Cisco Nexus 9000 Series NX-OS Release Notes, Release 7.0(3)I7(8)

This document describes the features, caveats, and limitations of Cisco NX-OS Release 7.0(3)I7(8) software for use on the following switches:

- Cisco Nexus 9000 Series
- Cisco Nexus 31128PQ
- Cisco Nexus 3164Q
- Cisco Nexus 3232C
- Cisco Nexus 3264Q

For more information, see Related Content.

Date	Description
September 29, 2020	Upgrade and Downgrade section revised.
June 30, 2020	Added CSCvu20429 to Open Issues.
March 10, 2020	Added CSCvr09175 and CSCvr14976 to the Resolved Issues.
March 5, 2020	Added EPLD Release Notes to New Documentation.
March 4, 2020	Cisco NX-OS Release 7.0(3)I7(8) became available.

Contents

New Software Features

Feature	Description
ECMP Load Balancing	Support added for configuring the ECMP load-sharing algorithm based on inner NVGRE header. For more information, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 7.x.
Enabling syslog messages to account link level pause frames	Support to enable syslog messages to account all the incoming global and link level pause frames. For more informatin, see the Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide, Release 7.x.
Enabling syslog messages to account packet drops	Support to enable syslog messages to account packet drops on multicast queues for no-drop class. For more information, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 7.x.
Interface Port Channel	Added support to select the configuration a port channel and then apply that configuration to the member ports of all the configured port channels using the interface port-channel all command. For more information, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 7.x.
Link Layer Discovery Protocol (LLDP) Multi-Neighbor Support on Interfaces	Support for up to three (3) neighbors per interface. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 7.x.
Link Layer Discovery Protocol (LLDP) Multi-Neighbor Support on Port Channels	Support on LLDP on interface port channels. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 7.x.
Link Layer Flow Control (LLFC) Watchdog	Support for reacting to LLFC packets on a PFC-enabled interface by shutting the no-drop queue until a timer resets it. For more informatin, see the Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide, Release 7.x.
MACsec	Added support for MACsec on Cisco Nexus N9K-X9732C-FX line card. For more information, see the Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 7.x.
SSH Algorithm Support	The ssh ciphers and ssh kexalgos commands were modified. The aes256-gcm keyword was added to the ssh ciphers command and ecdh-sha2-nistp384 keyword was added to the ssh kexalgos command. For more information, see the Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 7.x.

New Hardware Features

There are no new hardware featues in this release.

Open Issues

Bug ID	Description
CSCvq62128	Headline: Config change of deleting cast-group and enabling IR under member VNI, fails Symptoms: On NVE1, config change of deleting mcast-group and enabling IR under member VNI, fails. Workarounds: Wait for a while after deleting mcast-group, and then enable IR under member VNI.
CSCvq71546	Headline: MTS leak on VTP when vlan creation with more than supported range is tried with RSTP Symptoms: Create large set of VLANs -> command fails with following message: ERROR: VLAN creation failed : Maximum vlan limit(507) reached for RSTP mode System side - mts leak is observed for MTS_OPC_VLAN_MGR_VLAN_CREATED in VTP queue. Workarounds: Move to config-vlan mode using existing VLAN in system and then enter the exit command.
CSCvr47876	Headline: Port-channel ECN marked packets statistics is incorrect on show policy-map int detail Symptoms: Port-channel ECN marked packets statistics is incorrect on show policy-map int detail Workarounds: Use the "show queuing" or "show queuing tabular" commands to check the counter.
CSCvs37619	Headline: SSO is causing heavy permanent traffic drop && lot of v4, v6 adjacencies are tentative Symptoms: Traffic drop due to adjacencies are not learned after multiple SSOs Workarounds: Clearing MAC will resolve the issue
CSCvs52365	Headline: n9k - VXLAN - L3 traffic incorreclty policed when CIR is reached Symptoms: VXLAN - L3 traffic is incorrectly policed when CIR is reached Workarounds: None
CSCvs19118	Headline: Multicast traffic forwarded with TTL 0 Symptoms: Multicast traffic forwarded with TTL 0 Workarounds: None
CSCvs62874	Headline: interface port-channel all fails when sub interfaces present Symptoms: interface port-channel all fails Workarounds: Remove all sub interfaces from running config

CSCvs66847	Headline: While doing ND ISSU from GMR6 to GMR7 on vPC primary seeing momentary traffic loss Symptoms: While doing ND ISSU from GMR6 to GMR7.44 on Cisco Nexus 9500 platform swtiches (vPC Primary) seeing momentary unicast traffic loss. Workarounds:N/A
CSCvs85921	Headline: Need to add config check for LLDP port-channel feature on vPC, FEX Pos Symptoms: When an LLDP port channel is enabled on a port channel which is configured later for vPC or FEX , the LLDP multiple neighbor feature might not work as expected. Workarounds: Disable the LLDP feature and re-enable the LLDP feature. Add back any non-default LLDP configuration that might have been present earlier on the switch.
CSCvs88642	Headline: 3 msec packet loss on port-channel member down for flows hashing to non-impacted member port Symptoms: sub-second packet loss on port-channel member down for flows hashing to non-impacted member port Workarounds: None
CSCvs89480	Headline: First Generation N9K: Pvlan l2 traffic drop observed after remove and reconfiguring Pvlan Symptoms: Traffic and other control traffic get dropped in this port. CC will fail for this port. Workarounds: Interface flap will recover the port from issue state.
CSCvs90704	Headline: Reload ASCII causes source IP as 0x0 Symptoms: Analytics FT records will be dropped as the source address of packet will be 0x0. Workarounds: Unconfigure and reconfigure the FT analytics configuration
CSCvs93457	Headline: QoS:Queue dropped pkts not updated for QOS group 0/7 in sh policy-map int eth x/x type queuing Cli Symptoms: The drop stats for last two data queues in queuing policy are not displayed in "show policy interface Ethernet <intf> type queuing" cmd on Nexus3000. Workarounds: Drop stats for all queues can be seen with this command instead: show queuing interface eth <intf>.
CSCvt04520	Headline: PCIE error seen on 9364 in syslog Symptoms: PCIE Correctable error messages seen in syslog Workarounds: None

CSCvu20429	Headline: Storm control commands broadcast/muliticast added to interface configs after non disruptive ISSU Symptoms: After multiple non disruptive ISSUs, the following commands were added to the interface configuration causing complete connectivity issues. For instance, non-disruptive ISSU was performed as below versions and all L2/L3 interfaces were added with below commands. I7.0(3)I4(1) > 7.0(3)I7(7)> 7.0(3)I7(8) interface Ethernet1/17 link transmit reset-skip no link dfe adaptive-tuning storm-control broadcast level pps 0 <- added after the upgrade storm-control multicast level pps 0 <- added storm-control unicast level pps 0 <- added switchport virtual-ethernet-bridge <- added Workarounds: Reconfigure the same commands on effected ports and then remove it as indicated below. configure terminal interface e1/17 storm-control broadcast level pps 0 storm-control multicast level pps 0 storm-control unicast level pps 0 switchport virtual-ethernet-bridge config t int eth 1/17 no storm-control broadcast level pps 0 no storm-control multicast level pps 0 no storm-control unicast level pps 0 no switchport virtual-ethernet-bridge Or Write erase and reapply the original configurations.

Resolved Issues

Bug ID	Description
CSCvb84849	Headline: Need support for DOM on FEX HIF ports Symptom: When entering the show interface ethxxx/y/z transceiver detail command on a Cisco Nexus 9000 Series switch (FEX HIF), we see that DOM is not supported. This defect is an enhancement to support DOM on the Cisco Nexus 9000 FEX HIFs. Workaround: None.

Bug ID	Description
CSCvi58641	Headline: eth_port_channel core ended in loader> after wr era + copy cfg start + boot build 466 Symptom: eth_port_channel core had been observed Workaround: NA
CSCvi91868	Headline: Increased CPU usage for nsusd process (25%) Symptom: Increased CPU usage for nsusd process (25%) Workaround: None
CSCvj03640	Headline: vPC setup: after reload, seeing ETHPORT-3-IF_ERROR_VLANS_REMOVED console logs per VLAN Symptoms: This error notification is when a VLAN is removed due to vPC check. It is expected to show up on the screen but the issue is that the error message was being displayed per VLAN. In a fully scaled setup, we would see around 4k error messages scrolling on console. Fix: Created a single error message for all VLANs that are suspended. Displayed it as VLAN_LIST. Workarounds: NA
CSCvj57391	Headline: NVE may not show up as CFS application after reload/bootup Symptom: NVE may not show up as registered with CFS. This can lead to inconsistency in respect to NVE Sync: - OVSDB setup may observe no VNI hashed replication list on vPC secondary due to no BFD sync possible. - VLAN consistency check may fail with VXLAN multi-homing setup (no vPC) Workaround: Remove NV overlay feature: # no feature nv overlay Add overlay feature: # feature nv overlay
CSCvn64028	Headline: Nexus 9000: L2 QOS TCAM resources not released when policy-map applied with and without "no-stats" Symptoms: On a Nexus 9000 device, if a QoS policy is applied to an interface with the "no-stats" keyword (which enables label sharing) after it was previously applied without the "no-stats" keyword, the QoS policy uses the same amount of TCAM resources as it normally would without the "no-stats" keyword. Workarounds: No known non-disruptive workaround is known for this issue at this time. Reloading the Nexus 9000 device with "no-stats" keyword configuration in place will cause TCAM resources to be correctly allocated after the device comes back online.
CSCvn75318	Headline: bgp nxos: not able to delete "advertisement-interval" when inheritance is configured Symptoms: Delete on the “advertisement interval fails. Workaround: None

