Cisco Nexus 9000 Series NX-OS Release Notes, Release 7.0(3)I2(4)

This document describes the features, caveats, and limitations for Cisco NX-OS Release 7.0(3)I2(4) software for use on the Cisco Nexus 9000 Series switches, the Cisco Nexus 31128PQ switch, and the Cisco Nexus 3164Q switch. Use this document in combination with documents listed in *Related Documentation*.

Note: Starting with Cisco NX-OS Release 7.0(3)I2(1), the Cisco NX-OS image filename has changed to start with "nxos" instead of "n9000."

Table 1 shows the online change history for this document.

Table 1. Online History Change

Date	Description
September 15, 2016	Created the release notes for Release 7.0(3)I2(4).

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 9000 Series uses an enhanced version of Cisco NX-OS software with a single binary image that supports every switch in the series, which simplifies image management.

System Requirements

This section includes the following sections:

- Supported Cisco Software Releases
- Supported Device Hardware
- Supported Optics
- Supported FEX Modules

Supported Cisco Software Releases

Table 2 summarizes information about the Cisco Nexus platforms and software release versions that Cisco OpenFlow Plug-in supports.

Table 2. Cisco Plug-in for OpenFlow Compatibility Matrix

Switches	Cisco Plug-in for OpenFlow
Cisco Nexus 9300 Series switches and Cisco Nexus 31128PQ switches NX-OS 7.0(3)I2(1)	ofa-2.1.0-r1-nxos-SPA-k9.ova

Supported Device Hardware

Table 3 lists the Cisco Nexus 9000 Series hardware that Cisco NX-OS Release 7.0(3)I2(4) supports. For additional information about the supported hardware, see the Hardware Installation Guide for your Cisco Nexus 9000 Series device.

Table 3. Cisco Nexus 9000 Series Hardware

Product ID	Hardware	Quantity
N9K-C9516	Cisco Nexus 9516 16-slot chassis	1
N9K-C9516-FM	Cisco Nexus 9500 Series fabric module	3-6 depending on the line card
N9K-C9516-FAN	Cisco Nexus 9516 fan trays	3
N9K-C9508	Cisco Nexus 9508 8-slot chassis	1
N9K-C9508-FM	Cisco Nexus 9508 Series fabric module	3-6 depending on the line card
N9K-C9508-FAN	Cisco Nexus 9508 fan trays	3
N9K-X9564PX	Cisco Nexus 9500 Series 48-port, 1-/10-Gbps SFP+ plus 4-port QSFP I/O module	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 16 in the Cisco Nexus 9516
N9K-X9564TX	Cisco Nexus 9500 Series 48-port, 1-/10-Gbps BASE-T plus 4-port QSFP I/O module	■ Up to 8 in the Cisco Nexus 9508 ■ Up to 4 in the Cisco Nexus 9504 ■ Up to 16 in the Cisco Nexus 9516

Product ID	Hardware	Quantity
N9K-X9536PQ	Cisco Nexus 9500 36-port, 40 Gigabit Ethernet QSFP aggregation module	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 16 in the Cisco Nexus 9516
N9K-X9636PQ	Cisco Nexus 9500 Series 36-port 40-Gigabit QSFP I/O module **Note:** Not supported on the Cisco Nexus 9516 switch (N9K-C9516).	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508
N9K-X9464PX	Cisco Nexus 9500 Series 48-port 10-Gigabit SFP+ plus 4-port QSFP I/O module	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 16 in the Cisco Nexus 9516

Product ID	Hardware	Quantity
N9K-X9464TX	Cisco Nexus 9500 Series 48-port 10-GBASE-T plus 4-port QSFP I/O module	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 16 in the Cisco Nexus 9516
N9K-X9432PQ	Cisco Nexus 9500 Series 32-port 40-Gigabit QSFP I/O module **Note:** The Cisco Nexus X9432PQ I/O module supports static breakout.	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 16 in the Cisco Nexus 9516
N9K-X9408PC-CFP2	Cisco Nexus 9500 Series 8-port 100-Gigabit CFP2 I/O module for the Cisco Nexus 9504, 9508, and 9516 modular switches	■ Up to 4 in the Cisco Nexus ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 16 in the Cisco Nexus 9516
N9K-SC-A	Cisco Nexus 9500 Series System Controller Module	2
N9K-SUP-A	Cisco Nexus 9500 Series supervisor module	2
N9K-SUP-B	Cisco Nexus 9500 Series supervisor B module	2

Product ID	Hardware	Quantity
N9K-PAC-3000W-B	Cisco Nexus 9500 Series 3000 W AC power supply	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 10 in the Cisco Nexus 9516
N9K-C9504	Cisco Nexus 9504 4-slot chassis	1
N9K-C9504-FM	Cisco Nexus 9504 fabric module	3 to 6 depending on line card
N9K-C9504-FAN	Cisco Nexus 9504 fan trays	3
N9K-C9396PX	Cisco Nexus 9300 48-port, 1/10-Gigabit Ethernet SFP+ and 12-port, 40-Gigabit Ethernet QSPF switch	1
N9K-C9396TX	Cisco Nexus 9300 48-port, 1/10-Gigabit Ethernet BASE-T and 12-port, 40-Gigabit Ethernet QSFP switch	1
N9K-C9372PX	Cisco Nexus 9300 48-port, 1/10-Gigabit Ethernet SFP+ and 6-port, 40-Gigabit Ethernet QSFP switch	1
N9K-C9372PX-E	An enhanced version of the N9K-C9372PX.	
N9K-C9372TX	Cisco Nexus 9300 48-port, 1/10-Gigabit Ethernet BASE-T and 6-port, 40-Gigabit Ethernet QSFP switch	1
N9K-C9332PQ	Cisco Nexus 9300 32-port, 40-Gigabit Ethernet QSFP switch with support for 4x10G breakout mode ■ Ports 1 to 26 (except 13 and 14) support 4x10G breakout mode. ■ Ports 27 to 32 (ALE uplink ports) support using QSA for 10G SFP/SFP+ transceivers in QSFP+ ports	1

