Cisco Nexus 3000 Series NX-OS Release Notes, Release 6.0(2)U6(7)

This document describes the features, bugs, and limitations for Cisco Nexus 3000 Series and Cisco Nexus 3100 Series switches. Use this document in combination with documents listed in the "Obtaining Documentation and Submitting a Service Request" section.

Note: Release notes are sometimes updated with new information about restrictions and bugs. See the following website for the most recent version of the Cisco Nexus 3000 Series release notes: http://www.cisco.com/c/en/us/support/switches/nexus-3000-series-switches/products-release-notes-list.html.

Table 1 shows the online change history for this document.

Table 1. Online History Change

Date	Description
July 28, 2016	Created NX-OS Release 6.0(2)U6(7) release notes
August 30, 2016	Added a point in Upgrade Guidelines section for bug ID CSCva97678.
October 19, 2016	Added a point in Upgrade Guidelines section for bug ID CSCvb78728.
February 16, 2017	Added new hardware N3K-C3172PQ-XL, N3K-C3132Q-XL, and N3K-C3172TQ-XL under Table 2.
August 30, 2017	Modified Upgrade Guidelines section for bug ID CSCvb78728.
November 29, 2017	Modified the requirements while upgrading from Cisco NX-OS Release 6.0(2)U6(2) (CSCvb78728).
January 04, 2018	Added CSCvh18571 to Known Behaviors section.

Contents

Introduction

Release 6.0(2)U6(7) enables you to upgrade to Cisco NX-OS Release 7.0(3)I2(1). However, for Cisco Nexus 3000 vPC topologies, a non-disruptive upgrade from Cisco NX-OS Release 6.0(3)U6(3) to Release 7.0(3)I2(1) is not supported as the upgrade will cause a traffic disruption. When you upgrade a Cisco Nexus 3000 Switch from Cisco NX-OS Release 6.0(3)U6(3) to another Device Under Test (DUT) running Cisco NX-OS Release 7.0(3)I4(x) or later, and if the upgrading DUT is in a vPC configuration, it is likely that one vPC peer is running 7.0(3)I4(x) and while the other is running the 6.0(3)U6(3) version. If both the vPC peers have the command "spanning-tree port type edge default" configured globally, then the mismatch of TLVs between the asymmetric versions, a type-1 inconsistency error gets triggered and the Multichassis EtherChannel Trunk (MCT) link fails.

Note: It is highly recommended that customers with vPC topologies wait for the next maintenance release of 7.0(3)I4(x) to avoid traffic disruption during the upgrade.

System Requirements

This section includes the following topics:

- Memory Requirements
- Hardware Supported
- Twinax Cable Support on Cisco Nexus 3000 Switches
- Cisco QSFP 40-Gbps Bidirectional Short-Reach Transceiver

Memory Requirements

The Cisco NX-OS Release 6.0(2)U6(7) software requires 135 MB of flash memory.

Hardware Supported

Cisco NX-OS Release 6.0(2)U6(7) supports the Cisco Nexus 3000 Series switches. You can find detailed information about supported hardware in the Cisco Nexus 3000 Series Hardware Installation Guide.

Table 2 shows the hardware supported by the Cisco NX-OS Release 6.x software. Table 3 shows the hardware supported by the Cisco NX-OS 5.x releases.

Table 4 shows the transceivers supported by the Cisco NX-OS Release 6.x software. Table 5 shows transceivers supported by the Cisco NX-OS 5.x releases.

Table 2. Hardware Supported by Cisco NX-OS Related 6.x Software.

Hardware	Part Number	Supported Cisco NX-OS Release		
		U1 Series	U2-U3 Series	U4-U6 Series

Hardware	Part Number	Supported Cisco NX-OS Release		
		U1 Series	U2-U3 Series	U4-U6 Series
Cisco Nexus 3172PQ-XL Switch	N3K-C3172PQ-XL	X		
Cisco Nexus 3132Q-XL Switch	N3K-C3132Q-XL	X		
Cisco Nexus 3172TQ-XL Switch	N3K-C3172TQ-XL	X		
Cisco Nexus 3132Q-X switch	N3K-C3132Q-40GX			X
Cisco Nexus 3172TQ switch	N3K-C3172TQ-10GT		X	X
Cisco Nexus 3172PQ switch	N3K-C3172PQ-10GE		X	X
Cisco Nexus 3132Q switch	N3K-C3132Q-40GE		X	X
Cisco Nexus 3016 switch	N3K-C3016Q-40GE	X	X	X
Cisco Nexus 3048 switch	N3K-C3048TP-1GE	X	X	X
Cisco Nexus 3064-TQ switch	N3K-C3064TQ-10GT	X	X	X
Cisco Nexus 3064-X switch	N3K-C3064PQ-10GX	X	X	X
Cisco Nexus 3064-E switch	N3K-C3064PQ-10GE	X	X	X
Cisco Nexus 3064 switch	N3K-C3064PQ	X	X	X
Cisco Nexus 3048 fan module with forward airflow (port-side exhaust)	N3K-C3048-FAN	X	X	X
Cisco Nexus 3048 fan module with reverse airflow (port-side intake)	N3K-C3048-FAN-B	X	X	X
Cisco Nexus 3064-T 500W forward airflow (port-side exhaust) AC power supply	NXA-PAC-500W	X	X	X
Cisco Nexus 3064-T 500W reverse airflow (port-side intake) AC power supply	NXA-PAC-500W-B	X	X	X
Cisco Nexus 3064-X forward airflow (port-side exhaust) AC power supply	N3K-C3064-X-FA-L3	X	X	X
Cisco Nexus 3064-X reversed airflow (port-side intake) AC power supply	N3K-C3064-X-BA-L3	X	X	X
Cisco Nexus 3064-X forward airflow (port-side exhaust) DC power supply	N3K-C3064-X-FD-L3	X	X	X
Cisco Nexus 3064-X forward airflow (port-side intake) DC power supply	N3K-C3064-X-BD-L3	X	X	X

