Cisco Nexus 3000 Series NX-OS Release Notes, Release 9.3(4)

This document describes the features, issues, and limitations of Cisco NX-OS Release 9.3(4) software for use on Cisco Nexus 3000, 3100, 3200, 3400-S, 3500 and 3600 switches. For more information, see *Related Documentation*.

Note: The Cisco Nexus 34180YC and 3464C platform switches are not supported in Cisco NX-OS Release 9.3(4).

Table 1: Online History Change

Date	Description
Jan 18, 2021	Updated the Upgrade and Downgrade section for Compact NX-OS Image.
October 19, 2020	Updated the Upgrading Cisco Nexus 3000 Series Switches section.
April 29, 2019	Created the release note for Release 9.3(4).

Contents

New Software Features

Table 2: New Software Features

Feature	Description
Pre-compacted NX-OS Images	Cisco Nexus 3048, 3064, 3132 (except for the N3K-C3132Q-V), and 3172 platform switches with a model number that does not end in -XL must run a "compact" NX-OS software image due to limited bootflash space. This "compact" image can be created using the NX-OS Compact Image procedure; alternatively, a compact NX-OS software image can be downloaded directly from Cisco's Software Download website. This requirement does not apply to any other model of Cisco Nexus 3000 or 3100 series switch. This requirement does not apply to the Nexus 3132Q-V switch. For more information, see the following documents: • "Upgrade and Downgrade" section in this document. • Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide, Release 9.3(x)
128x100G | 30x400G + 2x200G Breakout Port Mode Support	Added support to two hardware profile port modes (128 * 100G - 30 * 400G + 2 * 200G and 128 * 100G - 32 * 400G) on Cisco Nexus 3408-S switches. For more details, see the Cisco Nexus 3400-S NX-OS Interfaces Configuration Guide, Release 9.3(x).
Dynamic Buffer Sharing	Support for configuring drop and no-drop buffer sharing within a slice. For more details, see the Cisco Nexus 3400-S NX-OS QoS Configuration Guide, Release 9.3(x).
Support Port-Channel Sub-Interface Statistics	Added support to additional statistical counters such as IPV4 InPkts, IPV6 InPkts, IPV4 OutPkts, IPV6 OutPkts, IPV4 InOctets/Bytes, IPV6 InOctets/Bytes, IPV4 OutOctets/Bytes, IPV6 OutOctets/Bytes on Cisco Nexus 3408-S switches. For more details, see the Cisco Nexus 3400-S NX-OS Interfaces Configuration Guide, Release 9.3(x).

New Hardware Features

Cisco NX-OS Release 9.3(4) does not include any new hardware.

Release Versioning Strategy

Cisco Nexus 9000 Series switches and the Cisco Nexus 3000 Series switches use the same NX-OS binary image also called the "unified" image. The binary image covers the Cisco Nexus 9300 and 9500 and Cisco Nexus 3100, 3200, 3400-S, 3500, and 3600 platform switches. Cisco NX-OS Release 9.2(1) was the first release that adopted unified version numbering. With unified version numbering, the platform designator is obsolete.

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.

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

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 9.3(4)I9(1). The "I9(1)" portion of the string can be safely ignored. It will later appear as 9.3(4).

Note: Cisco NX-OS Release 9.3(4) runs on all Cisco Nexus 3000 Series switches except the Cisco Nexus 34180YC and 3464C platform switches.

Open Issues

The following tables lists the Open Issues in Cisco Nexus 3000, 3100, 3200, 3400-S, 3500 and 3600 Series switches in Cisco NX-OS Release 9.3(4). Click the Bug ID to search the Cisco Bug Search Tool for additional information about the bug.

- Open Issues in Cisco Nexus 3000, 3100, 3200 and 3400-S Switches
- Open Issues in Cisco Nexus 3500 Switches

Table 3: Open Issues in Cisco Nexus 3000, 3100, 3200 and 3400-S Series Switches

Bug ID	Description
CSCvt56182	**Headline**: 9.3(3) to 9.3(4): ND ISSU on LXC TOR causing transient traffic drop **Symptom**: 9.3(3) to 9.3(4): ND ISSU on LXC TOR causing transient traffic drop when we have the BFD enabled as the BFD is going down and coming up during the ND ISSU. **Workaround**: Remove the BFD and add it again.
CSCvt67180	**Headline**: Cisco Nexus C34200YC: CRC seen on 25g AOC links with port flap script/peer reload **Symptom**: CRC errors on ports having SFP28 AOC cables. **Workaround**: Perform `shut` and `no shut` of the port.