Product ID	Hardware	Quantity
N9K-C93128TX	Cisco Nexus 9300 switch with 96 1-/10-Gigabit BASE-T ports and eight 40-Gigabit Ethernet QSPF ports (The 1-/10-Gigabit BASE-T ports also support a speed of 100 Megabits.)	1
N9K-C93120TX	Cisco Nexus 93120TX switch with 96 1-/10-Gigabit BASE-T ports and 6 QSFP uplink ports	
N9K-PAC-650W	Cisco Nexus 9300 650 W AC power supply, hot air out (red) **Note:** For use with the Cisco Nexus 9396 switch (N9K-C9396PX).	2 or less
N9K-PAC-650W-B	Cisco Nexus 9300 650 W AC power supply, cold air in (blue) **Note:** For use with the Cisco Nexus 9396 switch (N9K-C9396PX).	2 or less
N9K-PAC-1200W	Cisco Nexus 9300 1200 W AC power supply, hot air out (red) **Note:** For use with the Cisco Nexus 93128 switch (N9K-C93128TX).	2 or less
N9K-PAC-1200W-B	Cisco Nexus 9300 1200 W AC power supply, cold air in (blue) **Note:** For use with the Cisco Nexus 93128 switch (N9K-C93128TX).	2 or less
N9K-C9300-FAN1	Cisco Nexus 9300 fan 1, hot air out (red) **Note:** For use with the Cisco Nexus 9396 switch (N9K-C9396PX).	3
N9K-C9300-FAN1-B	Cisco Nexus 9300 fan 1, cold air in (blue) **Note:** For use with the Cisco Nexus 9396 switch (N9K-C9396PX).	3
N9K-C9300-FAN2	Cisco Nexus 9300 fan 2, port side intake (red) **Note:** For use with the Cisco Nexus 93128 switch (N9K-C93128TX).	3
N9K-C9300-FAN2-B	Cisco Nexus 9300 fan 2, port side exhaust (blue) **Note:** For use with the Cisco Nexus 93128 switch (N9K-C93128TX).	3
NXA-FAN-30CFM-F	Cisco Nexus 9300 fan, port-side exhaust **Note:** For use with the Cisco Nexus 9332PQ, 9372PX, and 9372TX switches (N9K-C9332PQ, N9K-C9372PX, and N9K-9372TX).	4

Product ID	Hardware	Quantity
NXA-FAN-30CFM-B	Cisco Nexus 9300 fan, port-side intake **Note:** For use with the Cisco Nexus 9332PQ, 9372PX, and 9372TX switches (N9K-C9332PQ, N9K-C9372PX, and N9K-9372TX).	4
N9K-M12PQ	Cisco Nexus GEM 9300 uplink module, 12-port, 40-Gigabit Ethernet QSPF **Note:** The front-panel ports on these GEM modules do not support auto negotiation with copper cables. Manually configure the speed on the peer switch.	1 (required)
N9K-M6PQ	Cisco Nexus GEM 6-port 40-Gigabit Ethernet uplink module for the Cisco Nexus 9396PX, 9396TX, and 93128TX switches **Note:** The front-panel ports on these GEM modules do not support auto negotiation with copper cables. Manually configure the speed on the peer switch.	1
N9K-M6PQ-E	An enhanced version of the N9K-M6PQ.	
N9K-M4PC-CFP2	Cisco Nexus 9300 uplink module for the 93128TX (2 active ports), 9396PX (4 active ports), and 9396TX (4 active ports) Top-of-rack switches	1

Table 4 lists the Cisco Nexus 3164Q switch hardware that Cisco NX-OS Release 7.0(3)I2(4) supports.

Table 4. Cisco Nexus 3164Q Switch Hardware

Product ID	Hardware	Quantity
N3K-C3164Q-40GE	Cisco Nexus 3164Q switch	1
N9K-C9300-FAN3	Cisco Nexus 3164Q fan module	3
N9K-PAC-1200W	Cisco Nexus 3164Q 1200W AC power supply	2

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

Table 5 lists the Cisco Nexus 31128PQ switch hardware that Cisco NX-OS Release 7.0(3)I2(4) supports.

Table 5. Cisco Nexus 31128PQ Switch Hardware

Product ID	Hardware	Quantity
N3K-C31128PQ-10GE	Nexus 31128PQ, 96 SFP+ ports, 8 QSFP+ ports, 2RU switch	1

Supported Optics

See the *Cisco 10-Gigabit Ethernet Transceiver Modules Compatibility Matrix* for a list of supported optical components.

