Cisco Nexus 3000 Series NX-OS Release Notes, Release 9.3(2)

This document describes the features, caveats, and limitations of Cisco NX-OS Release 9.3(2) software for use on Cisco Nexus 3000, 3100, 3200, 3400, 3500, 3600 switches. Use this document in combination with documents listed in the *Related Documentation* section.

Table 1 shows the online change history for this document.

Table 1 Online History Change

Date	Description
October 19, 2020	Updated the Upgrading Cisco Nexus 3000 Series Switches section.
March 13, 2020	Updated upgrade path section to reflect the limitations of CSCvt02249.
November 07, 2019	Created the release note for Release 9.3(2).

Contents

Introduction

Cisco NX-OS software is a data center-class operating system designed for performance, resiliency, scalability, manageability, and programmability at its foundation. The Cisco NX-OS software provides a robust and comprehensive feature set that meets the requirements of virtualization and automation in mission-critical data center environments. The modular design of the Cisco NX-OS operating system makes zero-impact operations a reality and enables exceptional operational flexibility.

The Cisco Nexus 3000 Series, which includes the Cisco Nexus 3000, 3100, 3200, 3400, 3500, and 3600 Series switches, and the Cisco Nexus 9000 Series switches run the same binary image, also called the "unified" image.

Cisco NX-OS Release 9.2(1) is the first release that adopts unified version numbering. As more platforms have been added, there is no need to have a "platform" designator as used in the past.

An example of a previous release number is: 7.0(3)I7(4). In this format, the 'I' is the platform designator.

Moving forward for the previously identified platforms, we will be adopting the simplified 3-letter versioning scheme. For example, a release with X.Y(Z) would mean:

X – Unified release major

Y- Major/Minor release

Z – Maintenance release (MR)

Where the Z = 1 is always the first FCS release of a Major/Minor release.

Note: In order to accommodate upgrade compatibility from an older software version that is expecting a platform designator, when the install all command is entered or the show install all impact command is entered, the version string appears as 9.2(1)I9(1). The "I9(1)" portion of the string can be safely ignored. It will later appear as 9.2(1).

This section includes the following:

- Cisco Nexus 3000 Series Switches

- Cisco Nexus 3100 Series Switches

- Cisco Nexus 3200 Series Switches

- Cisco Nexus 3400 Series Switches

- Cisco Nexus 3500 Series Switches

- Cisco Nexus 3600 Series Switches

Cisco Nexus 3000 Series Switches

The Cisco Nexus 3000 Series switches are high-performance, high-density, ultra-low-latency Ethernet switches that provide line-rate Layer 2 and Layer 3 switching.

For information about the Cisco Nexus 3000 Series, see the *Cisco Nexus 3000 Series Hardware Installation Guide*.

Cisco Nexus 3100 Series Switches

The Cisco Nexus 3100 Series switches are high-performance, high-density, ultra-low-latency Ethernet switches that provide line-rate Layer 2 and Layer 3 switching.

For information about the Cisco Nexus 3100 Series, see the Cisco Nexus 3000 Series Hardware Installation Guide.

Cisco Nexus 3200 Series Switches

The Cisco Nexus 3200 Series switches are highly programmable with comprehensive features such as low latency, 16-MB buffer space and 10/25/40/50/100-Gbps connectivity.

For information about the Cisco Nexus 3200 Series, see the *Cisco Nexus 3000 Series Hardware Installation Guide*.

Cisco Nexus 3400 Series Switches

The Cisco Nexus 3400 Series switches are Quad Small Form-Factor Pluggable – Double Density (QSFP-DD) switch with 32 ports that are backward-compatible with QSFP+, QSFP28, and QSFP56. Each QSFP-DD port can operate at 400, 100, 50, 40, and 25 Gbps.

For information about the Cisco Nexus 3400 Series, see the *Cisco Nexus 3400 Series Hardware Installation Guide*.

Cisco Nexus 3500 Series Switches

The Cisco Nexus 3500 platform is an extension of the Cisco Nexus 3000 Series of 100M, 1, 10, and 40 Gigabit Ethernet switches built from a switch-on-a-chip (SoC) architecture. Switches in the Cisco Nexus 3500 series include Algorithm Boost (or Algo Boost) technology that is built into the switch application-specific integrated circuit (ASIC). Algo Boost allows the Cisco Nexus 3548 switch to achieve Layer 2 and Layer 3 switching latencies of less than 200 nanoseconds (ns). In addition, Algo Boost contains several innovations for latency, forwarding features, and performance visibility, including two configurable modes for low latency:

- Normal mode: This mode is suitable for environments needing low latency and high scalability.

