Cisco Nexus 9000 Series NX-OS Release Notes, Release 9.3(8)

This document describes the features, issues, and exceptions of Cisco NX-OS Release 9.3(8) software for use on Cisco Nexus 9000 Series switches.

Note: The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

The following table lists the changes to this document.

Table 1. Changes to this Document

Date	Description
August 6, 2021	Cisco NX-OS Release 9.3(8) became available.
October 5, 2021	Added details about 'Thousand Eyes (TE) Integration' feature in the 'New and Enhanced Software Features' section.

New and Enhanced Software Features

New Features	
Feature	**Description**
Thousand Eyes (TE) Integration	Introduced Thousand eyes integration support with Cisco Nexus 9000 Series switches. For product overview look at: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/at-a-glance-c45-2431016.html It is a must to install the following general SMU when TE integration is performed: nxos.CSCvz52812-n9k_ALL-1.0.0-9.3.8.lib32_n9000.tar For SMU installation please refer to the following guide: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/system-management/b-cisco-nexus-9000-series-nx-os-system-management-configuration-guide-93x/b-cisco-nexus-9000-series-nx-os-system-management-configuration-guide-93x_chapter_010111.html

The enhanced feature listed below are existing features introduced in earlier releases but enhanced with new support in Cisco NX-OS Release 9.3(8).

Enhanced Features	
Feature	**Description**
SNMP Salt Hash	With this enhancement the hashed passwords are integrated with salt to generate the final digest password to avoid security concerns for SNMPv3 users. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x) .

New Hardware Features

There are no new hardware features introduced in Cisco NX-OS Release 9.3(8).

Open Issues

Bug ID	Description
CSCvy62164	Headline: Crash in Nexus 9000 Fatal Module Error when downgrading - service port_client hap reset Symptoms: During downgrade from 9.3.7 to 9.3.6, vPC peer switch reloads due to " port_client" service crash: Service: port_client Description: Port Client Daemon Executable: /lc/isan/bin/port_client Workarounds: No workaround. The switch is reloaded when the issue is hit.
CSCvy90363	Headline: 9500-R :: Feature ptp causes the spine switch to intercept unicast ARP replies in VxLAN fabric Symptoms: The L2 adjacent host are not able to resolve each other's ARP across VxLAN fabric. The broadcasted ARP reply is flooded correctly and reaches all hosts, however the unicast ARP reply is lost inside of the fabric. In fact the ARP replies are redirected to SPINE CPU instead of being forwarded.

Bug ID	Description
	Other unicast communication works fine (for example - when we configure static ARPs). Workarounds: • Disable 'feature nv overlay' on spine. This will avoid this problem and also will ensure better hashing of packets over ECMP links. • Enable " arp suppression" or • Remove " feature ptp" from the spines. After doing so, " reload" or " reload ascii" is required to restore connectivity.
CSCvy82116	Headline: Vxlan unicast traffic drop due to mac learnt on FEXAA HIFVPC getting deleted on vpc primary. Symptoms: Mac address behind FEX AA VPC is getting deleted on primary vpc peer after reload of switch (primary reloaded followed by secondary). On secondary the MAC entry is present. This is causing VXLAN unicast traffic to get dropped. Workarounds: • Flap the HIFVPC interface. • Delete the particular mac address and allow mac to be learnt again.
CSCvz25260	Headline: NXOS - Additional prompt showing up when running guest-shell command. Symptoms: Running guestshell prompts for password which is unexpected after upgrading from switch with guestshell version 2.10 to NXOS version 9.3(8) or 10.1(2). Workarounds: Remove and re-enable guestshell after the upgrade.

Resolved Issues

Bug ID	Description
CSCvz05943	Headline: 100M link is down on N9K-C93180YC-FX side and up on peer side after port flap on post ND ISSU. Symptoms: Link may not come up after ISSU if you have a 100mb FX xcvr. Workarounds: You need to have physical OIR of 100mb FX xcvr to recover or you need to reload the switch.
CSCvx61330	Headline: Nexus 9000 aclqos cores - ERSPAN w/source VLAN mapped to VNI on certain ports Symptoms: Gen1 Nexus 9000 models may see a core file from the aclqos process when trying to do an ERSPAN on a VLAN mapped to a VNI, using ports from specific ASICs. Workarounds: None
CSCvx60758	Headline: Bringing up SPAN session silently fails when sFlow data sources are configured. Symptoms: A Nexus 9000 series switch configured with sFlow data sources is not able to administratively bring SPAN sessions online. This is the expected behaviour. However, no error message or feedback to the user is presented if one attempts to bring a SPAN session up while an sFlow data source is configured. Workarounds: There is no known workaround for this issue. This defect introduces an error message to the CLI of the switch when one attempts to bring a SPAN session up while sFlow data sources are configured on the switch.
CSCvy19448	Headline: SSH connection rejected with FIPS enabled using any SSH key. Symptoms: SSH connections will be rejected if the FIPS feature is enabled on release 9.3(7). Workarounds: Downgrade to release 9.3(6) or earlier, or upgrade to release 10.1(1) or later. There is a general available SMU to address this issue on release 9.3(7): https://software.cisco.com/download/home/286314783/type/286278856/release/9.3(7)

Bug ID	Description
	SMU installation instructions: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/system-management/b-cisco-nexus-9000-series-nx-os-system-management-configuration-guide-93x/b-cisco-nexus-9000-series-nx-os-system-management-configuration-guide-93x_chapter_010111.html
CSCvy24198	Headline: L2FM process crash after l2fm_mcec_get_mac_handler Symptoms: The L2FM process crashes after the vPC comes online. Workarounds: Disconnect the vPC peer link and upgrade both peers separately. After they are upgraded and the vPC is connected back, they should remain stable.
CSCvx60909	Headline: Installing multiple SMUs do not remain committed after reload Symptoms: When installing multiple SMUs which includes nxos.CSCvx18710-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000.tar (tar includes nxos.CSCvx18710_lc_x86-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000.rpm and nxos.CSCvx18710_lc_x86-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000.rpm), they do not remain committed after reload. Workarounds: Please use SMU 1.0.1 version for CSCvx18710. nxos.CSCvx18710-n9k_ALL-1.0.1-7.0.3.I7.9.lib32_n9000.rpm If 1.0.0 version (nxos.CSCvx18710-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000.tar) was previously installed then it needs to be deactivated, commit and remove before installing the new one using the below procedure: Step 1: Check if 1.0.0 is active switch# show install active Boot Image: NXOS Image: bootflash:/nxos.7.0.3.I7.9.bin Active Packages: nxos.CSCvx18710-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000 nxos.CSCvx18710_lc_x86-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000 Step 2: If 1.0.0 version is active, then deactivate it. This will require reload. switch# install deactivate nxos.CSCvx18710-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000 nxos.CSCvx18710_lc_x86-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000 ========== !!!WARNING!! This is a reload patch and system will be reloaded if you proceed with patch operation. ========== Do you want to continue (y/n)?: [n] y [#########################] 100% Step 3: Check show install inactive and make sure 1.0.0 version have inactive status and then do install commit Switch# show install inactive Boot Image: NXOS Image: bootflash:/nxos.7.0.3.I7.9.bin Inactive Packages: nxos.CSCvx18710-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000 nxos.CSCvx18710_lc_x86-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000 switch# install commit [#########################] 100% Step 4: Install remove 1.0.0 version switch# install remove nxos.CSCvx18710-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000 Proceed with removing nxos.CSCvx18710-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000? (y/n)? [n] y [#########################] 100%

Bug ID	Description
	switch# install remove nxos.CSCvx18710_lc_x86-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000 Proceed with removing nxos.CSCvx18710_lc_x86-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000? (y/n)? [n] y [#######################] 100% Step 5: Download 1.0.1 version and install add,activate,commit. This doesnt require reload infra-3164-2# install add nxos.CSCvx18710-n9k_ALL-1.0.1-7.0.3.I7.9.lib32_n9000.rpm activate Adding the patch (/nxos.CSCvx18710-n9k_ALL-1.0.1-7.0.3.I7.9.lib32_n9000.rpm) [#######################] 100% Activating the patch (/nxos.CSCvx18710-n9k_ALL-1.0.1-7.0.3.I7.9.lib32_n9000.rpm) [#######################] 100% switch# install commit [#######################] 100%
CSCvy41115	Headline: L2rib Process Crashes with a Hap Reset due to a Segmentation Fault Symptoms: A series of back-to-back L2RIB crashes may occur, followed by a reload of the switch. Workarounds: Disabling ARP suppression may help reduce the number of MAC-IP entries, and therefore avoid the crash.
CSCvy78329	Headline: n9k/ipv6: low memory in MTS due to high ICMPV6 control messages after large host move Symptoms: High MTS usage in below queues, slow response and possible crash on various processes due to no memory in MTS. High MTS queues: icmpv6/ICMPV6-CTRL netstack/IP MTS queue Workarounds: NA
CSCvu69869	Headline: Configuring " vpc role preempt" will cause vPCs with port-type network to go into BKN state. Symptoms: Nexus switch will show vPC port-channels that are configured for spanning-tree port-type network in BKN state after configuring " vpc role preempt" . Workarounds: Shut, no shut of the affected links on new vpc secondary should recover it.
CSCvw15473	Headline: MPLS LDP IGP SYNC is not working properly with ISIS. Symptoms: switch# show mpls ldp igp sync Ethernet1/1: LDP configured; LDP-IGP Synchronization enabled. Sync status: sync achieved; peer reachable. Sync delay time: 0 seconds (0 seconds left) IGP holddown time: infinite. Peer LDP Ident: 20.20.4.4:0 (GR) IGP enabled: isis-4766 Ethernet1/11: LDP not configured; LDP-IGP Synchronization enabled. Sync status: sync not achieved; peer reachable. Sync delay time: 0 seconds (0 seconds left) IGP holddown time: infinite. GR-only Reachability: 20.20.1.1:0 IGP enabled: isis-4766 Workarounds: NA
CSCvx02142	Headline: ISIS does not propagate topology information to MPLS-TE depending on TLV order. Symptoms: Some routers are not seen in MPLS-TE topology while ISIS is used as IGP.

