Cisco Nexus 9000 Series NX-OS Release Notes, Release 9.3(10)

© 2021 Cisco and/or its affiliates. All rights reserved.

This document describes the features, issues, and exceptions of Cisco NX-OS Release 9.3(10) 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
April 25, 2024	Added CSCwh50989 and CSCwe53655 to Open Issues.
July 13, 2022	Cisco NX-OS Release 9.3(10) became available.

© 2022 Cisco and/or its affiliates. All rights reserved.

New and Enhanced Software Features

There are no new software and hardware features introduced in Cisco NX-OS Release 9.3(10). The following table lists the enhancement done in Cisco NX-OS Release 9.3(10).

Enhancement	Description
Secure Erase	Added support for the following switches: N9K-C93180YC-FX TOR with FEX C2348UPQ For more information see, Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x).
DPLL Firmware Upgrade	Added support for the following switches: Cisco Nexus 93180YC-FX3 and 93180YC-FX3S platform switches. For more information see, Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x).

Open Issues

Bug ID	Description
CSCvz89475	Headline: N9300 sends NAT untranslated packets when one HW entry is already installed. Symptoms: With NAT pool configuration with overload and twice NAT configured, packets with untranslated address is seen in out to in direction. Workarounds: Configuring " ip nat translation creation-delay 0" can help by minimizing the time window for which untranslated packets are received. The problem can still be seen and hence not a complete workaround.
CSCwc11353	Headline: The " hardware profile multicast optimization disable" command is not persistent across reload. Symptoms: The " hardware profile multicast optimization disable" command is not persistent across reload. Workarounds: After switch reload: 1) Remove the command - no hardware profile multicast optimization disable. 2) Add the command again - hardware profile multicast optimization disable. 3) Reload all linecards.
CSCwc83676	Headline: tahusd process crash may be seen with IPv6 scale deployments on Cisco NX-OS Release 9.3(10). Symptoms: For Nexus 9300 and 9500 platform switches running Cisco NX-OS 9.3(10) codes with IPv6 route scale (32K and above) deployments, the show tech-support command output can result in a process crash, and the device reloads. Workarounds: To resolve this issue, use the reload SMU.
CSCwe53655	Headline: Revert reserved MAC blocking behavior for VRRP macs on SVIs Symptoms: User is not able to configure VRRP VMAC on SVI interfaces. Workarounds: None.
CSCwh50989	Headline: Custom COPP causing transit traffic to be punted to the CPU on Nexus 9300-GX2 Symptoms: When custom-COPP policy contains ACL rules which match on Layer 4 destination or source port, transit traffic also hits the COPP and the packets are copied to CPU. This causes duplication of traffic as CPU also routes the copied packets to the destination. Workarounds: Custom COPP policy using src/dst match mitigates punt for transit traffic.

© 2022 Cisco and/or its affiliates. All rights reserved.