- Warp mode: This mode consolidates forwarding operations within the switching ASIC, lowering latency by up to an additional 20 percent compared to normal operation.

Active buffer monitoring accelerates the collection of buffer utilization data in hardware, allowing significantly faster sampling intervals. Even on the lowest-latency switches, data packets can incur a millisecond or more of latency during periods of congestion. Previous buffer utilization monitoring techniques were based entirely on software polling algorithms with polling with higher polling intervals that can miss important congestion events.

For information about the Cisco Nexus 3500 Series, see the Cisco Nexus 3500 Series Hardware Installation Guide.

Cisco Nexus 3600 Series Switches

Cisco NX-OS software is a data center-class operating system designed for performance, resiliency, scalability, manageability, and programmability at its foundation. The Cisco NX-OS software provides a robust and comprehensive feature set that meets the requirements of virtualization and automation in mission-critical data center environments. The modular design of the Cisco NX-OS operating system makes zero-impact operations a reality and enables exceptional operational flexibility.

The Cisco Nexus 3600 Series includes Cisco Nexus C36180YC-R and Cisco Nexus C3636C-R switches. The Cisco Nexus C36180YC-R is a high-speed, high-density, 1, 10, 25, 40, or 100 Gigabit Ethernet switch designed for data center aggregation. The Cisco Nexus C3636C-R switch is a high-speed, high-density 40- or 100- Gigabit Ethernet (GE) switch designed for the data center spine.

For information about the Cisco Nexus 3600 Series, see the *Cisco Nexus 3600 Series Hardware Installation Guide*.

Licensing Requirements

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

System Requirements

- [Supported Device Hardware](#)

- [Supported Optics](#)

Supported Device Hardware

The following tables list the Cisco Nexus 3000 Series hardware that Cisco NX-OS Release 9.3(2) supports. For additional information about the supported hardware, see the Hardware Installation Guide for your Cisco Nexus 3000 Series devices.

- [Cisco Nexus 3000 and 3100 Series Switches](#)

- [Cisco Nexus 3000 and 3100 Series fans and fan trays](#)

- [Cisco Nexus 3200 Series Switches](#)

- [Cisco Nexus 3400 Series Switches](#)

- [Cisco Nexus 3500 Series Switches](#)

- [Cisco Nexus 3500 Series fans and fan trays](#)

- [Cisco Nexus 3600 Series Switches](#)

Table 2: Cisco Nexus 3000 and 3100 Series Switches

Product ID	Description
N3K-C3048TP-1GE	Cisco Nexus 3048 switch
N3K-C3064PQ	Cisco Nexus 3064 switch
N3K-C3064PQ-10GE	Cisco Nexus 3064-E switch

Product ID	Description
N3K-C3064PQ-10GX	Cisco Nexus 3064-X switch
N3K-C3064TQ-10GT	Cisco Nexus 3064-TQ switch
N3K-C31108PC-V	Cisco Nexus 31108PC-V switch
N3K-C31108TC-V	Cisco Nexus 31108TC-V
N3K-C31128PQ-10GE	Nexus 31128PQ, 96 x 10 Gb-SFP+, 8 x 10-Gb QSFP+, 2-RU switch.
N3K-C3132C-Z	Cisco Nexus 3132C-Z switch
N3K-C3132Q-40GE	Cisco Nexus 3132Q switch
N3K-C3132Q-40GX	Cisco Nexus 3132Q-X switch
N3k-C3132Q-V	Cisco Nexus 3132Q-V switch
N3K-C3132Q-XL	Cisco Nexus C3132Q-XL switch
N3K-C3164Q-40GE	Cisco Nexus 3164Q, 64 x 40-Gb SFP+, 2-RU switch
N3K-C3172PQ-10GE	Cisco Nexus 3172PQ switch
N3K-C3172PQ-XL	Cisco Nexus C3172PQ-XL switch
N3K-C3172TQ-10GT	Cisco Nexus 3172TQ switch
N3K-C3172TQ-XL	Cisco Nexus C3172TQ-XL switch

