Cisco Nexus 9000 Series NX-OS Release Notes, Release 9.3(9)

This document describes the features, issues, and exceptions of Cisco NX-OS Release 9.3(9) 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
February 8, 2022	Cisco NX-OS Release 9.3(9) became available.

New and Enhanced Software Features

There are no new software and hardware features introduced in Cisco NX-OS Release 9.3(9).

Open Issues

Bug ID	Description
CSCwa54414	Headline: Static MACs conf on int NVE deleted from vPC secondary after int NVE shut/no shut on vPC primary Symptoms: Static MACs configured on interface NVE may be deleted from vPC secondary device after interface NVE shutdown /no shutdown was executed on vPC primary. Workarounds: Delete/re-create the VLAN/VNI where the static MAC was originally configured and add back the static MAC on interface NVE. no vlan vlan vn-segment mac address-table static vni interface nve 1 peer-ip

CSCwa52532	Headline: Config Replace fails due to 'switchport mode' not supported on L3 interface
	
	Symptoms: When you perform Config Replace on a switch with switchport configuration present under an interface, CR might fail due to switchport not supported on a L3 interface:
	
	`interface Ethernet1/1`
	`switchport mode trunk`
	ERROR: Command validation failed. ERROR: eth1/1: 'switchport mode' is not supported on L3 interface
	
	The system default for all interfaces is to operate in L3 mode.
	Without 'switchport' issued initially to convert from L3 to L2 mode, 'switchport mode' will fail due to this.
	
	Workarounds:
	1) Edit the configuration file to include 'switchport' before 'switchport mode' under the interface configuration prior to performing Config Replace.
	2) Configure 'system default switchport' in global configuration causing the interfaces to operate in L2 mode by default.

CSCvy39573	Headline: Config replace fails with route-map config Symptoms: Config replace for match interface configurations under route-map is not successful. Workarounds: The order of the match interface should be the same.

Resolved Issues

Bug ID	Description
CSCvx88496	Headline: Telemetry source-interface unable to use dual stack Symptoms: When the source-interface is configured with ipv4 and ipv6 addresses at the same time?Only the newly configured address takes effect. When the device restart, the first address will take effect.When the source-interface is not configured, both ipv4 and ipv6 can take effect. Workarounds: do not configure source-interface under telemetry profile
CSCvz00192	Headline: IP SLA fails even when CLI can manually ping fine Symptoms: # ping x.x.x.x source x.x.x.x vrf MOBILE count 1000PING x.x.x.x. from x.x.x.x: 56 data bytes64 bytes from x.x.x.x: icmp_seq=0 ttl=254 time=3.853 ms64 bytes from x.x.x.x: icmp_seq=1 ttl=254 time=7.8 ms64 bytes from x.x.x.x: icmp_seq=2 ttl=254 time=7.967 ms sh track briefTrack Type Instance Parameter State Last Change 2 IP SLA 2 State DOWN 00:30:00 Here is the debug for the sla sender from the device that is seeing this issue:?debug ip sla sender all?2021 May 5 03:39:39.855590 sla_sender: IPSLA-OPER_TRACE:OPER:2 Starting icmpecho

Bug ID	Description
	operation - destAddr=x.x.x.x, sAddr=x.x.x.x2021 May 5 03:39:39.855706 sla_sender: sendLen 36 (fd 50) 2021 May 5 03:39:39.855724 sla_sender: IPSLA-OPER_TRACE:OPER:2 Socket fd 50, sent icmp packet 36 bytes seq 54379 2021 May 5 03:39:39.859206 sla_sender: recvLen 56 (fd 52) 2021 May 5 03:39:39.859227 sla_sender: packet is not for IPSLA 0 510382021 May 5 03:39:39.859244 sla_sender: recvLen -1 (fd 52) 2021 May 5 03:39:39.859274 sla_sender: ipsla_select: icmp-echo registered (non-batched reads)2021 May 5 03:39:40.474473 sla_sender: IPSLA-EVENT: mgd-evt type=0, component=0xdc489ff0 2021 May 5 03:39:40.474500 sla_sender: IPSLA-INFRA_TRACE:OPER:3 slaSchedulerEventWakeup 2021 May 5 03:39:59.854735 sla_sender: IPSLA-OPER_TRACE:OPER:2 Socket fd 50, sent icmp packet 36 bytes seq 54387 2021 May 5 03:39:59.863532 sla_sender: recvLen 56 (fd 52) 2021 May 5 03:39:59.863553 sla_sender: packet is not for IPSLA 0 51038 seems like this is stuck at 510382021 May 5 03:39:59.863570 sla_sender: recvLen -1 (fd 52) 2021 May 5 03:39:59.863602 sla_sender: ipsla_select: icmp-echo registered Workarounds: Reload or removefeature sla sender
CSCvz38944	Headline: N9k DHCPv6 Relay breaks after IPv6 snooping is removed Symptoms: Original Symptom from DHCPv6 Client perspective would be not receiving an IPv6 Address from the DHCPv6 server. CPU will only show the DHCPv6 solicit/Re-bind packets; Relay-FWD would NOT be originated by the n9k Workarounds: Reload fixes the issue(shut/no-shut of the SVIs Dont seem to fix the problem)
CSCwa52297	Headline: HSRP IPv6 Link local address not reachable Symptoms: ++Two Nexus9K in VPC with HSRP(IPv4 and IPv6) configured.++With NX-OS version 9.2.2 the HSRP IPv6 Link local address is reachable from the hosts connected downstream to a VPC++After upgrading the NX-OS to 9.3.7, The hosts loose connectivity to the HSRP IPV6 GW with link local addresses, all other IPV6 and Ipv4 are reachable. Workarounds: ++Failover/switchover the HSRP roles, will fix the issue.
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 others ARP accross 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.Other unicast communication works fine (eg. when we configure static ARPs) Workarounds: So far three possible workarounds were identified0. Disable 'featue nv overlay' on Spine. This will avoid this problem and also will ensure better hashing of packets over ECMP links.1. Enable " arp suppression" or.2. Remove " feature ptp" from the SPINES. After doing so " reload" or " reload ascii" is required to restore connectivity
CSCwa09450	Headline: SNMP memory allocation failure leads to a crash Symptoms: We see high values of RLIMIT and Total for the SNMP process, which leads to a crash Workarounds: There are no workarounds at the moment.The issue is being investigated.
CSCvy84652	Headline: N7K Doesn't flush locally generated default route after default route changes from bgp to ospf Symptoms: N7K/SUP3E Doesn't flush locally generated default route after default route changes from bgp to ospf Workarounds: clear the ospf neighbours
CSCvz05986	Headline: N9K/N7K - OSPF does not report syslog like EIGRP/BGP for Deadtimer Expired condition Symptoms: Neighbor Went down due to dead-timer expired (Note: interface didn't bounce)%OSPF-5-ADJCHANGE: ospf-1 [26244] Nbr X.X.X.X on Ethernet1/54 went DOWNAbove syslog does not reflect dead-timer expired like EIGRP/BGP. For Examplebgp- [26235] (test) neighbor x.x.x.x Down - sent: holdtimer expired error%EIGRP-5-NBRCHANGE_DUAL: eigrp-1 [26245] (test-base) IP-EIGRP(0) 1: Neighbor x.x.x.x (Ethernet1/54) is down: holding time expired Workarounds: N/A
CSCvz06050	Headline: N9K/N7K - OSPF event-history does not report event for Deadtimer Expired for Non-default VRF Symptoms: Neighbor Went down due to dead-timer expired (Note: interface didn't bounce)OSPF adjacency event-history does not show " DEADTIME" eventshow ip ospf internal event-history adjacency