Resolved Issues

Bug ID	Description
CSCwa58073	Headline: 'copy run start' failed after enabling 'feature bfd' due to DME failure Symptoms: Switch had a module inserted and configuration saved before module was removed or offlined, followed by a reload. Later, user tries to enable BFD then execute copy run start. Workarounds: Clear the “DME inconsistency:reload asciior” and clear “nxapi retries”.
CSCwa70394	Headline: BFD SMU installation in MM breaks micro-BFD Symptoms: If a switch is booted into maintenance mode with " system interface shutdown" in the profile, has SMU CSCvz71312 installed, and then exits maintenance mode - micro-bfd sessions stay in " session wait" indefinitely and never come up. This bug can also be reproduced if a switch is reloaded with its micro-BFD-enabled port disabled, has the SMU installed, and then the port enabled. Workarounds: To recover an affected port-channel:no port-channel bfd track-member-linkport-channel bfd track-member-link. The problem can be prevented by rebooting the switch after SMU installation.
CSCwa93243	Headline: N9K NAT crash when updating a L2 adjacent link Symptoms: We have a Nexus 9k switch that crashes on the NAT process, generating NAT core files. Workarounds: No workarounds are present at the moment.
CSCwb46172	Headline: N3K/N7K/N9K ARP statistics do not increment counter for ip proxy-arp and received arp requests. Symptoms: With 'ip proxy-arp enabled', " show ip arp statistics" do not reflect proxy-arp counter when proxy-arp occurs.Also observe the ARP received counters do not increment irrespective of any ip proxy arp configuration or proxy arp requests. Example:N7k-1# show ip arp statistics vlan 10snipReceived: Total 0 <<<<<<< Proxy arp 0 <<<<<<<snip Workarounds: Cosmetic counter issue, no workaround.
CSCwb60501	Headline: Nexus routing unicast packets destined to broadcast link layer address Symptoms: A Nexus switch receiving unicast packets destined for broadcast link layer address (ffff:ffff:ffff) routes packet to next hop instead of dropping on CloudScale management interface Workarounds: None.
CSCwa79808	Headline: Multiplier set to zero for TWAMP-TEST UDP packets Symptoms: NXOS running platforms set multiplier value at 0 on replying back while running as TWAMP server Workarounds: if the TWAMP client can ignore the Multiplier of zero.
CSCwa89845	Headline: Fretta-EOR: SC crash causes EPC/EOBC loss Symptoms: After a system controller crash, in rare cases a linecard may also crash, and there may be packet drops for control plane protocols afterwards. Workarounds: The EMON enhancements are added to 9.3.8 and higher releases could prevent this issue from happening.
CSCwa64058	Headline: %NTP-6-NTP_SYSLOG_WARN: : Failed to send MTS message to destination every 90 secs Symptoms: Following syslog message is seen every 90 seconds%NTP-6-NTP_SYSLOG_WARN: : Failed to send MTS message to destination (node = 0xfe000000, sap = 619), Opcode = MTS_OPC_CLOCK_CHANGE_NOTIF, errno = 32 Workarounds: Configure " logging level ntp 5" then above syslog message is masked(default is " logging level ntp 2").However almost syslog messages from ntp component are masked. There is no functional impact due to this log if there is no FEX module.
CSCuq79793	Headline: IPv6 ND processes NA with Link-layer address 0000.0000.0000 as valid Symptoms: IPv6 ND will install a neighbor entry for an IPv6 host that sends a NA who's Link-layer address field is populated with mac address 0000.0000.0000.

© 2022 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
	Workarounds: None.
CSCwa34646	Headline: Nexus OSPF process crash in N5k Symptoms: Nexus switch might experience an OSPF crash <pre>%SYSMGR-2-SERVICE_CRASHED: Service " __inst_001__ospf" (PID 6062) hasn't caught signal 11 (core will be saved). Reason: Reset triggered due to HA policy of Reset System version: 7.3(8)N1(1) Service: __inst_001__ospf hap resetVDC Module Instance Process-name PID Date(Year-Month-Day Time)--- ------ -------- --------------- -------- -------------------------1 1 1 ospf-100 6062 2021-11-13 18:37:21</pre> Workarounds: No know workaround
CSCwa43223	Headline: SNMP MIB CISCO-EIGRP-MIB table cEigrpInterfaceTable does not return the correct ifIndex Symptoms: SNMP MIB CISCO-EIGRP-MIB table cEigrpInterfaceTable is does not return the correct ifIndex Workarounds: No workaround available
CSCwa61442	Headline: OSPF Process Crash due to Heartbeat Failure Symptoms: A Nexus 7000 switch might experience an OSPF process crash due to a heartbeat failure:<pre>%SYSMGR-2-SERVICE_CRASHED: Service " __inst_002__ospf" (PID 12345) hasn't caught signal 6 (core will be saved).</pre>In the `show processes log details` we see:<pre>Service: __inst_002__ospfDescription: Open Shortest Path First Unicast Routing Protocol (OSPF)<snip>Death reason: SYSMGR_DEATH_REASON_FAILURE_HEARTBEAT (9)Last heartbeat 80.86 secs ago</pre> Workarounds: After the process crash, OSPF should come back up. However, it's possible that the switch later faces the same condition. Ensure stability in your network to minimize the number of LSUs that need to be processed.
CSCwa76446	Headline: Local-pt missing entries for direct routes under certain Conditions Symptoms: Multiple Symptoms are reported once the defect is hit. 1) Direct routes for IP addresses configured under SVI(Be it as a primary or a VIP under HSRP or any other FHRP) are missing. 2) show ip local-pt vrf all is missing the entries for Configured IP addresses or direct routes HSRP event history/show techs will show below errors <snip>768) Event:E_DEBUG, length:113, at 956423 usecs after Tue Nov 9 21:11:09 2021 [108] [1716/3]:Vlan3446[1/V4]: Postponing add VIP 172.16.144.0/25 to Netstack, VRF not inited, ifindex 0x9010D76 770) Event:E_DEBUG, length:74, at 919937 usecs after Tue Nov 9 21:11:09 2021 [108] [844/3]:Vlan3446[1/V4]: Group can not be enabled, IOD not yet inited 775) Event:E_DEBUG, length:115, at 919366 usecs after Tue Nov 9 21:11:09 2021 [108] [1716/3]:Vlan3446[1/V4]: Postponing add VIP 172.16.145.1/32 to Netstack, VRF not inited, ifindex 0x9010D76</snip> Workarounds: Only Disruptive workaround known as of now which is to Remove the SVI completely and re-configure.
CSCwb14542	Headline: Unexpected HSRP MAC refresh interval Symptoms: The configured HSRP mac-refresh interval on parent interface doesn't get applied to HSRP MGO follow groups configured on sub-interface. The follow groups still send hellos with the default mac-refresh interval of 60 sec. This can be seen in 'show hsrp detail' command output. Workarounds: Re-configure the mac-refresh command on parent interface once all the HSRP groups are configured.
CSCvt99891	Headline: ipmc index leak due to incomplete config session Symptoms: 1) Over course of config modifications especially when using configuration sessions for ACLs,not being able to config/add more ACEs with redirect action even before the specified limit is reached.Say the specified limit is 100 and number of unique ACE redirect action interface strings currently are 90.Adding one more ACE with unique ACE redirect action interface string should ideally work, but may fail due to this issue. Workarounds:

© 2022 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
	1) If you have configured the redirect acls (ACE entry having redirect port specified)using config sessions then you have to use config session method to unconfigure the acl ace entry .if you encounter the issue (redirect ports not getting printed for 'show run ' cmd in any ace rule) then unconfigure the rule it manually (using conf t)and then configure again via config session method. 2) It's not always possible to recover even if ACL config is completely removed and reapplied. This may necessitate a reload of the switch.
CSCvx76479	Headline: Port Security Static Mac entry cannot be configured on this type of int (any sw mode private-vlan) Symptoms: When attempting to configure switchport port-security mac-address x.x.x vlan x CLI error " Port Security Static Mac entry cannot be configured on this type of interface" is seen.9K(config-if)# switchport port-security mac-address x.x.x vlan yERROR: Interface eth1/1 Port Security Static Mac entry cannot be configured on this type of interface Workarounds: No known workaround besides removing the sw mode private-vlan subtype
CSCvy54756	Headline: SNMP set on sysName oid 1.3.6.1.2.1.1.5 creates cli-dme inconsistency between vdc and hostname Symptoms: Post snmp write operation that modified the vdc_hostname, it is noticed that the CLI prompt and the vdc_hostname were both updated (expected behavior). However, the switch hostname retained the old value (incorrect). Workarounds: To prevent overwriting operation via snmp, set the snmp-server community to read-only with (config)# snmp-server community <name> or(config)# snmp-server community <name> group network-operator
CSCvz04974	Headline: N9K: With Smart License config, `service " licmgr" hasn't caught signal 6 (core will be saved).` Symptoms: A Nexus 9000 may experience an unexpected reset of the licmgr process:%SYSMGR-STANDBY-2-SERVICE_CRASHED: Service " licmgr" (PID XXXX) hasn't caught signal 6 (core will be saved).%SYSMGR-STANDBY-2-SERVICE_CRASHED: Service " licmgr" (PID XXXX) hasn't caught signal 6 (core will be saved).The cores are visible in the 'show core' output:Switch# show coreVDC Module Instance Process-name PID Date(Year-Month-Day Time)--- ------ -------- --------------- -------- -------------------------1 1 1 licmgr XXXX XXXX-XX-XX XX:XX:XX1 1 1 licmgr XXXX XXXX-XX-XX XX:XX:XX Workarounds: There is no known workaround.
CSCvz42728	Headline: SNMPv2 -snmpNotifyFilterStorageType Integer returns as nonVolatile instead of permanent Symptoms: snmpwalk value is different for snmpNotifyFilterStorageTypeinstead of INTEGER: permanent(4) value returned is INTEGER: nonVolatile(3) Workarounds: This issue will not impact operation/functionality on device. Only, OID value can be wrong. So, avoid fetching the value of snmpNotifyFilterStorageType from NMS.
CSCvz56731	Headline: urib core observed with the initial bring-up of switch Symptoms: " urib" process Crash, after the Switch Initital Boot Workarounds: N/A
CSCvz72834	Headline: DHCP core at one of vPC peer while fetching relay stats through DHCPv6 Smart-Relay script Symptoms: " dhcp_snoop" process crashed while fetching relay stats through DHCPv6 Smart-Relay script Workarounds: N/A
CSCvz75894	Headline: N9500-R/N3600-R hardware application counters may get corrupted Symptoms: N9500-R/N3600-R running 9.3(x) version of converged code may experience hardware counter corruption causing specific application counters to show incorrect information. Workarounds: Reload will clear the issue but it can resurface
CSCvz86496	Headline: duplicate host ID in pathtrace output Symptoms: in VXLAN EVPN setup " pathtrace nve ip unknown..." command return output with duplicate ip/hostnames on the traffic path