Bug ID	Description
CSCvo39486	Headline: Vsh crash with frequent executing show logging onboard exception-log Symptoms: nexus switches may crash with Non-sys-mgr cores. This is due to the frequent running command show logging onboard | no-more # sh cores VDC Module Instance Process-name PID Date(Year-Month-Day Time) --- ------ -------- --------------- -------- ------------------------- 1 2 1 non-sysmgr 29571 2019-11-17 22:06:13 1 2 1 non-sysmgr 29746 2019-11-17 22:06:14 1 2 1 non-sysmgr 29835 2019-11-17 22:09:27 Workaround: Avoid running the commands too often or code upgrade when fix available in 9.2.4
CSCvo75725	Headline: [NBM] mrib refreshing routes and takes around 1hr to age out 50 flows Symptoms: Mroute entry is seen even though there is no such traffic flow ingressing the switch. PIM event history shows that the route was active, was deleted when it expired, but then was re-added immediately upon a notification from Mrib. This cycle of delete/re-add continues thereafter every 3 mins, until the mroute eventually gets deleted without being re-added. Sometimes this cycle takes up to an hour. Workaround: There is no workaround for this issue.
CSCvo94814	Headline: PTP auto-log creation is failing when high clock corrections occur Symptoms: A Cisco Nexus device would report the following in the log if the PTP auto-log creation fails while observing high PTP corrections: 2019 Mar 22 15:06:16 %USER-0-SYSTEM_MSG: Not able to create logfile /bootflash/ptp/auto_ptp_dbg_log_1.log, err 2(No such file or directory) - please remove/rename file ptp under /bootflash, check diskspace etc. - ptp Workarounds: There is no functionality impact to PTP except that the high clock corrections need to be investigated.

Bug ID	Description
CSCvp34985	Headline: tahusd process crash after enabling QSA/SFP(+) interface in the unsupported configuration Symptoms: N9K-C93180LC-EX might experience a crash in the "tahusd" process when physically inserting a third-party 10 Gbps SFP into a 40 Gbps or 100 Gbps QSFP breakout cable. `show logging nvram` %$ VDC-1 %$ %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "tahusd" (PID 30508) hasn't caught signal 11 (core will be saved). %$ VDC-1 %$ %SYSMGR-SLOT1-2-HAP_FAILURE_SUP_RESET: Service "tahusd" in vdc 1 has had a hap failure Workarounds: 1) Use a Cisco-branded SFP in the QSFP 2) If the "hardware profile port mode" configuration is also inappropriate, either: 2a) Remove / change the QSFP breakout cables to match the "hardware profile portmode" configuration seen via "show run | grep portmode" 2b) Change the "hardware profile portmode" configuration to match the number and type of QSFP breakout cables installed, and reload
CSCvp69490	Headline: Irvine : vsh core seen in steady state with traffic running [without any triggers] Symptoms: The vsh.bin process may crash and generate a core file. Workarounds: None.
CSCvp71637	Headline: Evaluation of n9k-standalone-sw for Intel 2019.1 QSR - MDS Symptoms: The product Cisco Nexus 3000 Series Switches;Cisco Nexus 9000 Series Switches in standalone NX-OS mode includes an Intel CPU that is affected by the vulnerability identified by the following Common Vulnerability and Exposures (CVE) ID: CVE-2018-12127 -- Microarchitectural Load Port Data Sampling (MLPDS) CVE-2018-12126 -- Microarchitectural Store Buffer Data Sampling (MSBDS) CVE-2018-12130 -- Microarchitectural Fill Buffer Data Sampling (MFBDS) CVE-2019-11091 -- Microarchitectural Uncacheable Data Sampling (MDSUM) Cisco has reviewed this product and concluded that it is affected by this vulnerability. Fixed software information will be updated as part of this Release Note Enclosure. Workarounds: In the event that the Cisco Nexus switch owner does not need to execute additional third-party software on their switches, they may further restrict access to the various shell environments through the configuration. This will remove shell access for all users, including admin and dev-ops users. >> Disable access to the host shell by configuring "no feature bash" >> Remove the guest shell by executing "guestshell destroy" >> Change any configuration setting user's shell from bash to vsh: "username <user> shelltype vsh" >> Remove any users with dev-ops role >> Disable openflow feature If any shell access mentioned in the 'Conditions' section is required, make sure the user does not run code/binary software from untrusted 3rd parties.

Bug ID	Description
CSCvp73845	Headline: Tunnels have zero outer SrcIp/SMAC or encapped traffic blackholed after destination adjacency change Symptoms: tunnel encapsulated data plane traffic is sent with external header Source IP address 0.0.0.0 and external Source MAC address 00:00:00:00:00:00 unicast traffic fails or tunnel encapsulated data plane traffic is blackholed, for example. not seen in SPAN, due to tunnel HW programming with Dest MAC 00:00:00:00:00:00 Workarounds: corrective action: flap the tunnel interface
CSCvq06837	Headline: config-replace show patch shows " switchport access vlan 1 " additionally to the actual patch Symptoms: switch(config-if)# configure replace bootflash:rollback.cfg show-patch Version match between user file and running configuration. Pre-check for User config PASSED <SNIP> interface Ethernet1/4 switchport access vlan 1 <<<<<<<<<<<<<<<<<<<<<<<< interface Ethernet1/5 Workarounds: NA
CSCvq17082	Headline: N9K: mrouter port is not created dynamically based on dummy PIM Hellos from OTV ED Symptoms: Despite the OTV, ED sends the dummy PIM hellos out the site internal interface and the Cisco Nexus 9000 Series switch receives them on inband. The IGMP Snooping process is not aware of them and so it doesn't dynamically create the mrouter port towards the OTV ED in question. Workarounds: Configure the port towards OTV ED as static mrouter port:vlan configuration 11 ip igmp snooping mrouter interface eth1/1
CSCvq33217	Headline: SAN-PO from NPV N9k to an FC switch will not come up Symptoms: SAN port-channel between NPV Cisco Nexus 9K to a Fibre Channel switch such as MDS/Cisco Nexus 5K/6K will not come up in non trunk mode. Workarounds: Configure the SAN port-channel to be a trunk and allow required VSANs on it.

Bug ID	Description
CSCvq53750	Headline: N9K-EX : no shut of admin down port leads to fatal error in device DEV_SUGARBOWL_ASIC error message Symptoms: When traffic was input to the Cisco Nexus 9300-EX, the following error might be seen. 2018 Nov 16 12:33:00.348 Nexus9K %PLATFORM-5-MOD_STATUS: Module 4 current-status is MOD_STATUS_ONLINE/OK 2019 May 10 16:49:52.509 Nexus9K %ETHPORT-5-IF_ADMIN_UP: Interface Ethernet4/22 is admin up . 2019 May 10 16:49:52.754 Nexus9K %MODULE-4-MOD_WARNING: Module 4 (Serial number: xxxxxxx) reported warning due to fatal error in device DEV_SUGARBOWL_ASIC (device error 0xc0401203) Workarounds: TBD
CSCvq56189	Headline: DHCP request with BCAST flag set might result in control plane failure Symptoms: Receiving a DHCP request with the broadcast flag set might wedge the buffers on Cisco Nexus 93180 switches. This results in CPU-bound packets failing to be processed. Workarounds: Don't mismatch the set qos-group and set cos values. If traffic is set to a specific QoS group, set the cos value of that traffic to the same number.
CSCvq61369	Headline: Cisco Nexus 9000 Series switches encapsulate with incorrect/null source IP address and MAC address Symptoms: Connectivity to destination prefixes through a tunnel interface on a Cisco Nexus 9000 Series switch might be broken. The Cisco Nexus 9000 Series switch begins to incorrectly encapsulate packets with the following properties: +++ A null (0.0.0.0) or incorrect source IP address +++ A null (0000.0000.0000) or incorrect source MAC address. As a result, the switch on the remote end of the tunnel discards the incorrectly-encapsulated packets on ingress, since they do not appear to be coming from the correct switch. Workarounds: No known workarounds to this issue exist at this time.
CSCvq63483	Headline: RMAC in L2RIB points to the wrong NH despite URIB having the correct information Symptoms: The router MAC used to route through L3VNI, points to the wrong next-hop in L2RIB, despite BGP having learned the correct route with the proper NH information. In contrast, the URIB has the correct information (both L2RIB and URIB are getting the next hop from BGP). Depending on the topology, this might cause severe packet loss or total traffic blackhole. Workarounds: 1. Flap the L3 VLAN having the spurious RMAC. This will flush out the wrong entries from L2RIB. 2. If many such VLANs are affected, interface NVE can be flapped.