Bug ID	Description
	ospf 1 [26244]: : Nbr x.x.x.x: DOWN --> INIT, event HELLORCVD ospf 1 [26244]: : Created new neighbor 192.168.20.2 ospf 1 [26244]: : Nbr x.x.x.x: DOWN --> DOWN, event ADJOK Workarounds: N/A
CSCvz17681	Headline: Snapshot creation permission denied Symptoms: Snapshot creation may fail with "Error:13(Permission denied)" , when different users with different roles were used to create snapshots previously. Workarounds:
CSCwa00776	Headline: *,G on LHR devices having incoming interface as null and RPF neighbor as 0.0.0.0 Symptoms: mroutes are not getting created, missing OIFs or (*,G) may have NULL RPF. Routes not getting created after clear, or routes not expiring. pim txlists are wrong, MRIB member marker missing. All this is due to pim txlists getting corrupted and pim stopping sending updates to mrib. Below is one symptom.*,G on LHR devices having incoming interface as null and RPF neighbor as 0.0.0.0. Below output from non-working scenario:# sh ip mroute 239.0.0.5 vrf blueIP Multicast Routing Table for VRF "blue" (*, 239.0.0.5/32), uptime: 00:00:07, igmp ip Incoming interface: Null, RPF nbr: 0.0.0.0 Outgoing interface list: (count: 1) Vlan105, uptime: 00:00:07, igmpBelow output after sup-failover:# sh ip mroute 239.0.0.5 vrf blueIP Multicast Routing Table for VRF "blue" (*, 239.0.0.5/32), uptime: 00:02:59, ip pim igmp Incoming interface: mti2, RPF nbr: 10.1.2.3 Outgoing interface list: (count: 1) Vlan105, uptime: 00:00:02, igmp Workarounds: Restart of pim process or Sup-failover resolves this problem.
CSCvv01406	Headline: EIGRP Neighbor flapped when adjust the time to past Symptoms: # show clock 09:01:36.172 UTC Wed Jul 15 2020 <<<<<<<< Time source is Hardware Calendar# clock set 05:00:00 15 july 2020 <<<<<<<< modify the time to the past cause the eigrp neighbor flappingWed Jul 15 05:00:00 UTC 2020# terminal monitor 2020 Jul 15 05:00:12 SWITCH %EIGRP-5-NBRCHANGE_DUAL: eigrp-1 [3813] (default-base) IP-EIGRP(0) 1: Neighbor 10.x.x.x (Ethernet1/XX) is down: Interface Goodbye received2020 Jul 15 05:00:17 SWITCH %EIGRP-5-NBRCHANGE_DUAL: eigrp-1 [3813] (default-base) IP-EIGRP(0) 1: Neighbor 10.x.x.x (Ethernet1/XX) is up: new adjacency Workarounds: NONE
CSCvv35496	Headline: N9508 MacSec - interface stuck in Authorization pending state due to one way traffic Symptoms: The N9508 with N9K-X9732C-EXM doesn't establish macsec session on random ports with port status in Authorization pending. The interface on the switch shows TX counters but no RX counters increment because of which the session is stuck in Authorization pending.N9508# show int eth1/14Ethernet1/14 is down (Authorization pending) Workarounds: Reload of the affected card may help to bring up the stuck sessions. If the ports again go back into Authorization pending state, replacing the line card may help to bring up affected macsec sessions.
CSCvv65667	Headline: MAC ACL + MAC packet classification could not let IPv6 NS/NA pass through in N9K-C93600CD-GX Symptoms: With the configuration of MAC ACL + MAC packet classification, the port will deny IPv6 NS/NA packets. It caused the IPv6 traffic could not go through the port.Example configuration:mac access-list test statistics per-entry 10 permit any any 0x86dd <<<<< ethertype of IPv6 interface Ethernet2/1 switchport mac port access-group test mac packet-classify no shutdown Workarounds: None
CSCvv69606	Headline: N9K-GX	9.3(x)	Interface down or CDP/UDLD/BFD traffic impacted due to transceiver speeds on quad. Symptoms: Operating a link on N9K-C9364C-GX with one speed, adding a second link with different speed to the same quad group and attempting to bring the second port up.Interfaces will be stuck in link not connected state. Workarounds: Reload the switch to recover the interfaces

Bug ID	Description
CSCvv71655	Headline: Vxlan l2fm/mtm core seen during static mac install Symptoms: MTM cores which causes a module boot failure.The following may be seen in the log:`show logging log`2021 Jun 12 00:18:45 %$ VDC-1 %$ %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service " mtm" (PID 26683) hasn't caught signal 11 (core will be saved). Workarounds: No workaround.
CSCvv82134	Headline: N9K CDP EEM not working - Max Limit for CDP EEM events reached !! with single event Symptoms: When attempting to create CDP neighbor-discovery event under EEM applet, system will throw error indicating limit is reached even if no previous events are defined and you are only configuring a single port for event:n9k(config-applet)# event neighbor-discovery interface e1/1Max Limit for CDP EEM events reached !! Workarounds: No workarounds available.
CSCvw23087	Headline: N9K: Command parsing error on configuring an interface as a trunk Symptoms: Nexus 9000 returns "No Such Instance currently exists at this OID" SNMP get-response to a v2c snmp walk of the dot1dBasePortIfIndex MIB. Workarounds: N/A
CSCvw47922	Headline: Support for L3 sub-intf egress RACL on N9300-EX/FX Symptoms: Egress RACL not allowed on Layer 3 Sub-Int interface.N93180YC-FX-1(config)# int e1/17.10N93180YC-FX-1(config-subif)# ip access-group mc-test outCannot apply egress RACLs on sub-interfacesN93180YC-FX-1# show ip access-lists mc-testIP access list mc-test statistics per-entry 10 permit ospf 224.0.0.5/32 any [match=0] 20 permit ospf any 224.0.0.5/32 [match=93] 30 permit ospf 1.1.1.0/30 any [match=0] 40 permit ospf any 1.1.1.0/30 [match=0] 50 permit ip 1.1.1.0/30 any [match=0] 60 permit ip any 1.1.1.0/30 [match=5] 70 permit ip any 239.1.1.1/32 [match=0] 80 permit ospf 2.2.2.0/30 any [match=7] 90 permit ospf any 2.2.2.0/30 [match=0] 100 permit ip 2.2.2.0/30 any [match=5] 110 permit ip any 2.2.2.0/30 [match=0] 120 permit ospf 3.3.3.0/24 any [match=9] 130 permit ospf any 3.3.3.0/24 [match=0] 140 permit ip any 3.3.3.0/24 [match=0] 150 permit ip 3.3.3.0/24 any [match=0 Workarounds: None
CSCvw75391	Headline: n9k TRM L2/L3 mixed mode anchor DR wont form OILs after recovery from maintenance mode Symptoms: OIL for Mroutes missing the Vlans where the receivers are present Workarounds: Reload is known to fix the issue or restart bgp
CSCvw99262	Headline: ETHPM Lock seen with PCM/MACSEC race condition Symptoms: ETHPM lock may be seen when doing configuration change on MACSEC enabled Po Workarounds: Reload of the device is needed to clear the lock
CSCvx21260	Headline: Nexus 9000/3000 NXOS : M500IT Bootflash in readonly mode Symptoms: Nexus 9000/3000 switch bootflash goes into read-only mode with M500IT SSD drive after 28,224 power-on-hours (POH) for the first time.The bootflash will stop responding causing failure of operations such as config changes/save, read/write operations etc.syslogs will also indicate bootflash diagnostic test failure%$ VDC-1 %$ %DIAGCLIENT-2-EEM_ACTION_HM_SHUTDOWN: Test <BootFlash> has been disabled as a part of default EEM action%$ VDC-1 %$ %DEVICE_TEST-2-COMPACT_FLASH_FAIL: Module 1 has failed test BootFlash 5 times on device BootFlash due to error Failure Workarounds: Reload the switch. However, this failure will reappear after 1008 hours of operation.Upgrade the SSD Firmware using following options?Option 1 - Upgrade NXOS VersionThe new Firmware with the fix for this issue will be packaged in 9.3(7), 10.1(2) and later NXOS versions. ?Option 2 - Upgrade SSD FW using SMU This option will be available under NX-OS Software Maintenance Upgrades (SMU) for 7.0(3)I7(x), 9.2(x), 9.3(x) and 10.1(1) on affected PIDs?7.0(3)I7(9) SMU nxos.CSCvx21260-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000.rpm is applicable to NX-OS Software Release 7.0(3)I7(1) to 7.0(3)I7(9)?9.3(6) SMU nxos.CSCvx21260-n9k_ALL-1.0.0-9.3.6.lib32_n9000.rpm is applicable to NX-OS Software Release 9.2(1) - 9.2(4) and 9.3(1) - 9.3(6)?10.1(1) SMU nxos.CSCvx21260-n9k_ALL-1.0.0-10.1.1.lib32_n9000.rpm is applicable to NX-OS Software Release 10.1(1)?Option 3 - Upgrade SSD FW using scriptScript upgrade_m500_firmware.tar.gz will be available under NX-OS Firmware section for the affected PIDs. This same script can be used for any version from 7.0(3)I7(x), 9.2(x), 9.3(x), 10.1(1) 1.Copy