Supported FEX Modules

Cisco NX-OS Release 7.0(3)I2(4) supports the following FEXes on Cisco Nexus 9332PQ (support for 2300 only), 9372PX, 9372PX-E, 9396PX and 9500 Series Switches:

- Cisco Nexus 2224TP
- Cisco Nexus 2232PP
- Cisco Nexus 2232TM and 2232TM-E
- Cisco Nexus 2248PQ
- Cisco Nexus 2248TP and 2248TP-E
- Cisco Nexus 2348UPQ
- Cisco Nexus B22Dell
- Cisco Nexus B22HP
- Cisco Nexus NB22FTS
- Cisco Nexus NB22IBM
- Cisco Nexus 2348TQ

Note: Please note the following:

- The 9408 line card is not supported with the 2300 FEX.
- Cisco Nexus 9300 Series switches do not support FEX on uplink modules (ALE).

- For FEX HIF port channels, Cisco recommends that you enable STP port type edge using the **spanning tree port type edge [trunk]** command.
- The following Cisco FEX Switches have 40G QSFP uplinks as network interfaces:
  - 2248PQ
  - 2348UPQ
  - 2348TQ

To connect the above FEX(es) to a Cisco Nexus 9396PX leaf switch, a Cisco Nexus 9372PX leaf switch, or a supported Cisco Nexus 9500 10G line card, a set of breakout cables would be required.

Note: For Cisco Nexus 9500 switches, 4x10G breakout for FEX connectivity is not supported. Native 10G or 40G should be used.

New and Changed Information

This section lists the following topics:

- New Hardware Features in Cisco NX-OS Release 7.0(3)I2(4)
- New Software Features in Cisco NX-OS Release 7.0(3)I2(4)

New Hardware Features in Cisco NX-OS Release 7.0(3)I2(4)

Cisco NX-OS Release 7.0(3)I2(4) does not include new hardware features.

New Software Features in Cisco NX-OS Release 7.0(3)I2(4)

Cisco NX-OS Release 7.0(3)I2(4) does not include new software features.

Caveats

This section includes the following topics:

- Resolved Caveats—Cisco NX-OS Release 7.0(3)I2(4)
- Open Caveats—Cisco NX-OS Release 7.0(3)I2(4)

Resolved Caveats—Cisco NX-OS Release 7.0(3)I2(4)

Table 6 lists the Resolved Caveats in Cisco NX-OS Release 7.0(3)I2(4). Click the bug ID to access the Bug Search tool and see additional information about the bug.

Table 6 Resolved Caveats in Cisco NX-OS Release 7.0(3)I2(4)

Record Number	Description
CSCur60325	EIGRP can lead to query loop leading to SIA.
CSCus73649	LACP PDUs not received by the CPU. As a results, port-channel members are suspended. Nexus# show system internal pktmgr internal event-history lcache-err. No Memory available for pcm entry ifindex <hexa ID>.
CSCut01798	Two EIGRP routers keep retransmitting SIA-Query to each other and eventually result in SIA.
CSCuw87355	When EIGRP has an internal route, whose Admin-Distance is set to be greater than that of EIGRP-External routes, EIGRP sometimes installs the External routes into RIB properly, but keeps the internal route.as successor. this affects the updates sent to the neighbors.
CSCuw88700	vxlan: vni filter doesn't work for macs are learned on peerlink.
CSCux29178	On attaching a 4q template with 4 strict priority queues to an interface or system qos, the following syslog is seen: ACLQOS-SLOTX-2-ACLQOS_FAILED: ACLQOS failure: BCM SDK API bcm_cosq_gport_sched_set(515) failed for unit 0 with error Feature unavailable(-16) This is only a cosmetic issue and wouldn't have any effect on functionality.
CSCux37880	suppress the recurring system manager core-server core-client syslog.
CSCux39771	When ifAlias contains more than 64 characters, the linkUp/Down traps will turn 65 characters in ifAlias. The correct behavior for ifAlias in linkUp/linkDown traps are restricted to 64 characters. So the symptom is 1 extra character returned thru the trap output.
CSCux56726	FD is inaccessible for the routes learned from eigrp neighbor.
CSCux58771	When EIGRP has two paths with the same ReportedDistance, but different Feasible Distance, sometimes Higher FD can remain at the top of the sorted list of paths. This affects the advertisements sent to peers. It can happen so, when we have two internal routes with different AdminDistances (can be a summary with higher AD and a regular EIGRP internal route).

Record Number	Description
CSCux64033	BGP Inconsistent flags 0x900002 when host routes add it.
CSCuy47948	The flap of one lane is affecting the other and repeated sh/no shuts is causing all the lanes to go down. PSM4 tcvrs see flaps in 50g and 25g mode.
CSCuy50611	A link goes up when inserting SFP without cables.
CSCuy68626	Remove snmp-server and rmon configuration by pipe and include option.
CSCuy81800	PBR Object-tracking with ₩"set ip default verify-availability₩" does not work.
CSCuy92527	The system encounters multiple aclqos process hap resets/crashes. The system could fail to communicate/forward traffic as a result of this problem: %$ VDC-1 %$ %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "aclqos" (PID 2826) hasn't caught signal 11 (core will be saved). %$ VDC-1 %$ %VMM-2-VMM_SERVICE_ERR: VDC1: Service SAP Aclmgr SAP for slot 1 returned error 0x41040037 (Linecard aclqos client crash) in if_bind sequence %$ VDC-1 %$ %SYSMGR-SLOT2-2-SERVICE_CRASHED: Service "aclqos" (PID 2804) hasn't caught signal 11 (core will be saved). %$ VDC-1 %$ %SYSMGR-SLOT2-2-SERVICE_CRASHED: Service "aclqos" (PID 2826) hasn't caught signal 11 (core will be saved). %$ VDC-1 %$ %VMM-2-VMM_SERVICE_ERR: VDC1: Service SAP Aclmgr SAP for slot 2 returned error 0x41040037 (Linecard aclqos client crash) in if_bind sequence
CSCuz01934	When trying to get output for "show logging last xxx" then "Internal error in displaying logfile - 40540001₩n" returned in nxapi.
CSCuz11060	Some of the commands like switchport, or no switchport, or channel-group X mode active, will take 3-4 minutes to apply. The bringup of the link takes additional time, and when it comes back up, the mac addresses are sometimes incorrectly learned on individual interfaces instead of port-channel.