Bug ID	Description
CSCvq65989	Headline: Link flap might cause the port to go down Symptoms: Topo: N9K-1(e1/1-e1/6)-----------(e1/1-e1/6)N9K-2 All e1/1-e1/6 configured 40G breakout to 10G on both N9Ks. Problem description: Flap ports e1/1-e1/6 on N9K-1 might cause ports down on N9K-2 Workarounds: 1. OIR transceiver 2. Reboot switch
CSCvq81539	Headline: multisite routed traffic is not decapsulated if uplink b/w Leaf and BGW is front panel port Symptoms: In case if uplink b/w L1 and BGW is T2 port, multisite routed traffic is not decapsulated. Multisite bridged traffic working fine. Bridged and routed traffic inside same fabric working fine. Workarounds: change front panel port from first generation N9K to DONNER
CSCvq93802	Headline: FHS config lost by upgrading from old version to 9.2(4) or 9.3(1) Symptoms: When upgrading from old version to the following version, FHS config will partially lost: 1. From Cisco NX-OS 9.2(3) or a previous version to new version Cisco NX-OS 9.2(4) 2. From Cisco NX-OS 7.0(3)I7(7) or a previous version to new version Cisco NX-OS 9.2(4) 3. From Cisco NX-OS 9.2(3) or a previous version to new version Cisco NX-OS 9.3(1) 4. From Cisco NX-OS 7.0(3)I7(7) or a previous version to new version Cisco NX-OS 9.3(1) Downgrading from Cisco NX-OS 9.2(4) or Cisco NX-OS 9.3(1) to Cisco NX-OS 9.2(3) and prior to Cisco NX-OS 7.0(3)I7(x) will also be impacted. Workarounds: Copy the original FHS config to a temp file, then deploy the config back to the upgraded box. 1. List all the FHS target related configuration 'show run dhcp' 2. Copy them and redeploy when the upgrading is done. The same workaround for downgrading from 9.2(4) or 9.3(1) to the old versions.
CSCvq95342	Headline: Intermittent VNI in DOWN state due to vni-add-await-buffer Symptoms: VNI in down state due to vni-add-await-buffer Workarounds: Remove entry and recreate resolves the issue.

Bug ID	Description
CSCvq95571	Headline: N9K: Radius authentication fails after reload/upgrade when DNS is used. Symptoms: Remote AAA/Radius authentication fails. Workarounds: remove/re-add the radius server configuration.
CSCvq96343	Headline: ERSPAN sends to wrong egress interface Symptoms: ERSPAN might stop updating the egress interface, although no route point to the previous egress interface, ERSPAN packets are still sent to this port, even if the egress interface has been updated via the "show monitor session all" command. Workarounds: None
CSCvr01970	Headline: speed xxxx under line console doesn't take effect Symptoms: "speed xxxx" under line console doesn't take effect (config-console)# speed 9600 (config-console)# show line console line Console: Speed: 38400 baud <<<<< Databits: 8 bits per byte Stopbits: 1 bit(s) Parity: none Modem In: Disable Modem Init-String - default : ATE0Q1&D2&C1S0=1\015 Statistics: tx:1652539 rx:0 Register Bits:RTS|DTR|05|c1|13|0b|60|00|aa| Workarounds: None
CSCvr04178	Headline: not able to configure max igmp snooping group-timeout 10080 Symptoms: Cisco Nexus 9000 When configuring the maximum "ip igmp snooping group-timeout 10080" under vlan configuration, the command is accepted but it not shown in the show run of the Vlan. A lower value than the limit 10080 is accepted, shown and taken correctly on the show commands show run vlan <vlanid> show ip igmp snooping vlan <vlanid> Workarounds: You can configure it as 'never' instead of the maximum limit.
CSCvr05025	Headline: Port-channel member ports will cost TCAM entries as well as port-channel Symptoms: Port-channel member port will cost some TCAM entries as well as port-channel. This will increase TCAM resource utilization Workarounds: Reload can recover it.

Bug ID	Description
CSCvr05981	Headline: Unexpected configuration refresh removes member VNI configurations Symptoms: Applying a config profile that toggles TRM causes L3VNIs to disappear from the configuration of NVE. Workarounds: Unknown.
CSCvr08446	Headline: FT flow records in Cisco Nexus 9300-EX ToR switches do not have the correct STEP field set Symptoms: The flow telemetry record exported from Cisco Nexus 9300-EX switches the source interface (STEP) field not set. Workarounds: None
CSCvr09175	Headline: Cisco NX-OS Software Cisco Discovery Protocol Remote Code Execution Vulnerability Symptoms: A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Note: Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-nxos-cdp-rce Workarounds: Please refer to the Security Advisory.
CSCvr11055	Headline: GRE traffic with payload that has the wrong IP header is dropped Symptoms: GRE traffic with payload that has the wrong IP header is dropped Workarounds: Downgrade to previous software version than Cisco NX-OS Release 7.0(3)I7(6).

Bug ID	Description
CSCvr14976	Headline: Cisco FXOS, IOS XR, and NX-OS Software Cisco Discovery Protocol DoS Vulnerability Symptoms: A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Note:Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-fxnxos-iosxr-cdp-dos Workarounds: Please refer to the Security Advisory.
CSCvr18104	Headline: IP forwarding is broken when the "hardware access-list tcam label ing-racl 9" command is entered. Symptoms: After entering the "hardware access-list tcam label ing-racl 9"command and rebooting the system, IP/ARP/ND forwarding is broken. You cannot ping directly connected interfaces. Workarounds: No workaround is available other than not entering these commands: hardware access-list tcam label ing-racl 9 unconfigure and reload no hardware access-list tcam label ing-racl 9
CSCvr22960	Headline: Longevity: nginx process getting killed - out of memory due to deadlock among DME threads Symptoms: The REST request from the switch might timeout or the user might observe an nginx core on the switch. The "show processes memory | grep nginx" command should show that nginx memory consumption is continuously increasing. Workarounds: No work around is needed in the case of a process core. The process will restart after a crash and there is no impact. In case of a REST timeout, "isan/bin/nginx" can be restarted to see if it fixes the issue.
CSCvr26376	Headline: NXA-PAC-1100W-P series power supply might not work if connected to the same ATS Symptoms: On the Cisco Nexus 9300 platform switches, if both power supplies connect to the same automatic transfer switch (ATS), and if the power feed to the ATS feed switches from one to another, redundancy might not work. Workarounds: Connect the power supplies to different automatic transfer switches for better resiliency.

Bug ID	Description
CSCvr30525	Headline: IGMPv3/MLD Snoop - Mcast Traffic Loss To All Receivers After One Receiver Sends Multiple Leaves Sysptoms: Multicast traffic loss to remaining receivers after one receiver sends multiple leaves in quick succession. Workarounds: Disable explicit host tracking under vlan configuration: configure terminal vlan configuration 10 no ip igmp snooping explicit-tracking
CSCvr31635	Headline: Crash at the moment of collecting stats for TAHUSD process Symptoms: TAHUSD core is produced in Cisco NX-OS Release 9.3(1) and later. Workarounds: None at the moment
CSCvr31693	Headline: MPLS transit forwarding affected through Cisco Nexus 9300-FX2 platform switches Symptoms: Connectivity/forwarding is impacted when an MPLS labelled frame transits through a Cisco Nexus 9300-FX2 platform switch. - QinQ switched frames with an MPLS label will miss one of the Dot1q tags. - MPLS labeled frames will not be VXLAN encapsulated by the ingress VTEP. They are incorrectly forwarded by the VTEP without a VXLAN header. Workarounds: No workaround available.
CSCvr32752	Headline: Cisco Nexus 93180LC-EX crashes due to tahusd process in disruptive upgrade from 7.0(3)I7(1) to 7.0(3)I7(6) Symptoms: - Cisco Nexus 93180LC-EX crashes due to tahusd process during disruptive upgrade from Cisco NX-OS Release 7.0(3)I7(1) to Cisco NX-OS Release 7.0(3)I7(6).- Switch is stuck in a boot loop after upgrading to Cisco NX-OS Release 7.0(3)I7(6). Workarounds: Disable bootup diagnostic tests globally before the upgrade and re-enable it after upgrade. That should allow you to move forward with the upgrade. The command to disable bootup tests from config mode is : switch(config)# diagnostic bootup level bypass Then re-enable complete diagnostics after upgrade : Disable bootup diagnostic tests globally before the upgrade and re-enable it after upgrade. That should be good workaround to move forward with the upgrade. The command to disable bootup tests from config mode is : switch(config)# diagnostic bootup level complete

Bug ID	Description
CSCvr36806	Headline: VXLAN: BUM traffic dropped on DCI/BL devices working as Bud node Symptoms: If the Cisco Nexus 9000 Series switches in a VXLAN multi-pod setup that were used to interconnect the DCI and were previously configured as BUD nodes (transit box + VTEP with VNI configured), you might experience drops in BUM traffic. Note that the previously configured VNI must have been using the same mcast group as the one used for transit traffic. Workarounds: - Reload the switch - Create the VNIs configuration for the VNIs present in the transit traffic (VLAN/VNI mapping and VNI config under NVE interface). Note that the same mcast group must be used.
CSCvr37533	Headline: The "show hardware capacity forwarding" command does not have complete output in JSON Symptoms: The "show hardware capacity forwarding" command is not completely JSONized Workarounds: None
CSCvr39030	Headline: VXLAN Encap packets sent with destination mac 00:00:00:00:00:00 when there is no ARP in Underlay Symptoms: On BGW, the overlay default route is pointing correctly to the shared border NVE (loopback 1): (See the BugSearch Tool for show command outputs.) Workarounds: Issue a ping on the BGW to the underlay nexthop to trigger an ARP request. (Static ARP does not work as a workaround.)
CSCvr39312	Headline: N9K-C92160YC-X // BGP - Some routes are forwarded via incorrect interface Symptoms: Several Cisco Nexus N9K-C92160YC-X switches running Cisco NX-OS Release 7.0(3)I7(4) code and placed in similar scenarios suffered the same hardware mis-programming. Workarounds: Use LPM heavy mode.
CSCvr40964	Headline: Community deletion leads to Assertion 'tmp_com == del_com' failed. Symptoms: %BGP-3-ASSERT: bgp-[29078] ../routing-sw/routing/bgp/bgp_pcl_cache.c:662: Assertion 'tmp_com == del_com' failed.%BGP-3-ASSERT: bgp [29078] -Traceback: bgp=0x100d2000 0x10349973 0x1048852e 0x10379c16 0x1037a135 0x1037aeaa 0x102365f9 0x1023d6ae 0x10240ee5 0x1024633 librsw_kstack.so=0xf3ec6000 librsw_kstack.so+0xac5cd libpthread.so.0=0xf362b000 libpthread.so.0+0* Workarounds: If we are using the set comm-list comlist delete command, the problem is not occurring. Not applicable in some scenarios.
CSCvr42254	Headline: MACsec ports are in (MACsec failure)/MACsec diagnostic is failing on module reload Symptoms: MACsec ports are in failure state or MACsec diagnostic is failing on module reload Workarounds: Enter the diagnostic bootup level minima command. Then reload the line card again.