Bug ID	Description
	upgrade_m500_firmware.tar.gz to switch bootflash.For 9500 Series Switches with Dual Supervisor, copy upgrade_m500_firmware.tar.gz to active as well as standby supervisor bootflash. Perform the upgrade first on standby supervisor and then active supervisor 2.Verify that upgrade_m500_firmware.tar.gz is in bootflashswitch# dir bootflash:	grep upgrade 2151467 Mar 08 19:17:00 2021 upgrade_m500_firmware.tar.gzIn case of Nexus 9500, verify upgrade_m500_firmware.tar.gz is also in Standby Supervisor bootflashswitch# dir bootflash://sup-standby/	grep upgrade 2151467 Mar 08 19:18:00 2021 upgrade_m500_firmware.tar.gz 3. Configure bash if not enabled and run bashswitch# feature bashswitch# run bash sudo subash-4.2# In case of Nexus 9500, login to standby supervisor for Nexus 9500 use rlogin command from active supervisorIf slot 28 is Standby supervisor, thenbash-4.2# rlogin sup28root@switch#If slot 27 is Standby supervisor, thenbash-4.2# rlogin sup27root@switch# 4.Copy the script from bootflash to /tmpbash-4.2# cp /bootflash/upgrade_m500_firmware.tar.gz /tmp 5.Uncompress the file in /tmp folderbash-4.2# cd /tmpbash-4.2# tar -xvzf upgrade_m500_firmware.tar.gzupgrade_m500_firmwareM500_MC03.binM500_MU05.bin 6.IMPORTANT - Execute the script upgrade_m500_firmware with no parametersbash-4.2# ./upgrade_m500_firmwareChecking SSD firmware ... Model Number: Micron_M500IT_MTFDDAT064SBD Serial Number: MSA2226001B Firmware Revision: MU01.00SSD Model: Micron_M500IT_MTCurrent SSD Firmware Version: 1Your SSD firmware needs update and will be upgradedUpdating the SSD firmware ... /dev/sda:fwdownload: xfer_mode=3 min=1 max=255 size=512.. Done. Model Number: Micron_M500IT_MTFDDAT064SBD Serial Number: MSA2226001B Firmware Revision: MU05.00Current SSD Firmware is 5SSD Firmware has been updated successfully Please Note: After Upgrade SSD Firmware will either be MU05.00 or MC03.00.
CSCvx23114	Headline: Breakout interface flaps on BearValley ports Symptoms: Multiple Symptoms may be seen.a) Breakout interfaces may flap unexpectedly on the Bear Valley port for no apparent reason and/orb) Some interfaces(other than the first interface in the breakout) may stay permanently down and/orc) First breakout Interface may experience a delayed link-up
CSCvx38173	Headline: VM Mobility issues seen, when inter-site connections between multisite flaps Symptoms: Mobility issues seen, when inter-site link between multisite flaps. Workarounds: None. But there is a easy recovery -> Clear the stale MAC entries at Site A immediately after the inter-site link failure
CSCvx50191	Headline: aclqos crash seen when peer switch is reloaded with tap-agg ACLs Symptoms: aclqos crash seen when peer switch is reloaded with tap-agg ACLs Workarounds: Remove tapagg as needed
CSCvx58626	Headline: SNMP Crash in Nexus9K after ISSU Upgrade Symptoms: Nexus9000 C9504, supervisor "N9K-SUP-A" crashed in during no disruptive upgrade from 7.0(3)I4(7) to 7.0(3)I7(9) aborting the ISSU:----- reset reason for module 28 (from Supervisor in slot 28) - --1) At 469702 usecs after Sun Jan 17 11:55:27 2021 Reason: Reset Requested by CLI command reload Service: Version: 7.0(3)I7(9)2) At 870075 usecs after Sun Jan 17 10:32:45 2021 <<<<<<<<<<<< Reason: Reset triggered due to HA policy of Reset Service: snmpd hap reset Version: 7.0(3)I7(9) Workarounds: None
CSCvx61532	Headline: CFS HAP reset and core file during system switchover Symptoms: A Nexus 9500 switch on 7.0(3)I7(x) version may undergo a HAP reset and generate a core file on performing a system switchover. Workarounds: None
CSCvx66678	Headline: RX==TX rate while port has "unidirectional send-only" configured and one fiber connected Symptoms: While "unidirectional send-only" command is configured and one TX fiber link is connected to corresponding port we can see that input and output rate is the same. With such configuration we should see only output rate and input rate should be 0. Workarounds: None