CSCvt73635	**Headline**: After downgrading **finrst-timeout and syn-timeout** never CLIs gets added to running config
	Symptom: User sees the following extra configuration when downgraded from Cisco NX-OS Release 9.3(4) to Cisco NX-OS Release 7.0(3)I7(8).
	`ip nat translation finrst-timeout never`
	`ip nat translation syn-timeout never`
	No functionality impact except for these extra configurations appearing after downgrade.
	Workaround: After downgrading to Cisco NX-OS Release 7.0(3)I7(8), user must first disable and then enable NAT feature and reconfigure NAT to delete the configuration.

Resolved Issues

The following tables list the Resolved Issues in Cisco Nexus 3000, 3100, 3200, 3400-S, 3500 and 3600 Series switches in Cisco NX-OS Release 9.3(4). Click the Bug ID to search the Cisco Bug Search Tool for additional information about the bug.

- Resolved Issues in Cisco Nexus 3000, 3100, 3200 and 3400-S Switches
- Resolved Issues in Cisco Nexus 3500 Switches
- Resolved Issues in Cisco Nexus 3600 Switches

Table 4: Resolved Issues in Cisco Nexus 3000, 3100, 3200, and 3400-S Series Switches

Bug ID	Description
CSCvp41943	**Headline**: Broadcom platforms may experience permanent PTP high correction **Symptom**: Constantly high PTP correction (~125/250ms) with no change in the grandmaster clock. **Workaround**: NA

CSCvr57711	**Headline**: Installer should abort the installation when BIOS extraction fails
	Symptom: Installer should abort the installation when BIOS extraction fails
	`BIOS extraction fails during upgrade.`
	`Images will be upgraded according to following table:`
	`Module    Image       Running-Version(pri:alt)          New-Version   Upg-Required`
	`------  ----------  --------------------------------  ------------------  ------------`
	`     1       nxos                         7.0(3)I7(5a)        7.0(3)I7(7)          yes`
	`     1       bios                    v4.4.0(11/06/2017)                           no-----------`
	`>New BIOS version is empty`
	Workaround: Issue has been addressed in 7.0(3)I7(7)

CSCvs80627	**Headline**: CoPP ACLs are not configured correctly on Cisco Nexus 3000 or 3100 series switches, after upgrading to releases 7.x or 9.x **Symptom**: A Nexus 3000 or 3100 series device that is upgraded from 6.x NX-OS software releases to 7.x or 9.x software releases (such as 7.0(3)I7(7) or 9.2(4)) may not configure CoPP ACLs as expected. As a result, the device may encounter issues with control plane traffic not being forwarded from the data plane to the control plane. For example, the device may stop receiving HSRP packets in the control plane. As a result, an Active/Active HSRP scenario may be observed on HSRP groups attached to a physical interface. **Workaround**: After upgrading the Nexus device, execute the initial setup configuration script and accept all default options. An example of this is shown below. Note that each default option does not need to be explicitly entered - hitting the "Enter" or "Return" key to accept the default option will proceed through the entire setup script successfully.
CSCvs96786	**Headline**: Buffer cell leak causing input discards on Cisco Nexus 31108 devices **Symptom**: Input discards across multiple interfaces. **Workaround**: Reload the switch.

Bug ID	Description
CSCvs49770	**Headline**: After modifying custom CoPP, ICMPv6 NS/ND dropping **Symptom**: On a Nexus 3000 series switch after modifying the control-plane policing policy (CoPP) following a specific set of steps IPv6 neighbors might not form. **Workaround**: Workaround is to add the copp-white-list-ums class towards the end, just before class-default in the custom CoPP policy
CSCvs54144	**Headline**: GARP Reply packet not copied to CPU on 100G link Eth1/49-52 on N3K-C31108PC-V **Symptom**: GARP reply packet received on 100G port eth1/50, 52 is not punted to CPU, but with 40G link, it is working fine. GARP request packet works fine on both links(100G, 400G) **Workaround**: 1. Use 40G link on Eth1/49-52 2. Use GARP Request instead of GARP reply if possible (that is coming from a host) 3. Via the bcm-shell, remove the "MyStationHit" from the "ARP Response XE ACL" rule ### Get ACL entry for ARP response N31108-8# show system internal access-list sup-redirect-stats | grep -i arp 2094 ARP Request XE ACL 23900 2095 ARP Response XE ACL 1 <=== 2096 ARP Response HG ACL for VxLAN F&L 0 Remove MyStationHit qualifier -> this will allow GARP response to hit this ACL N31108-8#bcm-shell module 1 "fp qual 2095 delete MyStationHit? Reinstall entry 2095 N31108-8#bcm-shell module 1 "fp entry reinstall 2095?
CSCvn78166	**Headline**: Cisco Nexus 3000 switches generates IGMP report with source 0.0.0.0 preventing the multicast group from timeout **Symptom**: • A pair of Nexuss3000 series switches in VPC • Multicast receiver connected via orphan port (not certain at this point if it's mandatory condition to hit the defect) • IGMP querier located behind a VPC port-channel • When the last receiver leaves the group (sends IGMP LEAVE message) - the N3000s keep sending the IGMP REPORTS towards the Querier • This causes the IGMP group never to timeout on the querier - traffic keeps being sent into the subnet even though there are no receivers listening to it **Workaround**: None