Bug ID	Description
	Workarounds: NA
CSCvx93145	Headline: Topology information is not propagated from ISIS to MPLS TE when authentication configured for ISIS Symptoms: MPLS TE topology (`show mpls traffic-eng topology`) contains no information on other expected nodes, and on those present in ISIS topology. Workarounds: Configure ISIS authentication on per-interface level and remove it from " router isis" section.
CSCvy28073	Headline: PIM crashes after configuring - ip pim rp-candidate Symptoms: The switch reloaded due to the following reason: Service: pim hap reset And there is a PIM core file in the output of - show core. Workarounds: None
CSCvw02706	Headline: DEVICE_TEST-2-AUTHENTICATION_FAIL: Module 27 ACT2-Instance-2 Symptoms: A Nexus 9500 switch may report the following in the log: Nexus9500(config)# 2020 Oct 8 09:09:50 %$ %DEVICE_TEST-2-AUTHENTICATION_FAIL: Module 27 ACT2-Instance-2: The system integrity check has failed during the boot-up sequence. Please contact Cisco's Technical Assistance Center for more information (message repeated 1 time) Workarounds: None
CSCvw29606	Headline: platform service may crash Symptoms: The Platform Manager service may crash on a Nexus switch. The following may be reported in the log:`show logging log`2020 Oct 28 21:28:14 %SYSMGR-3-HEARTBEAT_FAILURE: Service " Platform Manager" sent SIGABRT for not setting heartbeat for last 4 periods. Last heartbeat 95.59 secs ago.2020 Oct 28 21:34:35 %SYSMGR-2-HAP_FAILURE_SUP_RESET: Service " Platform Manager" in vdc 1 has had a hap failure2020 Oct 28 21:43:01 %SYSMGR-2-STANDBY_BOOT_FAILED: Standby supervisor failed to boot up. Workarounds: None
CSCvw41589	Headline: Nexus 3K/9K - VRRP with object tracking leading to Primary-Primary Symptoms: Having a track object configured under VRRP to decrement the priority. 1:a) when track does down it decrements the priority as expected b) When track comes up the priority is not returning to the default value 2:a) when track does down on VRRP MASTER so as to trigger a state change to BACKUP as priority is decremented, priority is decremented twice for vrrp group. b) When track comes up the priority is not returning to the default value Workarounds: Change the VRRP priority to restore the value+ remove and reapply the vrrp track configuration.
CSCvw42667	Headline: dhcp_snoop process may crash Symptoms: The dhcp_snoop process may crash on a Nexus switch. The following would be seen in the log:`show logging log`2021 Feb 17 11:24:53.667 %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service " dhcp_snoop" (PID 15642) hasn't caught signal 11 (core will be saved).2021 Feb 17 11:24:57.551 %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service " dhcp_snoop" (PID 12062) hasn't caught signal 11 (core will be saved).2021 Feb 17 11:24:57.553 %$ VDC-1 %$ %SYSMGR-2-HAP_FAILURE_SUP_RESET: Service " dhcp_snoop" in vdc 1 has had a hap failure. Workarounds: None
CSCvx25283	Headline: msdp owned (s,g) mroute does not inherit pim oif from (*,g) Symptoms: Receivers are not getting multicast stream. MSDP owned (S,G) mroute sync'd by MSDP peer/RP/Catalyst to RP/Nexus, does not inherit OIF from (*,G).Issue is specific to few groups, some groups are working fine too.

Bug ID	Description
	Workarounds: Adding static OIF (S,G) for outgoing interface. interface Ethernet x/y ip igmp static-oif multicast_group source multicast_sender_ip
CSCvx52141	Headline: NX-OS can't resolve IPv6 static recursive route with next-hop over EVPN Symptoms: Software forwarding fails for IPv6 addresses reachable via Static Route with next hop reachable over VXLAN EVPN. Example: ping6 will fail " No route to host" or Request timed out. Packets originated from software side NX-OS fail to leave the switch. Workarounds: Remove the static-route and redistribute EVPN route-type 5 static route from VTEP where next-hop is locally attached. Or, use static route with HMM tracking, in this case static-route can be used on all VTEP's with track object:conf tvrf context tenant-1 ipv6 route 2001:db8:0:547::1/128 2001:db8:8:28::10 track 211track 211 ipv6 route 2001:db8:8:28::10/128 reachability hmm vrf member tenant-1static route is active only on VTEP with next-hop learnt as HMM route.
CSCvx56128	Headline: VRF stuck in delete pending because BGP is not dropping the MTS_OPC_L3VM Symptoms: After vrf get deleted from router configuration under rare circumstances it can stuck in deletion state. This prevent user from re-configuring the vrf back and using it. Workarounds: Reload box or use different vrf name.
CSCvx57867	Headline: NVE:Snmpwalk/bulk on ciscoIfExtensionMib detects OID not increasing error & walk aborts. Symptoms: SNMPWalk on 1.3.6.1.2.1.2.2.1.2 (IF-MIB::ifDescr) does not show subinterfaces higher than 511 in case interface breakout is configured or nve is configured.$ snmpwalk -v2c -c test switch1<snippet>IF-MIB::ifIndex.1543525976 = INTEGER: 1543525976IF-MIB::ifIndex.1509949440 = INTEGER: 1509949440Error: OID not increasing: IF-MIB::ifIndex.1543525976Another example when NVE interface is configured:$snmpwalk -v 2c -c test switch1 1.3.6.1.2.1.2.2.1.1IF-MIB::ifIndex.436237312 = INTEGER: 436237312IF-MIB::ifIndex.436237824 = INTEGER: 436237824IF-MIB::ifIndex.1543525976 = INTEGER: 1543525976IF-MIB::ifIndex.1224736769 = INTEGER: 1224736769Error: OID not increasing: IF-MIB::ifIndex.1543525976>= IF-MIB::ifIndex.1224736769$ Workarounds: use sub-interface less than 512
CSCvx60909	Headline: N9k / Installing multiple SMUs do not remain committed after reload. Symptoms: When installing multiple SMUs which includes nxos.CSCvx18710-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000.tar (tar includes nxos.CSCvx18710_lc_x86-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000.rpm and nxos.CSCvx18710_lc_x86-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000.rpm), they do not remain committed after reload. Workarounds: Please use SMU 1.0.1 version for CSCvx18710. nxos.CSCvx18710-n9k_ALL-1.0.1-7.0.3.I7.9.lib32_n9000.rpmIf 1.0.0 version (nxos.CSCvx18710-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000.tar) was previously installed then it needs to be deactivated, commit and remove before installing the new one using the below procedure. Step 1: Check if 1.0.0 is active switch# show install activeBoot Image: NXOS Image: bootflash:/nxos.7.0.3.I7.9.binActive Packages: nxos.CSCvx18710-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000 nxos.CSCvx18710_lc_x86-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000 Step 2: If 1.0.0 version is active, then deactivate it. This will require reload. switch# install deactivate nxos.CSCvx18710-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000 nxos.CSCvx18710_lc_x86-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000 ========== !!!WARNING!!This is a reload patch and system will be reloaded if you proceed with patch operation. ========== Do you want to continue (y/n)?: [n] y[########################] 100% Step 3: Check show install inactive and make sure 1.0.0 version have inactive status and then do install commit Switch# show install inactiveBoot Image: NXOS Image: bootflash:/nxos.7.0.3.I7.9.binInactive Packages: nxos.CSCvx18710-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000 nxos.CSCvx18710_lc_x86-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000switch# install commit[########################] 100% Step 4: Install remove 1.0.0 versionswitch# install remove nxos.CSCvx18710-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000Proceed with removing nxos.CSCvx18710-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000? (y/n)? [n] y[########################] 100%switch# install remove nxos.CSCvx18710_lc_x86-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000Proceed with removing