Hardware	Part Number	Supported Cisco NX-OS Release		
		U1 Series	U2-U3 Series	U4-U6 Series
Cisco Nexus 3064 fan module with forward airflow (port-side exhaust); also used in the Cisco Nexus 3016	N3K-C3064-FAN	X	X	X
Cisco Nexus 3064 fan module with reverse airflow (port-side intake); also used in the Cisco Nexus 3016	N3K-C3064-FAN-B	X	X	X
Cisco Nexus 3000 power supply with forward airflow (port-side exhaust)	N2200-PAC-400W	X	X	X
Cisco Nexus 3000 power supply with reverse airflow (port-side intake)	N2200-PAC-400W-B	X	X	X
Cisco Nexus 2000 power supply with forward airflow (port-side exhaust)	N2200-PDC-400W	X	X	X
Cisco Nexus 2000 DC power supply with reverse airflow (port-side intake)	N3K-PDC-350W-B	X	X	X

Table 3. Hardware Supported by Cisco NX-OS Release 5.x Software

Hardware	Part Number	Supported Cisco NX-OS Release						
		U5 Series	U4 Series	U3 Series	U2 (2b – 2d) Releases	U2(2a) Release	U1(2) – U2(2) Releases	U1(1d) Release
Cisco Nexus 3016 switch	N3K-C3016Q-40GE	X	X	X	X	X	—	—
Cisco Nexus 3048 switch	N3K-C3048TP-1GE	X	X	X	X	—	—	—
Cisco Nexus 3064-TQ switch	N3K-C3064TQ-10GT	X[1]	—	—	—	—	—	—
Cisco Nexus 3064-X switch	N3K-C3064P10GX	X	X	X	—	—	—	—

[1] Recommended release for Cisco Nexus 3064-TQ switch is Cisco NX-OS Release 5.0(3)U5(1c) or later releases.

Hardware	Part Number	Supported Cisco NX-OS Release						
		U5 Series	U4 Series	U3 Series	U2 (2b – 2d) Releases	U2(2a) Release	U1(2) – U2(2) Releases	U1(1d) Release
Cisco Nexus 3064-E switch	N3K-C3064PQ-10GE	X	X	X	X	X	X	—
Cisco Nexus 3064 switch	N3K-C3064PQ	X	X	X	X	X	X	X
Cisco Nexus 3048 fan module with forward airflow (port-side exhaust)	N3K-C3048-FAN	X	X	X	X	—	—	—
Cisco Nexus 3048 fan module with reverse airflow (port-side intake)	N3K-C3048-FAN-B	X	X	X	X	—	—	—
Nexus 3064-T 500W forward airflow (port side exhaust) AC power supply	NXA-PAC-500W	X	X	—	—	—	—	—
Nexus 3064-T 500 W reverse airflow (port side intake) AC power supply	NXA-PAC-500W-B	X	X	—	—	—	—	—
Cisco Nexus 3064-X forward airflow (port-side exhaust) AC power supply	N3K-C3064-X-FA-L3	X	X	X	—	—	—	—

Hardware	Part Number	Supported Cisco NX-OS Release						
		U5 Series	U4 Series	U3 Series	U2 (2b – 2d) Releases	U2(2a) Release	U1(2) – U2(2) Releases	U1(1d) Release
Cisco Nexus 3064-X reversed airflow (port-side intake) AC power supply	N3K-C3064-X-BA-L3	X	X	X	—	—	—	—
Cisco Nexus 3064-X forward airflow (port-side exhaust) DC power supply	N3K-C3064-X-FD-L3	X	X	X	—	—	—	—
Cisco Nexus 3064-X forward airflow (port-side intake) DC power supply	N3K-C3064-X-BD-L3	X	X	X	—	—	—	—
Cisco Nexus 3064 fan module with forward airflow (port-side exhaust); also used in the Cisco Nexus 3016	N3K-C3064-FAN	X	X	X	X	X	X	X
Cisco Nexus 3064 fan module with reverse airflow (port-side intake); also used in the Cisco Nexus 3016	N3K-C3064-FAN-B	X	X	X	X	X	X	X

Hardware	Part Number	Supported Cisco NX-OS Release						
		U5 Series	U4 Series	U3 Series	U2 (2b – 2d) Releases	U2(2a) Release	U1(2) – U2(2) Releases	U1(1d) Release
Cisco Nexus 3000 power supply with forward airflow (port-side exhaust)	N2200-PAC-400W	X	X	X	X	X	X	X
Cisco Nexus 3000 power supply with reverse airflow (port-side intake)	N2200-PAC-400W-B	X	X	X	X	X	X	X
Cisco Nexus 2000 power supply with forward airflow (port-side exhaust)	N2200-PDC-400W	X	X	X	X	X	X	X
Cisco Nexus 2000 DC power supply with reverse airflow (port-side intake)	N3K-PDC-350W-B	X	X	X	X	X	X	X

Table 4. Transceivers Supported by Cisco NX-OS Release 6.x Software.