Bug ID	Description
CSCvx73823	Headline: N9K R-series: DEVICE_TEST-2-AUTHENTICATION_FAIL: Module 27 ACT2 Symptoms: A Nexus 9500 R-series may print the following logs:2021 Mar 16 23:14:51 switch %DEVICE_TEST-2-AUTHENTICATION_FAIL: Module 27 ACT2-Instance-1: The system integrity check has failed during the boot-up sequence. Please contact Cisco's Technical Assistance Center for more information Workarounds: None. The message is not service impacting
CSCvy10959	Headline: After ND ISSU, outdiscard counter displays wrong value even there is no drop Symptoms: After ND ISSU, discard counter displays wrong value even there is no drop Workarounds: After the ISSU if we issue the "clear counter" command then these drops will not be seen.
CSCvy33411	Headline: gnmi authentication with tacacs server fails if user is allowed only from a certain host Symptoms: gnmi requests fail with 'Authentication error' when a specific policy on ISE is configured to allow the tacacs user authenticate only from a certain host. Workarounds: None
CSCvy34183	Headline: PTPLC Core with tac-pac collection Symptoms: A crash due to a hap-reset in the ptplc process is seen: Reason: Reset Requested due to Fatal Module Error Service: ptplc hap reset Version: <output omitted> Workarounds: If a show tech is taken at regular intervals, reducing the frequency can reduce the odds of hitting the bug. Or collect individual outputs and exclude the 'show system internal ptplc log' command.
CSCvy54276	Headline: Virtual PO bring up failed after upgrading one peer to K on VMCT setup, vpc legs went down Symptoms: On N9336 deployment with vxlan, the" system nve peer-vni-counter" config takes long time to program the act tcam. Many mts transactions on on wait till the all programming is done and causes other side effects such as - interfaces not coming up- config changes hang until the mts transactions are completed Workarounds: The "system nve peer-vni-counter" is not needed in most vxlan deployments and can be removed from the config.
CSCvy55232	Headline: eth-port-sec cored after flapping interface configured with Eth Port Security Symptoms: The eth-port-sec process may crash after a flap of an interface configured with Ethernet Port Security. The following may be seen in the log:2021 Jul 28 22:21:45 %ETHPORT-5-IF_UP: Interface Ethernet1/15 is up in mode trunk2021 Jul 28 22:53:00 %ETHPORT-5-IF_DOWN_LINK_FAILURE: Interface Ethernet1/15 is down (Link failure)2021 Jul 28 22:53:01 fxg765swa6 %SYSMGR-2-SERVICE_CRASHED: Service "eth-port-sec" (PID 348) hasn't caught signal 11 (core will be saved). Workarounds: Avoid interface instability
CSCvy62164	Headline: Crash in N9K Fatal Module Error when downgrade - 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_clientDescription: Port Client DaemonExecutable: /lc/isan/bin/port_client Workarounds: No workaround. The switch is reloaded when the issue is hit.
CSCvy67232	Headline: %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "fcoelc" (PID 25997) hasn't caught signal 11 Symptoms: The service "fcoelc" crashes on a Cisco N9k that has a FCoE link. A core file will be generated due to the event.From NVRAM logs. Workarounds: none
CSCvy67509	Headline: Watchdog timeout reason may not be saved due to race condition Symptoms: After watchdog timeout reset there are no kernel logs or stack-traces available to determine a reason of the timeout, and reset-reason indicates that kernel did not receive NMI:----- reset reason for module 1 (from Supervisor in slot 1) ---1) At 123456 usecs after Sun May 01 01:02:00 2021 Reason:

Bug ID	Description
	Watchdog Timeout Service: HW check by card-client Version:" HW check by card-client" indicates that Kernel either didn?t receive NMI or kernel didn?t able to write the reset reason section. Workarounds: None
CSCvy68871	Headline: SVI counters not incrementing Symptoms: When hardware profle " svi-and-si" is enabled on the switch and a tunnel interface is configured/brought up the SVI counters will stop working Workarounds: None
CSCvz00772	Headline: After ND-ISSU SVI bd-label programmed wrong in BDState table when PACL label extended. Symptoms: Entries may get a PACL label programmed if the " hardware access-list tcam label ing-racl" is configured globally and no ACL is configured on the Nexus switch.
CSCvz02141	Headline: BGP IPv6 next hop should not contain link local address Symptoms: Loopback interface BGP IPv6 peering over its globally configured address results in the link-local also being populated in the next-hop advertisement. Workarounds: N/A
CSCvz02714	Headline: When having PVLAN promiscuous on trunk link BFD and ISIS not coming up Symptoms: Current config of 2 N9K-C93180YC-FX connected back to back with a trunk link with a combination of PVLAN, ISIS and BFD configuration.++ When the PO1 is configured as " Switchport mode trunk" , both the BFD and ISIS comes up.++ When the PO1 is configured as " switchport mode private-vlan trunk promiscuous" , BFD goes down and ISIS adjacency goes down.++ However, when we configure " OSPF" as a testing purpose, under the same SVI VLAN 14, it comes up fine. Workarounds: a. Provision a dedicated L2 trunk port (non PVLAN) between the switches.b. Remove BFD itself entirely for the time being to have isis adjacency – no feature BFD
CSCvz04580	Headline: N3408-S :: " log" keyword in ACL causes the traffic which otherwise would be blocked to hit CPU Symptoms: * so far issue seen on N3408-S platform – possibly others would also be affected.* traffic which should be blocked by the ACL seems to be allowed.* the issue seems to affect only traffic destined to the device – to the IP hosted on the switch itself* the transit traffic is filtered correctly Workarounds: Do not use " log" keyword in the ACLs
CSCvz07043	Headline: n9k: dot1q tag not removed on vxlan encap for classic VXLAN vlan Symptoms: Ingress VTEP do not remove dot1q tag when VXLAN encapsulate traffic send send to remote VTEP. This will cause that on remote (egress VTEP) traffic will have 2 dot1q TAGs and traffic will be dropped on destination host. Workarounds: Two possible workarounds: A) Do not have problem VLAN configured as access or as native on any portB) Configure " system dot1q-tunnel transit" with specific range that will NOT contain vlan that are not used for tunnel features as QinVNI/Selective QinVNI/Multitag or XconnectExample – VLAN 100 is a problem vlan and is not used for any tunnel feature – then workaround is exclude it from transit range:system dot1q-tunnel transit vlan 1-99,101-3967
CSCvz07052	Headline: n9k: dot1q tag not removed on vxlan encap for traffic arrived on subinterafce Symptoms: All traffic that arrive on L3 sub-interafce with dot1q encapsulation will retain dot1q tag when encapsulated to VXLAN and routed to remote VTEP. Workarounds: Remove ALL L3VNI VLANS " system dot1q-tunnel transit" As per documentation only Service Provider VLANs (vlans using tunnel feature as QinQ/QinVNI/Xconnect/Selective Qinvni and muttitag) should be defined in transit CLI using keyword VLAN
CSCvz07339	Headline: sysDescr doesnt return hardware type for Nexus9000 Symptoms: sysDescr doesn't return with snmp hardware type that includes " Nexus 9000" string. According to OID description we should return the system's hardware type. Workarounds: None