Record Number	Description
CSCuz20025	Cosmetic message while configuring port-channel in conf-sync mode. When using config sync on a N9K/N3K you may see the following message: **Conf-sync mode** Nexus(config-sync-sp-if)# interface port-channel 20 !im_get_ifindex_layermode failure 40480003 0 1:port-channel20 im_get_ifindex_p2p_mode failure 0x16000013, 40480003 0 1:port-channel20: Will not see the message in normal configuration **Normal mode** Nexus(config)# interface port-channel 100 Nexus(config-if)#
CSCuz73499	802.1p vlan tag=0 frame will get dropped on an access port which belong to a vlan with VNI configured.
CSCuz87765	Cu has setup where VPC port-channel (with __8__ member interfaces) is configured towards ASR9K cluster. Links towards one ASR are in hot-stabdby mode and __3000__ vlans are configured on that port-channel. When active part of a port-channel goes down it takes around 14-17 seconds to bring online hot-standby links.
CSCuz92169	When adding vlans on a Nexus 9000 system, if there are already large numbers (2k+) of vlans present, some delay in the CLI can be seen. The configuration cannot be saved.
CSCva01339	If MTU is configured on the member interfaces of the port-channel, and then the port-channel is created, the port-channel will not be assigned the correct MTU value.
CSCva04275	When programming allowed vlan ranges on a trunk, only part of them is configured and allowed. Running config and etpm have only part of the vlans configured.
CSCva19307	Block CLI to configure vpc on a L3 port-channel.
CSCva27106	Port-channel consistency failed due to SDK resource failure.
CSCva32918	No shut on a member interface of a port-channel which is already in up state, following error message is seen: 9K-1(config)# int e1/50 9K-1(config-if)# no shut Irresponsive app timeout (300 seconds).(uuid=306)

Record Number	Description
CSCva45063	Show tech dme or dme logs will indicate following log messages on active sup as well as standby. [aaa] [DBG4] [] Failed to send ICMP Request (101) for sys/userext/tacacsext/tacacsplusprovider-x.x.x.x Where x.x.x.x is the ip address of the tacacs or radius server.
CSCva47348	An N3K running nxos.7.0 has an IPv6 BGP session to a directly connected peer on a port-channel sub-interface. The peer addresses are link local addresses. The port-channel sub-interfaces have the same IPv6 link local address configured. If the link local address on an unrelated interface is changed a TCP reset gets sent for the IPv6 BGP session. Shut/no shut on the BGP interface is needed to recover.
CSCva56193	N9500 is a Border Leaf and learns prefix 172.21.26.0/24 via BGP in vrf from a firewall outside the fabric, and learns a default route from EVPN fabric in the same vrf from another Border Leaf. N0-DC1L-BLV-ZF-SV100# bcm-shell module 1 "l3 defip show" | grep 0.0.0.0 2304 3 0.0.0.0/0 00:00:00:00:00:00 100018 0 0 0 0 n <<< 3072 Global 0.0.0.0/0 00:00:00:00:00:00 149149 0 0 0 0 y When 9500 received packet from L3Vni destined to 172.21.26.0/24, it incorrectly forwards the packet using the default route programmed in VRF, instead of sending it to the fabric module that causes the packet to go into a loop.
CSCva64357	By default, the VSH daemon has console and vty exec-timeout turned off.
CSCva65202	The objects of type macAddress are shown as long ascii strings, instead of 6 byte hexa decimal values of the MAC address.
CSCva75326	LC would reset due to sysmgr resetting vntagc due to missing hearbeats. The following errors could appear in show logging nvram: VDC-1 %$ %SYSMGR-SLOT7-2-SERVICE_CRASHED: Service "vntagc" (PID 2816) hasn't caught signal 6 (core will be saved). VDC-1 %$ %MODULE-2-MOD_DIAG_FAIL: Module 7 reported failure due to Service on linecard had a hap-reset in device DEV_SYSMGR (device error 0x402) VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 7 detected Module-Type 48x1/10G SFP+ 4x40G Ethernet Module Model N9K-X9564PX VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 7 powered up
CSCva85104	Change HA policy of vntagc from reset to statuful. The vntagc crashes and related modules reset which cause route reconvergence again and packet loss.

Record Number	Description
CSCva90112	The FEX is running fine as of now. But they found that there was a ?fex? crash from the logfile. The customer observed this crash 2 times so far (during these 150 days). No impact observed.

Resolved PSIRT CVEs—Cisco NX-OS Release 7.0(3)I2(4)

Table 8 Open Caveats in Cisco NX-OS Release 7.0(3)I2(4) lists the Resolved PSIRT CVEs in Cisco NX-OS Release 7.0(3)I2(4). Click the bug ID to access the Bug Search tool and see additional information about the bug.