Transceivers[2]	Part Number	Supported Cisco NX-OS Release		
		U1 Series	U2 Series	U3-U6 Series
QSFP				
40GBASE-LR4 QSFP40G transceiver module (SMF)	QSFP-40G-LR4			X
40GBASE-CR4 QSFP+ direct-attach copper cable, 7 meters active	QSFP-H40G-ACU7M			X
40GBASE-CR4 QSFP+ direct-attach copper cable, 8 meters active	QSFP-H40G-ACU8M			X
40GBASE-CR4 QSFP+ direct-attach copper cable, 9 meters active	QSFP-H40G-ACU9M			X
40GBASE-CR4 QSFP+ direct-attach copper cable, 10 m active	QSFP-H40G-ACU10M			X
40G QSFP direct-attach active optical cable, 15 m	QSFP-H40G-AOC15M			X
QSFP to 4 x SFP 10Gbps active optical cable 15 m	QSFP-4X10G-AOC15M			X
QSFP 40G Bidirectional short-reach transceiver	QSFP-40G-SR-BD	X	X	X
QSFP 40G active optical cable 1 m	QSFP-H40G-AOC1M	X	X	X
QSFP 40G active optical cable 2 m	QSFP-H40G-AOC2M	X	X	X
QSFP 40G active optical cable 3 m	QSFP-H40G-AOC3M	X	X	X
QSFP 40G active optical cable 5 m	QSFP-H40G-AOC5M	X	X	X
QSFP 40G active optical cable 7 m	QSFP-H40G-AOC7M	X	X	X
QSFP 40G active optical cable 10 m	QSFP-H40G-AOC10M	X	X	X
QSFP to 4 x SFP 10Gbps active optical cable 1 m	QSFP-4X10G-AOC1M	X	X	X
QSFP to 4 x SFP 10Gbps active optical cable 2 m	QSFP-4X10G-AOC2M	X	X	X
QSFP to 4 x SFP 10Gbps active optical cable 3 m	QSFP-4X10G-AOC3M	X	X	X
QSFP to 4 x SFP 10Gbps active optical cable 5 m	QSFP-4X10G-AOC5M	X	X	X
QSFP to 4 x SFP 10Gbps active optical cable 7 m	QSFP-4X10G-AOC7M	X	X	X
QSFP to 4 x SFP 10Gbps active optical cable 10 m	QSFP-4X10G-AOC10M	X	X	X
Active copper splitter cable 7 m	QSFP-4x10G-AC7M[3]	X	X	X
Active copper splitter cable 10 m	QSFP-4x10G-AC10M[2]	X	X	X
Active copper QSFP transceiver module 7 m	QSFP-H40G-ACU7M[2]	X	X	X
Active copper QSFP transceiver module 10 m	QSFP-H40G-ACU10M[2]	X	X	X

[2] OIR is supported for all optical modules and transceivers in Cisco NX-OS Release 6.02 and later releases.
[3] Supported on the Cisco Nexus 3016, Cisco Nexus 3064-X, Cisco Nexus 3064-TQ, Cisco Nexus 3064, Cisco Nexus 3064-E, and all Cisco Nexus 3100 Series switches.

Transceivers[2]	Part Number	Supported Cisco NX-OS Release		
		U1 Series	U2 Series	U3-U6 Series
40GBASE-CSR4 QSFP transceiver module with multifiber push-on (MPO) connector 300 m	QSFP-40G-CSR4[2]	X	X	X
40GBASE-CSR4 QSFP transceiver module with MPO connector 300 m (using fiber splitter cables)	QSFP-40G-CSR4[2]	X	X	X
40GBASE-SR4 QSFP transceiver module with MPO connector 100 m	QSFP-40G-SR4[2]	X	X	X
40GBASE-SR4 QSFP transceiver module with MPO connector 100 m (using fiber splitter cables)	QSFP-40G-SR4[2]	X	X	X
40GBASE-LR4 QSFP transceiver module with LC connector 10 km (using single mode fiber)	QSFP-40GE-LR4	X	X	X
QSFP to SFP/SFP+ adapter	CVR-QSFP-SFP10G	X	X	X
40GBASE-CR4 passive copper cable, 1 m	QSFP-H40G-CU1M	X	X	X
40GBASE-CR4 passive copper cable, 3 m	QSFP-H40G-CU3M	X	X	X
40GBASE-CR4 passive copper cable, 5 m	QSFP-H40G-CU5M	X	X	X
QSFP to 4xSFP10G passive copper splitter cable, 1 m	QSFP-4SFP10G-CU1M	X	X	X
QSFP to 4xSFP10G passive copper splitter cable, 3 m	QSFP-4SFP10G-CU3M	X	X	X
QSFP to 4xSFP10G passive copper splitter cable, 5 m	QSFP-4SFP10G-CU5M	X	X	X
Revision 2 copper splitter cables 3 m	QSFP-4SFP10G-CU3 (Rev. 2)	X	X	X
Revision 2 copper splitter cables 5 m	QSFP-4SFP10G-CU5 (Rev. 2)	X	X	X
10-Gigabit				
10 db attenuator	FA-920-073-12310			X
10GBASE-ZR SFP+ module (single-mode fiber [SMF])	SFP-10G-ZR			X
Cisco QSFP to SFP/SFP+ Adapter (QSA) module	CVR-QSFP-SFP10G			X
Cisco QSFP to SFP/SFP+ Adapter (QSA) module with 10GBASE-DWDM	QSA w/ DWDM			X
10GBASE-DWDM 1558.98 nm SFP+ (100-GHz ITU grid)	DWDM-SFP10G-58.98			X
10GBASE-DWDM 1539.77 nm SFP+ (100-GHz ITU grid)	DWDM-SFP10G-39.77			X
10GBASE-DWDM 1561.41 nm SFP+ (100-GHz ITU grid)	DWDM-SFP10G-61.41			X
10GBASE-DWDM 1542.94 nm SFP+ (100-GHz ITU grid)	DWDM-SFP10G-42.94			X
10GBASE-DWDM 1553.33 nm SFP+ (100-GHz ITU grid)	DWDM-SFP10G-53.33			X
10GBASE-DWDM 1537.40 nm SFP+ (100-GHz ITU grid)	DWDM-SFP10G-37.40			X

