic is sent to the destination VDC or switch but it is not mapped to the ERSPAN destination port.

Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch configured with ERSPAN and running Cisco NX-OS Release 5.1 or a later release.

Workaround: None.

- CSCto35788

  Symptom: Following a supervisor switchover on a Cisco Nexus 7000 series switch, some MAC addresses will fail to be advertised through IS-IS across the Layer 2 extension through OTV.

  Conditions: This symptom might be seen after a supervisor switchover.

  Workaround: Clear the MAC address table for those MAC addresses on the OTV edge device where the host is located locally and IS-IS will start advertising it again.

- CSCto53699

  Symptom: After a link failure or network reconvergence following a link flap, some of the local hosts will not be able to connect to some of the remote hosts.

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

  - The OTV VDC has redundant links to local site aggregation switches. One link will be in spanning tree forwarding and the other link will be in Spanning tree blocking state.
  - A link failure or link flap occurred.
  - The OTV ARP-ND cache is not disabled on the OTV VDC.
  - The ARP entry for the remote host is on the ARP ND cache of the OTV VDC.
  - The local host does not have ARP entry for the remote host(s).

  Workaround: Disable the ARP ND cache on the OTV VDC.

- CSCto55861

  Symptom: In a vPC setup, if the source can be reached only from the secondary peer switch and if metrics are the same to reach the source, traffic will be blackholed for that source.

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

  - There is a vPC setup.
  - The source is in the Layer 3 domain.
  - The source is reachable from the secondary peer switch.
  - The metrics to reach the source are same on both the primary peer switch and the secondary peer switch.

  Workaround: None.

- CSCto95902

Symptom: A Link Aggregation Control Protocol (LACP) port channel will go into a suspend state if it is configured over back-to-back links in the same VDC. In this situation, the channel is suspended due to a misconfiguration.This issue can prevent a SCE cluster solution and similar deployments.

Conditions: This issue is seen only when the LACP channel is used on back-to-back links in the same VDCs. It is not seen on back-to-back links between different VDCs.

Workaround: Configure the mode for the LACP port channels to On.

- CSCtq20544

  Symptom: Following a reload of a Cisco Nexus 7000 Series switch with multiple VDCs, approximately 30 seconds of packet loss can be observed for traffic ingress on an Layer 3 interface and egress on a vPC.

  Conditions: This issue might be seen only when a whole chassis containing multiple VDCs is reloaded, and there are signs of a loop in the VDCs. (This issue has been observed once at a single location and has not been reproduced.)

  Workaround: Set the delay restore time to 1 (delay restore 1) to eliminate any difference between the Layer 3 and the vPC interface coming up.

- CSCtq43020

  Symptom: CoS to queue mappings in queuing class-maps do not take effect when there are no interfaces in the default VDC.

  Conditions: This symptom might be seen when there are no interfaces in the default VDC.

  Workaround: Allocate an interface in the default VDC before you modify the queuing class maps.

- CSCtq57911

  Symptom: GLBP AVG continues to redirect hosts to an old vMAC address even after the redirect timer expires.

  Conditions: This symptom might be seen when GLBP is configured.

  Workaround: Reload the Cisco Nexus 7000 Series switch.

- CSCtq96109

  Symptom: In a vPC+ setup, MAC addresses for orphan ports point to the GPC of a local switch ID in an AM or ARP adjacency. Layer 2 FM also displays these MAC addresses as pointing to (local-swid.0.lid) instead of to an Ethernet or a port-channel interface.

  Conditions: This symptom might be seen following a supervisor switchover.

  Workaround: Enter the **clear mac address-table dynamic address** *mac-address* command to help fix this issue. This bug affects only Cisco NX-OS Release 5.1(x) software.

- CSCtr00168

  Symptom: A Cisco Nexus 7000 Series switch loops when queried through SNMP for the object cpsIfPortSecurityEnable (1.3.6.1.4.1.9.9.315.1.2.1.1.1). This issue causes a failure of the eth_port_sec process, which in turn causes a failure of the supervisor module in Cisco NX-OS Release 5.1(4).

Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch running Cisco NX-OS Release 4.2(6) or later.

Workaround: None.

- CSCtr07544

  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: Configure the parallel links as members of a port channel to reduce or eliminate the looping of packets.

- CSCtr16400

  Symptom: MAC address resolution for HSRPv6 global VIP does not occur. On a Cisco Nexus 7000 Series switch, HSRPv6 is not able to add global VIP to ICMPv6 following a switch reload. The problem occurs when the switch reloads with a partial HSRPv6 configuration and global VIP is added after the reload. The global VIP is not added to ICMPv6.

  Conditions: The issue can be seen when the Cisco Nexus 7000 Series switch is running Cisco NX-OS Release 5.1(4) software, configured as follows:

  1. Reload the switch with HSRPv6 configured group (with/without GUVIP).

  ```
  interface ethernet <slot/port>
  hsrp ver 2
  hsrp 10 ipv6
  ip fe80::12
  ```

  2. After the reload, configure GUVIP on this HSRPv6 group.

  ```
  interface ethernet <slot/port>
  hsrp ver 2
  hsrp 10 ipv6
  ip 2001::1
  ```

  3. Check if the HSRP VIP is added into ICMPv6 by using the **show ipv6 icmp vaddr global** command.
  4. The new Global VIP is not seen as part of GUVIP address list in ICMPv6.

  Workaround: Remove the configured Link Local VIP and then reconfigure both Link Local VIP and Global VIP. For the previous configuration, enter the following commands:

  ```
  interface ethernet <slot/port>
  hsrp ver 2
  hsrp 10 ipv6
  no ip fe80::12
  ip fe80::12
  ip 2001::1
  ```

- CSCtr20824

Symptom: A Cisco Nexus 7000 Series switch might not forward multicast streams because of a hardware issue where multicast entries are not installed in the hardware. Lack of a hardware entry can be verified with the following commands:

show ip mroute source group

This output should be correct.

show forwarding multicast route source *source* **group** *group*

This output does not show the entry, as the entry is not created in hardware properly.

Conditions: The symptom can be verified with the following command:

```
sh system internal mfdm info statistics | egrep -i "delay|failed"
Number of index in delayed free <x> <<<< # around 65k
Number of L3 index alloc failed <x> <<<< continuously
incrementing
```

This queue is not expected to always be nonzero. It is normal for it to be nonzero. However, an indication of an issue is if the queue continues to steadily increase without decreasing. If the multicast environment is very dynamic, there is greater fluctuation in the number of entries in the queue.

Workaround: By default, starting in Cisco NX-OS Release 4.2(8), this enhancement causes an automatic detection and recovery mechanism that can detect if the "delayed free" queue reaches 16,000 entries. If it does, an automatic flush occurs. You can also manually flush this queue by entering the **test forwarding internal mfdm oiflist flush delayed-free-queue** command which is a nonservice impacting command.

- CSCtr40181

  Symptom: There is an inconsistency between an F1 series module's hardware MAC address table and the global l2fm software MAC address tables.

  Conditions: This issue might be seen after the following event sequence:

  – The keepalive link goes down.

  – The peer link goes down.

  – The keepalive and peer link come back up.

  – The vPC member interface goes down.

  Workaround: To work around this issue, follow these steps:

  1. Enter the **show system internal l2fm info move_db** command.
  2. If the output shows entries in the move database from port-channel to peer-link, enter the **debug l2fm clear move_db** command.

  Alternatively, you can reload the switch to work around this issue.

- CSCts28106

  Symptom: Trunking interfaces only allow VLAN1 forwarding.

  – The **show interface trunk** command shows the interface trunk status and allows all VLANs, but only forwards VLAN1.

  – The **show spanning-tree interface eX/Y active** command can see only VLAN1.

Conditions: This issue might be seen regardless of the M1 or F1 series module in use. It happens on some ports, but not on others.

Workaround: Delete all VLANs, reallocate interfaces to the VDC, recreate VLANs,

and change the state accordingly.

- CSCts72967

  Symptom: Configuring port security on an M1 series module in a Cisco Nexus 7000 Series switch that is running Cisco NX-OS Release 5.1(4) can cause incorrect programming in hardware on an F1 series module on the same port number. For example, configuring port security on the Ethernet 2/1 interface can affect the Ethernet 1/1 interface.

  Condition: This symptom might be seen when port security is configured on an M1 series module in a Cisco Nexus 7000 Series switch that is running Cisco NX-OS Release 5.1(4).

  Workaround: Configure port security on an M1 series module on an unused port that corresponds to the same port number on the F1 series module and then remove the port-security configuration.

Known Issues—Cisco NX-OS Release 5.1(6)

This section lists issues that are known to exist in Cisco NX-OS Release 5.1(6).

- CSCtn21586

  Symptom: A policy-based routing (PBR) policy on Layer 3 interfaces does not redirect traffic. As a result, the traffic takes the normal route.

  Conditions: This symptom might be seen if the same PBR policy is applied on multiple interfaces before the next hop adjacencies are resolved. It does not redirect the traffic correctly on some interfaces.

  Workaround: To work around this issue, do one of the following:

  - Apply the PBR policy after the next hop adjacencies are resolved.
  - If PBR traffic issues already exist, delete the route-map configuration present in the interface configuration and then reapply the same route-map configuration after the adjacencies are resolved.

- CSCtn91342

  Symptom: When you add FabricPath VLANs on a Cisco Nexus 7000 Series switch that is running Cisco NX-OS Release 5.1(3) or Release 5.2(x), the ELTM process might fail. Messages like the following indicate the failure.

  ```
  %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 15098) hasn't caught signal 11 (core
  will be saved).
  2011 Sep 14 18:36:54.579 s74050prd %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID
  22489) hasn't caught signal 11 (core will be saved).
  2011 Sep 14 18:36:55.119 s74050prd %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID
  22491) hasn't caught signal 11 (core will be saved).
  2011 Sep 14 18:36:55.720 s74050prd %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID
  22493) hasn't caught signal 11 (core will be saved).
  ```

  Conditions: This symptom might be seen when FabricPath VLANs are added on a Cisco Nexus 7000 Series switch that is running NX-OS Release 5.1(3) or Release 5.2(x).

  Workaround: This issue is resolved in NX-OS Release 5.2(1).

- CSCto31791

  Symptom: ERSPAN destination ports do not receive the copied traffic from ERSPAN sources. ERSPAN GRE encapsulated traffic is sent to the destination VDC or switch, but it is not mapped to the ERSPAN destination port.

  Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch configured with ERSPAN and running Cisco NX-OS Release 5.1 or a later release.

  Workaround: None.

- CSCto34686

  Symptom: VSH failed when collecting the output of the **show tech** command.

  Conditions: This symptom might be seen when OBFL logging for stats is enabled in Cisco NX-OS Release 4.2(8) and Release 5.2(x) releases. An ISSU or ISSD to an image without OBFL logging enabled can cause OBFL to display a CLI to query the driver with a out-of-range, undefined counter ID, which can cause VSH to fail.

  Workaround: Clear obfl counter-stats, obfl interrupt-stats, obfl error-stats before collecting the output of the **show tech** command.

- CSCto82419

  Symptom: NX-OS software fails to authenticate a user.

  Conditions: This symptom might be seen if remote AAA authentication is set for CMP-sup and the TACACS+ server is used as the AAA server, the Cisco NX-OS software fails to authenticate a user.

  Workaround: To avoid this issue, use the TACACS+ server when CMP authentication is used.

- CSCtq98318

  Symptom: Following a linecard reload or an ISSU, the download of Layer 2 or Layer route databases can time out. When this occurs, the mRIB mfdm route-buffer is depleted and no more route updates can be sent down.

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

  - There is a 32-port, 1/10 Gigabit Ethernet module (N7K-F132XP-15) in the switch
  - An ISSU or linecard reload occurs.
  - There are route updates during the linecard upgrade.

  Workaround: Perform a switchover to clear the mRIB route buffers.

- CSCtu34118

  Symptom: After you reload a module that has OSPF adjacencies known through its ports, a Cisco Nexus 7000 Series switch might not use the link for data where the OSPF neighbor is known, even though the neighbor is in the FULL state.

  Conditions: This symptom might be seen when the router link is not advertised by the Cisco Nexus 7000 Series switch in the type 1 LSA update.

  Workaround: The problem might correct itself after a full SPF is executed.

- CSCtx08234

  Symptom: An ACLQOS failure can occur on all modules when PBR is configured. The module can reload and one or more modules fail to allocate interfaces to the VDC. For interfaces that are allocated, if they are in a down state, the **no shut** command will not bring up the port.

  Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch that is running Cisco NX-OS Release 5.1(5).

  Workaround: There are several ways to recover from this issue:

  - Force a reload of the modules.
  - Perform a supervisor switchover.
  - Perform a system reload. In this case, do the following:
  - Do not copy the running configuration to the startup configuration to ensure that the switch comes up in the previous state.
  - Perform a write erase and reload the switch if the running configuration was copied to the startup configuration.

Resolved Caveats—Cisco NX-OS Release 5.1(6)

- CSCtl24854

  Symptom: A Cisco Nexus 7000 Series switch might be unreachable (through ping, HSRP, or Telnet), and stop routing all ingress traffic on an impacted module for a specific VLAN. Further analysis shows the RMAC of the impacted VLAN is not programmed in the hardware on the impacted module.

  Conditions: The specific trigger for this symptom is not known.

  Workaround: This issue is resolved.

- CSCtq38302

  Symptom: When an ASIC fatal error occurs, an EEM event resets the ASIC to recover from the condition and logs the information to the persistent (OBFL) log and exception log. However, if the fatal error is persistent, the EEM event continues to try to reset the ASIC to recover, which may not be desirable.

  Conditions: This symptom might be seen when a fatal error occurs on an ASIC.

  Workaround: This issue is resolved.

- CSCtq57911

  Symptom: GLBP AVG continues to redirect hosts to an old vMAC address even after the redirect timer expires.

  Conditions: This symptom might be seen when GLBP is configured.

  Workaround: This issue is resolved.

- CSCtr44645

Symptom: The Cisco Nexus OS contains a vulnerability that could allow an authenticated, local attacker to execute arbitrary commands on a targeted device. The vulnerability is due to improper sanitization of user-supplied values to command-line interface commands.

An authenticated, local attacker could exploit the vulnerability by issuing commands that contain malicious options on the device command-line interface. If successful, the attacker could gain elevated privileges on the targeted device.

Conditions: This symptom might be seen when injection is done with either the **less** or the **section** subcommand.

Workaround: This issue is resolved.

- CSCtr63517

  Symptom: The GLBP process might fail after you enter the **show glbp capabilities** command. The following message indicates the failure:

  ```
  %SYSMGR-2-SERVICE_CRASHED: Service "glbp" (PID 3908) hasn't caught signal 6 (core will
  be saved).
  ```

  Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch running Cisco NX-OS Release 5.1(2) or 5.1(4).

  Workaround: This issue is resolved.

- CSCtr74913

  Symptom: The aclqos process fails, which causes the linecard to reload.

  Conditions: This symptom might be seen when an existing access list is being updated and all of the following conditions are true:

  - Statistics is enabled on the policy.
  - The policy is active on interfaces.
  - The ACEs containing object groups are updated.

  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 the hardware which will result in traffic being switched incorrectly in the software and will cause poor performance.

  Conditions: This symptom might 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.

- CSCts51026

  Symptom: When a TACACS+ source-interface configuration is present, a small memory leak occurs for each TACACS+ authentication and authorization request.

  Conditions: This symptom might be seen only if a TACACS+ source-interface configuration is present.

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.

- CSCtt37768

  Symptom: MAC addresses that point toward a peer link (for hosts through orphan ports on the vPC peer) are removed from the linecard forwarding hardware.

  Conditions: This symptom might be seen when a remote MAC address has been incorrectly programmed, which allows it to be aged out, which in turn causes the problem.

  This issue affects all M1, F1, and F2 series modules in Cisco NX-OS Release 5.1(x), Release 5.2(x), and Release 6.0(x).

  Workaround:This issue is resolved.

- CSCtt38812

  Symptom: The core voltage of the naxos ASIC should be lowered.

  Workaround: This enhancement request is resolved.

- CSCtt44813

  Symptom: Following an upgrade from Cisco NX-OS Release 5.0(2a) to Release 5.1(x), the **show running-configuration** command does not display GLBP-related configurations. The **show startup-configuration** command has the correct information.

  This issue has no functional impact to the system; it is a display issue with the **show running-configuration** command for GLBP.

  Conditions: This symptom might be seen when you upgrade from Cisco NX-OS Release 5.0(2a) Release to 5.1(x).

  Workaround: This issue is resolved.

- CSCtt97253

  Symptom: The aclqos process might fail when you modify the IPv6 route map on an interface.

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

  - An IPv6 route map is configured with an ACL for matching.
  - Policy routing is enabled for the route map and is applied to an IPv6-enabled interface.

  You modify the ACL attached to the route map. For example, you add an entry. The addition fails and the following messages appear:

  ```
  ******
  2011 Oct 13 12:53:10 NDC1P03DSTSR05 %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "aclqos"
  (PID 1706) hasn't caught signal 11 (core will
  ```

```
be saved).
2011 Oct 13 12:53:13 NDC1P03DSTSR05 %ACLMGR-3-ACLMGR_VERIFY_FAIL: Verify failed:
client 8300016E, Linecard aclqos client crash
```

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.

- CSCtu00256

  Symptom: A Cisco Nexus 7000 Series switch running Cisco NX-OS Release 5.1(5) might unexpectedly fail due to an eth_pcm error.

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

  Workaround: This issue is resolved.

Resolved Caveats—Cisco NX-OS Release 5.1(5)

- CSCte19879

  Symptom: A service failure occurred during an ISSU on a Cisco Nexus 7000 Series switch. The following message appeared:

  ```
  1 [N7K-M108X2-12L]: %IPFIB-SLOT2-4-FIB_TCAM_PF_INSERT_FAIL: FIB TCAM prefix
  ```

  Conditions: This symptom was seen during an ISSU upgrade.

  Workaround: This issue is resolved.

- CSCti43396

  Symptom: When a module is down and the configuration is saved, the configuration for the down module may be lost.

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

  Workaround: This issue is resolved.

- CSCtk34535

  Symptom: A Cisco Nexus 7000 Series switch might reset due to a HAP policy of Reset in the Cisco Discovery Protocol (CDP).

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

Workaround: This issue is resolved.

- CSCtl07863

  Symptom: When the supervisor fails over to the standby supervisor, the NFM process on the newly active supervisor fails with the following message:

  ```
  %SYSMGR-2-SERVICE_CRASHED:Service "nfm" (PID 6705) hasn't caught signal 6 (core will
  be saved).
  ```

  Conditions: This symptom might be seen when NetFlow Exporter is configured and the switch has a large volume of NF exports.

  Workaround: This issue is resolved.

- CSCtn95934

  Symptom: The 10-Gbps fiber links flap between Cisco Nexus 7000 Series switches.

  Conditions: The issue might be seen when the following conditions apply:

  - The Cisco Nexus 7000 Series switch is running Cisco NX-OS Release 5.1(2).
  - The link connected between N7K-F132XP-15 modules.
  - Modules are connected over certain DWDM systems.

  Workaround: This issue is resolved.

- CSCto63293

  Symptom: The snmpd process randomly stops responding to SNMP requests on a Cisco Nexus 7000 Series switch.

  Conditions: This symptom might be seen on the default VDC.

  Workaround: This issue is resolved.

- CSCto74720

  Symptom: Occasionally, after the **terminal monitor** command is entered on a Cisco Nexus 7000 Series switch, no logging is printed to the terminal session.

  Conditions: This symptom might be seen with both Telnet and SSH on a switch running Cisco NX-OS Release 5.1(2) or Release 5.1(3).

  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.

- CSCtq37407

  Symptom: An snmpwalk of the CISCO-LAG-MIB causes a memory leak on a Cisco Nexus 7000 Series switch.

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

  Workaround: This issue is resolved.

- CSCtq37520

  Symptom: Following an ftp copy and an snmpwalk of the CISCO-FTP-CLIENT-MIB [1.3.6.1.4.1.9.9.80], a memory leak occurs in a Cisco Nexus 7000 Series switch.

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

  Workaround: This issue is resolved.

- CSCtq59609

  Symptom: In a dual-sided vPC setup, when one member link of each vPC pair is down or shut, there can be a software loop of IGMP Global Leave packets if there is a topology change. If this happens, it will lead to high CPU usage.

  Conditions: This issue might be seen only in dual-sided vPC setups when one member link of each vPC pair is down.

  Workaround: This issue is resolved.

- CSCtq89133

  Symptom: Following a switchover, a port flap results in only VLAN 1 being operational, while the rest of the VLANs in the allowed list stay down on the port.