Bug ID	Description
	nxos.CSCvx18710_lc_x86-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000? (y/n)? [n] y[########################] 100% Step 5: Download 1.0.1 version and install add,activate,commit. This doesn't require reloadinfra-3164-2# install add nxos.CSCvx18710-n9k_ALL-1.0.1-7.0.3.I7.9.lib32_n9000.rpm activate Adding the patch (/nxos.CSCvx18710-n9k_ALL-1.0.1-7.0.3.I7.9.lib32_n9000.rpm)[########################] 100%Activating the patch (/nxos.CSCvx18710-n9k_ALL-1.0.1-7.0.3.I7.9.lib32_n9000.rpm)[########################] 100%switch# install commit[########################] 100%
CSCvx66000	Headline: ECMP/port-channel hashing broken for non-GTP tunnelled unicast when gtpu load-sharing enabled Symptoms: Using the command ip load-sharing address source-destination gtpu rotate 32 may result in non-GTP traffic to be sprayed across ECMP paths for the same src/dst and l4 port numbers for the flow. This leads to out-of-order packets arriving at the destination with application performance issues. Workarounds: Disable gtpu load-sharing.
CSCvx76407	Headline: Port-security port with switchport mode private-vlan host goes Sec-violation errDisable when flapped. Symptoms: Port with both port-security sticky mac and switchport mode private-vlan host configured such as below goes " Sec-violation errDisable" when the interface flapped with the same device(mac address) attached to that interface. Workarounds: Remove port-security from the interface and then bounce the interface OR remove switchport mode private-vlan host for switchport mode access and then bounce the interface.
CSCvx89892	Headline: n9k F&L: NVE Interface state: nve-intf-del-peer-cleanup-pending after interface NVE shut Symptoms: NVE interface stuck in the down pending state after DOWN/UP event (either from CLI or due to nve loopback flap) and traffic is not forwarded to/from VXLAN fabric. NVE interface state: down/Lim Response pending Interface: nve1, State: Down, encapsulation: VXLAN VPC Capability: VPC-VIP-Only [notified] Local Router MAC: 0000.baba.baba Host Learning Mode: Data-Plane Source-Interface: loopbackXXX (primary: X.X.X.X, secondary: Y.Y.Y.Y) Source Interface State: Up Virtual RMAC Advertisement: No NVE Flags: LIM Response Pending Interface Handle: 0x49000001 Source Interface hold-down-time: 180 Source Interface hold-up-time: 30 Remaining hold-down time: 0 seconds Virtual Router MAC: 0000.abba.abba Interface state: nve-intf-del-peer-cleanup-pending When in this state Interface cannot be recovered by shut no shut NVE interface neither by flap of NVE loopback interface. Workarounds: None - Reload is the only recovery.
CSCvx89893	Headline: dme - vpc dual-active exclude interface-vlan fails for non-default reserved vlan Symptoms: *VLAN missing under vPC config when trying to use anything beyond 3967. (i.e. reserved by default VLANs) sh run | grep dual dual-active exclude interface-vlan <<< ======= vlan not seen Workarounds: *Use the default system reserved VLANs. OR *Upgrading from 9.3(4) with the config in place to an impacted version (9.3.5, 9.3.6 or 9.3.7) and the issue will not manifest unless changes are made to the dual-active exclude interface-vlan list or a " reload ascii" is performed.
CSCvx94820	Headline: OSPF memory leak causes OSPF process to crash Symptoms: The ospf process may crash due to a memory leak generating a core. `show cores`VDC Module Instance Process-name PID Date(Year-Month-Day Time) --- ------ -------- --------------- -------- ------------------------- 1 1 1 ospf-3001 27491 2021-02-18 02:08:30 Workarounds: 1. Avoid clearing routes if possible. 2. Manual restart of the process using:N9K# restart ospf <ospf-instance-name>
CSCvx96166	Headline: MAC addresses aren't fully synced between VPC peers

Bug ID	Description
	Symptoms: MAC addresses are being learnt on one VPC peer but not the other although ARP entries are there for the missing MACs. Its a VPC VLAN and its connected via a VPC port-channel. Workarounds: Use " clear mac address-table dynamic. address<>" to clear the mac and relearn
CSCvx98350	Headline: dhclient crash when offer contains " log-server" option Symptoms: dhcpclient process may crash.The following may be reported in the log:`show logging log`2021 Mar 5 02:59:09 %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service " dhclient" (PID 30316) hasn't caught signal 11 (core will be saved). Workarounds: None
CSCvy00029	Headline: Packets with a bad L4 checksum will be dropped in Nexus 9000-FX3 Symptoms: Packets received with bad L4 checksum will be dropped by the switch. Workarounds: There is no workaround available, upgrade to a fixed version.
CSCvy07465	Headline: VXLAN-EVPN IR - vMCT PIP replication for BUM broken when empty Remote IR list Symptoms: BUM traffic between VPC peers is not working in a VXLAN EVPN setup. Workarounds: Shut/no shut under VLAN mode:conf tvlan xshutno shut Or Remove VNI under NVE on VPC peers and re-add it.
CSCvy07799	Headline: Not able to configure Tx (or both) SPAN direction for FEX port-channel source interface Symptoms: N9K(config)# no monitor session 1N9K(config)# monitor session 1N9K(config-monitor)# source interface port-channel79 bothERROR: po79: TX span unsupportedN9K(config-monitor)# source interface port-channel79 txERROR: po79: TX span unsupportedN9K(config-monitor)# source interface port-channel79 rx Workarounds: if possible, use a fex port that is NOT a port-channel member or use a port-channel on the parent switch N9K(config)# no monitor session 10 N9K(config)# monitor session 10 N9K(config)# source interface Ethernet113/1/3 both N9K(config)# <<<<< command is correctly accepted
CSCvy07815	Headline: issues seen when gnmi/grpc connection with ipv6 default address connectivity Symptoms: Inband GRPC connections, from front panel ports, to the loopback interface using IPv6 for transport fail. The loopback is not answering, i.e. connection refused, inbound IPv6 connections on the configured GRPC port. switch# show run grpc<snip>feature grpcgrpc use-vrf defaultgrpc certificate mytrustpointgrpc port 15000switch# show run interface lo0<snip>interface loopback0 ip address 1.1.1.1/32 ipv6 address 2001:1:1:1::1/32From management station:[user@localhost ~]$ telnet 2001:1:1:1::1 15000Trying 2001:1:1:1::1...telnet: connect to address 2001:1:1:1::1: Connection refused[user@localhost ~]$ Workarounds: Before enabling GRPC for IPv6 transport, make sure that the Management interface is up/up and has IPv6 configured on it. switch# show run grpc ^% Invalid command at '^' marker. switch# switch# show run int mgmt 0<snip>interface mgmt0 vrf member management ip address 10.31.121.31/26 ipv6 address 2001::1/64switch(config)# feature grpc switch(config)# grpc use-vrf default switch(config)# grpc certificate mytrustpoint switch(config)# grpc port 15000From the management station:[user@localhost ~]$ telnet 2001:1:1:1::1 15000Trying 2001:1:1:1::1...Connected to 2001:1:1:1::1.Escape character is '^]'.^]telnet> qConnection closed.[user@localhost ~]$
CSCvy23061	Headline: Memory leak on smnp due to STATSCLIENT_MEM_lib_portcl_request Symptoms: The snmp process crashes with frequency showing the following log: ''%SYSMGR-2-SERVICE_CRASHED: Service " snmpd" (PID 19371) hasn't caught signal 6 (core will be saved).''The respective core files are corrupted due to memory leaking. The memory leak can be verified by comparing the output of ''show system internal snmp mem-stats detail'' in between crashes. Nexus#

Bug ID	Description
	show system internal processes memory PID TTY STAT TIME MAJFLT TRS RSS VSZ %MEM COMMAND12240 ? Ssl 00:43:42 0 0 2833048 3511816 11.5 /isan/bin/snmpd -fNexus#show system internal snmp mem-stats detailsPrivate Mem stats for UUID : Stats Client Library(1047) Max types: 57----------TYPE NAME ALLOCS BYTES CURR MAX CURR MAX 32 STATSCLIENT_MEM_lib_portcl_request 217206 217206 2798482104 2798482104 Nexus#show system internal processes memory PID TTY STAT TIME MAJFLT TRS RSS VSZ %MEM COMMAND12240 ? Ssl 00:51:34 0 0 3331808 4010504 13.5 /isan/bin/snmpd -fNexus#show system internal snmp mem-stats detailsPrivate Mem stats for UUID : Stats Client Library(1047) Max types: 57----------TYPE NAME ALLOCS BYTES CURR MAX CURR MAX 32 STATSCLIENT_MEM_lib_portcl_request 256648 256648 3306652832 3306652832 Workarounds: 1. Disable the polling of information from Fex with interfaces in failure state. 2. Avoid FEX interfaces in failure state.
CSCvy29240	Headline: All ports stop passing unicast traffic Symptoms: No unicast traffic is passed through the switch, starting from one port, issue then replicates to other ports as well. Workarounds: Reload. If detected in early stages, shut/no shut of the problematic port would work.
CSCvy33584	Headline: N9K: nginx session flood if switch removed from DCNM with tracker enabled Symptoms: As soon as switch is removed from DCNM, it becomes slow to respond and the sysinfo service crashes. Contrary to the log message, a core file may not be saved.%SYSMGR-2-SERVICE_CRASHED: Service " sysinfo" (PID 29474) hasn't caught signal 6 (core will be saved).Switch# run bashbash-4.3$ ps aux | grep nginx(Thousands of nginx_f worker sessions are printed in the format below)svc-nxa+ 5892 0.0 0.0 296772 5692 pts/14 Ss+ 15:21 0:00 nginx_f worker bash-4.3$ copy /volatile/nginx.log /bootflash/bash-4.3$ exitSwitch# show file bootflash:/nginx.log(Thousands of these entries are generated)_pterm_create_vsh_session:291 pid:5879 User sa-dcnm does not exists!pterm_get_vsh:810 pid:5879 couldn't create a vsh session Workarounds: Disable the DCNM tracker feature in DCNM, before deprovisioning the switch. If the switch is already in this state, destroy the guestshell and reload the switch.
CSCvy39404	Headline: Packet loss after reload of VXLAN BGP EVPN vPC VTEP with eBGP underlay Symptoms: Packet loss may be observed between hosts connected via vPC to vPC VTEPs in a VXLAN BGP EVPN fabric that uses eBGP as an underlay as one of the vPC VTEPs is coming online after a reload or power outage. Specifically, the packet loss starts after the vPC Delay Restore timer of the reloaded vPC peer expires. During this time, the NVE source loopback (that is, the loopback interface sourced with the " source-interface {interface}" command) is held in an Administratively Down state. The total duration of the packet loss will vary, but usually ranges from 60 seconds to several minutes depending on the precise vPC Delay Restore and NVE source loopback hold-down timers. Workarounds: You can proactively avoid this issue by ensuring the NVE source loopback hold-down timer is set to a value less than the vPC Delay Restore timer.
CSCvy39858	Headline: N9K-C9332C: Interfaces with 1Gbps transceivers do not go down when link signal is lost Symptoms: If a Nexus 9332C switch with GLC-SX-MMD transceivers inserted in Ethernet1/33 or Ethernet1/34 has either interface come up/up when link signal is received, the interfaces will not transition to a down state when link signal is lost on either interface. Workarounds: There is no known proactive workaround for this issue. To reactively work around this issue, you can administratively shut down the interface(s) on the affected device.
CSCvy55293	Headline: IP-in-IP packets dropped on the peer-link Symptoms: IP-in-IP tunnelled traffic may fail when forwarded from one leaf to another over