Table 7 Resolved PSIRT CVEs in Cisco NX-OS Release 7.0(3)I2(4)

Bug ID	Description
CSCuz92661	Cisco MDS 9000 Series Multilayer Switches, Cisco Nexus 3000 Series Switches, Cisco Nexus 5000 Series Switches, Cisco Nexus 6000 Series Switches, Cisco Nexus 7000 Series Switches, and Cisco Nexus 9000 Series Switches, include a version of ntpd that is affected by the vulnerabilities identified by the Common Vulnerability and Exposures (CVE) IDs: CVE-2016-4957, CVE-2016-4953, CVE-2016-4954, CVE-2016-4955, CVE-2016-4956 And disclosed in: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160603-ntpd One or more of the listed CVE ids affects this product.

Open Caveats—Cisco NX-OS Release 7.0(3)I2(4)

Table 8 lists the open caveats in Cisco NX-OS Release 7.0(3)I2(4). Click the bug ID to access the Bug Search tool and see additional information about the bug.

Table 8 Open Caveats in Cisco NX-OS Release 7.0(3)I2(4)

Bug ID	Description
CSCun26726	Assertion message will be seen on decoding HSRP frames, when the switch is using MD5 method for authentication.
CSCun34856	If a QoS policy is applied on a VLAN that is not active on any ports in the system, and if the TCAM Region for VLAN QoS is not carved, the error is not reported right away and is reported when the first port is brought up. Also, all the VLANs on that port are error-disabled instead of the VLAN that is affected.

Bug ID	Description
CSCuq03168	Microsoft NLB traffic being routed into the destination VLAN experiences packet loss.
CSCur30555	Show policy-map type queuing does not show statistics for FEX HIF interfaces.
CSCur37816	When QoS Lite TCAM is configured, policer violated statistics shown as part of "show policy-map interface ...", the commands are reported as 0 instead of NA (Not-Applicable).
CSCur46879	When ASCII replay is done with tunnel config, tunnels may flap.
CSCur59482	Policer action with CIR as percentage, is not supported when QoS policy of type "qos" is applied with "no-stats" keyword.
CSCur61647	Even though there are no QoS classification policies currently active on any of the FEX HIF interfaces, "show incompatibility ..." command still reports FEX QoS incompatibility during downgrade from 3.2 to earlier versions of software.
CSCur87839	Traffic cannot be PBRed if the "set ip next-hop" reachability is across the VPC peer-link due to local VPC-leg down.
CSCus06693	ERSPAN session goes to error state if the configured erspan destination ip is a port-channel sub-interface. switch# show monitor Session State Reason Description ------- ----------- ---------- ---------- 1 error Generic error switch#
CSCus07061	When a remote end of a vPC port channel member is shut down, the local end takes ~10 seconds to shutdown. This is only seen when the port channel is 'active', i.e., has LACP enabled. This issue is not seen when the local end of the port channel member is shut or when the cable is pulled from the remote end.
CSCus58475	Vntag-mgr timeout after changing vlans for range of 20 vPC port-channels.

Bug ID	Description
CSCus63613	When a user reloads the active supervisor, the standby supervisor also reloads. During the reload process, the Service Policy Manager (SPM) cannot send data to the standby supervisor. A syslog is observed, notifying the active supervisor that the Service Policy Manager (SPM) has not successfully updated its data base to the standby supervisor. The active supervisor reloads the standby supervisor again, and the standby supervisor eventually reaches a good standby state.
CSCuu31392	ERSPAN packets are dropped on the intermediate switches if more than one ERSPAN session resolves over 40 Gig uplinks on a TOR.
CSCuu33640	An ITD policy is shown in "no shut" state. However, no policy is actually applied to the ingress policy if an invalid ACL is used for "exclude."
CSCuv90152	Packets are accepted on hifpc member in suspended state.
CSCuv96382	For single label mpls/stripped tap-agg packets, when "mpls strip dest-mac xxxx.xxxx.xxxx" CLI is configured dmac is not re-written on modular (EOR) setup. The same will work on TOR.
CSCuw02188	If both vrf-context creation and vrf-aware-nat are configured in parallel, then, NAT might not be able to program these VRF-NAT entries.
CSCux15156	When policy-map is copied through "qos copy policy-map....", the newly created policy-map cannot be modified or deleted.
CSCuy96592	NXAPI may return incorrect return values when deleting an entity that does not exist.
CSCuz92169	When adding vlans on a N9K system, where already a large amounts (2K+) of vlans are present, some delay in the CLI can be seen. Configuration cannot be saved.

Upgrade Instructions

To perform a software upgrade, follow the installation instructions in the *Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide*.

Note:

- When upgrading to 7.0(3)I2(4), Guest Shell automatically upgrades from 1.0 to 2.0. In the process, the contents of the guest shell 1.0 root filesystem will be lost. To keep from losing important content, copy any needed files to /bootflash or an off-box location before upgrading to 7.0(3)I2(4).
- Performing a disruptive upgrade from Release 7.0(3)I2(2) to Release 7.0(3)I2(4) causes VRFs and VLANs that were created using **auto-pull** in Release 7.0(3)I2(2) to become inaccessible. Attempts at accessing the VRFs or VLANs will result in the following error message: Irresponsive app timeout (300 seconds).(uuid=380)

Downgrade Instructions

Disable the Guest Shell if you need to downgrade from Cisco NX-OS Release 7.0(3)I2(4) to an earlier release.

Note:

- Downgrading with PVLANs configured is only supported with 6.1(2)I3(4x) releases.
- For a boot-variable change and reload to a 7.0(3)I1(1x) release, the PVLAN process is not brought up, and the PVLAN ports are kept down. For a boot-variable change to the 6.1(2)I3(3) release and earlier, an ASCII replay will be tried, but feature PVLANs and other PVLAN configurations will fail.