Table 3: Cisco Nexus 3000 and 3100 Series Fans, Fan Trays and Power Supplies

Product ID	Description
N2200-PAC-400W	Cisco Nexus 2000 or Nexus 3000 400W AC power supply, forward airflow (port side exhaust)
N2200-PAC-400W-B	Cisco Nexus 2000 or 3000 400W AC power supply with reverse airflow (port-side intake).
N2200-PDC-400W	Cisco Nexus 2000 or Nexus 3000 400W DC power supply, forward airflow (port side exhaust)
N3K-C3048-FAN	Cisco Nexus 3048 fan module with forward airflow (port-side exhaust)
N3K-C3048-FAN-B	Cisco Nexus 3048 fan module with reverse airflow (port-side intake)
N3K-C3064-X-BA-L3	Cisco Nexus 3064-X reversed airflow (port-side intake) AC power supply
N3K-C3064-X-BD-L3	Cisco Nexus 3064-X forward airflow (port-side intake) DC power supply
N3K-C3064-X-FA-L3	Cisco Nexus 3064-X forward airflow (port-side exhaust) AC power supply
N3K-C3064-X-FD-L3	Cisco Nexus 3064-X forward airflow (port-side exhaust) DC power supply
N3K-PDC-350W-B	Cisco Nexus 2000 DC power supply with reverse airflow (port-side intake)
N3K-PDC-350W-B	Cisco Nexus 2000 or Nexus 3000 350W DC power supply, reversed airflow (port side intake)
NXA-FAN-30CFM-B	Cisco Nexus 2000 or Nexus 3000 individual fan, reversed airflow (port side intake)
NXA-FAN-30CFM-F	Cisco Nexus 2000 or Nexus 3000 individual fan, forward airflow (port side exhaust
NXA-PAC-500W	Cisco Nexus 3064-T 500W forward airflow (port-side exhaust) AC power supply

Product ID	Description
NXA-PAC-500W-B	Cisco Nexus 3064-T 500W reverse airflow (port-side intake) AC power supply

Table 4: Cisco Nexus 3200 Series Switches

Product ID	Description
C1-N3K-C3232C	Cisco Nexus 3232C switch.
N3K-C3264C-E	Cisco Nexus 3264C-E switch.
N3K-C3264Q	Cisco Nexus 3264Q switch.

Table 5: Cisco Nexus 3400 Series Switches

Product ID	Description
N3K-C3464C	Nexus 3464C, 64x100 Gb QSFP28, 2x10 Gb SFP+, 2-RU switch.
N3K-C34180YC	Nexus 34180YC, 48x10/25 G + 6x40/100G, 1-RU switch.

Table 6: Cisco Nexus 3500 Series Switches

Product ID	Description
N3K-C3524P-10G	Cisco Nexus 3524 switch
N3K-C3524P-10GX	Cisco Nexus 3524 switch, 24 SFP+
N3K-C3524P-XL	Cisco Nexus 3524-XL switch
N3K-C3548P-10G	Cisco Nexus 3548 switch
N3K-C3548P-10GX	Cisco Nexus 3548x switch, 48 SFP+
N3K-C3548P-XL	Cisco Nexus 3548-XL switch

Table 7: Cisco Nexus 3500 Series Fans, Fan Trays and Power Supplies

Product ID	Description
N2200-PAC-400W	Cisco Nexus 2000 or Nexus 3000 400W AC power supply, forward airflow (port side exhaust)

Product ID	Description
N2200-PAC-400W-B	Cisco Nexus 2000 or Nexus 3000 400W AC power supply, reversed airflow (port side intake)
N2200-PDC-400W	Cisco Nexus 2000 or Nexus 3000 400W DC power supply, forward airflow (port side exhaust)
N3K-PDC-350W-B	Cisco Nexus 2000 or Nexus 3000 350W DC power supply, reversed airflow (port side intake)
NXA-FAN-30CFM-B	Cisco Nexus 2000 or Nexus 3000 individual fan, reversed airflow (port side intake)
NXA-FAN-30CFM-F	Cisco Nexus 2000 or Nexus 3000 individual fan, forward airflow (port side exhaust

Table 8: Cisco Nexus 3600 Series Switches

Product ID	Description
N3K-C3636C-R	The Cisco Nexus 3636C-R is a 1 rack unit (RU) switch with 36 100-Gigabit QSFP28 ports, 40-Gigabit QSFP, 2 management ports, 1 console port, and 1 USB port. The switch supports both port-side exhaust and port-side intake airflow schemes. The switch has two power supplies, one for operations and the other for redundancy. Both power supplies must be either AC power supplies or DC power supplies.
N3K-C36180YC-R	The Cisco Nexus 36180YC-R is a 1 rack unit (RU) switch with 48 1/10/25-Gigabit SFP ports and 6 40-Gigabit QSFP/100-Gigabit QSFP28 ports, 1 management port, 1 console port, and 1 USB port. The switch supports both port-side exhaust and port-side intake airflow schemes. The switch has two power supplies, one for operations and the other for redundancy. Both power supplies must be either AC power supplies or DC power supplies.

Supported Optics

To determine which transceivers and cables are supported by Cisco Nexus 3000 Series switches, see the Transceiver Module (TMG) Compatibility Matrix.