Transceivers[2]	Part Number	Supported Cisco NX-OS Release		
		U1 Series	U2 Series	U3-U6 Series
10GBASE-DWDM 1542.14 nm SFP+ (100-GHz ITU grid)	DWDM-SFP10G-42.14			X
10GBASE-DWDM 1556.55 nm SFP+ (100-GHz ITU grid)	DWDM-SFP10G-56.55			X
10GBASE-DWDM 1550.92 nm SFP+ (100-GHz ITU grid)	DWDM-SFP10G-50.92			X
10GBASE-DWDM 1531.12 nm SFP+ (100-GHz ITU grid)	DWDM-SFP10G-31.12			X
10GBASE-DWDM long-range transceiver module 80 km with single mode duplex fiber	DWDM-SFP10G-C			X
10GBASE-DWDM long-range transceiver module 80 km with single mode duplex fiber	DWDM-SFP10G	X	X	X
10GBASE-SR SFP+ module (multimode fiber [MMF])	SFP-10G-SR	X	X	X
10GBASE-LR SFP+ module (single-mode fiber [SMF])	SFP-10G-LR	X	X	X
10GBASE-ER SFP+ module (single-mode fiber [SMF])	SFP-10G-ER	X	X	X
10GBASE-ZR SFP+ module (single-mode fiber [SMF])[4]	SFP-10G-ZR[3]	X	X	X
10GBASE-DWDM SFP+ module (single-mode fiber [SMF])[3]	10-2767-01[3]	X	X	X
Active Twinax cable assembly, 7 m	SFP-H10GB-ACU7M	X	X	X
Active Twinax cable assembly, 10 m	SFP-H10GB-ACU10M	X	X	X
10GBASE-CU SFP+ cable 1 m (Twinax cable)	SFP-H10GB-CU1M	X	X	X
10GBASE-CU SFP+ cable 1.5 m (Twinax cable)	SFP-H10GB-CU1-5M	X	X	X
10GBASE-CU SFP+ cable 2 m (Twinax cable)[4]	SFP-H10GB-CU2M[5]	X	X	X
10GBASE-CU SFP+ cable 3 m (Twinax cable)	SFP-H10GB-CU3M	X	X	X
10GBASE-CU SFP+ cable 5 m (Twinax cable)	SFP-H10GB-CU5M	X	X	X
10GBASE-CU SFP+ cable 2.5 m (Twinax cable)[4]	SFP-H10GB-CU2-5M[4]	X	X	X
Active optical cable 1 m	SFP-10G-AOC1M[5]	X	X	X
Active optical cable 2 m	SFP-10G-AOC2M	X	X	X
Active optical cable 3 m	SFP-10G-AOC3M[5]	X	X	X
Active optical cable 5 m	SFP-10G-AOC5M[5]	X	X	X
Active optical cable 7 m	SFP-10G-AOC7M[5]	X	X	X
Active optical cable 10 m	SFP-10G-AOC10M	X	X	X
1-Gigabit Ethernet				

[4] Supported on the Cisco Nexus 3064-E and Cisco Nexus 3064-X switches.
[5] Supported on the Cisco Nexus 3048, Cisco Nexus 3064-X, Cisco Nexus 3064, and Cisco Nexus 3064-E switches.

Transceivers[2]	Part Number	Supported Cisco NX-OS Release		
		U1 Series	U2 Series	U3-U6 Series
Gigabit Ethernet SFP, LC connector SX transceiver (MMF)	GLC-SX-MMD **Note:** GLC-SX-MMD is supported on all Cisco Nexus 3000 Series Switches except for the Cisco Nexus 3064-T. Please refer to the comparability matrix for all the supported platforms.			X
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF)	GLC-LH-SMD			X
Cisco QSFP to SFP/SFP+ Adapter (QSA) module with GLC-T	QSA w/ GLC-T			X
1000BASE-T SFP	GLC-TE			X
Cisco QSFP to SFP/SFP+ Adapter (QSA) module with GLC-TE	QSA w/ GLC-TE			X
Cisco QSFP to SFP/SFP+ Adapter (QSA) module with SFP-GE-T	QSA w/SFP-GE-T			X
1000Base-BX fiber transceiver	GLC-BX-D[5]	X	X	X
1000Base-BX fiber transceiver	GLC-BX-U[5]	X	X	X
1000BASE-EX fiber transceiver module, SMF	GLC-EX-SMD	X	X	X
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF)	GLC-LH-SM[5]	X	X	X
1000BASE-LX/LH SFP transceiver module for MMF and SMF	GLC-LH-SMD[5]	X	X	X
Gigabit Ethernet SFP, LC connector SX transceiver (MMF)	GLC-SX-MM[4]	X	X	X
Gigabit Ethernet SFP, LC connector SX transceiver (MMF)	GLC-SX-MMD **Note:** GLC-SX-MMD is supported on all Cisco Nexus 3000 Series Switches except for the Cisco Nexus 3064-T. Please refer to the comparability matrix for all the supported platforms.	X	X	X
1000BASE-T SFP[6]	GLC-T[5]	X	X	X
1000BASE-ZX fiber transceiver module, SMF, 1550 nm	GLC-ZX-SMD	X	X	X
1000BASE-T SFP transceiver module with extended operating temperature range	SFP-GE-T[5]	X	X	X

[6] Supported on the Cisco Nexus 3048, Cisco Nexus 3064-E, and Cisco Nexus 3064-X switches. Not supported on Cisco Nexus 3132Q-X.

Transceivers[2]	Part Number	Supported Cisco NX-OS Release		
		U1 Series	U2 Series	U3-U6 Series
100-Mbps Ethernet				
100BASE-FX SFP module for Gigabit Ethernet ports GLC-GE-100FX[7]	10-2019-02[7]			100BASE-FX SFP module for Gigabit Ethernet ports GLC-GE-100FX

Note: The Cisco Nexus 3000 supports 1,000 and 10,000 speeds while using SFP+ with Cisco QSA [CVR-QSFP-SFP10G] (and a maximum of 6 QSAs). The 100 speed is not supported on the SFP+ along with QSA, but using any speed 100 is supported on the SFP+.

Table 5 Transceivers Supported by Cisco NX-OS Release 5.x Software.