CSCvt56401	**Headline**: ACL QoS crash seen when new class-map (with object-group ACL) is added to active QoS policy on the system/interface.
	
	Symptom:
	device rebooted and following logs could see
	`2010 Feb 19 10:09:37 switch %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "aclqos" (PID 3201) hasn't caught signal 11 (core will be saved).`
	`2010 Feb 19 10:09:38 switch %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "aclqos" (PID 3915) hasn't caught signal 11 (core will be saved).`
	`2010 Feb 19 10:09:38 switch %SYSMGR-SLOT1-2-HAP_FAILURE_SUP_RESET: Service "aclqos" in vdc 1 has had a hap failure`
	`2010 Feb 19 10:09:38 switch %SYSMGR-SLOT1-2-LAST_CORE_BASIC_TRACE: fsm_action_become_offline: PID 17099 with message Could not turn off console logging on vdc 1 error: mts req-response with syslogd in vdc 1 failed (0xFFFFFFFF).`
	Workaround: Remove "service-policy type qos input SET-QOS-Group" under "system qos". Add new group in this qos. Re-apply the "service-policy type qos input SET-QOS-Group" to "system qos".

Table 5: Resolved Issues in Cisco Nexus 3500 Series Switches

Bug ID	Description
CSCvc53438	**Headline**: Shared tree takes up to 60 seconds to be pruned after 2nd receiver joins **Symptom**: Receivers will receive duplicated packets for 60 seconds or less, 10 to 15 seconds after a new receiver joins the shared tree. **Workaround**: On the IHRs, make the IIF of the source and share tree the same. This will not prevent the IHR of sending the *,G PIM Join towards the RP, but will drop the packets on shared tree.
CSCvt50489	**Headline**: Cisco Nexus 3500 switches stop sending PTP delay-response messages **Symptom**: PTP client reporting high PTP correction. **Workaround**: Flip-flop GPE16 interrupt from bash prompt: 1. echo disable > /sys/firmware/acpi/interrupts/gpe16 2. echo enable > /sys/firmware/acpi/interrupts/gpe16
CSCvs63415	**Headline**: N3K-C3548P arp packet cannot punt to CPU after configure ip dhcp relay address on SVI **Symptom**: N3K-C3548P arp packet cannot punt to CPU after configure ip dhcp relay address on SVI **Workaround**: NA
CSCvt34933	**Headline**: Cisco Nexus 3500 Switches reports high PTP correction in milli-seconds after reselecting original GM **Symptom**: Cisco Nexus 3500 Switches reports high PTP correction. **Workaround**: Reload the device.
CSCvt31282	**Headline**: L3 connectivity issue due to hardware adjacency table mis-programming **Symptom**: Unknown unicast traffic is not gleaned. Nexus will not punt the traffic to CPU and ARP will not be forged which will cause connectivity issue once the ARP entry will time out. **Workaround**: Ping the host from the switch SVI to maintain the ARP entry
CSCvp87785	**Headline**: N3500: 7.0(3)I7(x); Peer-gateway feature does not work with guard-vpc-peergw-mac **Symptom**: A Nexus 3500 Series Switch running 7.0(3)I7(x) converged code may fail to route traffic for its vPC Peer's GW MAC address (i.e broken Peer-Gateway functionality). This may lead to traffic black-holing due to vPC Loop Prevention depending on traffic hashing. **Workaround**: Remove the "mac address-table guard-vpc-peergw-mac" configuration; SVIs may need to be flapped afterward.
CSCvs97553	**Headline**: ARP/HSRP Cannot be punt to CPU after some link state change **Symptom**: In warp/normal mode, if the interface has some changes such as shutdown or unplugging the optical module, the remaining Layer 2 interfaces will fail to send ARP/HSRP packets to the CPU, whether unicast ARP or broadcast ARP. **Workaround**: Use static ARP. Do not remove the optical module or shutdown port.
CSCvt09871	**Headline**: Interfaces connected with certain DAC cables may show as "not supported" **Symptom**: Certain DAC used on Cisco Nexus 3548 switches may show "transceiver is not supported".