Bug ID	Description
	vpc peer-link in a vxlan environment. There is no impact for GRE traffic. Workarounds: Adjust routing preferences to forward such traffic locally on the switch instead of crossing peer-link.
CSCvy57340	Headline: FIPs mode enabled+ nxapi disabled: switch reload allows access to nginx/nxapi sandbox port 80,443 Symptoms: 1. Switch reports ports 80 and 443 are open despite feature nxapi disabledTDC1P1-Rack01-BMC-1# show sockets connection tcp | in '*(80)|*(443)' n 1[host]: tcp LISTEN 0 *(80) <<< port should be closed Wildcard 0 *(*)--[host]: tcp6 LISTEN 0 *(80) <<< port should be closed Wildcard 0 *(*)--[host]: tcp LISTEN 0 *(443) <<< port should be closed Wildcard 0 *(*)--[host]: tcp6 LISTEN 0 *(443) <<< port should be closed Wildcard 0 *(*) 2. user admin with valid password can open browser to NXAPI Sandbox despite feature disabled3. with feature bash enabled, find that nginx process was restarted, despite feature nxapi disabledTDC1P1-Rack01-BMC-1# run bash sudo pgrep -l nginx12616 nginx14059 nginx_1_fe14138 nginx_1_fe Workarounds: In this scenario an ACL can be used on mgmt0 interface to prevent access to the 80 & 443 service. Example:!ip access-list DENY-NXAPI 10 deny tcp any any eq 443 20 deny tcp any any eq www 30 permit ip any any !interface mgmt0 ip access-group DENY-NXAPI in!Note: There are normally restrictions when using an ACL with NX-API when it is configured to use a VRF. See https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/101x/programmability/cisco-nexus-9000-series-nx-os-programmability-guide-release-101x/m-n9k-nx-api-cli-101x.html, section - "Restricting Access to NX-API" for more details. For the purposes of this defect and workaround those limitations are not applicable.
CSCvy65701	Headline: N9K-C93180YC-FX3 vPC fabric peering- Vxlan traffic fails to be bounced over fabric-ports Symptoms: The issue is seen specific to FX3 model of N9K switches in a specific scenario of VXLAN operation. It is reproducible consistently Broken state scenario- Vxlan encapsulated traffic encapsulated traffic is received from remote TEP and it is destined for a host attached behind local VPC port-channel, but local leg of that VPC port-channel is down. We expect the local TEP to de-capsulate this traffic and then encapsulate back (Outer source IP being local loopback and dest IP being loopback of other member of it's VPC) to send it towards Spines/fabric-ports to make sure that reaches the other member of VPC where, the only active member of given VPC port-channel exists .But while using FX3, we could see that traffic in given scenario is not being bounced towards fabric ports and being black holed Forwarding decision from Ingress forwarding controller does not seem to be happening correctly on FX3 chassis when one of the vPC leg is shut Vs other platforms like GC-XFP etc. Destination index should be pointing back to uplink and packet should be bounced towards spine with a new outer IP encapsulation for Spine to route that to other member of VPC, but the index itself is shown incorrect in case of FX3. Workarounds: NA
CSCvy68524	Headline: Aclqos crash on ravl_insert and ravl_free Symptoms: aclqos process crash2021 Jun 8 03:35:29.789 RMD03-NX_LB-01 %$ VDC-1 %$ %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "aclqos" (PID 28000) hasn't caught signal 11 (core will be saved).2021 Jun 8 03:35:30.407 RMD03-NX_LB-01 %$ VDC-1 %$ %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "aclqos" (PID 8248) hasn't caught signal 11 (core will be saved).2021 Jun 8 03:35:31.026 RMD03-NX_LB-01 %$ VDC-1 %$ %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "aclqos" (PID 8469) hasn't caught signal 11 (core will be saved).2021 Jun 8 03:35:31.640 RMD03-NX_LB-01 %$ VDC-1 %$ %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "aclqos" (PID 8477) hasn't caught signal 11 (core will be saved)May also see the TCAM resource exhaustion logs like below-2021 May 22 18:47:26.685 RMD03-NX_LB-01 %$ VDC-1 %$ %ACLQOS-SLOT1-2-ACLQOS_OOTR: Tcam resource exhausted: Ingress RACL [ing-racl]2021 May 22 18:47:26.713 RMD03-NX_LB-01 %$ VDC-1 %$ %RPM-2-PPF_SES_VERIFY: rpm [31668] PPF session verify failed in client aclqos(Line card 1/VDC NONE/UUID 366) with an error 0x41040069(Sufficient free entries are not available in TCAM bank)2021 May 22

Bug ID	Description
	18:48:47.213 RMD03-NX_LB-01 %$ VDC-1 %$ %ACLQOS-SLOT1-2-ACLQOS_OOTR: Tcam resource exhausted: Ingress RACL [ing-racl]2021 May 22 18:48:47.240 RMD03-NX_LB-01 %$ VDC-1 %$ %RPM-2-PPF_SES_VERIFY: rpm [31668] PPF session verify failed in client aclqos(Line card 1/VDC NONE/UUID 366) with an error 0x41040069(Sufficient free entries are not available in TCAM bank)2021 May 22 18:51:05.725 RMD03-NX_LB-01 %$ VDC-1 %$ %ACLQOS-SLOT1-2-ACLQOS_OOTR: Tcam resource exhausted: Ingress RACL [ing-racl]2021 May 22 18:51:05.749 RMD03-NX_LB-01 %$ VDC-1 %$ %RPM-2-PPF_SES_VERIFY: rpm [31668] PPF session verify failed in client aclqos(Line card 1/VDC NONE/UUID 366) with an error 0x41040069(Sufficient free entries are not available in TCAM bank)2021 May 22 20:28:43.847 RMD03-NX_LB-01 %$ VDC-1 %$ %ACLQOS-SLOT1-2-ACLQOS_OOTR: Tcam resource exhausted: Ingress RACL [ing-racl]2021 May 22 20:28:43.909 RMD03-NX_LB-01 %$ VDC-1 %$ %RPM-2-PPF_SES_VERIFY: rpm [31668] PPF session verify failed in client aclqos (Line card 1/VDC NONE/UUID 366) with an error 0x41040069(Sufficient free entries are not available in TCAM bank) Workarounds: None
CSCvy73232	Headline: N9k ITD-NAT and User defined PBR applied to same interface may cause inconsistencies in aclqos table Symptoms: ITD NAT Traffic sent to node with incorrect DMACaclqos is mis-matched b/w ASIC instances Workarounds: If feasible, remove PBR from the SVI (copy run start) and the affected nexus 9k would have to be reloaded with " reload ascii" .
CSCvy88454	Headline: Packets forwarded with Incorrect MPLS labels when using N9k layer 2 evpn over segment routing Symptoms: Spines drop the Labelled Packets from Leaf switches. Incorrect Outer label for MPLS packets in some cases, multiple labels are also seen (more than 2). Workarounds: Once impacted by this defect, the only way to restore is by Removing SPAN/SFLOW(if feasible) and " copy run start" , reload.
CSCvy89592	Headline: N9K/FX Series - Egress IFACL Label allocation Exhaustion/Failure is handled incorrectly Symptoms: When Egress IFACL label allocation is reached; BFD flaps or traffic gets policed on port where egress QOS policy (policer) is not configured. Workarounds: Do not apply policies on more than the supported Hardware limit. Remove the policy from an interface.
CSCvy99573	Headline: PBR not correctly programmed with scaled L2 egress port-channel Symptoms: With PBR redirected to a next hop adjacent via a L2 port-channel, the PBR can become mis-programmed and blackhole traffic. May be observed when initially configuring or when adding links to an already provisioned port-channel. Workarounds: Constrain port-channel to 31 ports or less.
CSCvz17536	Headline: Traffic blackhole when both uplinks of compute to ToR are flapped Symptoms: Setup is CVIM running 3.4.4 with N9K ToR pairs running 9.3.7 Compute Nodes <--> Leaf pair <---> Spines <-----> ECX (Juniper) <--->CE (Juniper)When both uplinks from Compute to ToR pair are flapped , traffic is blackholed. Workarounds: Ping compute VTEP IP from ECX node or Leaf node OR restart VPP on compute node.
CSCvy90700	Headline: Mac address disabled on ports after removing VPC Peer-link from configuration Symptoms: After removing VPC peer-link from configuration router mac addresses from VPC peer will not be learnt again. If using BFD you can see the following error under: sh bfd neighbors detail: sh bfd neighbors details OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int Vrf Type 10.3.200.254 10.3.200.253 1090519044/0 Down N/A(3) Down Vlan200 default SH Session state is Down and not using echo functionSession type: SinglehopLocal Diag: 0, Demand mode: 0, Poll bit: 0, Authentication:

Bug ID	Description
	NoneMinTxInt: 0 us, MinRxInt: 0 us, Multiplier: 0Received MinRxInt: 0 us, Received Multiplier: 0Holdown (hits): 0 ms (0), Hello (hits): 0 ms (0)Rx Count: 0, Rx Interval (ms) min/max/avg: 0/0/0 last: 0 ms agoTx Count: 0, Tx Interval (ms) min/max/avg: 0/0/0 last: 0 ms agoRegistered protocols: ospfDowntime: 0 days 0 hrs 1 mins 28 secs, Downcount: 0Last packet: Version: 0 - Diagnostic: 0 State bit: AdminDown - Demand bit: 0 Poll bit: 0 - Final bit: 0 Multiplier: 0 - Length: 24 My Discr.: 0 - Your Discr.: 0 Min tx interval: 0 - Min rx interval: 0 Min Echo interval: 0 - Authentication bit: 0 Hosting LC: 0, Down reason: No Diagnostic, Reason not-hosted: if_index type invalid <<<<<<<<<<< Workarounds: Reload the box.
CSCvy49381	Headline: QOSMGR_MEM_port_grp_mem_t memory leak in the ipqosmgr process Symptoms: Crash of ipqosmgr process due to a memory leak with core and process log files.%SYSMGR-2-SERVICE_CRASHED: Service "ipqosmgr" (PID 32142) hasn't caught signal 6 (core will be saved). Workarounds: None.
CSCvy61697	Headline: Multicast traffic is not forwarded out on ports 5 through 8 on N9K-X9408PC-CFP2. Symptoms: Multicast traffic is not forwarded out on ports 5 through 8 of the 100G Line card-N9K-X9408PC-CFP2. Workarounds: None. Moving the ports to any interfaces that are part of the first ASIC Instance (1 through 4) will be a viable workaround provided those interfaces are not currently used.
CSCvy56677	Headline: Nexus 9000 - NTP access-group peer command not working after reload. Symptoms: NTP “access-group peer” command doesn't work after reload. Switch can sync with NTP server that is not defined in Access-group entry. Workarounds: Removing and reapplying the NTP access-group command resolves the issue.

Device Hardware

The following tables list the Cisco Nexus 9000 Series hardware that Cisco NX-OS Release 9.3(8) supports. For additional information about the supported hardware, see the Hardware Installation Guide for your Cisco Nexus 9000 Series device.

Table 1. Cisco Nexus 9500 Switches

Product ID	Description
N9K-C9504	7.1-RU modular switch with slots for up to 4 line cards in addition to two supervisors, 2 system controllers, 3 to 6 fabric modules, 3 fan trays, and up to 4 power supplies.
N9K-C9508	13-RU modular switch with slots for up to 8 line cards in addition to two supervisors, 2 system controllers, 3 to 6 fabric modules, 3 fan trays, and up to 8 power supplies.
N9K-C9516	21-RU modular switch with slots for up to 16 line cards in addition to two supervisors, 2 system controllers, 3 to 6 fabric modules, 3 fan trays, and up to 10 power supplies.

Table 2. Cisco Nexus 9500 Cloud Scale Line Cards

Product ID	Description	Maximum Quantity		
		Cisco Nexus 9504	Cisco Nexus 9508	Cisco Nexus 9516
N9K-X97160YC-EX	Cisco Nexus 9500 48-port 10/25-Gigabit Ethernet	4	8	16

Product ID	Description	Maximum Quantity		
		Cisco Nexus 9504	Cisco Nexus 9508	Cisco Nexus 9516
	SFP28 and 4-port 40/100 Gigabit Ethernet QSFP28 line card			
N9K-X9732C-EX	Cisco Nexus 9500 32-port 40/100 Gigabit Ethernet QSFP28 line card	4	8	16
N9K-X9732C-FX	Cisco Nexus 9500 32-port 40/100 Gigabit Ethernet QSFP28 line card	4	8	16
N9K-X9736C-EX	Cisco Nexus 9500 36-port 40/100 Gigabit Ethernet QSFP28 line card	4	8	16
N9K-X9736C-FX	Cisco Nexus 9500 36-port 40/100 Gigabit Ethernet QSFP28 line card	4	8	16
N9K-X9788TC-FX	Cisco Nexus 9500 48-port 1/10-G BASE-T Ethernet and 4-port 40/100 Gigabit Ethernet QSFP28 line card	4	8	16

Table 3. Cisco Nexus 9500 R-Series Line Cards

Product ID	Description	Maximum Quantity	
		Cisco Nexus 9504	Cisco Nexus9508
N9K-X9636C-R	Cisco Nexus 9500 36-port 40/100 Gigabit Ethernet QSFP28 line card	4	8
N9K-X9636C-RX	Cisco Nexus 9500 36-port 40/100 Gigabit Ethernet QSFP28 line card	4	8
N9K-X9636Q-R	Cisco Nexus 9500 36-port 40 Gigabit Ethernet QSFP line card	4	8
N9K-X96136YC-R	Cisco Nexus 9500 16-port 1/10 Gigabit, 32-port 10/25 Gigabit, and 4-port 40/100 Gigabit Ethernet line card	4	8

Table 4. Cisco Nexus 9500 Classic Line Cards

Product ID	Description	Maximum Quantity		
		Cisco Nexus 9504	Cisco Nexus 9508	Cisco Nexus 9516
N9K-X9408C-CFP2	Line card with 8 100 Gigabit CFP2 ports	4	8	16
N9K-X9432C-S	Cisco Nexus 9500 32-port 40/100 Gigabit Ethernet QSFP28 line card	4	8	N/A
N9K-X9432PQ	Cisco Nexus 9500 32-port 40 Gigabit Ethernet QSFP+ line card	4	8	16
N9K-X9636PQ	Cisco Nexus 9500 36-port 40 Gigabit Ethernet QSFP+ line card	4	8	N/A
N9K-X9464PX	Cisco Nexus 9500 48 1/10-Gigabit SFP+ and 4-port 40-Gigabit Ethernet QSFP+ line card	4	8	16
N9K-X9464TX	Cisco Nexus 9500 48 port 1/10-Gigabit BASE-T Ethernet and 4-port 40-Gigabit Ethernet QSFP+ line card	4	8	16
N9K-X9464TX2	Cisco Nexus 9500 48 port 1/10-Gigabit BASE-T Ethernet and 4-port 40-Gigabit Ethernet QSFP+ line card	4	8	16
N9K-X9536PQ	Cisco Nexus 9500 36-port 40 Gigabit Ethernet QSFP+ line card	4	8	16
N9K-X9564PX	Cisco Nexus 9500 48 1/10-Gigabit SFP+ and 4 port 40-Gigabit Ethernet QSFP+ line card	4	8	16
N9K-X9564TX	Cisco Nexus 9500 48 port 1/10-Gigabit BASE-T Ethernet and 4 port 40-Gigabit Ethernet QSFP+ line	4	8	16

Product ID	Description	Maximum Quantity		
		Cisco Nexus 9504	Cisco Nexus 9508	Cisco Nexus 9516
	card			

Table 5. Cisco Nexus 9500 Cloud Scale Fabric Modules

Product ID	Description	Minimum	Maximum
N9K-C9504-FM-E	Cisco Nexus 9504 100-Gigabit cloud scale fabric module	4	5
N9K-C9508-FM-E	Cisco Nexus 9508 100-Gigabit cloud scale fabric module	4	5
N9K-C9508-FM-E2	Cisco Nexus 9508 100-Gigabit cloud scale fabric module	4	5
N9K-C9516-FM-E	Cisco Nexus 9516 50-Gigabit cloud scale fabric module	4	5
N9K-C9516-FM-E2	Cisco Nexus 9516 100-Gigabit cloud scale fabric module	4	5

Table 6. Cisco Nexus 9500 R-Series Fabric Modules

Product ID	Description	Minimum	Maximum
N9K-C9504-FM-R	Cisco Nexus 9504 100-Gigabit R-Series fabric module	4	6
N9K-C9508-FM-R	Cisco Nexus 9508 100-Gigabit R-Series fabric module	4	6