Software Maintenance Upgrades

For information about software maintenance upgrades, see the "Performing Software Maintenance Upgrades" section in the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide.

Note: If you perform a software maintenance upgrade (SMU) and later upgrade your device to a new Cisco NX-OS software release, the new image will overwrite both the previous Cisco NX-OS release and the SMU package file.

Limitations

This section lists limitations related to Cisco NX-OS Release 7.0(3)I2(4).

- For the NX-OS 7.0(3)I2(4) release, the VXLAN network identifier (VNID) 16777215 is reserved and should not be configured explicitly.
- Generation 1 100G line cards (N9K-X9408PC-CFP2) and generic expansion modules (N9K-M4PC-CFP2) only support 40G flows.
- N9K-X9408PC-CFP2 line cards do not support port channeling.
- In-Service Software Upgrades (ISSU) are not supported on Cisco Nexus 9000 Series switches.

- CoPP (Control Plane Policing) cannot be disabled. If you attempt to disable it in Cisco NX-OS Release 7.0(3)I3(1), an error message appears. In previous releases, attempting to disable CoPP causes packets to be rate limited at 50 packets per seconds.
- Skip CoPP policy option has been removed from the Cisco NX-OS initial setup utility because using it can impact the control plane of the network.
- hardware profile front portmode command is not supported on the Cisco Nexus 9000 Series switches.
- PV (Port VLAN) configuration through an interface range is not supported.
- Layer 3 routed traffic for missing Layer 2 adjacency information is not flooded back onto VLAN members of ingress units when the source MAC address of routed traffic is a non-VDC (Virtual Device Context) MAC address. This limitation is for hardware flood traffic and can occur when the SVI (Switched Virtual Interface) has a user-configured MAC address.
- neighbor-down fib-accelerate command is supported in a BGP (Border Gateway Protocol)-only environment.
- Uplink modules should not be removed from a Cisco Nexus 9300 Series switch that is running Cisco NX-OS Release 7.0(3)I2(4). The ports on uplink modules should be used only for uplinks.
- PortLoopback and BootupPortLoopback tests are not supported.
- PFC (Priority Flow Control) and LLFC (Link-Level Flow Control) are supported for all Cisco Nexus 9300 and 9500 Series hardware except for the 100G 9408PC line card and the 100G M4PC generic expansion module (GEM).
- FEXes configured with 100/full-duplex speed, without explicitly configuring the neighboring device with 100/full-duplex speed, will not pass data packet traffic properly. This occurs with or without the link appearing to be "up."
  - **no speed**–Auto negotiates and advertises all speeds (only full duplex).
  - **speed 100**–Does not auto negotiate; pause cannot be advertised. The peer must be set to not auto negotiate (only 100 Mbps full duplex is supported).
  - **speed 1000**–Auto negotiates and advertises pause (advertises only for 1000 Mbps full duplex).
- Eight QoS groups are supported only on modular platforms with the Cisco Nexus 9300 N9K-M4PC-CFP2 uplink module, and the following Cisco Nexus 9500 Series line cards:
  - N9K-X9636PQ
  - N9K-X9464PX
  - N9K-X9464TX
  - N9K-X9432PQ

- Cisco NX-OS Release 7.0(3)I2(4) supports flooding for Microsoft Network Load Balancing (NLB) unicast mode on Cisco Nexus 9500 Series switches but not on Cisco Nexus 9300 Series switches. NLB is not supported in max-host system routing mode. NLB multicast mode is not supported on Cisco Nexus 9500 or 9300 Series switches.

Note: To work around the situation of Unicast NLB limitation, we can statically hard code the ARP and MAC address pointing to the correct interface. Please refer to bug ID CSCuq03168 in detail in the "Open Caveats—Cisco NX-OS Release 7.0(3)I2(4)" section.

- TCAM resources are not shared when:
  - Routed ACL (Access Control List) is applied to multiple SVIs in the egress direction
  - Applying VACL (VLAN ACL) to multiple VLANs
- Cisco Nexus 9000 Series switch hardware does not support range checks (layer 4 operators) in egress TCAM. Because of this, ACL/QoS policies with layer 4 operations-based classification need to be expanded to multiple entries in the egress TCAM. Egress TCAM space planning should take this limitation into account.
- Applying the same QoS policy and ACL on multiple interfaces requires applying the **qos-policy** with the **no-stats** option to share the label.
- Multiple port VLAN mappings configured on an interface during a rollback operation causes the rollback feature to fail.
- The following switches support QSFP+ with the QSA (QSFP to SFP/SFP+ Adapter) (40G to 10G QSA):
  - N9K-C93120TX
  - N9K-C93128TX
  - N9K-C9332PQ
  - N9K-C9372PX
  - N9K-C9372PX-E
  - N9K-C9372TX
  - N9K-C9396PX
  - N9K-C9396TX

Note: The Cisco Nexus 9300 support for the QSFP+ breakout has the following limitations:

- Only 10G can be supported using QSA on 40G uplink ports on N9300 switches in NX-OS.
- 1G with QSA is not supported.

- For the Cisco Nexus 9332PQ switch, all ports except 13-14 and 27-32 can support breakout
- All ports in the QSA speed (see the configuration guide) group must operate at the same speed

---

- The following switches support the breakout cable (40G ports to 4x10G ports):
  - N9K-C9332PQ
  - N9K-X9436PQ
  - N9K-X9536PQ
- Weighted ECMP (Equal-Cost Multi-Path) Nexus 3000 feature is not supported on the Cisco Nexus 9000 Series switch.
- Limitations for ALE (Application Link Engine) uplink ports are listed at the following URL:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/ale_ports/b_Limitations_for_ALE_Uplink_Ports_on_Cisco_Nexus_9000_Series_Switches.html

Guidelines and Limitations for Private VLANs

This section provides guidelines and limitations for configuring private VLANs.