© 2022 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
	Workarounds: use vebrose output:" pathtrace nve ip unknown ... verbose req-stats"
CSCvz93280	Headline: N9K-C93180YC-FX3: After replacing 1Gig Fiber SFP with 1Gig Copper SFP the port will not come up. Symptoms: Swap from 1Gig Fiber SFP (i.e GLC-LH-SMD) to 1Gig Copper SFP (i.e. GLC-TE).The 1Gig copper port will not come up. Workarounds: If you need to swap from 1Gig Fiber SFP to 1Gig Copper SFP do the following:Remove 1Gig Fiber SFPInsert 10Gig Fiber SFP. (Link does not need to come up SFP just needs to be registered by the switch)Remove 10Gig Fiber SFP.Insert 1Gig Copper SFP.1Gig Copper port should now come up.-OR-Reload switch.
CSCwa03051	Headline: KR2F:NGOAM core on build 108 Symptoms: " NGOAM" process crashes due to cgroup is running out of memory, creating a Core File Workarounds: Disabled NGOAM, crashing stopped
CSCwa33163	Headline: show ip route route uptime refreshed for all next hops when one next hop goes down Symptoms: Show ip route route uptime is reset for all NHs when NH goes down Workarounds: None, this is cosmetic issue
CSCwa35644	Headline: VSH crash is in syscli (show tech) after 2days longevity run Symptoms: Arbitrary vsh core listed in show command o/p. Not a persistent issue and was only noticed rarely. Workarounds: NA
CSCwa52532	Headline: Config Replace fails due to `switchport mode` not supported on L3 interface Symptoms: When we 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. Workarounds: 1) Edit the configuration file to include `switchport` before `switchport mode` under the interface config prior to performing Config Replace 2) Configure `system default switchport` in global config causing the interfaces to operate in L2 mode by default
CSCwa56558	Headline: IMR8: MTS leak between lldp dcx sap and Qosmgr SAP after enabling feature lldp Symptoms: `show system internal mts buffers summary` or `detail`seeing 100+ stuck MTS buffers on pers_q between lldp dcx sap and Qosmgr SAPNexus- switch# show system internal mts buffers summary* recv_q: not received yet (slow receiver)* pers_q/npers_q/log_q: received not dropped (leak)node sapno recv_q pers_q npers_q log_q app/sap_descriptionsup 456 0 129 0 0 lldp/Dcx SAP Workarounds: -Disable feature LLDP
CSCwa58339	Headline: Mapping from parentObjectIndex to cbQosCMname is not working for copp policer. Symptoms: Unable to match CoPP cbQosPoliceStats to a specific class-map. It does not match the cbQosClassMapCfg tables.Policy-map instance ID is 721420396 Class-map instance ID is 721420302 Drops for control-plane match policy ID but not class-map ID 721420396.721420413cbQosPolicyMapCfg SNMPv2-SMI::enterprises.9.9.166.1.6.1.1.1.721420396 = STRING: ?copp-system-p-policy-strict?cbQosClassMapCfg SNMPv2-SMI::enterprises.9.9.166.1.7.1.1.1.721420302 = STRING: ?copp-system-p-class-monitoring?cbQosPoliceStats SNMPv2-SMI::enterprises.9.9.166.1.17.1.1.20.721420396.721420413 = Counter64: 30426Example: Policy copp profile strict nplab05dldr127# show policy-map interface control-plane class copp-system-p-class-monitoring Control PlaneService-policy input: copp-system-p-policy-strictclass-map copp-system-p-class-monitoring (match-any) match access-group name copp-system-p-acl-icmp match access-group name copp-system-p-acl-icmp6 match access-group name copp-system-p-acl-traceroute set cos 1 police cir 360 kbps , bc 128000 bytes module 1 : transmitted 1121102210 bytes; dropped 30426