Bug ID	Description
CSCvr43781	Headline: After a disruptive upgrade of Cisco Nexus 9000 to 7.0(3)I7(6), control plane is stuck. Symptoms: After upgrade or reload of a Cisco Nexus 9500 platform switch with -S LC/FM might experience control plane traffic issues. Workarounds: None, as additional reloads might re-trigger issue.
CSCvr45143	Headline: Fatal SAP 28 pile up post SNMP crashes. Symptoms: Customer sees frequent MTS build up for SAP 28 after 3 consecutive crashes. Workarounds: Manually clear the SAP 28. However, this does not stop pile up.
CSCvr45179	Headline: SNMP crash seen due to corrupted TLV Symptoms: SNMP crashes: Switch# show cores vdc-all VDC Module Instance Process-name PID Date(Year-Month-Day Time) --- ------ -------- --------------- -------- ------------------------- 1 1 1 snmpd 3777 2019-09-18 11:49:04 1 1 1 snmpd 10845 2019-09-19 17:06:59 1 1 1 snmpd 10809 2019-09-19 17:07:15 Workarounds: Disabling SNMP might prevent the crash from happening.
CSCvr54760	Headline: Packets looping on internal ports of LC and FM after replacing N9K-X97160YC-EX with N9K-X9736C-FX Symptoms: High bandwidth utilization on internal module ports with minimal traffic on front-facing portsMight impact traffic on ports that use the affected linecard module as internal ports are almost saturated Workarounds: FM reload fixes the issue. We can reload FMs one by one so that traffic will not be impacted.
CSCvr56864	Headline: Nexus 9K Sysmgr crash while rotating log Symptoms: A Nexus 9K running 7.0(3)I7(6) could experience a crash in the System Manager (sysmgr) process. 'show logging onboard internal reset-reason' shows a crash in "sysmgr stateful recovery":Reset Reason for this card:Image Version : 7.0(3)I7(6)Reset Reason (LCM): Unknown (0) at time Sun Aug 18 10:49:45 2019Reset Reason (SW): Reset triggered due to HA policy of Reset (16) at time Sun Aug 18 10:44:40 2019 Service (Additional Info): sysmgr stateful recovery Workarounds: None

Bug ID	Description
CSCvr57551	Headline: N9k reloads with Kernel panic - unable to handle kernel paging request Symptoms: N9k/N3164 reloads with kernel panic with below logs in "show logging nvram" 2019 Dec 13 13:18:12.348 N3164-Switch %$ VDC-1 %$ %KERN-1-SYSTEM_MSG: [6665558.814641] [1576243092] BUG: unable to handle kernel paging request at 00000000d7626824 – kernel 2019 Dec 13 13:18:12.348 N3164-Switch %$ VDC-1 %$ %KERN-1-SYSTEM_MSG: [6665558.913324] [1576243092] IP: [<ffffffffa126d3da>] mts_fast_sys_send+0x98a/0xd80 [klm_mts] – kernel 2019 Dec 13 13:18:17.371 N3164-Switch %$ VDC-1 %$ %KERN-1-SYSTEM_MSG: [6665563.510253] [1576243096] RIP [<ffffffffa126d3da>] mts_fast_sys_send+0x98a/0xd80 [klm_mts] - kernel Workarounds: None
CSCvr60736	Headline: Unable to save running config, gets error that memory is full Symptoms: You might not able to save the configuration and the following is reported in the log:%SYSMGR-2-NON_VOLATILE_DB_FULL: System non-volatile storage usage is unexpectedly high at 100%. Workarounds: NA
CSCvr62735	Headline: BGP attribute-map for aggre address sets the last attribute without matching the prefix list. Symptoms: bgp aggregate-address command using attribute-map option, it is not able to match and set according to the configuration. Will only set the last set community configured under the route-map. Workarounds: The workaround is to configure individual route-maps for each aggregate address and then set the community or other attributes in the respective route-maps
CSCvr63838	Headline: SNMP walk using OID 1.3.6.1.2.1.1 returns NULL [Expert Info (Note/Response): endOfMibView] Symptoms: N9508/N9504 Running 9.2.3 in vPC Workarounds: Work around is to remove the community string and the mib view command and add them back
CSCvr67397	Headline: Netflow / destination command is broken in rollback/patch Symptoms: The destination subcommand in Netflow configuration may not be interpreted properly by the Nexus parser when entered. Workarounds:
CSCvr68876	Headline: N9K-X9736C-FX // debounce time Unexpected Behaviour Symptoms: N9k // N9K-X9736C-FX // DWDM Interface Flap when DWDM link protection is triggered Workarounds: N/A
CSCvr69670	Headline: Dynamic NAT configuration on the N9k causes L2 forwarding issues. Symptoms: L2 traffic destined to a MAC not belonging to the Cisco Nexus 9000 Series switch is software switched (CPU punt) and dropped, which should not be the case. Workarounds: disable NAT

Bug ID	Description
CSCvr70914	Headline: Kernel Panic generates Kernel Trace instead of Stack Trace Symptoms: A Cisco Nexus 9000 or 3164 switch running 7.0(3)I7(6) might crash due to a kernel panic. Usually the kernel panic generates a stack trace which is reviewed using the `show logging onboard stack-trace` command. But in this case, the show command generated a kernel trace instead of a stack trace. Due to the missing stack trace, we can't determine the reason for the kernel panic. Workarounds: Most of the kernel panics happen due to a Machine Check Exception(MCE) event. In this case, we can't determine the reason for the kernel panic due to the missing stack trace. The recommendation is to monitor on first occurrence and replace the hardware on repeated kernel panics.
CSCvr73261	Headline: Copy run start fails on Cisco Nexus 3500 switch due to service "confelem" failure Symptoms: On a Cisco Nexus 3500 you might be unable to copy running-configuration to startup-configuration due to the confelem process failing to store it's configuration. Workarounds: -NA
CSCvr80704	Headline: Configure replace fails when 'switchport trunk allowed vlan' list is too large Symptoms: ++ When backing up your running configuration via 'copy running-configuration bootflash:backup-config', then execute 'configure replace bootflash:backup-config', the message 'Configure replace failed. Use 'show config-replace log verify' or 'show config-replace log exec' to see reasons for failure' will be displayed++ When running 'show config-replace log verify' the below output is presented. Workarounds: ++ Shorten the list of the 'switchport trunk allowed vlan' list in the configuration file you are using for 'configure replace', then add any missing VLANs manually after the 'configure replace' task completes successfully.
CSCvr81063	Headline: Native VLAN hardware mis-programming happens in tah after upgrade to 7.0.3.I7.7 with LACP individual Symptoms: Nexus 93180YC-EX running 7.0.3.I7.7 Workarounds: None
CSCvr83020	Headline: Unexpected reload of ipqosmgr process while applying 'service-policy type qos input' on range of PCs Symptoms: Configuring "service-policy type qos input" under range of port-channel interfaces causes unexpected reload related to ipqosmgr process. Workarounds: Do not use a range of port-channels while configuring QoS. Add QoS configuration one by one.
CSCvr87436	Headline: Wrong output of 'show snapshots compare' command with multiple VRFs Symptoms: The output of `show snapshots compare snap_before_maintenance snap_after_maintenance` is incorrect then having multiple VRFs configured on the Cisco Nexus device. Workarounds: none