Transceivers	Part Number	U5 Series	U4(1) Release	U3 Series	U1 – U2 Series
Active copper splitter cable 7 m	QSFP-4x10G-AC7M[8]	X	—	—	—
Active copper splitter cable 10 m	QSFP-4x10G-AC10M[8]	X	—	—	—
Active copper QSFP transceiver module 7 m	QSFP-H40G-ACU7M[8]	X	—	—	—
Active copper QSFP transceiver module 10 m	QSFP-H40G-ACU10M[8]	X	—	—	—
40GBASE-CSR4 QSFP transceiver module with MPO connector 300 m	QSFP-40G-CSR4[8]	X	X	—	—
40GBASE-CSR4 QSFP transceiver module with MPO connector 300 m (using fiber splitter cables)	QSFP-40G-CSR4[8]	X	X	—	—

[7] Supported on the Cisco Nexus 3064, Cisco Nexus 3064-E, and Cisco Nexus 3064-X switches. For the GLC-GE-100FX, only part number 10-2019-02 is supported.
[8] Supported on the Cisco Nexus 3016, Cisco Nexus 3064-X, Cisco Nexus 3064-TQ, Cisco Nexus 3064, and Cisco Nexus 3064-E switches.

Transceivers	Part Number	U5 Series	U4(1) Release	U3 Series	U1 – U2 Series
40GBASE-SR4 QSFP transceiver module with MPO connector 100 m	QSFP-40G-SR4[8]	X	X	X	X
40GBASE-SR4 QSFP transceiver module with MPO connector 100 m (using fiber splitter cables)	QSFP-40G-SR4[8]	X	X	X	X
40GBASE-CR4 passive copper cable, 1 m	QSFP-H40G-CU1M	X	X	X	X
40GBASE-CR4 passive copper cable, 3 m	QSFP-H40G-CU3M	X	X	X	X
40GBASE-CR4 passive copper cable, 3 m	QSFP-H40G-CU3M	X	X	X	X
40GBASE-CR4 passive copper cable, 5 m	QSFP-H40G-CU5M	X	X	X	X
QSFP to 4xSFP10G passive copper splitter cable, 1 m	CU5M CU1M	X	X	X	X
QSFP to 4xSFP10G passive copper splitter cable, 3 m	QSFP-4SFP10G-CU3M	X	X	X	X
QSFP to 4xSFP10G passive copper splitter cable, 5 m	QSFP-4SFP10G-CU5M	X	X	X	X
Revision 2 copper splitter cables 3 m	QSFP-4SFP10G-CU3 (Rev. 2)	X	—	—	—
Revision 2 copper splitter cables 5 m	QSFP-4SFP10G-CU5 (Rev. 2)	X	—	—	—
10-Gigabit					
10GBASE-SR SFP+ module (multimode fiber [MMF])	SFP-10G-SR	X	X	X	X

Transceivers	Part Number	U5 Series	U4(1) Release	U3 Series	U1 – U2 Series
10GBASE-LR SFP+ module (single-mode fiber [SMF])	SFP-10G-LR	X	X	X	X
10GBASE-ER SFP+ module (single-mode fiber [SMF])	SFP-10G-ER	X	X	X	X
10GBASE-ZR SFP+ module (single-mode fiber [SMF])[9]	SFP-10G-ZR[9]	X	X	X	—
10GBASE-DWDM SFP+ module (single-mode fiber [SMF]) [9]	10-2767-01[9]	X	X	X	—
10GBASE-CU SFP+ cable 1 m (Twinax cable)	SFP-H10GB-CU1M	X	X	X	X
10GBASE-CU SFP+ cable 3 m (Twinax cable)	SFP-H10GB-CU3M	X	X	X	X
10GBASE-CU SFP+ cable 5 m (Twinax cable)	SFP-H10GB-CU5M	X	X	X	X
10GBASE-CU SFP+ cable 2 m (Twinax cable)3[10]	SFP-H10GB-CU2M[10]	X	X	—	—
10GBASE-CU SFP+ cable 2.5 m (Twinax cable) [10]	SFP-H10GB-CU2-5M3[10]	X	X	—	—
Active optical cable 1 m	SFP-10G-AOC1M[11]	X	—	—	—
Active optical cable 3 m	SFP-10G-AOC3M[11]	X	—	—	—
Active optical cable 5 m	SFP-10G-AOC5M[11]	X	—	—	—

[9] Supported on the Cisco Nexus 3064-E and Cisco Nexus 3064-X switches.
[10] Supported on the Cisco Nexus 3048, Cisco Nexus 3064-X, Cisco Nexus 3064, and Cisco Nexus 3064-E switches.
[11] Supported on the Cisco Nexus 3048, Cisco Nexus 3064-E, and Cisco Nexus 3064-X switches.

Transceivers	Part Number	U5 Series	U4(1) Release	U3 Series	U1 – U2 Series
Active optical cable 7 m	SFP-10G-AOC7M[11]	X	—	—	—
1-Gigabit Ethernet					
1000BASE-T SFP[11]	GLC-T[11]	X	X	X	X
Gigabit Ethernet SFP, LC connector SX transceiver (MMF)	GLC-SX-MM[10]	X	X	X	X
Gigabit Ethernet SFP, LC connector SX transceiver (MMF)	GLC-SX-MMD **Note:** GLC-SX-MMD is supported on all Cisco Nexus 3000 Series Switches except for the Cisco Nexus 3064-T. Please refer to the comparability matrix for all the supported platforms.	X	X	—	—
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF)	GLC-LH-SM[11]	X	X	X	X
1000BASE-LX/LH SFP transceiver module for MMF and SMF	GLC-LH-SMD[11]	X	—	—	—
1000Base-BX fiber transceiver	GLC-BX-U[11]	X	—	—	—
1000Base-BX fiber transceiver	GLC-BX-D[11]	X	—	—	—
1000BASE-T SFP transceiver module with extended operating temperature range	SFP-GE-T[11]	X	—	—	—
100-Mbps Ethernet					

Transceivers	Part Number	U5 Series	U4(1) Release	U3 Series	U1 – U2 Series
100BASE-FX SFP module for Gigabit Ethernet ports GLC-GE-100FX[12]	10-2019-02[12] GLC-GE-100FX	X	X	X	X

Twinax Cable Support on Cisco Nexus 3000 Switches

Starting with Cisco Release NX-OS 5.0(3)U1(1), the following algorithm is used to detect copper SFP+ twinax, QSFP+ twinax, and QSFP+ splitter cables on Cisco Nexus 3000 Series switches.