Bug ID	Description
	Workaround: Remove and reinsert the SFP

CSCvt25753	**Headline**: IGMPv3 leave from single host causes OIL flush until next query on Cisco Nexus 3500 Switches
	Symptom: When Nexus 3500 has downstream host using IGMPv3 and the host sends a leave for the multicast group the mroute OIL gets flushed and other hosts lose the multicast stream even though their interface is still populated in the IGMP snooping table.
	Workaround: Disable explicit host tracking under VLAN configuration:
	`configure terminal`
	`vlan configuration 10`
	`no ip igmp snooping explicit-tracking`

CSCvs45104	**Headline**: Interface remain down after errdisable auto-recovery **Symptom**: An interface will remain down as 'link not connected' after err-disable auto-recovery has removed the state of errdisable. **Workaround**: Apply 'shutdown' and then 'no shutdown' under the affected interface to bring it back up.
CSCuz19834	**Headline**: NX-OS is missing subnet check when considering new IGMP querier **Symptom**: Layer 3 IP IGMP querier ip address belongs to an ip in different subnet. **Workaround**: None
CSCvf00752	**Headline**: On Cisco Nexus 3500 Switches, multicast stops working with IGMP host-proxy, lose (S,G) **Symptom**: Under normal operation the Cisco Nexus 3500 Switches may stop processing multicast traffic when using the IGMP host-proxy feature. The (S,G) entry will no longer be programmed on the switch. **Workaround**: Check show IP interface <intf> and check for multicast routing. If that's disabled, remove and replace the IGMP host-proxy configuration.
CSCvg13002	**Headline**: On Cisco Nexus 3500 Switches, igmp ssm-translate not working after reload **Symptom**: Reload of switch causes the CLI command for adding the igmp ssm-translate rules to be missed. igmpv2 join is not translated to igmpv3 and SG is not created as expected. **Workaround**: Reprogram the ssm-translate rules via CLI manually after reload. Default L3 interfaces and add the configuration back.
CSCvf29916	**Headline**: RPF for PIM BiDir not getting updated on bring up of primary RP **Symptom**: PIM BIDIR entry has old RPF OIF after RPF change. **Workaround**: Shut/no shut of the old RPF interface.

Known Issues

The following tables lists the known behaviors in Cisco Nexus 3000, 3100, 3200, 3400-S, 3500 and 3600 Series switches in Cisco NX-OS Release 9.3(4). Click the bug ID to search the Cisco Bug Search Tool for details about the bug.

Table 6: Known Behaviors in Cisco Nexus 3000 and 3100 Series Switches

Bug ID	Description
CSCvg03567	**Headline**: With switchport mac-learn disable command, MACs are still learnt on VNI enabled VLAN. **Symptom**: **`switchport mac-learn disable`** command/ configuration has no effect on VNI enabled VLAN. **Workaround**: None.
CSCvg68550	**Headline**: The MPLS SR outputs stats incremented for all FECs with same next-hop during POP (swap with 3). **Symptom**: For Broadcom ASIC Based Trident series platform, In the MPLS SR topology the TX output stats are getting incremented for all FEC with same next hop. **Workaround**: None.
CSCvi54469	**Headline**: N3K-C34180YC: Non default Etherype settings not working. **Symptom**: **`switchport dot1q ethertype`** command not configurable on N3K-C34180YC. **Workaround**: None.