Bug ID	Description
CSCvr97047	Headline: Debounce is not working for N9K-C9364C using LR4 transceiver and link flaps Symptoms: For the N9K-C9364C switch, after configuring debounce to max value we do see link flap and time for link to come up is high+ Issue is noticed for LR4 transceiver+ Issue is not noticed for other optics (ex SR4) Workarounds: Use SR4 optics
CSCvr98425	Headline: Nexus 3500 BGP-3-ASSERT syslog in IPv4 Multicast AF with Ext. Communities Symptoms: A Cisco Nexus 3500 platform switch configured as a BGP speaker that receives a prefix in the IPv4 multicast address-family with an Extended Communities attribute might produce a "BGP-3-ASSERT" syslog. The specific syslog will vary depending upon the NX-OS software release that the device is running.A Cisco Nexus 3500 platform switch running 6.x code may see the following syslog: 3548# show logging logfile | include ignore-case assert<snip>2019 Nov 6 17:33:11 3548 %BGP-3-ASSERT: bgp-49657 [4530] ../routing-sw/routing/bgp/bgp_import.c:1781: Assertion `0' failed.2019 Nov 6 17:33:11 3548 %BGP-3-ASSERT: bgp-49657 [4530] -Traceback: 0x81b5b63 0x820a9b0 0x820b53b 0x8135d8b 0x8137452 0x8137d58 librsw.so+0xa2107 libpthread.so.0+0x6140 libc.so.6+0xcedee A Cisco Nexus 3500 platform switch running 7.x code may see the following syslog: 3548# show logging logfile | include ignore-case assert <snip> 2019 Nov 6 16:20:49 3548 %BGP-3-ASSERT: bgp- [29626] ../routing-sw/routing/bgp/bgp_import.c:3756: Assertion `0' failed.2019 Nov 6 16:20:49 3548 %BGP-3-ASSERT: bgp- [29626] -Traceback: bgp=0x10001000 0x10278973 0x103e8380 0x103e8767 0x103e9091 0x10181553 0x10187621 0x1018d125 librsw_kstack.so=0xf3ecf000 librsw_kstack.so+0xac5cd libpthread.so.0=0xf3634000 libpthread.so.0+0x69ab libc.so.6=0xf34a4000 libc.s* A Cisco Nexus 3500 platform switch running 9.x code might see the following syslog: 2019 Nov 6 17:01:39 3548 %BGP-3-ASSERT: bgp- [667] ../routing-sw/routing/bgp/bgp_import.c:4424: Assertion `0' failed.2019 Nov 6 17:01:39 3548 %BGP-3-ASSERT: bgp- [667] -Traceback: bgp=0x100dd000 0x103082ba 0x1044cacb 0x1044ce13 0x1044d47a 0x10238207 0x1023d529 0x1024234b librsw_kstack.so=0xf64d2000 librsw_kstack.so+0x9fb07 libpthread.so.0=0xf62b5000 libpthread.so.0+0x62be libc.so.6=0xf5910000 libc.s* This symptom is observed regardless of whether the device is configured to perform inter-VRF leaking or not. No impact is observed to the device's ability to forward traffic, and the relevant prefix is installed in the BGP table in the VRF where it is received without issue. Workarounds: No workaround is known for this issue at this time.
CSCvr99094	Headline: Storm control gets triggered even when threshold is not reached Symptoms: Storm control gets triggered when ESXi doing vmotion or reload even when threshold is not reached. Workaround: None

Bug ID	Description
CSCvs00052	Headline: vpcm process memory leak @ libnve.so and libvlan_mgr_mcec.so Symptoms: Command `show vpc consistency-parameters global` or `show vpc consistency-parameters vlans` on the vPC VTEP (VXLAN setup) might cause a slow memory leak in libnve.so library, which in the long term perspective can cause the vPC process to be unresponsive or crash. You may also experience this issue by running `show run`: N9k# sh run The following SAPs did not respond within the expected timeframe Pending SAPS:450 Printing Ascii configuration for remaining SAPs... Workarounds: In the unlikely event of hitting this issue, please contact Cisco Support Ceter for further verification. Alternatively, you can consider chassis reload.
CSCvs00062	Headline: N9K crashing at the moment of using a flow exporter Symptoms: At the moment of having Netflow exporter configured in a N9K, it's crashing. Workarounds: None.
CSCvs00187	Headline: vsh.bin process crash Symptoms: The vsh.bin process might crash when attempting to access the Cisco Nexus switch via SSH and the MTS payload of the authentication packets is corrupted. This will be reported in the log as follows: `show logging nvram` 2019 Sep 11 21:51:44.634 %DAEMON-2-SYSTEM_MSG: fatal: PAM: pam_setcred(): Authentication failure - dcos_sshd[11625] 2019 Sep 17 22:45:01.610 %SYSMGR-2-LAST_CORE_BASIC_TRACE: : PID 5631 with message vsh.bin(non-sysmgr) crashed, core will be saved . Workarounds: None
CSCvs00400	Headline: Kernel panic and reload due to Watchdog Timeout after link flaps Symptoms: A Nexus 93180YC-EX may experience a crash due to Kernel Panic due to high number of interrupts. Workarounds: Correct fiber issues or removed unused transceivers.
CSCvs00775	Headline: PTP Packets punted when feature ptp is enabled/disabled Symptoms: PTP packets punted to CPUTransit PTP packets on a Cisco Nexus 9000 Series switch will be dropped Workarounds: Configure feature ptpreload of the N9k boxDONOT attempt to reload active FM which will not resolve this issue.

Bug ID	Description
CSCvs00971	Headline: An interface may forward disallowed VLAN traffic over a trunk Symptoms: Port forwards VLAN traffic even after such VLAN is removed from trunk port Workarounds: Remove "lacp vpc-convergence"
CSCvs07119	Headline: IGMPv3 report being looped on VXLAN vPC Symptoms: Customer seeing MAC flaps for end hosts in VXLAN multifabric deployment when the VLAN is extended on the L2 DCI and IGMPv3 packets are sent by the host towards the fabric. Workarounds: Issue is not seen in 7.0.3.I7.4 code.
CSCvs07510	Headline: Storm control policer became 0x0 after duplicate policer index programmed incorrectly Symptoms: Incoming traffic classified by storm-control traffic type dropped on interface due to storm policer rate becoming 0x0. Workarounds: Int po25 Storm-control broadcast level 0.03 Storm-control broadcast level 0.02 This will refresh po25 policer to 0.02
CSCvs08067	Headline: aclqos crash without device rebooting Symptoms: On a Cisco Nexus N9K-X9700-FX based lines cards with continuous SNMP polling the card may become low in heap memory when in uptime for ling. There is a memory leak in one particular stats polling . Workarounds: none
CSCvs09021	Headline: policyelem crash as soon we configure the flow-monitor on vlan Symptoms: configuring the flow-monitor on VLANs Workarounds: None
CSCvs10850	Headline: Unable to toggle the interface snmp trap configuration after upgrade Symptoms: The command execution on the CLI and accounting log is successful, but the same is not get applied under the running-configuration. Workarounds: The workaround is to re-apply the existing configuration and then apply the desired configuration.

Bug ID	Description
CSCvs16170	Headline: corrupted/incorrect router ID sent in update packet for external routes. Symptoms: A Cisco Nexus device configured with EIGRP redistributing static routes might advertise incorrect Originating Router ID in the updates for some prefixes if the 'metric version 64bit' router configuration is used. The corrupted RID values vary by Cisco NX-OS release. Workarounds: A temporary fix can be achieved by: + Flapping the EIGRP neighborships. 'clear ip eigrp neighbors *' <-- disruptive + Flapping the EIGRP process. 'router eigrp 1 ; shut ; no shut' <-- disruptive + Removing the 'metric version 64bit' configuration.
CSCvs20278	Headline: SVI is down while VLAN has active port after port flapping Symptoms: SVI is down while VLAN has active port Workarounds: Workaround #1 Remove the affected SVI VLAN and add it back Workaround #2 Reload can solve this issue.
CSCvs21823	Headline: Negotiation issue with Intel X10SDV - port flapping multiple times Symptoms: Negotiationissue with Intel X10SDV - port flapping multiple times before staying up Workarounds: none
CSCvs23022	Headline: Cisco Nexus 9500 SC EOBC Reloads on 7.0(3)I7.7 Symptoms: SC reloads are experienced while running in steady state on 7.0(3)I7(7) Workarounds: Disable emon reload behavior withdebug system internal emon no-reload
CSCvs23562	Headline: MALLOC_FAILED: mcastfwd [27776] m_copyin failed in mfwd_ip_main() Symptoms: 2019 Nov 18 22:12:11 N9300 mcastfwd[1983]: m_copyback: m_get() fails. 2019 Nov 18 22:12:10 N9300 %MCASTFWD-3-MALLOC_FAILED: mcastfwd [1983] m_copyin failed in mfwd_ip_main() 2019 Nov 18 22:12:11 N9300 mcastfwd[1983]: m_copyback: m_get() fails. 2019 Nov 18 22:12:20 N9300 %MCASTFWD-4-SYSLOG_SL_MSG_WARNING: MCASTFWD-3-MALLOC_FAILED: message repeated 1 times in last 377 sec Workarounds: Restart mcastfwd process
CSCvs23623	Headline: Using GRE, inner DSCP value is not copied to the outer DSCP on N9K. Symptoms: Using GRE, inner DSCP value is not copied to the outer DSCP on N9K. Workarounds: NA

Bug ID	Description
CSCvs25533	Headline: Multicast Storm-control not working for Cisco Nexus 9000 Symptoms: Storm-control not working properly for multicast traffic. Workarounds: Enter the ‘no ip igmp snooping’ command.
CSCvs29433	Headline: EIGRP learned routes flapping when associated prefix-list is modified Symptoms: Topology N9K-1--------EIGRP--------N9K2 Prefix-list configured on N9K-1 matching static routes That prefix-list is configured under route-map This route-map is used redistribute static routes into EIGRP When new entry is added to a prefix-list on N9K1, EIGRP learned routes on N9K-2 flaps If we use OSPF as routing protocol, we don't see route flap Workarounds: None
CSCvs30042	Headline: Nexus 93180YC-FX does not encapsulate traffic destined to Tunnel interface (GRE) Symptoms: ++ Using GREv6/IPv4 or GREv4/IPv4, tunnel encapsulation is failing to occur on specifically the Nexus 93180YC-FX++ On the Nexus 93180YC-EX, we are seeing proper encapsulation occurring using the same configuration++ When looking at the 'show hardware internal tah l3 tunnel' output, the encapsulation looks proper Workarounds: ++ No workaround available