Table 7. Cisco Nexus 9500 Fabric Modules

Product ID	Description	Minimum	Maximum
N9K-C9504-FM	Cisco Nexus 9504 40-Gigabit fabric module	3	6
N9K-C9508-FM	Cisco Nexus 9508 40-Gigabit fabric module	3	6
N9K-C9516-FM	Cisco Nexus 9516 40-Gigabit fabric module	3	6
N9K-C9504-FM-S	Cisco Nexus 9504 100-Gigabit fabric module	4	4
N9K-C9508-FM-S	Cisco Nexus 9508 100-Gigabit fabric module	4	4

Table 8. Cisco Nexus 9500 Fabric Module Blanks with Power Connector

Product ID	Description	Minimum	Maximum
N9K-C9508-FM-Z	Cisco Nexus 9508 Fabric blank with Fan Tray Power Connector module	N/A	2
N9K-C9516-FM-Z	Cisco Nexus 9516 Fabric blank with Fan Tray Power Connector module	N/A	2

Table 9. Cisco Nexus 9500 Supervisor Modules

Supervisor	Description	Quantity
N9K-SUP-A	1.8-GHz supervisor module with 4 cores, 4 threads, and 16 GB of memory	2
N9K-SUP-A+	1.8-GHz supervisor module with 4 cores, 8 threads, and 16 GB of memory	2
N9K-SUP-B	2.2-GHz supervisor module with 6 cores, 12 threads, and 24 GB of memory	2

Supervisor	Description	Quantity
N9K-SUP-B+	1.9-GHz supervisor module with 6 cores, 12 threads, and 32 GB of memory	2

NOTE: N9K-SUP-A and N9K-SUP-A+ are not supported on Cisco Nexus 9504 and 9508 switches with -R line cards.

Table 10. Cisco Nexus 9500 System Controller

Product ID	Description	Quantity
N9K-SC-A	Cisco Nexus 9500 Platform System Controller Module	2

Table 11. Cisco Nexus 9500 Fans and Fan Trays

Product ID	Description	Quantity
N9K-C9504-FAN	Fan tray for 4-slot modular chassis	3
N9K-C9508-FAN	Fan tray for 8-slot modular chassis	3
N9K-C9516-FAN	Fan tray for 16-slot modular chassis	3

Table 12. Cisco Nexus 9500 Power Supplies

Product ID	Description	Quantity	Cisco Nexus Switches
N9K-PAC-3000W-B	3 KW AC power supply	Up to 4 Up to 8 Up to 10	Cisco Nexus 9504 Cisco Nexus 9508 Cisco Nexus 9516
N9K-PDC-3000W-B	3 KW DC power supply	Up to 4 Up to 8 Up to 10	Cisco Nexus 9504 Cisco Nexus 9508 Cisco Nexus 9516
N9K-PUV-3000W-B	3 KW Universal AC/DC power supply	Up to 4 Up to 8 Up to 10	Cisco Nexus 9504 Cisco Nexus 9508 Cisco Nexus 9516
N9K-PUV2-3000W-B	3.15-KW Dual Input Universal AC/DC Power Supply	Up to 4 Up to 8 Up to 10	Cisco Nexus 9504 Cisco Nexus 9508 Cisco Nexus 9516

Table 13. Cisco Nexus 9200 and 9300 Fans and Fan Trays

Product ID	Description	Quantity	Cisco Nexus Switches
N9K-C9300-FAN1	Fan 1 module with port-side intake airflow (burgundy coloring)	3	9396PX (early versions)
N9K-C9300-FAN1-B	Fan 1 module with port-side exhaust airflow (blue coloring)	3	9396PX (early versions)
N9K-C9300-FAN2	Fan 2 module with port-side intake airflow (burgundy coloring)	3	93128TX 9396PX 9396TX
N9K-C9300-FAN2-B	Fan 2 module with port-side exhaust airflow (blue coloring)	3	93128TX 9396PX 9396TX
N9K-C9300-FAN3	Fan 3 module with port-side intake airflow (burgundy coloring)	3	92304QC 9272Q[a] 93120TX
N9K-C9300-FAN3-B	Fan 3 module with port-side exhaust airflow (blue coloring)	3	92304QC 9272Q[a] 93120TX
NXA-FAN-160CFM-PE	Fan module with port-side exhaust airflow (blue coloring)	3	9364C[a] 93360YC-FX2

Product ID	Description	Quantity	Cisco Nexus Switches
NXA-FAN-160CFM-PI	Fan module with port-side intake airflow (burgundy coloring)	3	9364C[a] 93360YC-FX2
NXA-FAN-160CFM2-PE	Fan module with port-side exhaust airflow (blue coloring)	4	9364C-GX
NXA-FAN-160CFM2-PI	Fan module with port-side intake airflow (burgundy coloring)	4	9364C-GX
NXA-FAN-30CFM-B	Fan module with port-side intake airflow (burgundy coloring)	3	92160YC-X 9236C[a] 93108TC-EX 93108TC-FX[a] 93180LC-EX[a] 93180YC-EX 93180YC-FX[a] 9332PQ 9372PX 9372PX-E 9372TX 9372TX-E 9348GC-FXP[a]
NXA-FAN-30CFM-F	Fan module with port-side exhaust airflow (blue coloring)	3	92160YC-X 9236C[a] 93108TC-EX 93108TC-FX[a] 93180LC-EX[a] 93180YC-EX 93180YC-FX[a] 9332PQ 9372PX 9372PX-E 9372TX 9372TX-E 9348GC-FXP
NXA-FAN-35CFM-PE	Fan module with port-side exhaust airflow (blue coloring)	4	92300YC[a] 9332C[a] 93108TC-FX3P 93180YC-FX3S[b]
		6	9316D-GX 93600CD-GX
NXA-FAN-35CFM-PI	Fan module with port-side intake airflow (burgundy coloring)	4	92300YC[a] 9332C[a] 93108TC-FX3P 93180YC-FX3S[b]
		6	9316D-GX 93600CD-GX
NXA-FAN-65CFM-PE	Fan module with port-side exhaust airflow (blue coloring)	3	93240YC-FX2[a] 9336C-FX2[a]
NXA-FAN-65CFM-PI	Fan module with port-side exhaust airflow (burgundy coloring)	3	93240YC-FX2[a] 9336C-FX2[a]

[a] For specific fan speeds see the Overview section of the Hardware Installation Guide.

[b] This switch runs with +1 redundancy mode so that if one fan fails, the switch can sustain operation. But if a second fan fails, this switch is not designed to sustain operation. Hence before waiting for the major threshold temperature to be hit, the switch will power down due to entering the **fan policy trigger** command.

Table 14. Cisco Nexus 9200 and 9300 Power Supplies

Product ID	Description	Quantity	Cisco Nexus Switches
NXA-PAC-500W-PE	500-W AC power supply with port-side exhaust airflow (blue coloring)	2	93108TC-EX 93180LC-EX

Product ID	Description	Quantity	Cisco Nexus Switches
			93180YC-EX 93180YC-FX
NXA-PAC-500W-PI	500-W AC power supply with port-side intake airflow (burgundy coloring)	2	93108TC-EX 93180LC-EX 93180YC-EX 93180YC-FX
N9K-PAC-650W	650-W AC power supply with port-side intake (burgundy coloring)	2	9332PQ 9372PX 9372PX-E 9372TX 9372TX-E 9396PX 9396TX
N9K-PAC-650W-B	650-W AC power supply with port-side exhaust (blue coloring)	2	9332PQ 9372PX 9372PX-E 9372TX 9372TX-E 9396PX 9396TX
NXA-PAC-650W-PE	650-W power supply with port-side exhaust (blue coloring)	2	92160YC-X 9236C 92300YC 93180YC-FX3S 92304QC 93108TC-EX 93180YC-EX
NXA-PAC-650W-PI	650-W power supply with port-side intake (burgundy coloring)	2	92160YC-X 9236C 92300YC 93180YC-FX3S 92304QC 93108TC-EX 93180YC-EX
NXA-PAC-750W-PE	750-W AC power supply with port-side exhaust airflow (blue coloring) [1]	2	9336C-FX2 93240YC-FX2 9332C 9336C-FX2
NXA-PAC-750W-PI	750-W AC power supply with port-side exhaust airflow (burgundy coloring) [1]	2	9336C-FX2 93240YC-FX2 9332C 9336C-FX2
NXA-PAC-1100W-PE2	1100-W AC power supply with port-side exhaust airflow (blue coloring)	2	93240YC-FX2 9332C 9316D-GX 9336C-FX2 93600CD-GX
NXA-PAC-1100W-PI2	1100-W AC power supply with port-side intake airflow (burgundy coloring)	2	93240YC-FX2 9332C 9316D-GX 9336C-FX2 93600CD-GX
NXA-PAC-1100W-PI	Cisco Nexus 9000 PoE 1100W AC PS, port-side intake	2	93108TC-FX3P
NXA-PAC-1100W-PE	Cisco Nexus 9000 PoE 1100W AC PS, port-side exhaust	2	93108TC-FX3P
NXA-PAC-1900W-PI	Cisco Nexus 9000 PoE 1900W AC PS, port-side intake	2	93108TC-FX3P
N9K-PAC-1200W	1200-W AC power supply with port-side intake airflow (burgundy coloring)	2	93120TX
N9K-PAC-1200W-B	1200-W AC power supply with port-side exhaust airflow (blue coloring)	2	93120TX
NXA-PAC-1200W-PE	1200-W AC power supply with port-side exhaust airflow (blue coloring)	2	9272Q 93360YC-FX2 9364C
NXA-PAC-1200W-PI	1200-W AC power supply with port-side intake airflow (burgundy coloring)	2	9272Q 93360YC-FX2