To see the transceiver specifications and installation information, see https://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-installation-guides-list.html.

New and Changed Information

This section lists the new and changed information in Cisco NX-OS Release 9.3(2):

- New Supported Hardware Features

- New Software Features and Enhancements

New Supported Hardware Features

Cisco NX-OS Release 9.3(2) does not include any new hardware.

New Software Features and Enhancements

Cisco NX-OS Release 9.3(2) supports the following new software features:

Fundamentals Features

- Erase Configuration — Added support for the management IPv6 address and route to preserve after the write erase operation in Cisco Nexus 3000 Series.

  For more information, see the Cisco Nexus 3000 Series NX-OS Fundamentals Configuration Guide, Release 9.3(x)

Caveats

The open and resolved caveats 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.

All caveats listed in this section are those that were reported against the Cisco Nexus 3000 Series Switches.

All Cisco Nexus 3000 and 9000 Series switches run the same unified binary image. Because some caveats listed against the Cisco Nexus 9000 Series switches could also be applicable to the Cisco Nexus 3000 Series switches, we recommend that you review the list of caveats in the Cisco Nexus 9000 Series NX-OS Release Notes for this release to see if they are applicable to your network configuration.

This section includes the following topics:

- Resolved Caveats-Cisco NX-OS Release 9.3(2)

- Open Caveats-Cisco NX-OS Release 9.3(2)

- Known Behaviors-Cisco NX-OS Release 9.3(2)

Resolved Caveats-Cisco NX-OS Release 9.3(2)

The following tables list the Resolved Caveats in Cisco Nexus 3000, 3100, 3200, 3400, 3500 and 3600 Series switches in Cisco NX-OS Release 9.3(2). Click the Bug ID to search the Cisco Bug Search Tool for additional information about the bug.

- Resolved Caveats in Cisco Nexus 3000, 3100, 3200 and 3400 Switches

- Resolved Caveats in Cisco Nexus 3500 Switches

- Resolved Caveats in Cisco Nexus 3600 Switches

Table 8: Resolved Caveats in Cisco Nexus 3000, 3100, 3200, and 3400 Series Switches

Bug ID	Description
CSCvd69433	PIM neighborship remains up even after breaking neighborship on peer.
CSCvn05569	Port-Channel remains suspended after a reload on Cisco Nexus C3264C Switch.
CSCvn22108	Cisco Nexus 3000 switch does not forward DHCP offer with broadcast bit set towards client over vPC.
CSCvn24150	PTP crashes after removing PTP on the slave interface followed by *show ptp clock* command.
CSCvn27071	Private VLAN configured VPCs failed on upgrade due to native VLAN mismatch on Cisco Nexus 3000 Switches.
CSCvn34433	On Cisco Nexus 3064 switches continue clk_flush. Kernel and I2c access fail with *neutron_usd* errors
CSCvn71311	IPv6 CoPP - ICMP triggering duplicate traffic
CSCvn78166	Cisco Nexus 3000 Switch generates IGMP report with source 0.0.0.0 preventing the multicast group from timeout
CSCvn78894	On a Cisco Nexus 3000 Switch, user with priv-0 can create/delete svi configuration.
CSCvq37646	Cisco Nexus 3000 Switch hangs and then reloads after 30-90 mins because panic on OOM is disabled.
CSCvq83081	N9K-C9332PQ: Port 14 and 15 links go down with QSA+10G tranceiver on Port 13 or 14
CSCvr05274	OSPF process crashes.
CSCvr19390	Post TCAM Carving reload, Cisco Nexus 3000 Switch gets stuck into boot loop.
CSCuy12344	PFM: nuova_sys_i2c_read_byte_data failed

Table 9: Resolved Caveats in Cisco Nexus 3500 Series Switches

Bug ID	Description
CSCvb94339	Multicast LPM table on a Cisco Nexus 3500 Switch incorrectly full.
CSCvc53438	Shared tree takes up to 60 seconds to be pruned after 2nd receiver joins.
CSCvi09279	SNMPd crashed when preforming SNMP bulk query.
CSCuq69820	Broadcast traffic dropped with too-low storm control threshold.
CSCuz30590	Cisco Nexus 3500 Switch should reject RACL on L2 ports configuration.
CSCvg13002	On a Cisco Nexus 3500 Switch, igmp ssm-translate does not working after reload.
CSCvf29916	RPF for pim bidir not getting updated on bring up of primary RP.
CSCve89395	Cisco Nexus 3500 Switch duplicates multicast packets due to delayed pruning of new *G path.
CSCuz19834	NX-OS is missing subnet check when considering new IGMP querier.
CSCvm18200	On a Cisco Nexus 3500 Switch, control-plane flaps after tx-ring recovery.