Bug ID	Description
CSCvz07646	Headline: lldp neighbor information dispeared if configured 'no lldp tlv-select power-management' Symptoms: If configure 'no lldp tlv-select power-management', 'show lldp neighbor' won?t show neighbor information and the below two counters in ?show lldp traffic? keep increasing.N9K-1(config)# show lldp neighborsERROR: No neighbour information <<<N9K-1(config)# show lldp traffic LLDP traffic statistics: Total frames transmitted: 252 Total entries aged: 4 Total frames received: 156 Total frames received in error: 124 <<< Total frames discarded: 124 <<< Total unrecognized TLVs: 0 Total flap count: 4
CSCvz09834	Headline: N9500-R/N3600 CoPP policer counters are incorrect after upgrade to 9.3.7 Symptoms: CoPP policer counters across all classes are incorrect. Workarounds: N/A
CSCvz14788	Headline: Type 5 l2vpn evpn routes are not advertised to multisite peers under certain conditions Symptoms: Two Symptoms may be seen:1) Site local prefixes(Type 5) received from local leaf switches are not advertised to remote Multisite Border Gateway Peers by the site Border Gateway2) Site local prefixes(Type 5) are incorrectly advertised by Multisite Border Gateway to remote Multisite Border Gateway peer when a route-map is supposed to be denying those prefixes Workarounds: For symptom 1), Either add a more specific permit above any deny sequence(specifically for the routes are blocked) or If feasible, remove the route-map completelyNo possible workaround so far for the symptom 2 mentioned above.
CSCvz16442	Headline: N9k - Reduce syslog severity for new PFC syslogs Symptoms: Below syslog are introduced recently which are severity 2 and fill up the nvram logs very quickly. Due to these repeated syslogs, other important syslog roll over pretty quickly and nvram logs are becomes less useful. Reduce the severity to S3 so that they're logged into normal logging and not into nvram logs. Message 1:2021 Jun 15 20:08:37.620 Nexus-switch %$ VDC-1 %$ %-SLOT1-2-BCM_UNEXPECTED_PFC_FRAMES: Ethernet1/7 received 20 unexpected PFC frames for COS 5Message 2:2021 May 24 11:10:48.541 Nexus-switch %$ VDC-1 %$ %-SLOT1-2-BCM_SYSLOG_LLFC_PAUSE_FRAME: 2 LLFC pause frames received on Ethernet1/28 Workarounds: None
CSCvz16757	Headline: N9k should not allow secondary IP address to be configured as PIM RP Symptoms: S,G Joins are not sent from the PIM any cast RP switch Workarounds: Remove the secondary IP address configuration and apply the PIM RP address as a primary IP address under loopback
CSCvz22694	Headline: Type 2 l2vpn evpn routes are not advertised to Multisite Peer under certain conditions Symptoms: Two symptoms will be seen;1) Type 2 Routes that are supposed to be blocked by a route-map will be incorrectly advertised to BGW Peer2) Type 2 Routes that are supposed to be advertised by a route-map permit statement, will NOT be advertised to multisite peer(incorrect behavior) Workarounds: NoneClearing/restarting BGP might NOT fix the problemReload also will NOT fix this problemIf feasible, removing route-map applied on the BGP peer will fix this issue.
CSCvz24559	Headline: N95R do not send PTP Delay Response packets Symptoms: Nexus 9500-R does not send PTP delay-response (if mxster port) OR delay-request (if slxve port) packets at the configured frequency and high corrections are observed on slxve port. Workarounds: 1. Remove pim sparse-mode config on SVI interface where the IGMP report arrives.2. Configure IGMP policy to block group 224.0.1.129.
CSCvz24626	Headline: Nexus 9000 Crash with BROADWELL_FPGA_WDT_GPIO_LEVEL_MASK Error Symptoms: Multiple crashes seen on N9K-C9348GC-FXP crashed while upgrading from version 9.3.5 to 9.3.7 without generating core file but with below reset reason: Reason: Reset Requested due to Fatal System ErrorService: sysmgr failed to re-register with heartbeat klm generating the following logs; %KERN-0-SYSTEM_MSG: [58291.070595] BROADWELL gpio_level_reg1=a89b4e35 gpio_use_sel_1=bd6defff gpio_io_sel_1=82fa6ef3 - kernel %KERN-0-SYSTEM_MSG: [58291.172828] BROADWELL gpio_level_reg2=fe8b4b91 gpio_use_sel_2=02fe4e37

Bug ID	Description
	gpio_io_sel_2=1d9abf26 - kernel %KERN-0-SYSTEM_MSG: [58291.275059] NMI due to BROADWELL_FPGA_WDT_GPIO_LEVEL_MASK error - kernel << %KERN-0-SYSTEM_MSG: [58291.346040] Uhhuh. NMI received for unknown reason 3d on CPU 0. - kernel %KERN-0-SYSTEM_MSG: [58291.417013] Do you have a strange power saving mode enabled? - kernel %KERN-0-SYSTEM_MSG: [58291.484867] Dazed and confused, but trying to continue - kernelOnce triggered due to upgrade to 9.3.7, continued with multiple other crashes on downgrade back to 9.2(4) . Workarounds: NONEIf suspected to be hitting this defect, Open a TAC case with the following outputs:show hardware internal dev-versionshow hardware internal versionshow env power detailshow system internal kernel messages
CSCvz25728	Headline: VPC legs on secondary put in BKN state after MCT Flap on primary Symptoms: During ascii replay or Post-ND ISSU MCT flap all the vpc legs went in blocking state, Workarounds: Flapping all the vpc legs
CSCvz29954	Headline: DHCPv6 advertise packets are sent with wrong Destination MAC when IPv6 Snooping is enabled Symptoms: DHCPv6 Advertise Packets are originated by n9k with wrong DMAC(specifically 0000.1c20.0005). DMAC may depend on the options that are received on the n9k from the DHCPv6 server within the Relay-Reply packet Workarounds: None other than removing IPv6 snooping(if feasible)
CSCvz34154	Headline: VRRP Groups 254 and 255 do not update tracked object status. Symptoms: VRRP showing a tracked object status that is incorrect per show track x for the object.show vrrp det int vlan xVlanx - Group 254 or 255 (IPV4)<snip> Tracked object id is x, with x and state Down show track xTrack x Interface port-channelx IP Routing IP Routing is UP x changes, last change 00:11:07 Tracked by: Track List 10 Delay up 30 secs, down 5 secs Workarounds: Use another group that is not 254 or 255*You can remove and reapply the vrrp configuration to refresh the tracked object status but it will fail again on the next transition to up or down.
CSCvz38543	Headline: N9k Type-7 to Type-5 LSA translation is not happening when Link-ID is in host IP range Symptoms: Issue is seen when type 7 LSA will be received with Link ID as host IP range. Workarounds: None
CSCvz41769	Headline: N9K Interface Microflaps May Cause All Control & Data-Plane Traffic to Fail Symptoms: A Nexus 9000 Series Switch with Cloud-Scale ASIC architecture (-EX, -FX, -FX2,(not GX, not GX2b) etc) may experience a condition where interface microflaps lead to the switch being unable to pass any traffic from either the control-plane or the data-plane. In this condition, buffer exhaustion syslogs may or may not be seen. All control plane protocols will fail, and multiple interfaces may slowly increment output discards, even with little to no egress traffic shown for the interface's egress rate."Microflaps" are link failures which occur and recover within the configured Link Debounce time (100ms by default). There are no syslog indications of a port experiencing microflaps, nor are microflaps often a cause for concern if they never lead to true link failure. Workarounds: - Reload- If condition is detected early enough, flapping the port experiencing the microflaps may recover the switch- If upgrading is not feasible, "link debounce time 0" can temporarily prevent a microflapping port from triggering the condition. This will disable the link debounce timer, and force a full reinitialization of the link in the event any loss of signal is detected. For a microflapping port, this may lead to rapid link failures, though the overall integrity of the switch will be maintained.
CSCvz42021	Headline: port-channel interface deletion through netconf running datastore causes switch stuck for ~5min Symptoms: After a port-channel is deleted through Netconf edit-config request, device is stuck for ~5min Workarounds: Send the Netconf request through candidate datastore. This candidate netconf request works successfully without any issues
CSCvz43052	Headline: Nexus 3000 switches cannot form IS-IS adjacency over vPC Peer-Link Symptoms: Nexus 3000 series switches that are configured to form an IS-IS adjacency between two vPC peers across the vPC Peer-Link will not successfully form an IS-IS adjacency between each other.