Product ID	Description	Quantity	Cisco Nexus Switches
			9364C
N9K-PUV-1200W	1200-W Universal AC/DC power supply with bidirectional airflow (white coloring)	2	92160YC-X 9236C 92300YC 92304QC 9272Q[1] 93108TC-EX 93108TC-FX 93360YC-FX2 93180YC-FX3S 93120TX 93128TX 93180LC-EX 93180YC-EX 93180YC-FX 9364C
NXA-PDC-930W-PE	930-W DC power supply with port-side exhaust airflow (blue coloring)	2	9272Q 93108TC-EX 93180YC-EX 93360YC-FX2 93180YC-FX3S 93120TX 93180YC-FX 9364C 92160YC-X
NXA-PDC-930W-PI	930-W DC power supply with port-side intake airflow (burgundy coloring)	2	9272Q 93108TC-EX 93180YC-EX 93360YC-FX2 93180YC-FX3S 93120TX 93180YC-FX 9364C 92160YC-X
NXA-PDC-1100W-PE	1100-W DC power supply with port-side exhaust airflow (blue coloring)	2	93240YC-FX2 93600CD-GX 9316D-GX 9332C 9336C-FX2
NXA-PDC-1100W-PI	1100-W DC power supply with port-side intake airflow (burgundy coloring)	2	93240YC-FX2 93600CD-GX 9316D-GX 9332C 9336C-FX2
UCSC-PSU-930WDC	930-W DC power supply with port-side intake (green coloring)	2	92160YC-X 9236C 92304QC 9272Q 93108TC-EX 93120TX 93128TX 93180YC-EX 9332PQ 9372PX 9372PX-E 9372TX 9372TX-E 9396PX 9396TX
UCS-PSU-6332-DC	930-W DC power supply with port-side exhaust (gray coloring)	2	92160YC-X 9236C 92304QC 9272Q 93108TC-EX 93120TX

Product ID	Description	Quantity	Cisco Nexus Switches
			93128TX 93180YC-EX 9332PQ 9372PX 9372PX-E 9372TX 9372TX-E 9396PX 9396TX
NXA-PHV-1100W-PE	1100-W AC power supply with port-side exhaust airflow (blue coloring)	2	93240YC-FX2 9336C-FX2
NXA-PHV-1100W-PI	1100-W AC power supply with port-side intake airflow (burgundy coloring)	2	93240YC-FX2 9336C-FX2
NXA-PAC-2KW-PE	2000-W AC power supply with port-side exhaust airflow (blue coloring)	2	9364C-GX
NXA-PAC-2KW-PI	2000-W AC power supply with port-side intake airflow (burgundy coloring)	2	9364C-GX
NXA-PDC-2KW-PE	2000-W DC power supply with port-side exhaust airflow (blue coloring	2	9364C-GX
NXA-PDC-2KW-PI	2000-W DC power supply with port-side intake airflow (burgundy coloring)	2	9364C-GX
N2200-PAC-400W	400-W AC power supply with port-side exhaust airflow (blue coloring)	2	92348GC-X
N2200-PAC-400W-B	400-W AC power supply with port-side intake airflow (burgundy coloring)	2	92348GC-X
N2200-PDC-350W-B	350-W DC power supply with port-side intake airflow	2	92348GC-X
N2200-PDC-400W	400-W DC power supply with port-side exhaust airflow (blue coloring)	2	92348GC-X

Table 15. Cisco Nexus 9200 and 9300 Switches

Cisco Nexus Switch	Description
N9K-C92160YC-X	1-RU Top-of-Rack switch with 48 10-/25-Gigabit SFP+ ports and 6 40-Gigabit QSFP+ ports (4 of these ports support 100-Gigabit QSFP28 optics).
N9K-C92300YC	1.5-RU Top-of-Rack switch with 48 10-/25-Gigabit SFP28 ports and 18 fixed 40-/100-Gigabit QSFP28 ports.
N9K-C92304QC	2-RU Top-of-Rack switch with 56 40-Gigabit Ethernet QSFP+ ports (16 of these ports support 4x10 breakout cables) and 8 100-Gigabit QSFP28 ports.
N9K-C92348GC-X	The Cisco Nexus 92348GC-X switch (N9K-C92348GC-X) is a 1RU switch that supports 696 Gbps of bandwidth and over 250 mpps. The 1GBASE-T downlink ports on the 92348GC-X can be configured to work as 100-Mbps, 1-Gbps ports. The 4 ports of SFP28 can be configured as 1/10/25-Gbps and the 2 ports of QSFP28 can be configured as 40- and 100-Gbps ports. The Cisco Nexus 92348GC-X is ideal for big data customers that require a Gigabit Ethernet ToR switch with local switching.
N9K-C9236C	1-RU Top-of-Rack switch with 36 40-/100-Gigabit QSFP28 ports (144 10-/25-Gigabit ports when using breakout cables)
N9K-C9272Q	2-RU Top-of-Rack switch with 72 40-Gigabit Ethernet QSFP+ ports (35 of these ports also support 4x10 breakout cables for 140 10-Gigabit ports)
N9K-C93108TC-EX	1-RU Top-of-Rack switch with 48 10GBASE-T (copper) ports and 6 40-/100-Gigabit QSFP28 ports
N9K-C93108TC-EX-24	1-RU 24 1/10GBASE-T (copper) front panel ports and 6 40/100-Gigabit QSFP28 spine facing ports.
N9K-C93108TC-FX	1-RU Top-of-Rack switch with 48 100M/1/10GBASE-T (copper) ports and 6 40-/100-Gigabit QSFP28 ports
N9K-C93108TC-FX-24	1-RU 24 1/10GBASE-T (copper) front panel ports and 6 fixed 40/100-Gigabit Ethernet QSFP28 spine-facing ports.
N9K-C93108TC-FX3P	1-RU fixed-port switch with 48 100M/1/2.5/5/10GBASE-T ports and 6 40-/100-Gigabit QSFP28 ports
N9K-C93120TX	2-RU Top-of-Rack switch with 96 1/10GBASE-T (copper) ports and 6 40-Gigabit QSFP+ ports
N9K-C93128TX	3-RU Top-of-Rack switch with 96 1/10GBASE-T (copper) ports and an uplink module up to 8 40-Gigabit QSFP+ ports

Cisco Nexus Switch	Description
N9K-C9316D-GX	1-RU switch with 16x400/100/40-Gbps ports.
N9K-C93180LC-EX	1-RU Top-of-Rack switch with 24 40-/50-Gigabit QSFP+ downlink ports and 6 40/100-Gigabit uplink ports. You can configure 18 downlink ports as 100-Gigabit QSFP28 ports or as 10-Gigabit SFP+ ports (using breakout cables).
N9K-C93180YC-EX	1-RU Top-of-Rack switch with 48 10-/25-Gigabit SFP28 fiber ports and 6 40-/100-Gigabit QSFP28 ports
N9K-C93180YC-EX-24	1-RU 24 1/10/25-Gigabit front panel ports and 6-port 40/100 Gigabit QSFP28 spine-facing ports
N9K-C93180YC-FX	1-RU Top-of-Rack switch with 10-/25-/32-Gigabit Ethernet/FC ports and 6 40-/100-Gigabit QSFP28 ports. You can configure the 48 ports as 1/10/25-Gigabit Ethernet ports or as FCoE ports or as 8-/16-/32-Gigabit Fibre Channel ports.
N9K-C93180YC-FX-24	1-RU 24 1/10/25-Gigabit Ethernet SFP28 front panel ports and 6 fixed 40/100-Gigabit Ethernet QSFP28 spine-facing ports. The SFP28 ports support 1-, 10-, and 25-Gigabit Ethernet connections and 8-, 16-, and 32-Gigabit Fibre Channel connections.
N9K-C93180YC-FX3	48 1/10/25 Gigabit Ethernet SFP28 ports (ports 1-48) 6 10/25/40/50/100-Gigabit QSFP28 ports (ports 49-54)
N9K-C93180YC-FX3S	48 1/10/25 Gigabit Ethernet SFP28 ports (ports 1-48) 6 10/25/40/50/100-Gigabit QSFP28 ports (ports 49-54)
N9K-C93216TC-FX2	2-RU switch with 96 100M/1G/10G RJ45 ports, 12 40/100-Gigabit QSFP28 ports, 2 management ports (one RJ-45 and one SFP port), 1 console, port, and 1 USB port.
N9K-C93240YC-FX2	1.2-RU Top-of-Rack switch with 48 10-/25-Gigabit SFP28 fiber ports and 12 40-/100-Gigabit Ethernet QSFP28 ports.
N9K-C9332C	1-RU fixed switch with 32 40/100-Gigabit QSFP28 ports and 2 fixed 1/10-Gigabit SFP+ ports.
N9K-C9332PQ	1-RU switch with 32 40-Gigabit Ethernet QSFP+ ports (26 ports support 4x10 breakout cables and 6 ports support QSFP-to-SFP adapters)
N9K-C93360YC-FX2	2-RU switch with 96 10-/25-Gigabit SFP28 ports and 12 40/100-Gigabit QSFP28 ports
N9K-C9336C-FX2	1-RU switch with 36 40-/100-Gb Ethernet QSFP28 ports.
N9K-C9348GC-FXP	Nexus 9300 with 48p 100M/1 G, 4p 10/25 G SFP+ and 2p 100 G QSFP
N9K-C93600CD-GX	1-RU fixed-port switch with 28 10/40/100-Gigabit QSFP28 ports (ports 1-28), 8 10/40/100/400-Gigabit QSFP-DD ports (ports 29-36)
N9K-C9364C	2-RU Top-of-Rack switch with 64 40-/100-Gigabit QSFP28 ports and 2 1-/10-Gigabit SFP+ ports. - Ports 1 to 64 support 40/100-Gigabit speeds. - Ports 49 to 64 support MACsec encryption. Ports 65 and 66 support 1/10 Gigabit speeds.
N9K-C9364C-GX	2-RU fixed-port switch with 64 100-Gigabit SFP28 ports.
N9K-C9372PX	1-RU Top-of-Rack switch with 48 1-/10-Gigabit SFP+ ports and 6 40-Gigabit QSFP+ ports
N9K-C9372PX-E	An enhanced version of the Cisco Nexus 9372PX-E switch.
N9K-C9372TX	1-RU Top-of-Rack switch with 48 1-/10GBASE-T (copper) ports and 6 40-Gigabit QSFP+ ports
N9K-C9372TX-E	An enhanced version of the Cisco Nexus 9372TX-E switch.
N9K-C9396PX	2-RU Top-of-Rack switch with 48 1-/10-Gigabit Ethernet SFP+ ports and an uplink module with up to 12 40-Gigabit QSFP+ ports
N9K-C9396TX	2-RU Top-of-Rack switch with 48 1/10GBASE-T (copper) ports and an uplink module with up to 12 40-Gigabit QSFP+ ports