If the attached interconnect (transceiver) is a copper SFP+ twinax or QSFP+ twinax cable:

- Verify the transceiver SPROM to match the Cisco magic code.
- If the check succeeds, bring up the interface. Otherwise, print the following warning message appears stating that a non-Cisco transceiver is attached and that you should try to bring up the port.

  2009 Oct 9 01:46:42 switch %ETHPORT-3-IF_NON-CISCO_TRANSCEIVER: Non-Cisco transceiver on interface Ethernet1/18 is detected.

  If the attached transceiver is a QSFP+ splitter cable, then no special check is performed. The Cisco NX-OS software tries to bring up the port.

  The following disclaimer applies to non-Cisco manufactured and non-Cisco certified QSFP copper splitter cables:

  If a customer has a valid support contract for Cisco Nexus switches, Cisco TAC will support twinax cables that are a part of the compatibility matrix for the respective switches. However, if the twinax cables are not purchased through Cisco, a customer cannot return these cables through an RMA to Cisco for replacement.

  If a twinax cable that is not part of the compatibility matrix is connected into a system, Cisco TAC will still debug the problem, provided the customer has a valid support contract on the switches. However TAC may ask the customer to replace the cables with Cisco qualified cables if there is a situation that points to the cables possibly being faulty or direct the customer to the cable provider for support. Cisco TAC cannot issue an RMA against uncertified cables for replacement.

Cisco QSFP 40-Gbps Bidirectional Short-Reach Transceiver

The Cisco QSFP 40-Gbps Bidirectional (BiDi) transceiver is a short-reach pluggable optical transceiver with a duplex LC connector for 40-GbE short-reach data communications and interconnect applications by using multimode fiber (MMF). The Cisco QSFP 40-Gbps BiDi transceiver offers a solution that uses existing duplex MMF infrastructure for 40-GbE connectivity. With the Cisco QSFP 40-Gbps BiDi transceiver, customers can upgrade their network from 10-GbE to 40-GbE without incurring any fiber infrastructure upgrade cost. The Cisco QSFP 40-Gbps BiDi transceiver can enable 40-GbE connectivity in a range of up to 100 meters over OM3 fiber, which meets most data center reach requirements. It complies with the Multiple Source Agreement (MSA) QSFP specification and enables customers to use it on all Cisco QSFP 40-Gbps platforms and achieve high density in a 40-GbE network. It can be used in data centers, high-performance computing (HPC) networks, enterprise and distribution layers, and service provider transport applications.

[12] Supported on the Cisco Nexus 3064, Cisco Nexus 3064-E, and Cisco Nexus 3064-X switches. For the GLC-GE-100FX, only part number 10-2019-02 is supported.

New and Changed Information

This section lists the new and changed features in 6.0(2)U6(7) and includes the following topics:

- New Software Features
- New Hardware Features

New Software Features

This release contains the following new software features:

- **Non-ECN capable behavior enhancement**

  This enhancement allows non-ECN traffic to pass through at maximum threshold and enables the usage of peak cells that ECN traffic is allocated with before being tail dropped.

- **Reload-tracker**

  This enhancement enables the Cisco Nexus device to generate syslog messages every hour by default if a reload is required due to changes in configuration. The syslog message generation can be set from 0 to 24 (in hours) where 0 disables the syslog message generation and 1 is the default.

- **Priortize PACL over SUP TCAM for DHCP**

  This enhancement enables priority for PACL over SUP TCAM for DHCP. During this configuration, when any action on the PACL region has a conflicting action in the SUP region, PACL entry takes priority over the SUP entry.

- **Secure Login enhancements**

  The Secure Login enhancements allow users to enhance the security of a router by configuring options to automatically block further login attempts during a possible denial-of-service (DoS) attack.

New Hardware Features

This release does not contain any new hardware features.

Caveats

The open and resolved bugs and the known behaviors for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Note: You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. if you do not have one, you can register for an account.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

- Resolved Bugs in this Release
- Open Bugs for this Release
- Known Behaviors for this Release

Resolved Bugs in this Release

Table 7 lists descriptions of resolved bugs in Cisco NX-OS Release 6.0(2)U6(7). You can use the record ID to search the Cisco Bug Search Tool for details about the bug.

Table 6 Cisco NX-OS Release 6.0(2)U6(7) —Resolved Bugs

Record Number	Resolved Bug Headline
CSCux19326	The Secure Shell (SSH) disconnects while using Python twisted framework to initiate SSH.