Bug ID	Description
CSCvs32425	Headline: The "ip igmp static-oif" command can take effect on the PIM DR and non-DR interfaces (SVI) Symptoms: Multicast stream | L3 link | N9K-1 ---- L3 link ---- N9K-2 (no vPC involved) \\ / \\ VLAN 101 / \\ / L2 switch | | Receiver Configured "ip igmp static-oif x.x.x.x" on both (SVI 101) of N9Ks. N9K (DR and non-DR interfaces) will have the static OIF for SVI and it causes the duplicate multicast traffic due to two valid OIFs. Workarounds: 1/ only configure static-oif in DR interface 2/ use dynamic join (IGMP report) rather than static oif
CSCvs33520	Headline: Access-list TCAM entry does not program option fields configuerd in access-list Symptoms: Access-list does not match host-unreachable, redirect icmp traffic. Workarounds: Unknown at this time

Bug ID	Description
CSCvs35347	Headline: N9K-C9396 // OID Return Wrong Values Symptoms: On, N9K-C9396 while queuing for a DOM values via SNMP walk, some times the OID returns as "No Such Instance" randomly and reads fine after some time. Tue Dec 3 12:28:36 EST 2019 SNMPv2-SMI::enterprises.9.9.91.1.1.1.1.4.300007047 = INTEGER: 32582 .... Tue Dec 3 12:28:37 EST 2019 SNMPv2-SMI::enterprises.9.9.91.1.1.1.1.4.300007047 = No Such Instance currently exists at this OID .... Tue Dec 3 12:28:41 EST 2019 SNMPv2-SMI::enterprises.9.9.91.1.1.1.1.4.300007047 = No Such Instance currently exists at this OID .... Tue Dec 3 12:28:59 EST 2019 SNMPv2-SMI::enterprises.9.9.91.1.1.1.1.4.300007047 = No Such Instance currently exists at this OID .... Tue Dec 3 12:29:03 EST 2019 SNMPv2-SMI::enterprises.9.9.91.1.1.1.1.4.300007047 = INTEGER: 32691 Workarounds: Depends on the number of ports on the setup. The rate of the error can be reduced by matching the SNMP query frequency with the DOM read back timer callback frequency. Configure SNMP query at a rate matching the DOM read back timer: (PC_FCOT_POLL_TIME/2) / (num_ports) ; Where: PC_FCOT_POLL_TIME = 10 minutes num_ports = total number of Physical ports supported by the switch PORT_POLL_DDM_INCREMENT = 4 For example, On an N9K-C9396, which is a 48 port switch SNMP poll interval can be set to not less than and multiple of: (10x60/2) / (48) seconds = 6.25 seconds per port NOTE: This workaround applies only if the SNMP query is done for all ports linearly. Not guaranteed to work for random port queries.
CSCvs42206	Headline: Multi-site EVPN: traffic might be dropped towards Layer3 if only a Layer3 extension is configured Symptoms: If only a Layer 3 extension is configured on the BGW, traffic towards these destinations might be dropped Workarounds: Configure L2VNI on BGW.

Bug ID	Description
CSCvs43518	Headline: After upgrading to 7.0.3.I7.7 the port-channels got misconfigured and not possible to remove VLANS Symptoms: After upgrade to GMR from any prior releases, when port-profile type ethernet or interface-vlan and their subcommands are used, many configurations are not applied to DME. DME database is out of sync with running configuration. The switch might be functional. However, subsequent configuration on most commands might not work. Workarounds: Reload with ascii replay of the startup configuration. For example, reload ascii. It is not easy for users to remove the use of port-profile type [ethernet|interface-vlan] <>, subcommands and the applying the port-profile commands on the interface before upgrade.
CSCvs44582	Headline: NVE 1 stays UP on vPC secondary when peer-link down Symptoms: When vPC peer-link down, NVE 1 on vPC secondary might stay in UP status in “show interface.show nve interface” and “show nve interface nve 1 detail” displays the interface state as down. In "show nve interface nve 1 detail", the status is stuck in "Interface state : nve-intf-del-peer-cleanup-pending". Workarounds: Reloading vPC secondary
CSCvs46710	Headline: Memory leak leads to crash on callhome Symptoms: Memory leak of callhome process will lead to this process to crash:%SYSMGR-2-SERVICE_CRASHED: Service "callhome server" (PID 27043) hasn't caught signal 6 (core will be saved). Workarounds: Unknown
CSCvs51172	Headline: N9K-X9788TC-FX continuously aging out MAC addresses Symptoms: Partial MAC address is aged out and deleted with each hit of aging time and is quickly relearned Workarounds: none
CSCvs56058	Headline: N9K: aclqos crashes and generates core dump Symptoms: N9K: aclqos crashes and generates core dump Workarounds: None at this moment.
CSCvs62874	Headline: interface port-channel all command fails when sub interfaces are present Symptoms: interface port-channel all fails Workarounds: Remove all sub interfaces from running config.

Bug ID	Description
CSCvs68751	Headline: CBL blocked state on BCM after interface comes up on FEX Symptoms: After bringing up the FEX interface by inserting a cable, some switch interfaces can end up in a Blocking state from the BCM perspective. STP is forwarding from the software perspective. Workarounds: 1.Apply configuration on FEX interface then attach the cable. 2. Use PVSTP.
CSCvs69425	Headline: Refresh profile CLI will fail when updating the Old profile with new profile Symptoms: Refresh profile CLI will fail when updating the Old profile with new profile Workarounds: Apply configs manually rather than pushing via profile or from DCNM
CSCvs75273	Headline: CLI 'show hardware capacity forwarding' fails to produce JSON L2 related output Symptoms: Broken json-pretty output for 'show hardware capacity forwarding' cli. Workarounds: N/A
CSCvs75586	Headline: IP/GRE traffic not matching TapAgg ACL Symptoms: . GRE traffic is not being matched by ACE with gre/ip and redirect option. Workarounds: Not availble
CSCvs77955	Headline: N9K-C9348GC link up delay on usd level after reloaded Symptoms: . After N9K-C9348GC reloaded, we observed the port of Catalyst was brought up earlier than N9K-C9348GC by about 18 seconds. Workarounds: N/A

Bug ID	Description
CSCvs90075	Headline: Cisco Nexus 9000/VXLAN - Forwarding broken due to inner Dot1Q copied during VXLAN Encap Symptoms: . Inner dot1q tag retained for regular trunk ports breaking connectivity as destination port receives two dot1q tags. Hosts across different leaf switches in VXLAN EVPN Fabric. Workarounds: Do not use the "system dot1q-tunnel transit" command if there are no variants of QinVNI ports configured on the VTEPs. OR, configure any spare interface (doesn't need to be UP) with the following configuration on each VTEP (both in case of vPC): (Supported with N9300-FX/FXP/FX2 platform switches) interface Ethernet1/x switchport switchport mode trunk switchport trunk allow-multi-tag switchport trunk allowed vlan <x> x = any vlan with vn-segment enabled. Example: VLAN Segment-id ---- ----------- 10 1010
CSCvt01676	Headline: Cisco Nexus 9000 crash when name based NTP server is configured and switch restart Symptoms: . Cisco Nexus 9000 crash with following error message VDC-1 %$ %NTP-2-NTP_SYSLOG_INIT_FAIL: : Failed to restart NTPd sh system reset-reason Reason: Reset triggered due to HA policy of Reset Service: ntp hap reset Version: 7.0(3)I7(7) Workarounds: Remove name-based NTP configuration and apply IP-based NTP configuration Or Reload ASCII

Bug ID	Description
CSCvt06406	Headline: bcm_l2_register_callback causes 9500 module reload. Symptoms: . In certain instances, we see a hap reset generating a core for BCM-USD causing a module to reload. exception information --- exception instance 1 ---- Module Slot Number: 1 Device Id : 134 Device Name : System Manager Device Errorcode : 0x0000030b Device ID : 00 (0x00) Device Instance : 00 (0x00) Dev Type (HW/SW) : 03 (0x03) ErrNum (devInfo) : 11 (0x0b) System Errorcode : 0x401e008a Service on linecard had a hap-reset Error Type : FATAL error PhyPortLayer : 0x0 Port(s) Affected : Error Description : bcm_usd hap reset DSAP : 0 (0x0) UUID : 1 (0x1) Time : Thu Jan 2 16:49:07 2020 (Ticks: 5E0E1F03 jiffies) `show cores` VDC Module Instance Process-name PID Date(Year-Month-Day Time) --- ------ -------- --------------- -------- ------------------------- 1 1 1 bcm_usd 8252 2020-01-02 16:49:07 Workarounds: None

Known Issues

Bug ID	Description
CSCvc95008	On Cisco Nexus 9300-EX, 9348GC-FXP, 93108TC-FX, 93180YC-FX, 9336C-FX2, and 93240YC-FX2 switches, when 802.1q EtherType has changed on an interface, the EtherType of all interfaces on the same slice will be changed to the configured value. This change is not persistent after a reload of the switch and will revert to the EtherType value of the last port on the slice.

- In the NX-API sandbox, whenever XML or JSON output is generated for the show run command or the show startup command, the output contains additional characters.

For example,

```
</nf:source>          <============nf: is extra
```

<namespace> : extra characters are seen with XML and JSON from NX-API.