CSCvm57658	On a Cisco Nexus 3500 Switch, BFD flaps due to inband Xmit stuck.
CSCvm78215	Cisco Nexus 3500 Switch SPAN sessions down due to *No hardware resource*.
CSCvm95517	Cannot configure "dual-active exclude interface-vlan" command on a Cisco Nexus 3500 Switch.
CSCvn26864	Cisco Nexus 3500 Switch responds to uc PTP delay request sending uc delay response with all zero dmac.
CSCvn28481	Cisco Nexus 3500 Switch fails to produce routing hash information in WARP mode with error 0x410a0001.
CSCvn31364	On Cisco Nexus 3500 Switches, SNMP poll return need to be 1 second.
CSCvn59780	Unexpected CPU response latency of 50-150ms after upgrade to 6.0(2)A8(10a) on Cisco Nexus 3500 Switches.
CSCvn62696	Unable to edit a large ACL when applied on a routed interface.
CSCvo11873	Cisco Nexus 3500 Switch normal lookup takes precedence over WARP mode lookup in WARP mode.
CSCvo31230	Cisco Nexus 3500 Switches does not forward DHCP offer with broadcast bit received on the same interface.
CSCvq36494	PIM-BiDir looping multicast traffic until TTL expiry on Cisco Nexus 3500 Switches.
CSCvq36765	Known unicast is suppressed
CSCvq61783	On Cisco Nexus 3500 Switches, turning on "vlan dot1q tag native" causes packets to be tagged with dot1q even on access port.
CSCvq97992	On Cisco Nexus 3500 Switches, PIM-BiDir MFDM-2-MFDM_UNSUPPORTED_BIDIR_GROUP_RANGE
CSCvq99242	Cisco Nexus 3500 Switches does not enable ABM after reload, ABM syslog does not work.
CSCvr16876	SNMP Polling for output discards not reporting
CSCvf00752	On Cisco Nexus 3500 Switches multicast stops working with igmp host-proxy, lose (S,G)
CSCvf02296	LHR may multiply multicast traffic due to *G fwd-ing and delayed SGR prune on Cisco Nexus 3500 Switches.
CSCvj14778	On Cisco Nexus 3500 Switches, inracl with log keyword does not block traffic when applied to NAT interfaces.

Table 10: Resolved Caveats in Cisco Nexus 3600 Series Switches

Bug ID	Description
CSCve02254	Some BGP prefixes with multiple paths are not advertised
CSCvg80943	SNMPd memory leaks xxxx bytes on libnetsnmp.so.0 after overnight/longevity runs
CSCvm79067	RWE loopback/L2ACL GOLD test needs to be enabled for all N9k/N3k-R TORs to verify inband path

11

CSCvo55700	CRC errors occur on the neighbor devices when connects QSFP-100G-LR4-S on N3K-C36180YC-R switch.
CSCvq29005	Multicast traffic inter R-line cards lost instantaneously when IGMP join/leave repeatedly.

Open Caveats-Cisco NX-OS Release 9.3(2)

The following tables lists the Open Caveats in Cisco Nexus 3000, 3100, 3200, 3400, 3500 and 3600 Series switches in Cisco NX-OS Release 9.3(2). Click the Bug ID to search the Cisco Bug Search Tool for additional information about the bug.

- Open Caveats in Cisco Nexus 3000, 3100, 3200, 3400 Switches
- Open Caveats in Cisco Nexus 3500 Switches
- Open Caveats in Cisco Nexus 3600 Switches

Table 11: Open Caveats in Cisco Nexus 3000, 3100, 3200 and 3400 Series Switches

Bug ID	Description
CSCvn28015	Installation of N3K-LAN2K9 license on Cisco Nexus 3264C-E and Cisco Nexus 3464C switches fails, but the LAN features work.
CSCvn28036	Installation of N3K-STR1K9 on Cisco Nexus 34180YC and Cisco Nexus 3132C-Z fails, but telemetry features work.

Open Caveats in Cisco Nexus 3500 Series Switches

There are no open caveats in Cisco NX-OS Release 9.3(2).

Table 13: Open Caveats in Cisco Nexus 3600 Series Switches

Bug ID	Description
CSCvq36718	With CU3M cable and 40/100BiDi in the same BV ports (i.e.23-24), seeing FCS error packets or link flap running traffic.

Known Behaviors -Cisco NX-OS Release 9.3(2)

The following tables lists the known behaviors in Cisco Nexus 3000, 3100, 3200, 3400, 3500 and 3600 Series switches in Cisco NX-OS Release 9.3(2). Click the bug ID to search the Cisco Bug Search Tool for details about the bug.