Record Number	Resolved Bug Headline
CSCuy47744	For Nexus devices running in ALPM Mode and IPv6 is enabled, incorrect parity error handling causes SDK routing programming failure.
CSCuy63666	Cisco Nexus 3000 series switches accept PBR TCAM region carving with no available TCAM space.
CSCuz15584	vPC process crash on SVI configuration and bring up.
CSCuz72951	BGP IPv6 neighbor is configured with conditional default originate based on the presence of an IPv6 route in the RIB.
CSCuy87703	Cisco Nexus 3172 switch performs a Silent Reload while deleting the interface.
CSCuz00736	The NETCONF <get> Request for **show boot** command displays no output.
CSCuz36820	On a Cisco Nexus 3000 series switch with four individual fans, when one of the fans is removed and reinserted, the pfma process will get cored during that time of module insertion.
CSCuz40585	When a DSCP value is set to 8 for ERSPAN packets, the mirrored packet is marked to its equivalent TOS value.
CSCuz61655	The bcm_usd service crashes unexpectedly due to HA Policy of Reset.
CSCuz76071	TACACS authentication fails on a Cisco Nexus 3000 Series device with an error displayed in the TACACS debugs.
CSCva03834	Intermittent error messages can be seen either for Power Supply 1 or Power Supply 2. Recovery message usually appears after 30 seconds-2 minutes of error message display.
CSCva15296	Priortize PACL over SUP TCAM for DHCP.
CSCva28734	On a Cisco Nexus 3000 series switch with Trident+ ASIC, setting "hardware profile tcam region ifacl 0" has no effect.
CSCva30223	Changing default http or https ports on NXAPI gives an error.
CSCva51908	On Cisco Nexus 3000 series switches, vPC loop prevention gets broken after peer-link member ports flap.
CSCva01669	After enabling or disabling the SSH, bind errors can be seen which will break the SSH functionality.
CSCuy88327	On Cisco Nexus 3000 series switches, CLI or Syslog or SNMP support is desired for features pending reload.
CSCuq04309	Cisco Nexus SNMPd process crashes after MTS queue is full.
CSCuu04259	Changing logging level not nvgened for ipfib.
CSCuu18724	MTS memory leak causes SNMPd process to crash multiple times.
CSCuv59159	Using "no lldp tlv-select dcbxp" on interfaces that are operational ON for PFC would only result in one side going to operational OFF while the other side stays in operational ON.
CSCux02038	On Cisco NX-OS software, non-RFC5952 compliant formatting of IPv6 addresses is observed.
CSCum35502	Users can log into a Cisco Nexus device and execute disallowed commands using remote shell facility.
CSCum47367	A vulnerability in Cisco TACACS command authorization code of Cisco NX-OS could allow an authenticated, local attacker to execute certain commands without being authorized by the Cisco TACACS server.

Open Bugs for this Release

Table 7 lists descriptions of open bugs in Cisco NX-OS Release 6.0(2)U6(7). You can use the record ID to search the Cisco Bug Search Tool for details about the bug.

Table 7 Cisco NX-OS Release 6.0(2)U6(7) —Open Bugs

Record Number	Open Bug Headline
CSCuq01107	When a vPC PO is shutdown, static MAC addresses pointing to it are flushed and traffic is flooded..
CSCur14762	After running **no shut** on a vPC peer-link, some packet duplication occurs for all the sourced multicast groups.
CSCur76020	VRRPv3 tracking support to be added.
CSCur96529	Error message failed to allocate shared memory for per-protocol nexthop (nh) type.
CSCus32402	Multihop Recursive routes may not be properly installed with MPLS static.
CSCut82376	An HW Tunnel Resource leak occurs while changing and reverting the tunnel source/destination.

Known Behaviors for this Release

Table 8 lists descriptions of known behaviors in Cisco NX-OS Release 6.0(2)U6(7). You can use the record ID to search the Cisco Bug Search Tool for details about the bug.

Table 8 Cisco NX-OS Release 6.0(2)U6(7) —Known Behaviors

Record Number	Open Bug Headline
CSCur60142	[no] **shutdown** is always displayed under **show running interface**.
CSCur78515	Port channel members go down after downgrading.
CSCus31911	After entering the **copy ABC running** command when the switch has a default/l2 CoPP profile and the file used in the command (ABC) has an L3 CoPP profile config, the PPS credit limit exceeded error is thrown for the copp-s-routingProto1 class-map.
CSCus98460	When the **neighbor-down fib-accelerate** command is used with a large number of unique BGP next hops, a build up of MTS messages is seen
CSCut34195	Repave with fastboot is supported only from 6.0(2)U6(1) and later.
CSCut49938	Ping fails with higher ping packet-size.
CSCuy08068	The Cisco Nexus 3000 Series switches may see an unexpected reload due to a hap reset with AFM service.
CSCvh18571	When you execute the command ***show platform fwm info stm-stats clear*** on Cisco Nexus 3000 Switches in a vPC environment, the vPC peer cannot learn MAC address from peer links or from local vPC legs. As a result, the MAC address synchronization over CFS fails which either results in missing MAC address entries or MAC address age timer expiry. Sometimes, the MAC address does not even show up in ***show mac address-table*** command because of this issue. You can work around this issue by upgrading to Cisco NX-OS Release 7.0(x) or by reloading the switch. The ***show platform fwm info stm-stats clear*** command is not recommended to debug general traffic unless instructed.

Large core files are split into 3 or more files. For example:

- 1405964207_0x101_fwm_log.3679.tar.gzaa
- 1405964207_0x101_fwm_log.3679.tar.gzab

- 1405964207_0x101_fwm_log.3679.tar.gzac

To decode the multiple core files, first club the files to a single file:

$ cat 1405964207_0x101_fwm_log.3679.tar.gz* > 1405964207_0x101_fwm_log.3679.tar.gz

Upgrade and Downgrade Guidelines

- Upgrading Cisco NX-OS Software by changing the boot-variables and performing a reload is not supported. This may result in unexpected behavior.
- Ensure that you use the **install all** command to upgrade the switch software from one Cisco NX-OS release to another.
- Cisco Nexus 3000 Series switches that use software versions older than Cisco NX-OS Release 5.0(3)U5(1) need to be updated to Cisco NX-OS Release 5.0(3)U5(1) before they are upgraded to Cisco NX-OS Release 6.0(2).
- Cisco NX-OS Release 5.0(3)U3(1) does not support a software upgrade from Cisco NX-OS Release 5.0(3)U2(2c). If you want to upgrade through this path, see CSCty75328 for details about how to work around this issue.

Note: It is recommended that you upgrade to Cisco NX-OS Release 6.0(2)U6(7) by using Cisco NX-OS install procedures.