- Configuring Private VLANs
- Secondary and Primary VLAN Configuration
- Private VLAN Port Configuration
- Limitations with Other Features

Configuring Private VLANs

Private VLANs have the following configuration guidelines and limitations:

- Private VLANs must be enabled before the device can apply the private VLAN functionality.
- VLAN interface feature must be enabled before the device can apply this functionality.
- VLAN network interfaces for all VLANs that you plan to configure as secondary VLANs should be shut down before being configured.
- When a static MAC is created on a regular VLAN, and then that VLAN is converted to a secondary VLAN, the Cisco NX-OS maintains the MAC that was configured on the secondary VLAN as the static MAC.

- Private VLANs support port modes as follows:
  - Promiscuous
  - Promiscuous trunk
  - Isolated host
  - Isolated host trunk
  - Community host
- When configuring PVLAN promiscuous or PVLAN isolated trunks, it is recommended to allow non-private VLANs in the list specified by the **switchport private-vlan trunk allowed id** command.
- Private VLANs are mapped or associated depending on the PVLAN trunk mode.
- Private VLANs support the following:
  - PACLs (Port Access Control Lists)
  - RACLs (Router Access Control Lists)
  - Layer 2 forwarding
  - PVLAN across switches through a regular trunk port
- Private VLANs support SVIs as follows:
  - SVI allowed only on primary VLANs
  - Primary and secondary IPs on the SVI
  - HSRP (Hot Standby Router Protocol) on the primary SVI
- Private VLANs support STP as follows:
  - RSTP (Rapid Spanning Tree Protocol)
  - MST (Multiple Spanning Tree)
- Private VLANs port mode is not supported on the following:
  - 40G interfaces of the Cisco Nexus C9396PX or Cisco Nexus C93128TX
  - Cisco Nexus 3164Q
- Private VLANs do not provide port mode support for the following:
  - Port channels

  - vPCs (Virtual Port Channels) interfaces

- Private VLANs do not provide support on breakout.
- Private VLANs do not provide support for the following:
  - IP multicast or IGMP snooping
  - DHCP (Dynamic Host Channel Protocol) snooping
  - PVLAN QoS
  - VACLs
  - VLAN Trunk Protocol (VTP)
  - Tunnels
  - VXLANs
  - SPAN (Switch Port Analyzer) when the source is a PVLAN VLAN
- Shared interfaces cannot be configured to be part of a private VLAN. For more details, see the *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*.
- The Cisco NX-OS CLI allows configuring multiple isolated VLAN configurations per PVLAN GROUP. However, such a configuration is not supported. A PVLAN group can have at most one isolated VLAN.

Secondary and Primary VLAN Configuration

Follow these guidelines when configuring secondary or primary VLANs in private VLANs:

- Default VLANs (VLAN1), or any of the internally allocated VLANs, cannot be configured as primary or secondary VLANs.
- VLAN configuration (config-vlan) mode must be used to configure private VLANs.
- Primary VLANs can have multiple isolated and community VLANs associated with it. An isolated or community VLAN can be associated with only one primary VLAN.
- Private VLANs provide host isolation at Layer 2. However, hosts can communicate with each other at Layer 3.
- PVLAN groups can have one isolated VLAN at most. Multiple isolated VLAN configurations per primary VLAN configurations are not supported.
- When a secondary VLAN is associated with the primary VLAN, the STP parameters of the primary VLAN, such as bridge priorities, are propagated to the secondary VLAN. However, STP parameters do not necessarily propagate

to other devices. You should manually check the STP configuration to ensure that the spanning tree topologies for the primary, isolated, and community VLANs match exactly so that the VLANs can properly share the same forwarding database.

- For normal trunk ports, note the following:
  - Separate instances of STP exist for each VLAN in the private VLAN.
  - STP parameters for the primary and all secondary VLANs must match.
  - Primary and all associated secondary VLANs should be in the same MST instance.
- For non-trunking ports, STP is aware only of the primary VLAN for any private VLAN host port; STP runs only on the primary VLAN for all private VLAN ports.

Note: Cisco recommends that you enable BPDU Guard on all ports that you configure as a host port; do not enable this feature on promiscuous ports.

- Private VLAN promiscuous trunk ports allow you to configure a maximum of 16 private VLAN primary and secondary VLAN pairs on each promiscuous trunk port.
- For private VLAN isolated trunk ports, note the following:
  - You can configure a maximum of 16 private VLAN primary and secondary VLAN pairs on each isolated trunk port.
  - The native VLAN must be either a normal VLAN or a private VLAN secondary VLAN. You cannot configure a private VLAN primary port as the native VLAN for a private VLAN isolated trunk port.
- Downgrading a system that has private VLAN ports configured requires unconfiguring the ports.
- Before configuring a VLAN as a secondary VLAN, you must shut down the VLAN network interface for the secondary VLAN.