  Conditions: This symptom might be seen when you change the VLAN state after modules are powered down, which causes PSS inconsistency. Once the modules are powered up and interfaces are created, perform a switchover. Entering the **shut** and **no shut** commands on the interface does not bring up any VLANs on the interface except VLAN 1.

  Workaround: This issue is resolved.

- CSCtq92515

  Symptom: When a PIM neighbor flaps, both devices consider themselves to be the DF. The new DF winner does not send or announce others, which causes two DF winners in the network.

  Conditions: This symptom might be seen when a PIM neighbor flaps due to the port-channel link flaps, and then elects two DF winners on the same link.

  Workaround: This issue is resolved.

- CSCtq98904

  Symptom: High memory utilization might occur for the sysmgr process.

Conditions: This issue might be seen when there have been many VDC reloads on the standby supervisor prior to a switchover.

Workaround: This issue is resolved.

- CSCtr33173

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

  ```
  %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.

- 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.

- CSCtr43139

  Symptom: After an ISSU and EPLD upgrade on a Cisco Nexus 7000 Series switch, the first switchover performed results in a failure of the UDLD process with multiple core files.

  Conditions: This issue might be seen at the first switchover after the upgrade. Further switchovers do not cause the problem.

  Workaround: This issue is resolved.

- CSCtr60037

Symptom: The **no exec-timeout** command does not return a console or VTY timeout to the 30-minute default.

Conditions: This symptom might be seen when you enter the **no exec-timeout** command. It does not restore the default 30-minute timeout. Instead, the timeout is set to zero.

Workaround: This issue is resolved.

- CSCtr71054

  Symptom: There is an inconsistency between ECMP next hops in the RIB and FIB. For example, the RIB might have more than one ECMP next hop, but the FIB has just one.

  Conditions: This symptom might be seen in a topology change if the cost of all ECMP next hops becomes worse, such as if there were four ECMP next hops with a metric of 100 and all of them moved to a cost of 200.

  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.

- 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.

- CSCtr93839

  Symptom: A memory leak occurs in the Spanning Tree Protocol (STP) after the maximum memory allowed (256 MB) is reached. STP statefully restarts and creates a core file. There is no impact on the STP operation. This symptom happens on a vPC primary in a vPC domain that is not root for the Multiple Spanning Tree (MST) protocol.

  Conditions: A memory leak can happen in a double-sided vPC between two vPC domains with MST and the peer-switch enabled. This symptom might be seen only if a vPC domain that is a root has a peer-switch enabled and operational and MST is used.

  Workaround: This issue is resolved.

- CSCtr97385

  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.

Resolved Caveats—Cisco NX-OS Release 5.1(4)

- CSCtg95381

  Symptom: A Cisco Nexus 7000 Series switch may redirect traffic to the CPU so that the traffic may experience random delays or drops. ARP is learned and FIB adjacency is in the FIB adjacency table.

  Conditions: This issue might be seen because of race conditions. Some hosts do not respond to the ARP refresh sent by the Cisco Nexus 7000 Series switch which in turn triggers a deletion of the ARP entry due to expiry. Because of this, the route delete notification is sent to URIB from the process. However, traffic still arrives at the given IP address. As a result, the next packet triggers ARP and ARP is learned from the host.

  Workaround: This issue is resolved.

- CSCtl89610

  Symptom: When traffic switches from a rendezvous point tree (RPT) to a shortest path tree (SPT), duplicate traffic can be seen. This is true if the RPF interface toward the RP and the source are different. This situation can last for a maximum of 60 seconds.

Conditions: This symptom might be seen immediately after a change from PRT to SPT.

Workaround: This issue is resolved.

- CSCtn70547

  Symptom: A port security trap not is raised if the policy is to shut down the port if a violation occurs.

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

  Workaround: This issue is resolved.

- CSCtn70579

  Symptom: When you attempt to use syslog traps for the port status, you can get unintelligible characters which makes the syslog message unreadable and unusable for information. For example, you might see:

  ```
  2011 Feb 11 17:09:36 lolcatz %ETH_PORT_SEC3-ETH_PORT_SEC_SECURITY_
  VIOLATION_MAX_MAC_VLAN: Port Ethernet1/2 moved to ^\1^H\214^^D state as host
  0000.0001.4266 is trying to access the port in vlan 666
  ```

  Conditions: This symptom might be seen when you use syslog traps to get the port status.

  Workaround: This issue is resolved.

- CSCtn81109

  Symptom: On a Cisco Nexus 7000 Series switch, the 32-port 10-Gigabit Ethernet SFP+ I/O module (N7K-M132XP-12) may report diagnostic failures after bootup. The **show diagnostic result module X** command shows one or more ports failing the PortLoopback test.

  ```
  Module 1: 10 Gbps Ethernet Module
          Test results: (. = Pass, F = Fail, I = Incomplete,
          U = Untested, A = Abort, E = Error disabled)
           5) PortLoopback:
            Port  17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
            -----------------------------------------------------
                   U  U  .  .  .  .  E  .  U  U  E  .  .  E  E  E <<====
  Nexus7000 may also report following message:
  %MODULE-4-MOD_WARNING: Module X (serial: <serial#>) reported warning on ports
  x/y-x/y (Ethernet) due to Loopback test failed.
  ```

  Conditions: This symptom can be seen immediately after a switch reboot (but not at every reboot, as the behavior occurs randomly). The following behaviors can be seen:

  - Failed ports may recover after some time.
  - Failing ports need not be successive.

  Workaround: This issue is resolved.

- CSCtn93962

Symptom: An STP frame that should have been sent over a vPC reaches the peer switch on the vPC peer link.

Conditions: This issue is seen only when the access switch reloads and the port-channel interfaces are split across the two vPC switches. This issue also requires a significant amount of STP traffic that originates from one of the vPC switches that goes to the access switch.

Workaround: This issue is resolved.

- CSCtn94017

  Symptom: When a GRE tunnel is configured between a Cisco Nexus 7000 Series switch and another device, the switch can fail when a ping is initiated from the remote side of the GRE tunnel to the IP address of the tunnel interface on the Cisco Nexus 7000 Series switch.

  Conditions: This symptom might be seen when the ping for the GRE tunnel is received on a F series module.The GRE tunnel should use a source and destination loopback interface. The trigger for this symptom can be traffic destined in-band over the GRE tunnel and switched from the F series module; however, the issue can also be triggered from an M series module given the correct sequence of triggers.

  Workaround: This issue is resolved.

- CSCto01869

  Symptom: Cisco Nexus 7000 Series modules do not learn MAC addresses, although the supervisor module appears to learn them correctly. This situation results in unicast flooding.

  The output of the **show mac address dynamic** command shows the MAC address, but the **show mac address-table** *module-number* **dynamic** command and the **show hardware mac address-table** *module-number* **dynamic** command do not show the MAC address.

  Conditions: This issue might be seen whenever the dynamic MAC entries have been cleared on the interface with the **clear mac address-table dynamic interface** *interface* command.

  Workaround: This issue is resolved.

- CSCto11782

  Symptom: OTV sites are not seen across the FabricPath cloud. This issue affects NX-OS Release 5.1(1), Release 5.1(2) and Release 5.1(3) releases only. No other releases are affected.

  Conditions: This symptom might be seen when OTV hellos that are sent over the FabricPath cloud to other OTV sites are lost and both OTV sides are seen as active.

  Workaround: This issue is resolved.

- CSCto13318

  Symptom: When a module reloads or the weighted random early detection (WRED) configuration changes on a Cisco Nexus 7000 Series switch, continuous partial traffic loss that is independent of the traffic rate and WRED thresholds can occur.

  Conditions: This symptom might be seen on a 32-port 10-Gigabit Ethernet SFP+ I/O module (N7K-M132XP-12) with egress queuing policies.

  Workaround: This issue is resolved.

- CSCto42908

  Symptom: The queue limit that is applied to an interface does not match the configuration.

  Conditions: This symptom might be seen when the applying non-default queueing policy to an interface results in the incorrect queue limit applied to the interface.

  Workaround: This issue is resolved.

- CSCto47841

  Symptom: Under extremely rare circumstances, a nondisruptive software upgrade from Cisco NX-OS Release 5.1(1) to Release 5.1(3) might cause all but one of the modules to fail, including the standby supervisor.

  Conditions: This symptom might be seen when a configuration is corrupted.

  Workaround: This issue is resolved.

- CSCto49052

  Symptom: Moving a MAC address on port-security ports causes an MTS buffer leak. The **show system internal mts buffer detail** command may not be helpful. Use the **show system internal mts buffer summary** command to troubleshoot the problem. You can see the following output:

  ```
  node    sapno   recv_q  pers_q  npers_q log_q
  sup     191     0       0       64126   0
  ```

  There is a large number under npers_q for sapno 191, which is port-security.

  ```
  switch# sh system internal mts memory mts buffer manager statistics
  shared memory pool at fcbae000-febae000 (size: 33554432 bytes)
  request_hi:      120928
  request_lo:      0
  mem_in_use:      16857088
  mem_free:        16697344
  ```

  If there is no free MTS buffer, the switch can lose most functions. For example, it cannot process the **show running configuration** command.

  To troubleshoot the problem, change the message level for l2fm to a number higher than 4 or above (that is, logging level l2fm 4). The default value is 2. The following is sample output:

  ```
  %L2FM-4-L2FM_MAC_MOVE: Mac xxxx.xxxx.xxx has moved from Eth<mod/port> to
  Eth<mod/port>
  ```

  Conditions: This issue can be seen in all NX-OS Release 4.1(x) software up to Release 4.2(6), and in all NX-OS Release 5.0(x) software, and all Release 5.1 software up to Release 5.1(3).

  Workaround: This issue is resolved.

- CSCto49126

  Symptom: A Cisco Nexus 7000 Series switch running NX-OS Release 5.1(3) and configured with port security will install a static MAC address in the hardware table regardless of the interface status.

  Conditions: This symptom might be seen when port security is configured for a switch port.

  Workaround: This issue is resolved.

- CSCto54463

  Symptom: A nondisruptive software upgrade (ISSU) from NX-OS Release 5.1(1) or Release 5.1(2) to Release 5.1(3) causes spanning tree bridge protocol data unit (BPDU) timeouts, Unidirectional Link Detection (UDLD) timeouts, and Enhanced Interior Gateway Routing Protocol (EIGRP) timeouts on adjacent devices which results in network disruptions.

  Conditions: This issue might be seen during a supervisor switchover or an ISSU.

  Workaround: This issue is resolved.

- CSCto54709

  Symptom: The incorrect weighted round-robin (WRR) configuration is applied to an interface.

  Conditions: This symptom might be seen when the WRR configuration on an interface is modified. The existing priority queue configuration is not considered which results in bandwidth being taken from the existing queue to be allocated to the priority queue.

  Workaround: This issue is resolved.

- CSCto63457

  Symptom: SNMP polling for OSPF MIBs on the Cisco Nexus 7000 Series switch causes the SNMP process to fail and a system switchover to occur.

  Conditions: This symptom might be seen when there is polling through SNMP for OSPF MIBs.

  Workaround: This issue is resolved.

- CSCto67986

  Symptom: A gratuitous ARP (GARP) storm can cause the MTS buffers to lock up which can cause connectivity issues on the network and eventually lead to a supervisor failover. The following syslog messages might be seen:

  ```
  %KERN-2-SYSTEM_MSG: mts_acquire_q_space() failing
  ```

  ```
  %SYSMGR-SLOT4-2-TMP_DIR_FULL: System temporary directory usage is unexpectedly high
  at 100%.
  ```

  You might also see the adjmg, l2fm, and arp processes running at a high utilization level.

  Conditions: This symptom is specific to a storm of GARPs from multiple hosts that claim the same IP address. This symptom causes the Cisco Nexus 7000 series switch to constantly update its ARP and adjacency tables which might result in an MTS buffer lockup.

  For a typical ARP storm caused by a bridging loop, this issue is not seen.

  Workaround: This issue is resolved.

- CSCto69635

  Symptom: Packets with a destination MAC address that is all zeroes get flooded when received on on a blocked stp-port and maintain a loop.

  Conditions: This symptom might be seen following a nondisruptive software upgrade from any Cisco NX-OS Release 4.2(x) to any Cisco NX-OS Release 5.x when the blocked ingress port is on a 48-port 1-Gigabit SFP I/O module (N7K-M148GS-11).

  Workaround: This issue is resolved.

- CSCto72064

  Symptom: Traffic drops for CoS 4 traffic.

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

  - There is CoS 4 traffic.
  - There is an ingress F1 series module and an egress M1 series module.
  - You are using the nondefault system QoS policy. (The default-nq-8e-policy is the default policy and it would have to be manually changed for this issue to be seen.)

  Workaround: This issue is resolved.

- CSCto98883

  Symptom: The maximum number of addresses in port security is reached even when the configuration is empty:

  ```
  ERROR: Maximum value reached, MAC address cannot be configured
  ```

  As a result, the correct port security address cannot be configured on the port.

  Conditions: This symptom might be seen in the port security configuration when the port security address has been added or removed several times.

  Workaround: This issue is resolved.

- CSCto99151

  Symptom: A security violation occurs for a MAC address that is configured as a secure MAC in the interface configuration.

  Conditions: This symptom might be seen if port security is used when secure MAC is configured on interfaces.

  Workaround: This issue is resolved.

- CSCtq29575

  Symptom: There are multiple symptoms:

  - A FEX access port learns the MAC address of a server (host) on the wrong VLAN.
  - A FEX access port learns the MAC address of a server (host) on two VLANs.
  - Traffic from a FEX access port is dropped even though the port is in forwarding state.

  Conditions: This symptom can be seen whenever a nondisruptive software upgrade from NX-OS Release 5.1(1) or Release 5.1(2) to Release 5.1(3) is performed with FEX access ports in the setup.

  Workaround: This issue is resolved.

- CSCtq62339

  Symptom: A Cisco Nexus 7000 Series switch may report a platform memory alert due to high memory utilization:

  ```
  %PLATFORM-2-MEMORY_ALERT: Memory Status Alert: MINOR. Usage 85% of Available Memory
  %PLATFORM-2-MEMORY_ALERT: Memory Status Alert: SEVERE. Usage 90% of Available Memory
  ```

The following commands display the status:

```
switch# sh system internal memory-status
MemStatus: Severe Alert
switch# sh system internal memory-alerts-log | inc "ALERT
INFO|MemTotal|MemFree|LowTotal|LowFree"
 MINOR ALERT INFO
MemTotal:      8254672 kB
MemFree:       4295324 kB
LowTotal:       727120 kB
LowFree:        109332 kB
 SEVERE ALERT INFO
MemTotal:      8254672 kB
MemFree:       4255408 kB
LowTotal:       727120 kB
LowFree:         72392 kB
```

Conditions: This symptom can be seen only if the following conditions are true:

- The switch is running a release between NX-OS Release 5.1(1) to Release 5.1(3). In these releases, the issue is exposed regardless of any feature that is enabled or disabled. There is no precondition for this issue.
- A low-memory condition is logged when the following formula is at or above the logging threshold:

  (LowTotal - LowFree) ÷ LowTotal x 100

  For example: (727120 - 72392) ÷ 727120 x 100 = 90% (threshold reached due to utilization in low region)
- The low memory condition has been seen after approximately 3 months of supervisor uptime.

Workaround: This issue is resolved.

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

- CSCte65416

  Symptom: Timeouts can occur on a Cisco Nexus 7000 Series switch when SNMP polling occurs.

  Conditions: This symptom might be seen because the internal timeout on SNMP polls is set at 4 seconds when it should be set at 3 seconds, which stops the polling timeout.

  Workaround: This issue is resolved.

- CSCtf29790

  Symptom: IPv6 Neighbor Discovery (ND) neighbors are not learned and IPv6 packet loss occurs because neighbors are not formed.

  Conditions: This symptom might be seen in a vPC topology with a peer-gateway configuration. During routing of an IPv6 Neighbor Solicitation (NS) or Neighbor Advertisement (NA) packet, the hop-limit is decremented on one of the switches, which causes a packet drop because the hop limit is not 255.

  Workaround: This issue is resolved.

- CSCtj44206

  Symptom: An internal queue overflows. The following syslog can be seen in the supervisor module's show logging output:

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

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

  Workaround: This issue is resolved.

- CSCtk56636

  Symptom: The login process occasionally fails.

  Conditions: This symptom might be seen when a script runs Telnet recursively and then abruptly terminates which causes the login process to fail. The occurrence of this issue is very rare, and the impact is minimal. Normal scripts and user logins are not impacted.

  Workaround: This issue is resolved.

- CSCtk57644

  Symptom: The load balancing value calculated in software and displayed through the CLI may not match the load balancing value that is actually calculated and used in the Cisco Nexus 7000 Series hardware.

  Conditions: This symptom might be seen when the VLAN of the packet is not the default VLAN and when the hardware configuration is L3 or L4 preference. When the packet carries the default VLAN and the preference is mixed, then the load balancing value calculated by software will be accurate.

  Workaround: This issue is resolved.

- CSCtk66841

  Symptom: If you perform a supervisor switchover or a nondisruptive software upgrade or downgrade, and you have a port-channel subinterface configured, the Cisco Nexus 32-port 10-Gigabit Ethernet SFP+ I/O module might fail.

  Conditions: This symptom might be seen when you have a port-channel subinterface configured and you perform a supervisor switchover or a nondisruptive software upgrade or downgrade.

  Workaround: This issue is resolved.

- CSCtk67264

  Symptom: When you downgrade from Cisco NX-OS Release 5.1(2) to NX-OS Release 5.1(1), any Fabric Extender (FEX) modules that are online are downgraded disruptively.

  Conditions: This symptom might be seen when FEX modules are attached to the switch during a downgrade from Cisco NX-OS Release 5.1(2) to NX-OS Release 5.1(1)

  Workaround: This issue is resolved.

- CSCtl04857

Symptom: If a user with the network-admin/vdc-admin role defined in TACACS tries to execute the **show run vdc-all** command from the default VDC, the command does not display the configuration from nondefault VDCs.

If you attempt to switch to the VDC and get the configuration, the following message displays:

```
!Running config for vdc: Cisco_Test

switchto vdc Cisco_Test
% Permission denied

Cmd exec error.
switchback
```

Conditions: This symptom might be seen for users whose roles are defined in AAA.

Workaround: This issue is resolved.

- CSCtl06601

  Symptom: MAC security does not work on ports that belong to a CTS ASIC that contains port 10. The output of the **show cts interface all** commands shows the SAP status as CTS_SAP_INCOMPLETE or CTS_SAP_FAILURE, and the status does not change to CTS_SAP_SUCCESS.

  Condition: This symptom might be seen on a Cisco Nexus 32-port, 10-Gigabit Ethernet SFP+ I/O module (N7K-M132XP-12) or a Cisco Nexus 32-port, 10-Gigabit Ethernet SFP+ I/O module XL (N7K-M132XP-12L) that runs Cisco NX-OS Release 5.0(3).

  Workaround: This issue is resolved.

- CSCtl08742

  Symptom: The contents of the VLAN Trunking Protocol (VTP) database file are overwritten and its size is set to 0 bytes.

  Conditions: This symptom might be seen if the VTP process restarts due to an internal failure.

  Workaround: This issue is resolved.

- CSCtl08798

  Symptom: Packets that originate from a supervisor module in a vPC+ setup are dropped after a vPC link failover.

  Conditions: This symptom might be seen only if a vPC+ is configured, one of the port-channel paths is down, and the native VLAN is in FabricPath mode.

  Workaround: This issue is resolved.

- CSCtl08902

  Symptom: If you do not change a configuration for several days on a nondefault VDC, you might not be able to make any changes to the port configurations. In particular, you can enter CLI commands, but they do not execute.

  Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch that runs Cisco NX-OS Release 4.2(4).

  Workaround: This issue is resolved.

- CSCtl09375

  Symptom: When HSRPv6 is configured, the Cisco Nexus 7000 Series switch does not honor the RS request from the host.

  Conditions: This symptom might be seen when a host reboots. It takes approximately 3 minutes to auto configure an IPv6 address.

  Workaround: This issue is resolved.

- CSCtl10832

  Symptom: IPv6 does not work in Cisco NX-OS Release 5.1(2) in a vPC or vPC+ setup when a peer gateway is configured.

  Conditions: This symptom might be seen when Neighbor Discovery Protocol (NDP) packets are routed on a remote vPC peer switch and the Time To Live (TTL) hop limit in the IPv6 header is decremented. When the packet reaches the vPC switch to which the NDP packet is destined, the TTL is not 255 and so it is dropped in the software.

  Workaround: This issue is resolved.

- CSCtl10879

  Symptom: IPv6 Neighbor Discovery (ND) neighbors are not learned and a IPv6 packet loss occurs because neighbors are not formed.

  Conditions: This symptom might be seen in a vPC+ topology with a peer-gateway configuration. During routing of an IPv6 Neighbor Solicitation (NS) or Neighbor Advertisement (NA) packet, the hop-limit is decremented on one of the switches, which causes a packet drop because the hop limit is not 255.

  Workaround: This issue is resolved.

- CSCtl11424

  Symptom: Incoming packets from a Layer 3 link that are destined to a peer switch virtual interface (SVI) MAC address might be dropped on the local Cisco Nexus 7000 Series switch. The packet arrives at the supervisor module on the local switch but is not forwarded over the peer link to the peer switch.

  Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch that is running Cisco NX-OS Release 5.1(2) with the vPC peer-gateway feature configured.

  Workaround: This issue is resolved. For additional information related to this issue, see the "Layer 3 Backup Routing VLAN" section on page 18.

- CSCtl47670

  Symptom: When there is a one-leg vPC going out of a Cisco Nexus 7000 Series 32-port, 1/10 Gigabit Ethernet module (N7K-F132XP-15), there is a possibility that traffic might be denied on the egress side of the N7K-F132XP-15 module.

  Condition: This symptom might be seen if you do not have one vPC connected out of the downstream switch, and the vPC on the peer Cisco Nexus 7000 Series switch to the downstream switch is down.

Workaround: This issue is resolved.

- CSCtl46762

  Symptom: When IP Source Guard is configured on an interface on a Cisco Nexus 7000 Series switch, the next-hop address is incorrect.

  Conditions: This symptom might be seen because of a sequencing issue between IP Source Guard and ARP. The route is created in the forwarding information base (FIB), with the next hop given by IP Source Guard, but it has a wrong address.

  Workaround: This issue is resolved.

- CSCtl53830

  Symptom: The flowcontrol configuration fails on a port-channel interface. The following message displays:

  ```
  %ETHPORT-2-IF_CRITICAL_FAILURE: (Debug syslog)Critical failure:
  ethpm_dce_gldb_get_pfc_for_ifindex returned error: , no such pss key
  ```

  Condition: This symptom might be seen under the following conditions:

  - The port-channel members are on a Cisco Nexus 32-port 1/10 Gigabit Ethernet module (N7K-F132XP-15).
  - The port channel is up.

  Workaround: This issue is resolved.

- CSCtl54029

  Symptom: When you configure flow control in a port-channel interface, the CLI hangs for almost 2 minutes and then the command fails with the following message:

  ```
  %ETHPORT-2-IF_CRITICAL_FAILURE: (Debug syslog)Critical failure:
  ethpm_dce_gldb_get_pfc_for_ifindex returned error: , no such pss key
  ```

  Then the port-channel configuration hangs. Shutting down the port channel fails or displays the error “service no responding.”

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

  - The port-channel members are on a Cisco Nexus 32-port 1/10 Gigabit Ethernet module (N7K-F132XP-15).
  - The port channel is up.
  - You perform an ISSU from Cisco NX-OS Release 5.1(1) to Release 5.1(2).

  Workaround: This issue is resolved.

- CSCtl54897

  Symptom: The ipqosmgr process fails while processing the **show startup-config ipqos** command.

  Conditions: This symptom might be seen when the cos-to-queue mapping changes and is saved to the startup configuration.

  Workaround: This issue is resolved.

- CSCtl58995

  Symptom: Upon an online insertion and removal (OIR) of certain X2-10GB-ER transceivers, the interface reports that the transceiver is unsupported:

```
2011 Jan 13 11:59:22 NB1 %$ VDC-1 %$ %ETHPORT-5-IF_HARDWARE: Interface Ethernet8/2,
hardware type changed to unknown
2011 Jan 13 11:59:22 NB1 %$ VDC-1 %$ %ETHPORT-3-IF_UNSUPPORTED_TRANSCEIVER:
Transceiver on interface Ethernet8/2 is not supported
2011 Jan 13 11:59:22 NB1 %$ VDC-1 %$ %ETHPORT-3-IF_SFP_ERROR: Interface Ethernet8/2,
invalid SFP detected
2011 Jan 13 11:59:22 NB1 %$ VDC-1 %$ %ETHPORT-5-IF_DOWN_NONE: Interface Ethernet8/2 is
down (None)
```

  Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch that is running NX-OS Release 5.1(2), when an X2-10GB-ER transceiver is inserted in the 8-port, 10-Gigabit Ethernet I/O module XL (N7K-M108X2-12L). The output of the **sh int eth8/2 transceiver** command shows the following information about the transceiver:

```
Ethernet8/2
    transceiver is present
    type is 10GBASE-ER
    name is CISCO-OPNEXT,INC
    part number is TRT7051EN-SMC-31
    revision is A1
    serial number is OPB13310234
    tranceiver type is X2 Medium
    bit Encoding is NRZ
    connector Type is SC
    protocol Type is 10GbE
    10GbE Code Byte 0 : 10GBASE-ER
    fiber Type Byte 0 : SM, Generic
    fiber Type Byte 1 : Unspecified
    transmission Range is 40000 (in m)
```

  Workaround: This issue is resolved.

- CSCtl59485

  Symptom: The output of the **show interface eth** *x/y* command shows that all the interfaces on a Cisco Nexus 32-port 1/10 Gigabit Ethernet module (N7K-F132XP-15) are in shared mode when they are not.

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

  Workaround: This issue is resolved.

- CSCtl60414

  Symptom: The **ip msdp reconnect-interval** command does not take effect if the interval is configured for less than 30 seconds.

  Conditions: This symptom might be seen only during a Multicast Source Discovery Protocol (MSDP) startup when a peer is getting established and the **ip msdp reconnect-interval** command specifies an interval of less than 30.

  Workaround: This issue is resolved.

- CSCtl62218

Symptom: Following an STP topology change (TCN), IGMP general queries triggered in the VLAN are sent with a maximum-response-time (MRT) of 1 second. The IGMP join reports for all groups in the VLAN are generated within the 1-second period, which causes a short burst that leads to reports getting dropped. As a result of the reports being dropped, convergence delays occur for multicast groups.

Conditions: This symptom might be seen following STP topology changes in the VLAN.

Workaround: This issue is resolved.

- CSCtl67036

  Symptom: A Cisco Nexus 7000 Series switch drop DHCP discovery packets with source IP address 0.0.0.0.

  Conditions: This symptom might be seen when the DHCP server and clients are in the same VLAN on a Cisco Nexus 32-port, 1/10 Gigabit Ethernet module (N7K-F132XP-15). After reloading a client, the module fails to get an IP address.

  Workaround: This issue is resolved.

- CSCtl77076

  Symptom: When large ACLs are applied in the egress direction, a flap can occur in the Open Shortest Path First (OSPF) protocol and in the Link Aggregation Control Protocol (LACP).

  Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch when large ACLs are applied in the egress directions.

  Workaround: This issue is resolved.

- CSCtl77505

  Symptom: Rollback verification fails because the running configuration fails to roll back to the previous checkpoint.

  Conditions: This symptom might be seen when the **switchport trunk vlan add** command is in the configuration.

  Workaround: This issue is resolved.

- CSCtl78370

  Symptom: When you remove the proxy forwarder M series module from a Cisco Nexus 7000 Series switch, the **hardware proxy layer-3 forwarding** command is disrupted for 5 minutes if a Cisco Trusted Security (CTS) port is configured on the M series module and the CTS port is a member of a port channel.

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

  - The module that is removed is the proxy forwarder.
  - CTS is configured on the module.
  - The CTS port is a member of a port channel.
  - All members of the port channel are on the same module that is removed.

  Workaround: This issue is resolved.

- CSCtl78583

  Symptom: When you enter the **clear mac address-table dynamic vlan** *vlan* command, the supervisor module might fail. Immediately after a supervisor switchover, the newly active supervisor module also might fail.

  Conditions: This symptom might be seen when the **vlan** keyword is present in the command and dynamic Layer 2 entries are present for the VLAN. Without the **vlan** keyword, this problem does not occur.

  Workaround: This issue is resolved.

- CSCtl85080

  Symptom: Incomplete Address Resolution Protocol (ARP) entries are observed on a Cisco Nexus 7000 Series switch, along with partial packet loss and a memory leak.

  Conditions: This symptom might be seen when ARP packets have a nonstandard size (that is, greater than 64 bytes).

  Workaround: This issue is resolved. For additional information about this issue, see the "Layer 3 Backup Routing VLAN" section on page 18.

- CSCtl91630

  Symptom: The ipqosmgr process fails if you enter the **show policy-map interface** command while running Cisco NX-OS Release 5.1(1), 5.1(1a), or 5.1(2).

  Conditions: This symptom might be seen if some members of a port channel are in the down state and you remove the down member from the port channel, which makes the database inconsistent. If you then enter the **show policy-map interface** command, the ipqosmgr process can fail.

  Workaround: This issue is resolved.

- CSCtl94248

  Symptom: Following a supervisor switchover or an ISSU, the port-channel linkage between ports gets broken in ipqos. If you then try to access a port by entering the **show policy-map int** command, ipqosmgr process fails.

  Conditions: This symptom might be seen on the Cisco Nexus 7000 Series 32-port, 1/10 Gigabit Ethernet module (F1-Series) when you have ports that are configured as port-channel members.The problem is that following the switchover, the port-channel node to the port-channel linkage does not get established because there are no default policies on the port channel on the Cisco Nexus 32-port 1/10 Gigabit Ethernet module (N7K-F132XP-15). As a result, the port-to-port-channel relationship does not come up. Previously, the port-channel node to the port-channel linkage was established by looking at the policies attached to the port channel and the effective destination for these policies.

  Workaround: This issue is resolved.

- CSCtn08545

  Symptom: The ACL entries in the hardware that correspond to an access group that is applied on a Layer 3 port-channel subinterface might disappear after a system reload.

  Conditions: This symptom might be seen when an ACL is applied on a Layer 3 port-channel subinterface.

Workaround: This issue is resolved.

- CSCtn12755

  Symptom: Packets to a specific destination are not transported over the OTV overlay interface.

  Conditions: This symptom might be seen when packets have the destination MAC address bits 48:44 =0x6. Bits 0:43 can assume any values, but if bits 48:44 have a value of 0x6, the packets are dropped.

  Workaround: This issue is resolved.

- CSCtn13364

  Symptom: Following an ISSU, certain traffic for a VLAN that was flowing correctly before the upgrade starts to drop. This situation can be caused by incorrect hardware ACL identifiers being programmed on the affected VLANs, even though there might not be any ACLs present.

  Conditions: This symptom might be seen following an ISSU from Cisco NX-OS Release 5.0(3) to Release 5.1(1a).

  Workaround: This issue is resolved.

- CSCtn32477

  Symptom: When you attempt to change the layer of a Layer 3 port that has subinterfaces, the switch hangs and the following output displays:

  ```
  switch(config)# int ethernet 1/3
  switch(config-if)# no shut
  ```

  The command does not execute successfully, which can be confirmed with the following **show** commands:

  ```
  switch(config-if)#
  switch# sh int e1/3
  Ethernet1/3 is down (Administratively down)
  ```

  Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch that runs Cisco NX-OS Release 5.x software and the **switchport** command is executed on an Layer 3 port containing subinterfaces.

  Workaround: This issue is resolved.

- CSCtn37687

  Symptom: When a vPC peer link is shut down, there is a high convergence number.

  Conditions: This symptom might be seen on a Cisco Nexus 8-port, 10-Gigabit Ethernet I/O module XL (N7K-M108X2-12L) and on a Cisco Nexus 32-port, 1/10 Gigabit Ethernet module (N7K-F132XP-15). The laser cut does not happen early when a vPC or a port channel is shut down. As a result, member ports do not go down quickly.

  Workaround: This issue is resolved.

- CSCtn42451

Symptom: When you try to apply a configuration in the default VDC, the switch hangs for approximately 60 seconds and displays the following output:

```
switch(config)# int ethernet 1/3
switch(config-if)# no shut
```

The command does not execute successfully, which you can verify with the following show commands:

```
switch(config-if)#
switch# sh int e1/3
Ethernet1/3 is down (Administratively down)
```

Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch running Cisco NX-OS Release 4.2(6) software when a **no shut** command is executed on a port-channel member.

Workaround: This issue is resolved.

- CSCtn46755

  Symptom: After configuring a port in a port channel on a Cisco Nexus 32-port, 1/10 Gigabit Ethernet module (N7K-F132XP-15) and saving the configuration, specific commands are not present on the physical interface after a switch reload.

  Conditions: This symptom might be seen on a Cisco Nexus 32-port, 1/10 Gigabit Ethernet module (N7K-F132XP-15) module if ports are added to a port channel and interface configuration settings are configured on the port channel. The changes that are inherited by the physical interface may not persist after a switch reload.

  Workaround: This issue is resolved.

- CSCtn46903

  Symptom: Applying an ASCII configuration to a running configuration takes a long time and some components can time out.

  Conditions: This symptom might be seen when applying an ASCII configuration file in which every VLAN has a unique attribute, such as “name,” and one VLAN at a time is created. The sudden load on the system can cause a timeout.

  Workaround: This issue is resolved.

- CSCtn46911

  Symptom: Connectivity through a second Cisco Nexus 7000 Series peer switch is completely lost following a switch reload or a device in the vPC that is not a switch is disconnected.

  Conditions: This symptom might be triggered by a Multiple Spanning Tree (MST) protocol root flap between two peer switches. The following conditions exist:

  – The device that is not a switch establishes a vPC with two Cisco Nexus 7000 switches.

  – Multiple Spanning Tree (MST) protocol is running and the first Cisco Nexus 7000 Series switch is the root.

  – A switch reload occurs or the third device becomes disconnected.

  – Spanning Tree Protocol (STP) shows all vPCs as forwarding, but PIXM shows that the vPC is blocking.

  Workaround: This issue is resolved.

- CSCtn27760

  Symptom: Following an ISSU, some Bidirectional Forwarding Detection (BFD) sessions on switch virtual interfaces (SVIs) do not come up.

  Conditions: This symptom might be seen if there are numerous BFD sessions over SVI interfaces and the member ports are spread across several modules. Some or all of the BFD sessions on the interfaces do not come up after an ISSU.

  Workaround: This issue is resolved; however, you should disable BFD before you upgrade to Cisco NX-OS Release 5.1(3) and enable it after the upgrade. For additional information about this issue, see the "Disabling BFD Prior to a Software Upgrade or Downgrade" section.

Resolved Caveats—Cisco NX-OS Release 5.1(2)

- CSCtg97904

  Symptom: Port access-lists that are applied on Layer 2 interfaces are not effective for bridged multicast traffic.

  Conditions: This symptom might be seen when port access-lists are applied on Layer 2 interfaces that are part of a switch virtual interface (SVI).

  Workaround: This issue is resolved.

- CSCti73225

  Symptom: A Cisco Nexus 7000 Series switch might reset with the service "ascii-cfg" and display the following log:

  ```
  %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service "ascii-cfg" (PID 6997) hasn't caught
  signal 11 (core will be saved).
  ```

  Conditions: This symptom might be seen when you implement a rollback, enter the **show diff** command, or configure any other feature that triggers a checkpoint or rollback.

  Workaround: This issue is resolved.

- CSCti77845

  Symptom: The HSRP delay reload feature does not work as expected.

  Conditions: This symptom might be seen when a Cisco Nexus 7000 Series switch that is running NX-OS Release 5.0(x) with the HSRP delay reload feature enabled is reloaded.

  Workaround: This issue is resolved.

- CSCti95653

  Symptom: FEX ID 100 cannot be configured.

  Conditions: When FEX ID 100 is configured, a nondisruptive software upgrade fails.

  Workaround: This issue is resolved.

- CSCtj52606

Symptom: A valid queuing service policy might not be applied correctly to hardware. An error message about attempting to configure more than 100 percent of bandwidth is usually displayed.

Conditions: This symptom might occur because the queuing service policy uses a partial number of the class maps that are available in the hardware for a given port type. For example, if there are two queues per port on the ingress port for the 48-port, 1-Gigabit Ethernet module (N7K-M148GS-11), the policy attempts to configure just one queue and leaves the other queue not configured by referring to one class map.

Workaround: This issue is resolved.

- CSCtj56845

  Symptom: When a Reverse Path Forwarding (RPF) change occurs, instability of processes on the switch can be observed. For example, IGMP can take 100 percent of the CPU, the virtual port channel (vPC) keepalive link might be lost, a vPC might become inconsistent due to a BPDU timeout on various VLANs, or the netstack process or other processes might fail.

  Conditions: This symptom might be seen when the system has a vPC and more than 5000 S,G entries change the RPF from one interface to another.

  Workaround: This issue is resolved.

- CSCtj59752

  Symptom: Following a system switchover, some (*,G) entries became corrupted and were missing the RPF interface. As a result, when the traffic was stopped, some of the entries failed to come up.

  Conditions: This symptom might be seen after a system switchover.

  Workaround: This issue is resolved.

- CSCtj69147

  Symptom: Removing a port from a port channel for a FEX uplink causes QoS policies to be improperly applied on FEX ports.

  Conditions: This symptom might be seen when a QoS policy is applied on a FEX satellite port, and the FEX uplinks from the FEX module are linked to multiple modules.

  Workaround: This issue is resolved.

- CSCtj69423

  Symptom: Sometimes after the OTV feature is disabled and then enabled again, the CLI gets stuck and rejects any subsequent configuration command. This issue affects configuration commands not only for OTV, but for all Layer 3 features as well.

  Conditions: This symptom might be seen when the following sequence of events occur:

  - Enable the OTV feature with the **feature otv** command.
  - Configure OTV overlays.
  - Disable the OTV feature with the **no feature otv** command.
  - Reenable the OTV feature with the **feature otv** command.

  Workaround: This issue is resolved.

- CSCtj84923

  Symptom: When you downgrade from Cisco NX-OS Release 5.1(1) to NX-OS Release 4.2(4) on the Cisco Nexus 7018 switch, the modules reload if all five crossbar modules are not online.

  Conditions: You might see this symptom on the Cisco Nexus 7018 switch. The symptom is not seen on the Cisco Nexus 7010 switch

  Workaround: This issue is resolved.

- CSCtj89234

  Symptom: The Link Aggregation Control Protocol (LACP) standby link takes a long time to become active.

  Conditions: This symptom might be seen when a LACP standby link becomes active on a switch running Cisco NX-OS Release 5.1(1).

  Workaround: This issue is resolved.

- CSCtk13753

  Symptom: A ping sent to the management interface of a Cisco Nexus 7000 Series switch fails.

  Conditions: This symptom might be seen if a ping is to the management interface on a directly connected Cisco Nexus 7000 Series switch that is running Cisco NX-OS Release 4.2(4).

  Workaround: This issue is resolved.

- CSCtk16254

  Symptom: Entering the **show vpc consistency-parameters global** command causes the virtual port channel (vPC) service to fail.

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

  - Configuration inconsistencies exist as a result of copying and pasting a large configuration to to the switch.
  - If the VLAN interfaces are scattered (noncontiguous ranges), or the switch virtual interfaces (SVIs) are in different states (up/down).

  Workaround: This issue is resolved.

- CSCtk18406

  Symptom: The standby supervisor module fails to synchronize with the active supervisor module. The following error messages appear:

  ```
  2010 Nov 21 11:44:47 Switch %SYSMGR-2-SYNC_FAILURE_MSG_PAYLOAD: vdc 1: HA SYNC failure
  on sap=306 (errno -16) [recv] has high number of messages  The first and last 50
  messages contains: ^Iopcode 55301 - 100 messages
  2010 Nov 21 11:44:52 Switch %SYSMGR-2-SYNC_FAILURE_STANDBY_RESET: Failure in syncing
  messages to standby for vdc 1 causing  standby to reset.
  ```

  The standby supervisor module may also reset after the preceding messages appear.

  Conditions: This symptom might be seen in a dual-supervisor setup when NetFlow is enabled on a large number of interfaces and if there is a high amount of export data to be sent to the collectors.

  Workaround: This issue is resolved.

- CSCtk54305

  Symptom: A CLI command to create a VLAN returns the following error:

  ```
  No VLAN resource available for VLAN creation.
  ```

  Conditions: This symptom might be seen when the switch has a large number of VLANs with discontinuous VLAN IDs.

  Workaround: This issue is resolved.

- CSCtk60515

  Symptom: An upgrade to Cisco NX-OS Release 5.1(2), or a downgrade from NX-OS Release 5.1(2) can fail with the error “SRG processing failed” when there are multiple virtual device contexts (VDCs).

  Conditions: This symptom might be seen randomly, depending on the Messages and Transactional Services (MTS) dynamic Service Access Point (SAP) assignments in the nondefault VDCs.

  Workaround: This issue is resolved.

- CSCtk83829

  Symptom: Packet loss occurs when a virtual port channel (vPC) peer-link is on an F1 module, or port channel vPCs are terminated on F1 modules.

  Conditions: This symptom might be seen when the peer-gateway is enabled. Connectivity loss to the virtual IP (VIP) or switch virtual interface (SVI) might occur. A similar symptom might occur when orphan devices target the default gateway (vPC Hot Standby Router Protocol (HSRP)) or beyond.

  Workaround: This issue is resolved.

- CSCtl00453

  Symptom: If there is more than one link that is connected to a Cisco Nexus 7000 Series switch from a fabric extender (FEX) module, and if there is a module in slot 1 of the Cisco Nexus 7000 Series switch, then the module in slot-1 will reload three times and stay powered-down

  Conditions: This symptom might be seen when all three of the following conditions are met:

  – A module should be present in slot 1 of the chassis.

  – A FEX should be connected across different modules.

  – This is the first time this FEX is connected to the Cisco Nexus 7000 Series switch chassis.

  Workaround: This issue is resolved.

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

- CSCtj71855

  Symptom: The security process fails when FIPS mode is enabled and a FIPS failure image is installed on the switch.

Conditions: This symptom might be seen if FIPS mode is enabled and an instrumented FIPS failure image is loaded on the switch for evaluation purposes.

Workaround: This issue is resolved.

- CSCtj76903

  Symptom: The security process fails if FIPS mode is enabled and you enter the **copy running-config** command with a normal image and then subsequently load the switch with the FIPS failure image.

  Conditions: This symptom might be seen if FIPS mode is enabled and you enter the **copy running-config** command with a normal image and then load the instrumented FIPS failure image on the switch for evaluation purposes.

  Workaround: This issue is resolved.

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

- CSCta03634

  Symptom: All member objects of a track list are lost after a configuration rollback.

  Conditions: This symptom occurs only when tracking objects of type “track list.” The sequence of events that trigger this symptom are as follows:

  1. Create a track list with some number of objects configured as members of the track list.
  2. Create a checkpoint.
  3. Roll back to the created checkpoint.

  Workaround: This issue is resolved.

- CSCta32738

  Symptom: Under certain conditions, TrustSec 802.1AE security negotiations between ports might not complete successfully.

  Conditions: You might see this symptom if you have 10-Gbps ports running in full rate dedicated mode as part of a port channel with the Cisco TrustSec 802.1AE Encryption/Authentication feature enabled.

  Workaround: This issue is resolved.

- CSCta58181

  Symptom: When you specify a MAC ACL for a WCCP redirect-list and/or service-list of a service group and that ACL is applied to an interface, the SBADDFAIL syslog appears to indicate an invalid ACL. After you receive this error and you change the redirect ACL, the WCCP redirect for the service group is not programmed in the hardware. The syslog is as follows:

```
Event:E_DEBUG, length:124, at 108444 usecs after Thu Jul
9 00:38:49 2009
[105] WCCP-EVNT: Send to SPM: Req Id:0x18cb62, Policy
ID:0, OpMode:DEL, Inte rface:ALL, Type:Match node update,
Match id: 417

Event:E_DEBUG, length:74, at 108200 usecs after Thu Jul  9
```

```
00:38:49 2009
[105] WCCP-EVNT: vrf default service 61: Request to
DELETE Redirect-List <>

Event:E_DEBUG, length:190, at 75267 usecs after Wed Jul  8
23:58:29 2009
[105] WCCP-EVNT: Rx from SPM: Req id:0x17f5fe, Policy
ID:1, OpMode:ADD, Inte rface:Ethernet9/1, Type:INGRESS
Redirect, Request status:FAILED, Error code:0x4116000f, Error
string:Invalid format

Event:E_DEBUG, length:116, at 27246 usecs after Wed Jul  8
23:58:29 2009
[105] WCCP-EVNT: Send to SPM: Req id:0x17f5fe, Policy
ID:1, OpMode:ADD, Inte rface:Ethernet9/1, Type:INGRESS Redirect

Event:E_DEBUG, length:80, at 645750 usecs after Wed Jul  8
23:58:15 2009
[105] WCCP-EVNT: vrf default service 61: Request to ADD
```

Conditions: You might see this symptom when you use a MAC ACL (not an IP ACL) to specify the service-list or redirect-list.

Workaround: This issue is resolved.

- CSCtb67491

  Symptom: When DHCP configuration ACLs are applied to a module that has an incompatible configuration or insufficient resources, the DHCP snooping service displays the message: DHCP_SNOOP-3-HWPGMFAILURE. This behavior is expected. However, when the incompatible configuration or resource restriction is removed, subsequent DHCP configurations will not take effect on such modules and no redirect ACLs are programmed. As a result, DHCP snooping or relay does not work as expected.

  Conditions: This symptom occurs only where there is an incompatible configuration (such as resource pooling for example, which is not supported with the DHCP feature) or insufficient resources on the module, and the DHCP configuration is applied within the first 30 seconds of enabling DHCP with the **feature DHCP** command. This symptom may also occur when the module reloads and incompatible DHCP configuration are applied automatically by the DHCP feature.

  Workaround: This issue is resolved.

- CSCtb73380

  Symptom: Redistribution based on IP next-hop only works for BGP. Redistribution does not work for any other protocols.

  Conditions: This symptom might be seen because Cisco NX-OS does not support redistribution into EIGRP based on IP next-hop.

  Workaround: This issue is resolved.

- CSCtd59280

  Symptom: Following a restart, OSPF v3 fails to generate an intra-area Link Service Advertisement (LSA) from the IPv6 loopback interface if there are no IPv4 addresses on the interfaces.

  Conditions: You might see this symptom if you do not have any IPv4 addresses on the loopback interfaces.

Workaround: This issue is resolved.

- CSCtd86861

  Symptom: DOM (Digital Optical Monitoring) is disabled for X2 transceivers with the manufacturer's part number QFBR-7502-CS3 because these X2 transceivers do not support DOM.

  Workaround: This issue is resolved.

- CSCte50182

  Symptom: Layer 2 Protocol Tunneling (L2PT) is not part of the vPC consistency check across 802.1Q tunnel ports.

  Conditions: You might see this symptom under these conditions:

  - L2PT is enabled on a 802.1Q tunnel port on a local switch.
  - An 802.1Q tunnel port without L2PT is configured on the vPC peer switch.
  - These ports are part of a vPC.

  The vPC consistency check does not report an error about the missing L2PT configuration on one of the ports that is part of the vPC.

  Workaround: This issue is resolved.

- CSCtf14834

  Symptom: Detecting a newly inserted SFP can take as long as 30 seconds.

  Conditions: This symptom might be seen on N7K-M148GT-11, the 48-Port Ethernet I/O module, if a majority of the ports are populated with Copper SFPs and the Copper SFP ports are configured as non-autonegotiate.

  Workaround: This issue is resolved.

- CSCtg06552

  Symptom: Under certain specific configuration conditions, the following syslog might be seen following a switch reload. None of the physical interfaces are visible in the output of the **show interface** command:

  ```
  VMM-2-VMM_TIMEOUT: VDC1: Service SAP 377 timed out in INSERT_SEQ sequence
  ```

  Conditions: You might see this symptom after a switch reload only when a previously entered **copy running-config startup-config** command was executed at the same time a configuration session mode command such as the **verify** command, **commit** command, or **abort** command was being processed from a different console or Telnet session. In addition, QoS configurations within the configuration session mode (created using the **configuration session** *session-name* command) must exist. This situation can occur in any VDC.

  Workaround: This issue is resolved.

- CSCtg10624

  Symptom: An Ethernet interface on the 32-port 10-Gigabit Ethernet SFP+ I/O module (N7K-M132XP-12) might go down, and it will not come back up if you enter the **shut** command followed by the **no shut** command.

Conditions: This symptom might be seen if the interface is configured for Cisco Trusted Security (CTS) encryption. The problem is intermittently triggered during the CTS rekey operation, which is a normal function of CTS.

Workaround: This issue is resolved.

- CSCtg79256

  Symptom: All X2 optical transceivers takes 60 seconds to initialize. After inserting an X2 transceiver, the following syslog message displays:

  ```
  2010 May 15 02:10:13 switch %ETHPORT-5-IF_HARDWARE: Interface Ethernet8/1, hardware
  type changed to Transceiver initialization in progress. Can take up to 60 seconds
  ```

  Conditions: You might see this symptom under normal operating conditions for a Cisco Nexus 7000 Series device.

  Workaround: This issue is resolved.

- CSCtg82227

  Symptom: Preconfigured Enhanced Interior Gateway Routing Protocol (EIGRP) interface commands do not take effect after EIGRP has been enabled on an interface.

  Conditions: You might see this symptom if the configuration was done manually, starting with preconfigured commands.

  Workaround: This issue is resolved.

- CSCtg84010

  Symptom: When daylight saving time is configured on a switch, creating a new user with an expiry date or modifying the expiry date for an existing user might fail, depending on the expiry date.

  Conditions: You might see this symptom under the following conditions:

  - Daylight saving time (summer time) is configured.
  - The current date and time on the switch is within the daylight saving time zone and the expiry date that you are trying to configure is outside the daylight saving time zone and vice-versa.

  Workaround: This issue is resolved.

- CSCtg89227

  Symptom: Following a supervisor switchover on a Cisco Nexus 7000 Series switch, the Border Gateway Protocol (BGP) peer router repeatedly outputs the following BGP error:

  ```
  "%TCP-6-BADAUTH: No MD5 digest from"
  ```

  Conditions: This symptom might be seen when a BGP peer is established with an MD5 password.

  Workaround: This issue is resolved.

- CSCtg93564

  Symptom: HSRP IPv6 groups get into the initializing state when the interface primary global unicast IPv6 address is removed.

Conditions: This symptom might be seen when the interface primary global unicast IPv6 address is removed and the HSRPv6 groups on that interface move into the initializing state, even if they are not configured to use a global unicast virtual address.

Workaround: This issue is resolved.

- CSCtg94800

  Symptom: Entering the **no ip** *ip-address* **secondary** command does not remove the secondary virtual IP address in the HSRP group.

  Conditions: You might see this symptom when you enter the **no ip** *ip-address* **secondary** command. The primary VIP can be removed with the **no ip** command, but once the secondary VIP is configured, the **no ip** command does not remove it.

  Workaround: This issue is resolved.

- CSCtg97144

  Symptom: After an ISSU from any Cisco NX-OS Release 4.2(x) to Cisco NX-OS Release 5.0(2), if there is a switch reload, followed by a supervisor switchover, HSRP groups might go into the INIT state.

  Conditions: This symptom may occur only if the running configuration is not saved to the startup configuration after the ISSU but before the switch reload.

  Workaround: This issue is resolved.

- CSCtg97784

  Symptom: When you remove an egress queuing policy from a port channel interface, you might see the following error message:

  ```
  Note: Service policy with name <policy-map-name> does not exist in output direction
  on interface: <if-name>
  ```

  Conditions: You might see this symptom if the port channel contains a mix of ports from the 8-port Gigabit Ethernet I/O module XL (N7K-M108X2-12L) and the 32-port 10-Gigabit Ethernet SFP+ I/O module (N7K-M132XP-12), and there is an egress queuing policy applied to the port channel.

  Workaround: This issue is resolved.

- CSCth02149

  Symptom: A Bidirectional Forwarding Detection (BFD) session goes down and fails to come back up.

  Conditions: You might see this symptom after a supervisor switchover, followed by a switch reload.

  Workaround: This issue is resolved.

- CSCth45939

  Symptom: IPv6 neighbor discovery does not work over the overlay.

  Conditions: This symptom might be seen when IPv6 neighbor discovery is sent over the overlay.

  Workaround: This issue is resolved.

- CSCth65452

  Symptom: When you change the default VRF to the nondefault VRF for the OTV join interface, traffic over the Unicast OTV GRE tunnel does not go through. In other words, Unicast traffic does not flow through the OTV sites that are connected by these internal OTV GRE tunnels. This issue does not occur if you use the default VRF for the OTV join interface.

  Conditions: You might see this symptom in NX-OS Release 5.0(3) when you change the default VRF to the nondefault VRF for the OTV join interface.

  Workaround: This issue is resolved.

- CSCth67182

  Symptom: The standby supervisor in a Cisco Nexus 7000 Series system might not take over as the active supervisor.

  Conditions: This symptom might be seen if there is an online insertion and removal (OIR) of the active supervisor before the standby supervisor is in a full HA state. While in this state, both Layer 2 and Layer 3 instability can occur.

  Workaround: This issue is resolved.

- CSCth79649

  Symptom: OTV failures impact the VLANs for which the system is not an authoritative edge device.

  Conditions: This symptom might be seen when there is an edge device failure.

  Workaround: This issue is resolved.

- CSCti07871

  Symptom: If you enter the **show running-config snmp** command, an extra line with **community-map** will appear in the configuration following a reload.

  Conditions: This symptom might be seen following switch reload.

  Workaround: This issue is resolved.

- CSCti13182

  Symptom: Following a reboot of a Cisco Nexus 7000 Series switch that has a logging server configuration saved, the system manager confcheck component might fail. As a result, the switch will continuously reboot. You might see a message like the following:

  ```
  2010 Jul 27 00:11:16 R20010-T-HAMAMATSUCHO %$ VDC-1 %$ Jul 27 00:11:16
  %KERN-2-SYSTEM_MSG: Starting kernel... -kernel
  ```

  ```
   writing reset reason 16, confcheck hap reset
  ```

  Conditions: This symptom might occur if you have a logging server configuration saved and the switch reboots. An example of a logging server configuration is as follows:

  ```
  logging server 10.91.96.128
  ```

  Workaround: This issue is resolved.

- CSCti20899

Symptom: An internal component repeatedly reports the status of transceivers, even if there are no changes in the status. As a result, the cIfXcvrMonStatusChangeNotif trap is repeatedly sent.

Conditions: This symptom might be seen when an internal component is configured to send a trap for every interval for all ports.

Workaround: This issue is resolved.

- CSCti22016

  Symptom: After you delete a TACACS server, a Cisco Nexus 7000 Series switch might fail and display the following message:

  ```
  %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service "Tacacs Daemon"
  ```

  If you enter the **show system reset-reason** command, the switch shows the following reset reason:

  ```
  Reason: Reset triggered due to HA policy of Reset , Service: Tacacs Daemon hap reset.
  ```

  Conditions: This symptom might be seen when there is a TACACS configuration change.

  Workaround: This issue is resolved.

- CSCti69564

  Symptom: Following an upgrade of the EPLD image on a supervisor module on a single-supervisor Cisco Nexus 7000 Series switch, the supervisor module may not boot up completely, but instead may hang during the bootup process.

  Conditions: This symptom might be seen if you upgrade a SUP Local Bus CPLD device as a part of the EPLD upgrade on the supervisor of a single-supervisor Cisco Nexus 7000 Series switch.

  Workaround: This issue is resolved.

- CSCti77870

  Symptom: The ELTMC process fails when VLANs that are part of a PVLAN trunk configuration are removed.

  Conditions: This symptom might occur when VLANs are removed from the PVLAN trunk for any given port. Due to internal race conditions, ELTMC attempts to access information that is already removed, and this results in the process failing.

  Workaround: This issue is resolved.

- CSCti92073

  Symptom: An IP multicast packet is not replicated for some interfaces in the outgoing interface list.

  Conditions: When a module reloads, some outgoing interfaces might not receive multicast packets. This situation might occur when an RPF interface for the groups is on the module being reloaded. While the module is still in the process of coming up, a control plane receives a join request for that group (via PIM or IGMP) on an interface on a different module. It is possible that the route update to include this newly added interface is missed. As a result, the newly added interface never receives traffic for this group.

  You can identify this issue by entering the **show forwarding distribution multicast route** command to show the outgoing interface where the packet is not replicated for that interface.

  Workaround: This issue is resolved.

- CSCtj24568

  Symptom: In Multiple Spanning Tree (MST) mode, with MST 0 (CIST) running in Layer 2 gateway STP mode and MST 1 (and any of the MST Instance) running in regular (non-Layer 2 gateway STP mode), changing the VLAN mode of **fabricpath vlan** from mode **CE** to mode **fabricpath** can result in links that connect directly between the Layer 2 gateway switches going into STP Layer 2 gateway inconsistency mode.

  Conditions: This symptom occurs only under the following conditions:

  - The mode is MST mode.
  - MST 0 (CIST) is running Layer 2 gateway STP mode.
  - There is a directly connected link between Layer 2 gateway switches (both of which have MST mode and MST 0 (CIST) is running Layer 2 gateway STP mode).
  - Any of the MST instance is not running in Layer 2 gateway mode.
  - The VLAN mode is changed from **fabricpath** to **ce**.

  Workaround: This issue is resolved.

- CSCtj25245

  Symptom: If there is a difference in an SNMP trap configuration between the current running configuration and the target checkpoint, a rollback of the trap configurations fails.

  Conditions: This symptom might be seen when there is a difference in an SNMP trap configuration between the current running configuration and the target checkpoint.

  Workaround: This issue is resolved.

- CSCtj40661

  Symptom: The following log occasionally does not get printed when a hap-reset occurs:

  ```
  This supervisor will temporarily remain online in order to collect show
  tech-support. This behavior is configurable via
  'system [no] auto-collect tech-support'
  ```

  Conditions: This symptom might be seen when a hap-reset occurs.

  Workaround: This issue is resolved.

- CSCtj42985

  Symptom: Upon applying configuration commands copied from the output of the **show run all** command, Layer 2 broadcast or multicast packets like ARP, HSRP, etc., do not get switched correctly. Similarly, the port-security feature might not work.

  Conditions: This symptom might be seen because the Layer 2 storm control rate-limiter prevents Layer 2 broadcast or multicast packets from being switched. The **show hardware rate-limit** command indicates that packets are dropped by this rate-limiter.

  Port-security packets will also be dropped, in a similar fashion.

  By default, the Layer 2 storm control and port-security rate-limiters are disabled.

  The reason for this issue is that, the **show run all** command incorrectly displays the following output for the default configuration:

```
hardware rate-limiter layer-2 storm-control 0
hardware rate-limiter layer-2 port-security 0
```

This means that the rate-limiter is enabled with 0 pps.

The output should be displayed as follows:

```
no hardware rate-limiter layer-2 storm-control
no hardware rate-limiter layer-2 port-security
```

Workaround: This issue is resolved.

- CSCtj45151

  Symptom: When the VLAN Trunking Protocol (VTP) is enabled on a device and a large number of VLANs are present in the system, entering the **vlan suspend** command for hundreds of VLANs can cause the internal VLAN manager process to fail.

  Conditions: This symptom might be seen when you try to execute the **vlan suspend** command on hundreds of VLANs at a time, which produces a large number of transactions. The VLAN manager is then very busy processing messages and can skip certain heartbeats that will cause it to fail.

  Workaround: This issue is resolved.

- CSCtj57488

  Symptom: If you enter the **fabricpath switch-id** command under a vPC domain, you might see the following error message:

  ```
  ERROR: Operation failed: Configured peer-link cannot act as a fabricpath port
  ```

  Conditions: This symptom might be seen when a peer link is configured but it is not a core port.

  Workaround: This issue is resolved.

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

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

The following are related Cisco NX-OS documents:

Cisco NX-OS Configuration Guides

Cisco Nexus 7000 Series NX-OS Getting Started with Virtual Device Contexts, Release 5.x

Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 5.x

Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x

Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide, Release 5.x

Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x

Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 5.x

Cisco Nexus 7000 Series NX-OS OTV Configuration Guide, Release 5.x

Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 5.x

Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x

Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide, Release 5.x

Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 5.x

Cisco NX-OS Licensing Guide

Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x

Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x

Cisco NX-OS XML Management Interface User Guide, Release 5.x

Cisco NX-OS System Messages Reference

Cisco Nexus 7000 Series NX-OS MIB Quick Reference

Configuring Feature Set for FabricPath

Cisco NX-OS Command References

Cisco Nexus 7000 Series NX-OS Command Reference Master Index, Release 5.x

Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference, Release 5.x

Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x

Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference, Release 5.x

Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x

Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference, Release 5.x

Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 5.x

Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference, Release 5.x

Cisco Nexus 7000 Series NX-OS FabricPath Command Guide, Release 5.x

Cisco Nexus 7000 Series NX-OS System Management Command Reference, Release 5.x

Other Software Document

Cisco Nexus 7000 Series NX-OS Troubleshooting Guide, Release 5.x

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 Nexus 7000 Series NX-OS Release Notes, Release 5.1