Bug ID	Description
	Workarounds: Create a dedicated Layer 3 connection between vPC peers and form IS-IS adjacencies over the dedicated Layer 3 connection instead of forming the IS-IS adjacency across the vPC Peer-Link.
CSCvz44412	Headline: N9K and N3K Switch 100Gig Interface won't come up after interface Flap

Symptoms: ++ Interface doesn't come Up after the shut/unshut on the Nexus 9500 With the LC N9K-X9736C-FX++ SFP used is the QSFP 40/100G-SRBD, Link between the Nexus 9500 and Nexus 3408

Workarounds: ++ Apply speed to 100Gig and disable auto negotation++ Shutdown the interfaces on both the sides, unshut the interface on N9K first and later on 3k |
| CSCvz55570 | Headline: Nexus 9k not sending authorization request

Symptoms: Nexus 9348 is being administered with ISE device administration feature which uses TACACS+When going through the aaa flow, we see authentication and accounting queries being send back to ISE. But authorization request are never send by the NXFrom ISE perspective, we always hit the correct policy. But authorization request never reaches ISE.

Workarounds: Configure Inband interface as global TACACS interface.--------------ip tacacs source-interface <Vlan123>   <<<<< the inband channel as global TACACS interfacetacacs-server host <X.X.X.X key> 7 <xyz> aaa group server tacacs+ tac_group   server <X.X.X.X>   source-interface <Vlan123> -------------- |
| CSCvz59638 | Headline: unable to change tcam carving

Symptoms: unable to change tcam carving

Workarounds: no |
| CSCvz63075 | Headline: N9500 - 802.1Q Header added to Inner Packet Tagging L3VNI VLAN Before Egress

Symptoms: Ingress traffic received on 9500 EVPN VTEP through N9K-X9564PX destined to a host learned from a remote VTEP via L3VNI of Tenant VRF will have a dot1q tag added to the packet prior to VXLAN Encapsulation tagging the L3VNI VXLAN VLAN. Route to DST from 9504 is learned through L3VNI - 7000700 (VLAN 700).

Workarounds: There is no workaround identified for this issue aside from downgrading to a release not exhibiting this issue. |
| CSCvz65993 | Headline: tahoe0 brought down resulting in inband connectivity failure

Symptoms: In version 9.2.3, Tahoe0 interfaces go down or not pass traffic rendering the switch unresponsive. One or more software components can fail such as diagnostic modules, L2ACL diagnostics, loopback test, kernel errors etcIn version 9.3.x, the switch reloads due to existing GOLD enhancements that can detect L2ACL diag failure and resets it.

Workarounds: Reload the device to clear the issue. |
| CSCvz67182 | Headline: n9k/xconnect: Xconnect traffic loss in Multicast underlay due to dot1q tag miss over MCT

Symptoms: Packet drop or duplicated traffic for VXLAN/xconnect traffic when traffic is passing over VPC PeerLink during failover scenario when all uplink are down

Workarounds: Use different vlan ID for backup underlay routing |
| CSCvz75541 | Headline: N9K-C93180YC-FX3 port bringup issue in FEX mode

Symptoms: When N9K-C93180YC-FX3 is used in FEX-mode, ports don't come up.

Workarounds: NA |
| CSCvz75734 | Headline: N9K EVPN route installs incorrect/random next-hop.

Symptoms: evpn route imported into vrf with bogus next-hop on a VTEP causing traffic to black-hole. |
| CSCvz75734 | Headline: N9K EVPN route installs incorrect/random next-hop.

Symptoms: evpn route imported into vrf with bogus next-hop on a VTEP causing traffic to black-hole.

Workarounds: delete "soft-reconfiguration inbound" CLI from template |

Bug ID	Description
CSCvz76262	Headline: ng-oam loop-detection stops preventing loop after modifying allowed vlan list on trunk Symptoms: NGOAM loop-detection fails to block a loop after list of allowed vlans on a trunk is modified. Workarounds: * shut / no shut problematic interface
CSCvz78704	Headline: ESI-RX-MS BUM traffic drop cross MS after config replace Symptoms: on mlag vpc border gateway, cross sites BUM traffic might be dropped after config-replace with non anycast border gateway configurations. Workarounds: Reload border gateway after configuration change.
CSCvz80795	Headline: n9k:CTS tagged packets are dropped upon receiving from N7k Symptoms: SGT Tagged packets received from n7k gets dropped by n9k Workarounds: None
CSCvz86703	Headline: nxos 9.3(8) ip radius-source interface not working Symptoms: mab/dot1x will failed due to ip-source interface not crafting the correct source address Workarounds: None
CSCvz89455	Headline: Seeing delayed linkup on QSA links on 9736C-FX LC. Symptoms: Some of QSA links are exhibiting delayed linkup. Time is more than 1 hour. This is seen on both regular & BV ports. Workarounds: None
CSCvz89560	Headline: netconf returns 'port already in a port-channel' error when phys interface goes first thru dme Symptoms: When a netconf edit-config request to add a member to the port-channel is sent, it returns an error - "ERROR: : port already in a port-channel, no config allowed" Workarounds: In the netconf edit-config payload, adding mtu property to the member interface is the workaround for this issue.'mtu' value of member interface should match with the 'mtu' value of port-channel interface.
CSCvz91416	Headline: n9k:CTS tagged packets are dropped in Non-default VRF with Subinterface Symptoms: OSPF route also not update Workarounds: USE default vrf
CSCvz93622	Headline: Layer 3 VNI SVI is down indicating "VLAN/BD is down" after upgrade. Symptoms: After disruptive upgrade from nxos 9.3(5) to nxos 9.3(8) the layer 3 vni svi on a leaf/Border Leaf/Border Gateway may stay down indicating "VLAN/BD is down" leading to connectivity issues. Workarounds: Shut/No-shut the L3 VNID SVINote that a reload might not fix it as next reload might also result in L3VNID SVI to remain in down/down
CSCvz98995	Headline: n9k/msite - DF bit not correctly programmed on DCI interafces Symptoms: In multisite with split horizon enabled "split-horizon per-site" there can be observed BUM (broadcast/multicast) packet drop after one of Anycast BGW is put in maintenance mode. When issue is present ELTM do not have configured DF bit for any VLAN. Workarounds: To prevent issue to happen Disable "split horizon" feature or reload device without maintenance mode.To recover from issue flap NVE interface on remaining ABGW (devices that are not in maintenance mode)
CSCwa04023	Headline: Nexus // IPv4 /32 host route not in target VRF with route leaking Symptoms: Transit traffic between hosts in 2 different vrf is punted to CPU instead of getting hardware switched. BGP is used to leak routes between these VRFs and a third VRF.Receive a /32 am host route in the source VRF. Workarounds: Statically assigning the ARP entry in the source VRF