Private VLAN Port Configuration

Follow these guidelines when configuring private VLAN ports:

- Use only the private VLAN configuration commands to assign ports to primary, isolated, or community VLANs.
- Layer 2 access ports that are assigned to the VLANs that you configure as primary, isolated, or community VLANs are inactive while the VLAN is part of the private VLAN configuration. Layer 2 trunk interfaces, which may carry private VLANs, are active and remain part of the STP database.
- Deleting a VLAN used in the private VLAN configuration causes private VLAN ports (promiscuous ports or host ports, not trunk ports) that are associated with the VLAN to become inactive.

Limitations with Other Features

Consider these configuration limitations with other features when configuring private VLANs:

Note: In some cases, the configuration is accepted with no error messages, but the commands have no effect.

- Ensure consistent PVLAN type, states and configuration across vPC peers. There is currently no PVLAN consistency check for vPC. Inconsistent PVLAN configs across vPV peers may end up in incorrect forwarding and impacts.
- Private VLAN ports can be configured as SPAN source ports.
- Private VLAN host or promiscuous ports cannot be SPAN destination ports.
- Destination SPAN ports cannot be isolated ports. However, a source SPAN port can be an isolated port.
- After configuring the association between the primary and secondary VLANs:
  - Dynamic MAC addresses that learned the secondary VLANs are aged out.
  - Static MAC addresses for the secondary VLANs cannot be created.
- After configuring the association between the primary and secondary VLANs and deleting the association, all static MAC addresses that were created on the primary VLANs remain on the primary VLAN only.
- In private VLANs, STP controls only the primary VLAN.

Note: See the *Cisco Nexus 9000 Series NX-OS Security Configuration Guide* for information on configuring static MAC addresses.

Unsupported Features

This section lists features that are not supported in the current release.

- VXLAN
- DHCP
- FEX
- Cisco Nexus 9408 Line Card and 9300 Series Leaf Switches
- Other Unsupported Features

VXLAN

This section lists VXLAN features that are not supported.

- TX SPAN (Switched Port Analyzer) for VXLAN traffic is not supported for the access-to-network direction.
- QoS classification is not supported for VXLAN traffic in the network-to-access direction.
- QoS buffer-boost is not applicable for VXLAN traffic.
- ACL and QoS for VXLAN traffic in the network-to-access direction is not supported.
- Native VLANs for VXLAN are not supported. All traffic on VXLAN Layer 2 trunks needs to be tagged.
- Consistency checkers are not supported for VXLAN tables.
- VXLAN routing and VXLAN Bud Nodes features on the 3164Q platform are not supported.
- DHCP snooping and DAI features are not supported on VXLAN VLANs.
- IGMP snooping is not supported on VXLAN VLANs.
- Static MAC pointing to remote VTEP is not supported with BGP EVPN.

VXLAN ACL Limitations

The following ACL related features are not supported:

- Ingress RACL that is applied on an uplink Layer 3 interface that matches on the inner or outer payload in the network-to-access direction (decapsulated path)
- Egress RACL that is applied on an uplink Layer 3 interface that matches on the inner or outer payload in the access-to-network direction (encapsulated path)
- Egress VACL for decapsulated VXLAN traffic

We recommend that you use a PACL or VACL on the access side to filter out traffic entering the overlay network.

DHCP

DHCP subnet broadcast is not supported.

FEX

- VTEP connected to FEX host interface ports is not supported.
- FEX is supported only on the Cisco Nexus 9332PQ, 9372PX, 9372PX-E and 9396PX and 9500 switches. It is not supported on the other Cisco Nexus 9300 Series.
- Cisco Nexus 9300 Series switches do not support FEX on uplink modules (ALE).

- FEX vPC is not supported between any model of FEX and the Nexus9300 (leaf switch) and 9500 Switches (EOR) as the parent switches
- ASCII replay with FEX needs be done twice for HIF configurations to be applied. The second time should be done after the FEXs have come up.
- IPSG is not supported on FEX ports.

Cisco Nexus 9408 Line Card and 9300 Series Leaf Switches

The following features are not supported for the Cisco Nexus line card (N9K-X9408PC-CFP2) and Cisco Nexus 9300 Series leaf switches with generic expansion modules (N9K-M4PC-CFP2):

- Breakout ports
- Port-channel (No LACP)
- vPC
- MCT (Multichassis EtherChannel Trunk)
- FEX
- PTP (Precision Time Protocol)
- PFC/LLFC
- 802.3x
- PVLAN
- Storm Control
- VXLAN access port.
- SPAN destination/ERSPAN destination IP
- Shaping support on 100g port is limited

Other Unsupported Features

The following lists other features not supported in the current release:

- Due to a Poodle vulnerability, SSLv3 is no longer supported.
- The Cisco Nexus 9300 Series switches do not support the 64-bit ALPM routing mode.

- IPSG is not supported on the following:
  - The last 6 40G physical ports on the 9372PX, 9372TX, and 9332PQ switches
  - All 40G physical ports on the 9396PX, 9396TX, and 93128TX switches

Related Documentation

The entire Cisco Nexus 9000 Series NX-OS documentation set is available at the following URL:

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

The Cisco Nexus 3164Q Switch - Read Me First is available at the following URL:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3164/sw/6x/readme/b_Cisco_Nexus_3164Q_Switch_Read_Me_First.html

The Cisco Nexus 31128PQ Switch - Read Me First is available at the following URL:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus31128/sw/readme/b_Cisco_Nexus_31128PQ_Switch_Read_Me_First.html

New Documentation

There is no new documentation for this release.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus9k-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation 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

Open a service request online at:

https://tools.cisco.com/ServiceRequestTool/create/launch.do

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.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Cisco Nexus 9000 Series NX-OS Release Notes, Release 7.0(3)I2(4)