- In Cisco NX-OS Release 5.0(3)U3(1), support for IPv6 has been added in Control Plane Policing (CoPP). To enable redirection of IPv6 control packets to the CPU, you must configure IPv6 CoPP on the system. Entering the **write erase** command on a device that runs Release 5.0(3)U3(1) automatically applies CoPP on the device and ensures that all IPv4 and IPv6-related CoPP configuration is set up correctly.
- If you upgrade from a Cisco NX-OS release that does not support the CoPP feature to a release that does support the CoPP feature, you must run the setup utility after the upgrade to enable CoPP on the device.
- If you upgrade from Cisco NX-OS Release 5.0(3)U2(2), which supports the CoPP feature, to Cisco NX-OS Release 5.0(3)U3(1), which adds CoPP classes for IPv6 support, you must run the setup script to enable the IPv6 CoPP feature on the device.
- In Cisco NX-OS Release 6.0(2)U2(2), the default interface name in LLDP MIB is in short form. To make it long form, you must set **lldp portid-subtype** to 1. In Cisco NX-OS Release 6.0(2)U2(3), this behavior was reversed. The default interface name in LLDP MIB is now in long form. To make it short form, you must set **lldp portid-subtype** to 0.
- If you have set **lldp port-subtype** to 1 and you are upgrading to Cisco NX-OS Release 6.0(2)U2(4), ensure that you set **lldp port-subtype** to 0.
- For the N3K-C3048TP-1GE-SUP platform, if you are using software versions older than Cisco NX-OS Release 5.0(3)U5(1), upgrade to Cisco NX-OS Release 5.0(3)U5(1) first, then upgrade to Cisco NX-OS Release 6.0(2)U6(2a), and finally upgrade to 6.0(2)U6(7) or a latest release.
- A Cisco Nexus 3048 switch may not boot up or become unusable after an upgrade to Cisco NX-OS Release 6.0(2)U6(7).
  Note: A Cisco Nexus 3048 switch requires an additional step when you upgrade from a software version older than Cisco NX-OS 6.0(2)U6(2), otherwise the switch can fail to boot. You must first upgrade the switch to Cisco NX-OS Release 6.0(2)U6(2a) and then upgrade to Cisco NX-OS Release 6.0(2)U6(7) or a later release. For more information, see: CSCvb78728.

Limitations

The following are the known limitations for Cisco NX-OS Release 6.0(2)U6(7):

- While installing the NXAPI https certificate that is present in the device, the following error message can appear if the user does not have the permission to install this certificate (See CSCup72219):

  Certificate file read error.Please re-check permissions.

- After configuring the NXAPI feature, the default http port (port 80) is still in the listening state even after we run the **no nxapi http** command. This results in the sandbox becoming accessible. Although the sandbox becomes accessible, HTTP requests from the sandbox to the device do not go through. Thus, the functionality is not affected. (See CSCup77051).
- Chunking is enabled while displaying XML output for any CLI, and html tags (& lt; and & gt;) are displayed instead of < and > both on the sandbox and while running the Python script (See CSCup84801).

  This is expected behavior. Each chunk should be in XML format for you to parse it and extract everything inside the <body> tag. This is done so that it can be later concatenated with similar output from all the chunks of the CLI XML output. After all the chunks are concatenated to get the complete XML output for the CLI, this complete XML output can be parsed for any parameter.

  The following workaround is recommended to address this issue:

  - Concatenate the <body> outputs from each chunk
  - Replace all the html tags (& lt; and & gt;) with < and >
  - Parse for any XML tag needed
- If you use the **write erase** command, you cannot view the output for the **show startup** *feature* command. To view the startup configuration, you must then use the **show startup-config** command. This limitation will remain until you run the **copy running-config startup-config** command. After that, the **show startup-config** feature command will display the feature-only configuration output as expected (See CSCuq15638).
- A Python traceback is seen while running the **show xml** command by using the Python shell. The exception type is httplib.IncompleteRead. This happens when you use Python scripts to leverage the NXAPI for retrieving switch data through XML or JSON. You should handle the exceptions in your Python scripts (See CSCuq19257).
- While upgrading to a new release, when you create a checkpoint without running the **setup** script, the checkpoint file does not contain the **copp-s-mpls** class. After you run the **write erase** command and reload the switch, the **copp-s-mpls** class is created when the default configuration is applied. When a rollback is done to this checkpoint file, it detects a change in the CoPP policy and tries to delete all class-maps. Because you cannot delete static class-maps, this operation fails and, in turn, the rollback also fails.

  This can also happen if you create a checkpoint, then create a new user-defined class and insert the new class before any other existing class (See CSCup56505).

  The following workarounds are recommended to address this issue:

  - Run setup after upgrading to a new release.
  - Always insert the new classes at the end before a rollback.
- After an interface is shut down and restarted, and after the device is reloaded, the following are observed (See CSCuh69660):

  - Any trunk port in the VLAN is treated as an IGMP snooping Active Port.
  - Access ports in the VLAN are not treated as IGMP snooping Active ports.
  - The FWM multicast flood-list for VLAN contains all trunk ports and mrouter ports.

  The following workarounds are recommended to address this issue:

  - Use the **show ip igmp snooping vlan** *x* command to see the Active Ports.
  - Use the **show platform fwm info vlan** *x* command to see the flood-list.
- When both the **ip icmp-errors source** and **ip source** *intf* **icmp error** commands are configured, then the command that is configured last takes effect.

Thereafter, if the last configured command is removed, the switch does not get configured with the command that was configured first.

- Users who upgrade to 6.0(2)U6(7) need to run the set up script if they want to enable the MPLS static or the VRRPv3 feature.
- Link Level Flow Control (LLFC) is not supported on Cisco Nexus 3000 series and Cisco Nexus 3100 series switches.

MIB Support

The Cisco Management Information Base (MIB) list includes Cisco proprietary MIBs and many other Internet Engineering Task Force (IETF) standard MIBs. These standard MIBs are defined in Requests for Comments (RFCs). To find specific MIB information, you must examine the Cisco proprietary MIB structure and related IETF-standard MIBs supported by the Cisco Nexus 3000 Series switch. The MIB Support List is available at the following FTP sites:

ftp://ftp.cisco.com/pub/mibs/supportlists/nexus3000/Nexus3000MIBSupportList.html

Related Documentation

Documentation for the Cisco Nexus 3000 Series Switch is available at the following URL:

http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus3k-docfeedback@cisco.com. We appreciate your feedback.

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.