Bug ID	Description
CSCwa07236	Headline: N9k VXLAN Encapsulation uses Incorrect Outer Destination IP Symptoms: VXLAN Encapsulated Packets are sent with Wrong Outer Destination IP address. URIB says the route is learnt from VTEP X, but Packets are encapsulated with outer DIP of VTEP Y. Workarounds: None.
CSCwa16832	Headline: No radius pacets after an OIR or switchover event on the active sup - N9K EOR Symptoms: Radius authentication failure and the following logs are displayed: MTR-2A-32-Core1# sh logg log | last 102021 Nov 8 16:25:41.268 MTR-2A-32-Core1 %RADIUS-3-RADIUS_ERROR_MESSAGE: Failed looking up IP address for RADIUS server 10.197.241.1922021 Nov 8 16:25:41.268 MTR-2A-32-Core1 %RADIUS-3-RADIUS_ERROR_MESSAGE: All RADIUS servers failed to respond after retries.2021 Nov 8 16:25:42.465 MTR-2A-32-Core1 %RADIUS-3-RADIUS_ERROR_MESSAGE: Failed looking up IP address for RADIUS server 10.197.241.192Ethanalyzer does not display the RADIUS PAP REQ packets and the next-hop will not see anything coming in Workarounds: None
CSCwa17807	Headline: n9k/VXLAN: MAC address not correctly learned after REMOTE -> LOCAL mac move Symptoms: MAC address are not correctly updated after large (more than 500 MAC addresses) are moved from remote VTEP to local VTEP. After the move MAC address table still point to remote VTEP and is not updated until GARP/ARP is received from host or ARP timeout Workarounds: Ensure host will send GARP/ARP after the move or downgrade to 9.3(7a)
CSCwa24516	Headline: ELTM process crashes while handling an MTS messages. Symptoms: A Nexus 9K switch running NX-OS 9.2(x) or 9.3(x) code may experience a HAP reset due to a segfault (signal 11) crash in the ELTM process when it is handling an MTS (Messaging and Transaction System) message. This is due to the fact that software level memory corruption has occurred. The actual feature that generated the MTS event that ELTM is handing can be random, as the corruption was caused by something prior. Workarounds: None.
CSCwa25046	Headline: BGP neighbor flapping when routes churn with soft-reconfig Symptoms: All bgp neighbor flap randomly Workarounds: remove soft-reconfig
CSCwa25377	Headline: psskmalloc: aclqos: error! malloc for km_p failed Symptoms: The memory allocation is failing for "aclqos" time to time when customer is trying to do some config changes. Workarounds: 1. Free up the memory using the command sequence provided, or++ Get access to bash shell++ Go to folder proc/sys/vm++ Monitor memory available from cache++ Change value with "echo 3 > drop_caches" ++ Monitor memory again with command cat/proc/meminfo |egrep -I -e "MemFree|MemAvail" Example:=======bash-4.3# cd /proc/sys/vmbash-4.3# cat /proc/meminfo | egrep -i -e 'memfree|memavail'MemFree: 16154452 kBMemAvailable: 17060220 kBbash-4.3# echo 3 > drop_cachesbash-4.3# cat /proc/meminfo | egrep -i -e 'memfree|memavail'MemFree: 16640264 kBMemAvailable: 17063700 kB2. Reload the switch.switch# reloadThis command will reboot the system. (y/n)? [n] y
CSCwa26796	Headline: Traffic is dropped while Initializing HIF after online fex Symptoms: Traffic is dropped while Initializing HIF after on-line fex Workarounds: n/a
CSCwa27101	Headline: MAC address was learnt from a STP(rstp) blocked port Symptoms: MAC address was learnt from a STP(rstp) blocked port. Workarounds: unknown

Bug ID	Description
CSCwa29328	Headline: dfe-tuning-delay 1500 cannot be configured Symptoms: dfe-tuning-delay 1500 cannot be configured on a port-channel interface even after deleting the configuration about port-channel. and after deleting the configuration about port-channel, dfe-tuning-delay 1500 can only be configured after configured [dfe-tuning-delay 1000]-------------------------------------switch(config-if)# show run inter e1/4interface Ethernet1/4 channel-group 1 mode active no shutdownswitch(config-if)# dfe-tuning-delay 1500switch(config-if)# show run inter e1/4interface Ethernet1/4 channel-group 1 mode active no shutdownswitch(config-if)# no channel-group 1 mode activeswitch(config-if)# show run inter e1/4 no shutdownswitch(config-if)# dfe-tuning-delay 1500switch(config-if)# show run inter e1/4interface Ethernet1/4 no shutdownswitch(config-if)# dfe-tuning-delay 1000switch(config-if)# show run inter e1/4interface Ethernet1/4 dfe-tuning-delay 1000 no shutdownswitch(config-if)# dfe-tuning-delay 1500switch(config-if)# show run inter e1/4interface Ethernet1/4 dfe-tuning-delay 1500 no shutdown----------------------------------- Workarounds: configure [dfe-tuning-delay 1000] and then [dfe-tuning-delay 1500] can be configured
CSCwa30060	Headline: Process swtele not running after initial bootup (no crash file generated) Symptoms: Switch boots up. Customer goes to configure Cloud Scale Telemetry feature. Finds that swtele feature is not running:looking at ps shows that swtele is not running:```plaintextslfsw20-s00-1# run bash ps aux	grep swteleslfsw20-s00-1# < ----- Process is not runningNormal switch output showing process is running:slfsw20-s00-2# run bash ps aux	grep swteleroot 9702 0.1 0.4 1433180 112564 ? Ssl Apr30 188:58 /lc/isan/bin/swtele --tcp-timeout 0 --ip-addr 127.1.2.1slfsw20-s00-2#Looks like swtele process never started. Workarounds: Reload the switch. Process starts up normally next time.
CSCwa34555	Headline: aclqos crash while changing policy-map Symptoms: Switch unexpected reload. Last reload reason showing: Last reset at 59767 usecs after Wed Nov 17 11:05:55 2021 Reason: Reset Requested due to Fatal Module Error System version: 7.0(3)I7(2) Service: System manageraclqos core files created due to this unexpected reload: SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "aclqos" (PID 30433) hasn't caught signal 11 (core will be saved). Workarounds: No workaround at the moment.
CSCwa35108	Headline: stale nexthop entry stuck in route table if VRF leaking Symptoms: Some OSPF routes are advertised in the BGP which are leaked to different VRF, once the OSPF routes reconverge in the sourcing VRF, those route will stuck in destination VRF and mark as (stale) in the VRF. Workarounds: Clear the route in the routing table
CSCwa45206	Headline: Tahusd core found for 9788TC2-FX LC on Chassis reload Symptoms: %KERN-2-SYSTEM_MSG: [6451477.977145] usd process 25139, uuid 1356 (0x54c) tahusd failed to send heartbeat - kernel%SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "tahusd" (PID 25139) hasn't caught signal 6 (core will be saved).%SYSMGR-SLOT1-2-HAP_FAILURE_SUP_RESET: Service "tahusd" in vdc 1 has had a hap failure%SYSMGR-SLOT1-2-LAST_CORE_BASIC_TRACE: fsm_action_become_offline: PID 12130 with message Could not turn off console logging on vdc 1 error: mts req-response with syslogd in vdc 1 failed (0xFFFFFFFF) . %SYSMGR-SLOT1-2-LAST_CORE_BASIC_TRACE: core_client_main: PID 10237 with message filename = 0x102_tahusd_log.25139.tar.gz . Workarounds: None
CSCwa48887	Headline: N9K EVPN LEAF hap reset or unresponsive when configuring checkpoints with NXAPI-DME REST Symptoms: Switch may become completely unresponsive and fully isolated * only chassis LED lit is STATUS light * console and management interface are unresponsive * control-plane stops responding * interfaces are all downOn more recent versions of code a hap reset will be detected, which causes the switch to self-reload and become operational again. On older versions of code when there is no hap-reset, the only way to recover is to manually power cycle the switch * Syslogs may show the following process crash: ascii-cfg * Switch may experience hap-resets for tahusd, l2fm, vdc_mgr or pltfm_configsh logg nvram	in core< snip >2021 Dec 11 05:40:38.782532 LEAF47 %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service "ascii-cfg" (PID 20023) hasn't caught signal 11 (core will be saved).2021 Dec 11 05:54:21.252051 LEAF47 %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service