Table 14 Known Behaviors in Cisco Nexus 3000 and 3100 Series Switches

Bug ID	Description
CSCvg03567	With switchport mac-learn disable cli, macs are still learnt on VNI enabled VLAN.

Bug ID	Description
CSCvg68550	The MPLS SR outputs stats incremented for all FECs with same next-hop during POP (swap with 3).
CSCvi54469	N3K-C34180YC: Non-default ethertype settings do not work.

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

- 1405964207_0x101_iftmc_log.3679.tar.gzaa

- 1405964207_0x101_iftmc_log.3679.tar.gzab

- 1405964207_0x101_iftmc_log.3679.tar.gzac

To decode the multiple core files, first club the files to a single file:
$ cat 1405964207_0x101_iftmc_log.3679.tar.gz* > 1405964207_0x101_iftmc_log.3679.tar.gz

Upgrading Cisco Nexus 3000 Series Switches

Upgrading Cisco Nexus 3000, 3100 Series Switches

To perform a software upgrade for Cisco Nexus 3000 and 3100 Series switches that run in N3K mode, follow the instructions in the Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide, Release 9.3(x).

To perform a software upgrade for Cisco Nexus 3100 Series switches that run in N9K mode, follow the instructions in the Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 9.3(x).

This section includes the following topics:

- Upgrade Path to Cisco NX-OS Release 9.3(2)

- Guidelines and Limitations - Upgrade

Upgrade Path to Cisco NX-OS Release 9.3(2)

- Non-disruptive standard ISSU on Cisco Nexus 3172PQ, 3172TQ, 3132Q, 3132Q-X, 3064, 3064-X, 3064-T, 3048, 3016 (4 GB low-memory platforms) is not supported to Cisco Nexus 9.3(1) and later releases

- Cisco Nexus 3132Q-XL, 3172PQ-XL, and 3172TQ-XL switches support an ISSU to Cisco NX-OS Release 9.3(1) and later releases. For the list of platforms and releases that support a non-disruptive In-Service Software Upgrade (ISSU) to Cisco NX-OS Release 9.3(2), see the Cisco NX-OS ISSU Support Matrix.

The following disruptive upgrade paths are supported:

- For Cisco Nexus 3048 switches, use one of the two following upgrade paths:
  - Release 6.0(2)U5(1) -> Release 6.0(2)U6(2a) -> Release 6.0(2)U6(10) -> Release 7.0(3)I7(8) -> Release 9.3(2)
  - Release 9.2(1) -> Release 9.2(4) -> Release 9.3(2)
- For Cisco Nexus 3000 and 3100 Series switches (except Cisco Nexus 3048, 3132C-Z, 3164Q, 31128PQ, and 3100-V switches), use one of the two following upgrade paths:

- Release 6.0(2)U5(1) -> Release 6.0(2)U6(10) -> Release 7.0(3)I7(8) -> Release 9.3(2)
    - Release 9.2(1) -> Release 9.2(4) -> Release 9.3(2)
- For Cisco Nexus 3132C-Z, 3164Q, 31128PQ, and 3100-V switches:
  Release 7.0(3)I2(1) or later -> Release 9.3(2)

Upgrade Guidelines and Limitations

The following guidelines and limitations are applicable when you upgrade to Cisco NX-OS Release 9.3(2):

- The only supported method of upgrading is install all from Release 6.0(2)U6(3a) or later due to the need to upgrade the BIOS. Without the Release 9.3(2) BIOS, the 9.3(2) image will not load.

- While performing a non-disruptive ISSU, VRRP and VRRPV3 will display the following messages:

    - If VRRPV3 is enabled:

      2015 Dec 29 20:41:44 MDP-N9K-6 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: ISSU ERROR: Service "vrrpv3" has sent the following message: Feature vrrpv3 is configured. User can change vrrpv3 timers to 120 seconds or fine tune these timers based on upgrade time on all Vrrp Peers to avoid Vrrp State transitions. – sysmgr

    - If VRRP is enabled:

      2015 Dec 29 20:45:10 MDP-N9K-6 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: ISSU ERROR: Service "vrrp-eng" has sent the following message: Feature vrrp is configured. User can change vrrp timers to 120 seconds or fine tune these timers based on upgrade time on all Vrrp Peers to avoid Vrrp State transitions. – sysmgr

- Change the port mode from oversubscribed to line-rate and then reload the switch:

    - On Nexus 31108PC-V and 31108TC-V switches, change from 48x10g+6x100g to 48x10g+4x100g+2x40g.