Table 16. Cisco Nexus 9000 Series Uplink Modules

Cisco Nexus Switch	Description
N9K-M4PC-CFP2	Cisco Nexus 9300 uplink module with 4 100-Gigabit Ethernet CFP2 ports. For the Cisco Nexus 93128TX switch, only two of the ports are active. For the Cisco Nexus 9396PX and 9396TX switches, all four ports are active.
N9K-M6PQ	Cisco Nexus 9300 uplink module with 6 40-Gigabit Ethernet QSFP+ ports for the Cisco Nexus 9396PX, 9396TX, and 93128TX switches.
N9K-M6PQ-E	An enhanced version of the Cisco Nexus N9K-M6PQ uplink module.
N9K-M12PQ	Cisco Nexus 9300 uplink module with 12 40-Gigabit Ethernet QSPF+ ports.

Optics

To determine which transceivers and cables are supported by a switch, see the Transceiver Module (TMG) Compatibility Matrix. To see the transceiver specifications and installation information, see the Install and Upgrade Guides.

Cisco Network Insights for Data Center

Cisco NX-OS Release 9.3(8) supports the Cisco Network Insights Advisor (NIA) and Cisco Network Insights for Resources (NIR) on Cisco Nexus 9200, 9300-EX, and 9300-FX platform switches and 9500 platform switches with -EX/FX line cards. For more information, see the Cisco Network Insights documentation.

Upgrade and Downgrade

To perform a software upgrade or downgrade, follow the instructions in the *Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 9.3(x)*. For information about an In Service Software Upgrade (ISSU), see the Cisco NX-OS ISSU Support Matrix.

Exceptions

Cisco Nexus 9200, 9300-EX, and 9300-FX Platform Switches

The following features are not supported for the Cisco Nexus 9200, 9300-EX, and 9300-FX platform switches:

- 64-bit ALPM routing mode
- Cisco Nexus 9272PQ and Cisco Nexus 92160YC platforms do not support the PXE boot of the Cisco NX-OS image from the loader.
- ACL filters to span subinterface traffic on the parent interface
- Egress port ACLs
- Egress QoS policer (not supported for Cisco Nexus 9200 platform switches). The only policer action supported is drop. Remark action is not supported on the egress policer.
- FEX (not supported for Cisco Nexus 9200 platform switches)
- GRE v4 payload over v6 tunnels
- IP length-based matches
- IP-in-IP (not supported on the Cisco Nexus 92160 switch)
- Maximum Transmission Unit (MTU) checks for packets received with an MPLS header
- NetFlow (not supported on Cisco Nexus 9200 platform switches)
- Packet-based statistics for Traffic Storm Control (only byte-based statistics are supported)
- PVLANs (not supported on Cisco Nexus 9200 platform switches)

- PXE boot of the Cisco NX-OS image from the loader (not supported for Cisco Nexus 9272PQ and 92160YC switches)
- Q-in-VNI (not supported on Cisco Nexus 9200 platform switches)
- Q-in-Q for VXLAN (not supported on Cisco Nexus 9200 and 9300-EX platform switches)
- Q-in-VNI (not supported on Cisco Nexus 9200 platform switches)
- Resilient hashing for port channels
- Rx SPAN for multicast if the SPAN source and destination are on the same slice and no forwarding interface is on the slice
- SVI uplinks with Q-in-VNI (not supported for Cisco Nexus 9300-EX platform switches)
- Traffic Storm Control for copy-to-CPU packets
- Traffic Storm Control with unknown multicast traffic
- Tx SPAN for multicast, unknown multicast, and broadcast traffic
- VACL redirects for TAP aggregation

Cisco Nexus 9300-FX3 Platform Switches

The following features are not supported for the Cisco Nexus 9300-FX3 Platform switches:

- ACL with DSCP Wildcard Mask
- ARP Suppression with Reflective Relay
- Dynamic ACL - Named ACL support for applying blacklist/limited VLAN access for devices
- ECMP Hashing based on GRE Inner IP Header
- Enhanced ISSU
- Enhanced Policy-Based Routing (ePBR)
- ePBR Multi-Hop
- ePBR with Probes
- ePBR with User-Defined Probes
- IPv6 MIB support (IP-MIB)
- Multicast Service Reflection (Ingress, PIM-border, Egress)
- Multiple LLDP neighbors per physical interface
- Secure VXLAN EVPN Multi-Site using CloudSec
- Selective Q-in-VNI + Advertise PIP on a VTEP
- Selective Q-in-VNI + VXLAN VLAN on the same port
- Standard ISSU
- Symmetric Hashing - ECMP (Inner DA)
- Unidirectional Ethernet (UDE)

- VXLAN EVPN with downstream VNI
- VXLAN over parent interface that also carries sub-interfaces

Cisco Nexus 9300-GX Platform Switches

The following features are not supported for the Cisco Nexus 9300-GX platform switches:

- Asymmetric PFC
- Autonegotiation on all ports
- FC-FEC for Cisco Nexus 9316D-GX and 93600CD-GX switches is not supported on the second lane of the 50x2 breakout port.
- FEX
- Multicast over GRE

Cisco Nexus N9K-X9408PC-CFP2 Line Card and 9300 Platform Switches

The following features are not supported for Cisco Nexus 9500 platform switches with the N9K-X9408PC-CFP2 line card and Cisco Nexus 9300 platform switches with generic expansion modules (N9K-M4PC-CFP2):

- 802.3x
- Breakout ports
- FEX (supported on some Cisco Nexus 9300 platform switches)
- Flows other than 40G
- Multichassis EtherChannel Trunk (MCT)
- NetFlow
- Port-channel (No LACP)
- PFC/LLFC
- Precision Time Protocol (PTP)
- PVLAN (supported on Cisco Nexus 9300 platform switches)
- Shaping support on 100g port is limited
- SPAN destination/ERSPAN destination IP
- Traffic Storm Control
- vPC
- VXLAN access port

FEX Modules

The following features are not supported for FEX modules:

- Active-Active FEX and straight-through FEX are not supported on the Cisco Nexus 92348GC switch.

- For Cisco Nexus 9500 platform switches, 4x10-Gb breakout for FEX connectivity is not supported.

Cisco Nexus N9K-X96136YC-R Line Card

The following features are not supported for Cisco Nexus 9500 platform switches with the N9K-X96136YC-R line card:

- Breakout
- PTP and gPTP

Cisco Nexus N9K-X9736C-FX Line Card

The following feature is not supported for Cisco Nexus 9500 platform switches with the N9K-X9736C-FX line card:

- Ports 29-36 do not support 1 Gbps speed.

Cisco Nexus 9500 Cloud Scale (EX/FX) Line Cards

The following features are not supported for Cisco Nexus 9500 platform switches with -EX/FX line cards:

- FEX
- IPv6 support for policy-based routing
- LPM dual-host mode
- SPAN port-channel destinations

Related Content

Cisco Nexus 9000 Series documentation: Cisco Nexus 9000 Series Switches

Cisco Nexus 9000 and 3000 Series NX-OS Switch License Navigator: Cisco Nexus 9000 and 3000 Series NX-OS Switch License Navigator

Cisco Nexus 9000 Series Software Upgrade and Downgrade Guide: Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 9.3(x)

Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes: Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes, Release 9.3(8)

Cisco Nexus 3000 and 9000 Series NX-API REST SDK User Guide and API Reference: Cisco Nexus NX-API Reference

Cisco NX-OS Supported MIBs:
ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html

Supported FEX modules: Cisco Nexus 9000 Series Switch FEX Support Matrix

Licensing Information: Cisco NX-OS Licensing Guide

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.

Legal Information