Bug ID	Description
	"ascii-cfg" (PID 26524) hasn't caught signal 11 (core will be saved).2021 Dec 11 06:04:31.746874 LEAF47 %$ VDC-1 %$ %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "tahusd" (PID 23621) hasn't caught signal 11 (core will be saved).2021 Dec 11 06:05:18.666840 LEAF47 %$ VDC-1 %$ %SYSMGR-SLOT1-2-LAST_CORE_BASIC_TRACE: core_client_main: PID 29910 with message filename = 0x102_tahusd_log.23621.tar.gz * We also see the following syslogs: high count of PFC frames reported%ACLQOS-SLOT1-2-ACLQOS_UNEXPECTED_PFC_FRAMES: Ethernet1/31 received 566935683072 unexpected PFC frames for COS 0 Workarounds: pro-active: use NXAPI-CLI to create/delete/list checkpoints. corrective action: * if the switch has become completely unresponsive and did not reload by itself, a manual power cycling will restore operation
CSCwa56859	Headline: Crash on N9K in VPC with port-security enabled on FEX interfaces Symptoms: Crash in eth-port-sec service.%SYSMGR-2-SERVICE_CRASHED: Service "eth-port-sec" (PID <>) hasn't caught signal 11 (core will be saved).# show coresVDC Module Instance Process-name PID Date(Year-Month-Day Time)--- ------ -------- --------------- -------- --------------- -----------1 1 1 eth-port-sec <> <> Workarounds: Remove unsupported configuration.
CSCvx31824	Headline: some ports get err-disabled after switch boot up Symptoms: After switch boot up, you may see some ports stuck in initializing status and get err-disabled finally. Reason is sequence timeout.%ETHPORT-5-IF_DOWN_ERROR_DISABLED: Interface Ethernet1/4 is down (Error disabled. Reason:sequence timeout)And there wiil be a "ipqosmgr" crash finally.>%SYSMGR-2-SERVICE_CRASHED: Service "ipqosmgr" (PID 28294) hasn't caught signal 6 (core will be saved) Workarounds: shut/not shut the port
CSCwa18174	Headline: Nexus 9K/3K BCM - Not all ECMP paths are programmed in hardware after microflap Symptoms: If an interface that is used as a ECMP next-hop experiences a micro flap, and the link comes back online within the configured debounce timer, then this particular interface will not be used in hardware for ECMP load-balancing. Workarounds: shutdown/no shutdown the affected interface
CSCvz22691	Headline: N3500 interfaces may stop processing rx traffic after connected host NIC flaps Symptoms: N3500 interface rx counters are not incrementing. Workarounds: Reload ascii of N3500.
CSCvz22936	Headline: N3500- show run all - lines are concatenated together in one single line Symptoms: Device not fixed yet with toggle command. All of these lines are concatenated together in one single line. Workarounds: none
CSCvz64655	Headline: Nexus 3548 ACL dropping initial fragmented UDP packet. Symptoms: When configuring an ACL on a L2 or L3 interface to permit fragmented traffic, if the protocol is UDP, the first/initial-fragment is dropped. Workarounds: Change the ACL statement to "ip" instead of "udp".
CSCwa48958	Headline: L3VNI goes down in system mode maintenance Symptoms: SVI/L3VNI goes down when implemented in Maintenance Mode and stays down after reload. Workarounds: None. L3VNI are brought up on reload to decrease convergence times when bringing device back out of maintenance mode.
CSCvz75486	Headline: N3K - BGP Checkpoint rollback failures for configs with inherit commands Symptoms: Checkpoint rollback failure when applying configuration under multiple BGP neighbour with inheriting peer template. Workarounds: None.

Bug ID	Description
CSCvx88496	Headline: Telemetry source-interface unable to use dual stack Symptoms: When the source-interface is configured with ipv4 and ipv6 addresses at the same time?Only the newly configured address takes effect. When the device restart, the first address will take effect.When the source-interface is not configured, both ipv4 and ipv6 can take effect. Workarounds: Do not configure source-interface under telemetry profile
CSCwa27750	Headline: Nexus stops responding to SNMP requests for CISCO-VTP-MIB::vlanTrunkPortTable Symptoms: Observed when Performing SNMP Walk from Nexus 9300 Device and MIB stopped working. SNMP Walk returned " No Such Object available on this agent at this OID" . Workarounds: As a workaround - 1. Reload the Switch 2. Kill or reload the snmp-daemon
CSCvz94723	Headline: N9300-FX fails to apply unique egress QoS policy to all L2 physical interfaces Symptoms: N9300-FX fails to apply unique egress QoS policy to more than 31 physical interfaces. Workarounds: N/A

Device Hardware

The following tables list the Cisco Nexus 9000 Series hardware that Cisco NX-OS Release 9.3(9) 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 SFP28 and 4-port 40/100 Gigabit Ethernet QSFP28 line card	4	8	16
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	4	8	16

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

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 card	4	8	16

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	4	5

Product ID	Description	Minimum	Maximum
	module		
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
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
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

Product ID	Description	Quantity	Cisco Nexus Switches
			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 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	2	9332PQ

Product ID	Description	Quantity	Cisco Nexus Switches
	coloring)		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 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

Product ID	Description	Quantity	Cisco Nexus Switches
			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 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	2	9364C-GX

Product ID	Description	Quantity	Cisco Nexus Switches
	airflow (blue coloring)		
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
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

Cisco Nexus Switch	Description
	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(9) 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

- gPTP

Note: One-step PTP is supported only on Cisco Nexus 9500-R series.

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(9)

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.