==============================

Device Hardware

The following tables list the Cisco Nexus 9000 Series hardware that Cisco NX-OS Release 7.0(3)I7(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 9000 Series Fabric Modules

Product ID	Hardware	Quantity for Maximum Bandwidth
N9K-C9504-FM	Cisco Nexus 9504 40-Gigabit fabric module	3 to 6 depending on line cards
N9K-C9504-FM-E	100-Gigabit -E fabric module (for the Cisco Nexus 9504 chassis) that supports the 100-Gigabit (-EX) line cards. When used, there must be 4 of these fabric modules installed in fabric slots 22, 23, 24, and 26.	4 5 when using the N9K-X9736C-FX line card.
N9K-C9504-FM-S	100-Gb -S fabric module (for the Cisco Nexus 9504 chassis) that supports the 100-Gigabit (-S) line cards. When used, there must be 4 of these fabric modules installed in fabric slots 22, 23, 24, and 26.	4
N9K-C9508-FM	Cisco Nexus 9508 Series 40-Gigabit fabric module	3-6 depending on the line cards

N9K-C9508-FM-E	100-Gigabit -E fabric module (for the Cisco Nexus 9508 chassis) that supports the 100-Gigabit (-EX) line cards. When used, there must be 4 of these fabric modules installed in fabric slots 22, 23, 24, and 26.	4 5 when using the N9K-X9736C-FX line card.
N9K-C9508-FM-S	100-Gigabit -S fabric module (for the Cisco Nexus 9508 chassis) that supports the 100-Gigabit (-S) line cards. When used, there must be 4 of these fabric modules installed in fabric slots 22, 23, 24, and 26.	4
N9K-C9508-FM-Z	Fabric blank with Fan Tray Power Connector module used in place of a fabric module that has been removed from fabric slots 22, 24, or 26 during lab verification test.	1
N9K-C9516-FM	Cisco Nexus 9500 Series 40-Gigabit fabric module	3-6 depending on the line cards
N9K-C9516-FM-E	100-Gb –E fabric module (for the Cisco Nexus 9516 chassis that supports the 100-Gb (-EX) line cards. When used, there must be four of these fabric modules installed in fabric slots 22, 23, 24, and 26.	4 5 when using the N9K-X9736C-FX line card.
N9K-C9516-FM-E2	16-slot fabric module for -E line cards.	4 – N9K-X97160YC-EX 4 – N9K-X9732C-EX 4 - (plus 1 for redundancy) – N9K-X9732C-FX 4 – N9K-X9736C-EX 5 – N9K-X9736C-FX 5 – N9K-X9736Q-FX 4 – N9K-X9788TC-FX
N9K-C9516-FM-Z	Fabric blank with Fan Tray Power Connector module used in place of a fabric module that has been removed from fabric slots 22, 24, or 26 during lab verification test.	1

Table 2 Cisco Nexus 9000 Series 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	3	92304QC	93120TX

Product ID	Description	Quantity	Cisco Nexus Switches	
	(burgundy coloring)		9272Q[1]	
N9K-C9300-FAN3-B	Fan 3 module with port-side exhaust airflow (blue coloring)	3	92304QC 9272Q[1]	93120TX
N9K-C9504-FAN	Fan tray for 4-slot modular chassis	3	9504	
N9K-C9508-FAN	Fan tray for 8-slot modular chassis	3	9508	
N9K-C9516-FAN	Fan tray for 16-slot modular chassis	3	9516	
NXA-FAN-160CFM-PE	Fan module with port-side exhaust airflow (blue coloring)	3	9364C	
NXA-FAN-160CFM-PI	Fan module with port-side intake airflow (burgundy coloring)	3	9364C	
NXA-FAN-30CFM-B	Fan module with port-side intake airflow (burgundy coloring)	3	92160YC-X 9236C[1] 93108TC-EX 93108TC-FX[1] 93180LC-EX[1] 93180YC-EX 93180YC-FX[1]	9332PQ 9348GC-FXP 9372PX 9372PX-E 9372TX 9372TX-E
NXA-FAN-30CFM-F	Fan module with port-side exhaust airflow (blue coloring)	3	92160YC-X 9236C[1] 93108TC-EX 93108TC-FX[1] 93180LC-EX[1] 93180YC-EX 93180YC-FX[1]	9332PQ 9348GC-FXP 9372PX 9372PX-E 9372TX 9372TX-E
NXA-FAN-35CFM-PE	Fan module with port-side exhaust airflow (blue coloring)	4	92300YC[1]	
NXA-FAN-35CFM-PI	Fan module with port-side intake airflow (burgundy coloring)	4	92300YC[1]	
NXA-FAN-65CFM-PE	Fan module with port-side exhaust airflow (blue coloring)	3	93240YC-FX2[1]	9336C-FX2[1]
NXA-FAN-65CFM-PI	Fan module with port-side exhaust airflow (burgundy coloring)	3	93240YC-FX2[1]	9336C-FX2[1]

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

Table 3 Cisco Nexus 9500 Platform Switches Line Cards

Product ID	Description	Maximum Quantity			Supporting Fabric Modules
		Cisco Nexus 9504	Cisco Nexus 9508	Cisco Nexus 9516	
N9K-X9408PC-CFP2	Line card with 8 100-Gigabit CFP2 ports	4	8	16	N9K-C9504-FM N9K-C9508-FM N9K-C9516-FM
N9K-X9432C-S	Line card with 32 100-Gigabit QSFP28 ports	4	8	16	N9K-C9504-FM-S N9K-C9508-FM-S --
N9K-X9432PQ	Line card with 32 40-Gigabit QSFP+ ports	4	8	16	N9K-C9504-FM N9K-C9508-FM N9K-C9516-FM
N9K-X9464PX	Line card with 48 1/10-Gigabit SFP+ ports and 4 40-Gigabit QSFP+ uplink ports	4	8	16	N9K-C9504-FM N9K-C9508-FM N9K-C9516-FM
N9K-X9464TX	Line card with 48 10GBASE-T (copper) ports and 4 40-Gigabit QSFP+ ports	4	8	16	N9K-C9504-FM N9K-C9508-FM N9K-C9516-FM
N9K-X9464TX2	Line card with 48 10GBASE-T (copper) ports and 4 40-Gigabit QSFP+ ports	4	8	16	N9K-C9504-FM N9K-C9508-FM N9K-C9516-FM
N9K-X9536PQ	Line card with 36 40-Gigabit ports	4	8	16	N9K-C9504-FM N9K-C9508-FM N9K-C9516-FM
N9K-X9564PX	Line card with 48 1-/10-Gigabit SFP+ ports and 4 40-Gigabit QSFP+ ports	4	8	16	N9K-C9504-FM N9K-C9508-FM N9K-C9516-FM
N9K-X9564TX	Line card with 48 1-/10GBASE-T (copper) ports and 4 40-Gigabit QSFP+ ports	4	8	16	N9K-C9504-FM N9K-C9508-FM N9K-C9516-FM
N9K-X9636PQ	Line card with 36 40-Gigabit QSFP+ ports	4	8	16	N9K-C9504-FM N9K-C9508-FM --
N9K-X9732C-EX	Line card with 32 40-/100-Gigabit QSFP28 ports	4	8	16	N9K-C9504-FM-E N9K-C9508-FM-E N9K-C9516-FM-E
N9K-X9732C-FX	Line card with 32 100 Gigabit Ethernet. Each QSFP28 supports 1x100-, 2x50-, 1x40-, 4x25-, 4x10-, and 1x1/10-Gigabit Ethernet. .	4	8	16	N9K-C9504-FM-E N9K-C9508-FM-E N9K-C9516-FM-E N9K-C9516-FM-E2
N9K-X9736C-EX	Line card with 36 40-/100-Gigabit	4	8	16	N9K-C9504-FM-E N9K-C9508-FM-E

	QSFP28 ports				N9K-C9516-FM-E
N9K-X9736C-FX	Line card with 36 1-/10-/40-/50-/100-Gigabit QSFP28 ports	4	8	16	N9K-C9504-FM-E N9K-C9508-FM-E N9K-C9516-FM-E
N9K-X9736Q-FX	Line card with 36 1-/10-/40-Gigabit QSFP28 ports	4	8	16	N9K-C9504-FM-E N9K-C9508-FM-E N9K-C9516-FM-E
N9K-X9788TC-FX	Line card with 48 1-/10-G BASE-T (copper) and 4 100-Gigabit QSFP28 ports	4	8	16	N9K-C9504-FM-E N9K-C9508-FM-E N9K-C9516-FM-E
N9K-X97160YC-EX	Line card with 48 10-/25-Gigabit SFP28 ports and 4 40-/100-Gigabit QSFP28 ports	4	8	16	N9K-C9504-FM-E N9K-C9508-FM-E N9K-C9516-FM-E

Table 4 Cisco Nexus 9000 Series Power Supplies

Product ID	Description	Quantity	Cisco Nexus Switches	
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
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	
N9K-PAC-3000W-B	3000-W AC power supply	Up to 4 Up to 8 Up to 10	9504 9508 9516	
N9K-PDC-3000W-B	3000-W DC power supply	Up to 4 Up to 8 Up to 10	9504 9508 9516	
N9K-PUV-1200W	3000-W Universal AC/DC power supply with bidirectional airflow (white coloring)	2	92160YC-X 9236C 92300YC 92304QC 9272Q 93108TC-EX	93120TX 93128TX 93180LC-EX 93180YC-EX