    - On Nexus 3132Q-V switches change from 32x40g or 26x40g to 24x40g.

- Change the switching-mode from cut-through to store-and-forward and then reload the switch.

- An error occurs when you try to perform an ISSU if you changed the reserved VLAN without entering the copy running-config save-config and reload commands.

- Subinterfaces cannot be used as network ports.

    - Cisco Nexus 3000-XL platforms do not support breakout using speed 10000 CLI command. Use the interface breakout module 1 port <num> map 10g-4x CLI command instead.

    - 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.

■ 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 9.3(2) need to run the set-up script if they want to enable the MPLS static or the VRRpv3 feature.

■ The following Cisco Nexus 9000 features are not supported on the Cisco Nexus 3100 Series switches in N3K or N9K mode:

    - FEX

    - Multicast PIM Bidir

    - Port VLAN (PV) switching and routing support for VXLAN

    - Auto-Config

    - Secure login enhancements:

        - Ability to block login attempts and enforce a quiet period

        - Ability to restrict the maximum login sessions per user

        - Ability to restrict the password length

- Ability to prompt the user to enter a password after entering the username

- Ability to hide the shared secret used for RADIUS or TACACS+ authentication or accounting

- SHA256 hashing support for encrypted passwords

- SHA256 algorithm to verify operating system integrity

- Non-hierarchical routing mode

- NX-API REST

- Link Level Flow Control (LLFC) is not supported on Cisco Nexus 3000 series and Cisco Nexus 3100 series switches.

- You can disable IGMP snooping either globally or for a specific VLAN.

- You cannot disable IGMP snooping on a PIM enabled SVIs. The warning message displayed is: IGMP snooping cannot be disabled on a PIM enabled SVIs. There are one or more VLANs with PIM enabled.

- The Cisco Nexus 3000 Series switches (non-XL platforms, having 4 GB RAM) cannot tftpboot non-compacted 9.3(2) software image from the loader prompt. Hence, you must keep one working image in the bootflash. Tftp of non-compacted can be supported only on the Cisco Nexus Series switches having 8 GB or more RAM (XL platform).

- Enhanced ISSU to Cisco NX-OS Release 9.3(2) is not supported.

- The following switches do not support an ISSU (nondisruptive upgrade) to Cisco NX-OS Release 9.3(2):

  - 3016Q

  - 3048TP

  - 3064PQ, 3064PQ-E, 3064PQ-X, and 3064TQ

  - 3132Q, 3132Q-X, 3172PQ, and 3172TQ

- Before performing an ISSU to Cisco NX-OS Release 9.3(2), you must configure the BGP graceful restart timer to 180 seconds for Cisco Nexus 3132Q-XL, 3172PQ-XL, 3172TQ-XL, and 3132Q-V platform switches.

- If you downgrade the Cisco Nexus device from Cisco NX-OS Release 9.3(2) to the previous NX-OS releases by setting the boot variables and reloading the switch, all earlier configurations of the segment-routing mpls will be lost.

Upgrading Cisco Nexus 3200 and 3400 Series Switches

To perform a software upgrade, follow the instructions in the Cisco Nexus 3400-S Series NX-OS Software Upgrade and Downgrade Guide, Release 9.3(x).

Upgrade Path to Cisco NX-OS Release 9.3(2)

For the list of platforms and releases that support a non-disruptive In-Service Software Upgrade (ISSU) to Cisco NX-OS Release 9.3(2), see the Cisco NX-OS ISSU Support Matrix.

The following disruptive upgrade paths are supported:

- For Cisco Nexus 3232C and 3264Q switches:

  Release 7.0(3)I3(1) or later -> Release 9.3(2)

- For Cisco Nexus 3264C-E switches:

  Release 9.2(1) or 9.2(2) -> Release 9.3(2)

- For Cisco Nexus 34180YC switches:

  Release 9.2(2) -> Release 9.3(2)

Upgrading Cisco Nexus 3500 Series Switches

To perform a software upgrade, follow the instructions in the Cisco Nexus 3500 Series NX-OS Software Upgrade and Downgrade Guide, Release 9.3(x). This section includes the following topics:

- Upgrade Path to Cisco NX-OS Release 9.3(2)

- Guidelines and Limitations - Upgrade

Upgrade Path to Cisco NX-OS Release 9.3(2)

The following disruptive upgrade paths are supported for the XL platforms:

- Release 7.0(3)I7(2) or after -> Release 7.0(3)I7(8) -> Release 9.3(2)
- Release 9.2(1) -> Release 9.2(4) -> Release 9.3(2)

The following disruptive upgrade paths are supported for the non-XL platforms:

- Release 6.0(2)A8(2) or later -> Release 6.0(2)A8(7b) or later -> Release 7.0(3)I7(8) or later -> 9.3(2)
- Release 6.0(2)A8(2) or later -> Release 6.0(2)A8(7b) or later -> Release 9.2(4) or later -> 9.3(2)
- Release 6.0(2)A7(2a) or earlier -> Release 6.0(2)A8(9) -> Release 7.0(3)I7(8) or later -> Release 9.3(2)
- Release 6.0(2)A7(2a) or earlier - > Release 6.0(2)A8(7b) or later -> Release 9.2(4) or later -> 9.3(2)

Upgrade Guidelines and Limitations

The following guidelines and limitations are applicable when you upgrade from Cisco NX-OS Release 7.0(3)I7(2) or later to Cisco NX-OS Release 9.3(2):

- If a custom CoPP policy is applied after upgrading to Cisco NX-OS Release 7.0(3)I7(2) or later, and if the Nexus 3548 switch is downgraded to Cisco NX-OS Release 5.0, where changes to the CoPP policy are not permitted, the custom CoPP policy is retained and cannot be modified.
- copy r s and reload is not a supported method for an upgrade.
- You must run the setup script after you upgrade to Cisco NX-OS Release 9.3(2).
- For Cisco Nexus 3548 and 3548-X switches, you must compact the software image before you upgrade from earlier releases to Cisco NX-OS Release 9.3(2). For the Cisco Nexus 3548-XL switch, compaction is not required.
- *install all* is the only upgrade method supported because of a BIOS upgrade requirement.

- The following limitations are applicable when you upgrade from Cisco NX-OS Releases 6.0(2)A8(7b), 6.0(2)A8(8), or 6.0(2)A8(9) to Cisco NX-OS Release 9.3(2):

  o If Cisco Catalyst devices are connected via a vPC to a pair of Nexus 3500 switches with the vPC peer switch feature enabled, a partial or complete network outage may be caused as a result of the Cisco Catalyst devices error-disabling their port-channel interfaces due to EtherChannel Guard. To prevent this from happening, we recommend that you temporarily disable the EtherChannel Guard feature on vPC-connected Cisco Catalyst devices while the Nexus 3500 devices are being upgraded. For more information, see CSCvt02249.

Upgrading Cisco Nexus 3600 Series Switches

To perform a software upgrade, follow the instructions in the Cisco Nexus 3600 Series NX-OS Software Upgrade and Downgrade Guide, Release 9.3(x).

Upgrade Path to Cisco NX-OS Release 9.3(2)

The following disruptive upgrade paths are supported:

- Release 9.2(1) or 9.2(2)-> Release 9.3(2)

- Release 7.0(3)F3(4) -> Release 9.3(2)*

- Release 7.0(3)F3(3c) -> Release 9.3(2)*

- Release 7.0(3)F3(3) -> Release 7.0(3)F3(4) -> Release 9.3(2)*

  * These upgrade paths require write erase and reload.

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

Unsupported Features

The following features are not supported for the Cisco Nexus 3232C and 3264Q switches:

- 3264Q and 3232C platforms do not support the PXE boot of the NX-OS image from the loader.

- Automatic negotiation support for 25-Gb and 50-Gb ports on the Cisco Nexus 3232C switch.

- Cisco Nexus 2000 Series Fabric Extenders (FEX)

- Cisco NX-OS to ACI conversion (The Cisco Nexus 3232C and 3264Q switches operate only in Cisco NX-OS mode.)

- DCBXP

- Designated router delay

- DHCP subnet broadcast is not supported

- Due to a Poodle vulnerability, SSLv3 is no longer supported

- FCoE NPV

- Intelligent Traffic Director (ITD)

- Enhanced ISSU. NOTE: Check the appropriate guide to determine which platforms support Enhanced ISSU.

- MLD

- NetFlow

- PIM6

- Policy-based routing (PBR)

- Port loopback tests

- Resilient hashing

- SPAN on CPU as destination

- Virtual port channel (vPC) peering between Cisco Nexus 3232C or 3264Q switches and Cisco Nexus 9300 platform switches or between Cisco Nexus 3232C or 3264Q switches and Cisco Nexus 3100 Series switches

- VXLAN IGMP snooping

Related Documentation

The entire Cisco Nexus 3000 Series NX-OS documentation set is available at the following URL:

https://www.cisco.com/c/en/us/support/switches/nexus-3000-series-switches/tsd-products-support-series-home.html

For Cisco Nexus 3000 Series switches that operate in N9K mode, see the Cisco Nexus 9000 Series NX-OS documentation:

http://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/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.

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