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
```

Table 7: Known Behaviors in Cisco Nexus 3500 Series Switches

Bug ID	Description
CSCvs16850	**Headline**: MTC does not support random-detect ECN. It only supports dctcp ecn. Unsupported cli has been removed for MTC. **Symptom**: MTC does not support random-detect ECN. It only supports dctcp ecn. Unsupported cli has been removed for MTC **Workaround**: Cisco Nexus 3500 switches support the command dctcp; but does not support random-detect ecn. The unsupported command (random-detect ecn) is removed in Cisco NX-OS Release 9.3(4). However, you may not get warnings or errors when you configure the command in releases earlier to Cisco NX-OS Release 9.3(4) and then upgrade to Cisco NX-OS Release 9.3(4). The unsupported command is retained in the running-configuration in such cases.

Device Hardware

The following tables list the Cisco Nexus 3000 Series hardware that Cisco NX-OS Release 9.3(4) 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-S Series Switches
- Cisco Nexus 3500 Series Switches
- Cisco Nexus 3500 Series fans and fan trays
- Cisco Nexus 3600 Series Switches

Table 8: 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
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 9: 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
NXA-PAC-500W-B	Cisco Nexus 3064-T 500W reverse airflow (port-side intake) AC power supply

Table 10: 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 11: Cisco Nexus 3400-S Series Switches

Product ID	Description
N3K-C3408-S	Cisco Nexus 3408-S switch with 32 ports of QSFP-DD.
N3K-C3432D-S	Cisco Nexus 3432D-S switch with 32ports of QSFP-DD.

Table 12: 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 13: 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)
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 14: 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.

Product ID	Description
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.

Upgrade and Downgrade

Upgrading Cisco Nexus 3000 and 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(4)
- Guidelines and Limitations - Upgrade

Upgrade Path to Cisco NX-OS Release 9.3(4)

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

- For Cisco Nexus 3264C-E switches:
  Release 9.2(1) -> Release 9.3(4)

Upgrade Guidelines and Limitations

The following guidelines and limitations are applicable when you upgrade to Cisco NX-OS Release 9.3(4):

- Cisco Nexus 3048, 3064, 3132 (except for the N3K-C3132Q-V), and 3172 platform switches with a model number that does not end in -XL must run a “compact” NX-OS software image due to limited bootflash space. This “compact” image can be created using the NX-OS Compact Image procedure; alternatively, a compact NX-OS software image can be downloaded directly from Cisco's Software Download website. This requirement does not apply to any other model of Cisco Nexus 3000 or 3100 series switch. This requirement does not apply to the Nexus 3132Q-V switch.
- The MD5/SHA512 checksum published on Cisco's Software Download website for a compact NX-OS software image may not match the MD5/SHA512 checksum of a compact image created through the NX-OS Compact Image procedure.
- 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(4) 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(4) is not supported.
- The following switches do not support an ISSU (nondisruptive upgrade) to Cisco NX-OS Release 9.3(4):
    - 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(4), 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(4) 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-S 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(4)

For the list of platforms and releases that support a non-disruptive In-Service Software Upgrade (ISSU) to Cisco NX-OS Release 9.3(4), 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(4)

- For Cisco Nexus 3264C-E switches:

  Release 9.2(1) or 9.2(2) -> Release 9.3(4)

- For Cisco Nexus 3408-S and 3432D-S switches:

  Release 9.2(2t) to 9.2(2v) -> Release 9.3(4)

  Release 9.2(2v) -> Release 9.3(4)

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(4)
- Guidelines and Limitations - Upgrade

Upgrade Path to Cisco NX-OS Release 9.3(4)

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

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

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(4)
- Release 6.0(2)A8(2) or later -> Release 6.0(2)A8(7b) or later -> Release 9.2(4) or later -> 9.3(4)
- 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(4)
- Release 6.0(2)A7(2a) or earlier - > Release 6.0(2)A8(7b) or later -> Release 9.2(4) or later -> 9.3(4)

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(4):

- 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(4).
- Cisco Nexus 3548 and 3548-X platform switches must run a "compact" NX-OS software image due to limited bootflash space. This "compact" image can be created using the NX-OS Compact Image procedure; alternatively, a compact NX-OS software image can be downloaded directly from Cisco's Software Download website. This requirement does not apply to the Cisco Nexus 3548-XL switch.
- The MD5/SHA512 checksum published on Cisco's Software Download website for a compact NX-OS software image may not match the MD5/SHA512 checksum of a compact image created through the NX-OS Compact Image procedure.
- *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(4):
  - 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(4)

The following disruptive upgrade paths are supported:

- Release 9.2(1) or 9.2(2)-> Release 9.3(4)
- Release 7.0(3)F3(4) -> Release 9.3(4)*
- Release 7.0(3)F3(3c) -> Release 9.3(4)*
- Release 7.0(3)F3(3) -> Release 7.0(3)F3(4) -> Release 9.3(4)*

* 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

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.

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.