Product ID	Description	Quantity	Cisco Nexus Switches	
			93108TC-FX	93180YC-FX 9364C
N9K-PUV-3000W-B	3000-W Universal AC/DC power supply	Up to 4 Up to 8 Up to 10	9504 9508 9516	
NXA-PAC-350W-PE	350-W AC power supply with port-side exhaust airflow (blue coloring)	2	9348GC-FXP	
NXA-PAC-350W-PI	350-W AC power supply with port-side intake airflow (burgundy coloring)	2	9348GC-FXP	
NXA-PAC-500W-PE	500-W AC power supply with port-side exhaust airflow (blue coloring)	2	93108TC-EX 93180LC-EX	93180YC-EX
NXA-PAC-500W-PI	500-W AC power supply with port-side intake airflow (burgundy coloring)	2	93108TC-EX 93180LC-EX	93180YC-EX
NXA-PAC-650W-PE	650-W power supply with port-side exhaust (blue coloring)	2	92160YC-X 9236C 92300YC	92304QC 93108TC-EX 93180YC-EX
NXA-PAC-650W-PI	650-W power supply with port-side intake (burgundy coloring)	2	92160YC-X 9236C 92300YC	92304QC 93108TC-EX 93180YC-EX
NXA-PAC-1100W-PE	1100-W AC power supply with port-side exhaust airflow (blue coloring)	2	9348GC-FXP	
NXA-PAC-1100W-PI	1100-W AC power supply with port-side intake airflow (burgundy coloring)	2	9348GC-FXP	
NXA-PAC-1100W-PE2	1100-W AC power supply with port-side exhaust airflow (blue coloring)	2	93240YC-FX2	9336C-FX2
NXA-PAC-1100W-PI2	1100-W AC power supply with port-side intake airflow (burgundy coloring)	2	93240YC-FX2	9336C-FX2
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-1200W-PE	1200-W AC power supply with port-side intake airflow (burgundy coloring)	2	9272Q	9364C
NXA-PAC-1200W-PI	1200-W AC power supply with port-side exhaust airflow (blue coloring)	2	9272Q	9364C

Product ID	Description	Quantity	Cisco Nexus Switches	
NXA-PDC-930W-PE	930-W DC power supply with port-side exhaust airflow (blue coloring)	2	93108TC-FX 93180LC-EX	93180YC-FX 9364C
NXA-PDC-930W-PI	930-W DC power supply with port-side intake airflow (burgundy coloring)	2	93108TC-FX 93180LC-EX	93180YC-FX 9364C
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
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

Table 5 Cisco Nexus 9500 Platform Switches 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

Table 6 Cisco Nexus 9000 Series 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-C9236C	1-RU Top-of-Rack switch with 36 40-/100-Gigabit QSFP28 ports (144 10-/25-Gigabit ports when using breakout cables)

Cisco Nexus Switch	Description
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-C9336C-FX2	1-RU switch with 36 40-/100-Gb Ethernet QSFP28 ports.
N9K-C9364C	2-RU Top-of-Rack switch with 64 40-/100-Gigabit QSFP28 ports and 2 1-/10-Gigabit SFP+ 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-FX	1-RU Top-of-Rack switch with 48 100M/1/10GBASE-T (copper) 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-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-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-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-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-C9348GC-FXP	Nexus 9300 with 48p 100M/1 G, 4p 10/25 G SFP+ and 2p 100 G QSFP
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
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

Cisco Nexus Switch	Description
	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 7 Cisco Nexus 9000 Series Uplink Modules

Product ID	Hardware
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.

Table 8 Cisco Nexus 9500 Platform Switches System Controller

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

Table 9 Cisco Nexus 3232C and 3264Q Switch Hardware

Product ID	Hardware	Quantity
N3K-C3232C	Cisco Nexus 3232C, 32 x 40-Gb/100-Gb 2 x 10-Gb SFP+, 1-RU switch	1
N3K-C3264Q	Cisco Nexus 3264Q, 64 x 40-Gb 2 x 10-Gb SFP+, 2-RU switch	1

Table 10 Cisco Nexus 3164Q Switch Hardware

Product ID	Hardware	Quantity
N3K-C3164Q-40GE	Cisco Nexus 3164Q, 64 x 40-Gb SFP+, 2-RU switch	1

Table 11 Cisco Nexus 31128PQ Switch Hardware

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

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 7.x*.

For information about an In Service Software Upgrade (ISSU), see the Cisco NX-OS ISSU Support application.

Note: Upgrading from Cisco NX-OS 7.0(3)I1(2), 7.0(3)I1(3), or 7.0(3)I1(3a) requires installing a patch for Cisco Nexus 9500 platform switches only. For more information on the upgrade patch, see Upgrade Patch Instructions.

Exceptions

Cisco Nexus 3232C and 3264Q Switches

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

- 3264Q and 3232C platforms do not support the PXE boot of the NX-OS image from the loader.
- Automatic negotiation support for 25-Gb and 50-Gb ports on the Cisco Nexus 3232C switch
- Cisco Nexus 2000 Series Fabric Extenders (FEX)
- Cisco NX-OS to ACI conversion (The Cisco Nexus 3232C and 3264Q switches operate only in Cisco NX-OS mode.)
- DCBXP
- Designated router delay
- DHCP subnet broadcast is not supported
- Due to a Poodle vulnerability, SSLv3 is no longer supported
- FCoE NPV
- Intelligent Traffic Director (ITD)
- Enhanced ISSU. NOTE: Check the appropriate guide to determine which platforms support Enhanced ISSU.
- MLD
- NetFlow
- PIM6
- Policy-based routing (PBR)
- Port loopback tests
- Resilient hashing
- SPAN on CPU as destination
- Virtual port channel (vPC) peering between Cisco Nexus 3232C or 3264Q switches and Cisco Nexus 9300 platform switches or between Cisco Nexus 3232C or 3264Q switches and Cisco Nexus 3100 Series switches
- VXLAN IGMP snooping

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

The following features are not supported for the Cisco Nexus 9200 platform switches and the Cisco Nexus 93108TC-EX and 93180YC-EX switches:

- 64-bit ALPM routing mode
- Cisco Nexus 9272PQ and Cisco Nexus 92160YC platforms do not support the PXE boot of the NXOS image from the loader.
- ACL filters to span subinterface traffic on the parent interface
- Egress port ACLs
- Egress QoS policer is supported on the Cisco Nexus 9300-EX and 9300-FX platform switches. It is not supported on the Cisco Nexus 9200 platform switch. The only policer action supported is drop. Remark action is not supported on egress policer.
- FEX (supported for Cisco Nexus 9300-EX platform switches but not for Cisco Nexus 9200 platform switches.)
- GRE v4 payload over v6 tunnels
- IP length-based matches
- IP-in-IP on Cisco Nexus 92160 switch
- ISSU enhanced is not supported on the Cisco Nexus 9300-FX platform switch.
- Layer 2 Q-in-Q is supported only on Cisco Nexus 9300-EX platform switches (93108TC-EX and 93180YC-EX) and Cisco Nexus 9500 platform switches with the X9732C-EX line card.
- MTU (Multi Transmission Unit) checks for packets received with an MPLS header
- NetFlow is not supported on Cisco Nexus 9200 platform switches. It is supported on Cisco Nexus 9300-EX and 9300-FX platform switches.
- Packet-based statistics for traffic storm control (only byte-based statistics are supported)
- PVLANs (supported on Cisco Nexus 9300 and 9300-EX platform switches but not on Cisco Nexus 9200 platform switches)
- Q-in-VNI is not supported on Cisco Nexus 9200 platform switches. Beginning with Cisco NX-OS Release 7.0(3)I5(1), Q-in-VNI is supported on Cisco Nexus 9300-EX platform switches.
- Q-in-Q for VXLAN is not supported on Cisco Nexus 9200 and 9300-EX platform switches

Q-in-VNI is not supported on Cisco Nexus 9200 platform switches (supported on Cisco Nexus 9300-EX platform switches)

- Resilient hashing for ECMP on the Cisco Nexus 9200 platform switches.
- Resilient hashing for port-channel
- 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 are not supported with 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 9500 Platform N9K-X9408PC-CFP2 Line Card and 9300 Platform Switches

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

- 802.3x
- Breakout ports
- FEX (this applies to the N9K-X9408PC-CFP2 and –EX switches, not all Cisco Nexus 9300 platform switches)
- MCT (Multichassis EtherChannel Trunk)
- NetFlow
- Only support 40G flows
- Port-channel (No LACP)
- PFC/LLFC
- PTP (Precision Time Protocol)
- PVLAN (supported on Cisco Nexus 9300 platform switches)
- Shaping support on 100g port is limited
- SPAN destination/ERSPAN destination IP
- Storm Control
- vPC
- VXLAN access port

N9K-X9732C-EX Line Card

The following features are not supported for Cisco Nexus 9508 switches with an N9K-X9732C-EX line card:

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

Related Content

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

Cisco Nexus 9000 Series Software Upgrade and Downgrade Guide is available at the following location: Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.x

The Cisco Nexus 3164Q Switch - Read Me First is available at the following location: Cisco Nexus 3164Q Switch – READ ME FIRST

The Cisco Nexus 31128PQ Switch - Read Me First is available at the following location: Cisco Nexus 31128PQ Switch – READ ME FIRST

The Cisco Nexus 3232C/3264Q Switch - Read Me First is available at the following location: Cisco Nexus 3232C and 3264Q Switches – READ ME FIRST

The Cisco Nexus 3000 and 9000 Series NX-API REST SDK User Guide and API Reference is available at the following location: Cisco Nexus NX-API References

New Documentation

The *Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes, Release 7.0(3)I7(8)* is available at the following location:
Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes, Release 7.0(3)I7(8)

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

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.