© 2022 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
	bytes; Workarounds: Use CLI / NXAPI rather than snmp to query the information
CSCwa60182	Headline: N9300-EX/FX may clear active NAT tcp session hw entry when other NAT tcp session sends tcp fin-ack Symptoms: Active NAT tcp session may get disconnected unexpectedly. Workarounds: While carving the TCAM region for TCP-NAT, increase the size by couple of more entries than what is required and this lessens the probability of the issue happening.
CSCwa67084	Headline: Optic QSFP-100G-SR4 Initialization Issue Symptoms: For Cisco Nexus 9000 switches, after reload of a peer device, causing a state transition on the optical link, the link may not come back up. This has been seen to occur when QSFP-100G-SR4 optics have been in use on the link and the link has been up for longer duration. The optic doesn't get initialized completely and software keeps waiting for optic initialization. The optics continuously report " CTLE status FAULT" fault in the output of " slot 1 show hardware internal tah event-history xcvr <port>" . command.module-1# show hardware internal tah event-history xcvr 506) Event:E_STRING, length:95, at 226616 usecs after Thu Jan 6 19:28:44 2022 tahusd_xcvr_100G_optic_tx_enable(7353): [inst=0 nxosport=196 mifpga_port:50] CTLE status FAULT <<<<< Workarounds: Re-seat the Optic physically or perform soft reset using below command. module-1# debug hardware internal tah mifpga qsa_reset <hex value of port>Example: Optic on port 50 can be reset using below hex value:module-1# debug hardware internal tah mifpga qsa_reset 0x32
CSCwa70932	Headline: Spanning Tree Protocol CLI output incorrectly suggests peer-switch is operational Symptoms: When the vPC Peer-Switch enhancement is configured on a pair of Nexus switches through the " peer-switch" vPC domain configuration command, neither switch is the Root Bridge for a specific vPC VLAN. The output of " show spanning-tree vlan <x>" for that VLAN suggests that the Bridge ID used by each switch is the vPC system MAC address shared between both vPC peers. Workarounds: There is no known workaround for this issue.
CSCwa73467	Headline: adding member to pc rejected if userCfgdFlags doesn't have admin_layer in nc pld but pc has it Symptoms: netconf request to add member port to the existing port-channel interface is rejected with the error - " port already in a port-channel, no config allowed Commit Failed" Workarounds: There are 2 workarounds, anyone can be chosen. 1) Re-create port-channel interface (remove and add it back) without switchport explicit config 2) In the netconf payload, add admin_layer to the userCfgdFlags of member port.
CSCwa73543	Headline: Nexus 9000-VXLAN IR peer is not built due to (evi deleted/disabled) after manual RT is configured Symptoms: Ingress replication list is not built because bgp l2vpn evpn route-type3 is not installed. Workarounds: Perform shut/no shut on NVE interfaceWait for NVE interface to come up then apply manual RT config
CSCwa77077	Headline: Nexus 9000 doesn't respond to the traceroute with ICMP Destination unreachable Symptoms: When Nexus is an intermediate hop to the traceroute, the nexus doesn't respond to the UDP messages hence it doesn't provide a trace of the path the packet took to reach the destination .Also, the packets will get dropped by the copp class copp-system-p-class-exception-diag switch# traceroute 172.16.2.2traceroute to 172.16.2.2 (172.16.2.2), 30 hops max, 40 byte packets 1 * * * >>>>>>>>>>> Nexus 2 172.16.2.2 (172.16.2.2) 1.223 ms 0.808 ms 0.643 msswitch# show policy-map interface control-plane class copp-system-p-class-exception-diagControl Plane Service-policy input: copp-system-p-policy-strict class-map copp-system-p-class-exception-diag (match-any) match exception ttl-failure match exception mtu-failure set cos 1 police cir 150 kbps , bc 32000 bytes module 1 : transmitted 0 bytes; >>>>>>>>>>> nothing is tranmistted 5-minute offered rate 0 bytes/sec conformed 0 peak-rate bytes/sec dropped 704 bytes; >>>>>>>>>>>> increasing 5-min violate rate 26 byte/sec violated 64 peak-rate byte/sec at Tue Jan 25 18:29:05 2022 Workarounds: downgrade to release 7.x or 9.2.x

© 2022 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwa78090	Headline: Pathtrace - duplicates are seen when TTL-exceeded message is hashed to wrong VPC peer (VXLAN) Symptoms: + Duplicates in pathtrace will be seen:B# pathtrace nve mac aa:aa:aa:aa:aa:bb 200 verbose max-ttl 100 Path trace Request to peer ip 10.21.0.10 source ip 10.11.0.10Sender handle: 5 Hop Code ReplyIP IngressI/f EgressI/f State========== 1 !Reply from 10.1.1.6, (SPINE) Eth1/51 Eth1/53 UP / UP 2 !Reply from 10.1.1.6, (SPINE) Eth1/51 Eth1/53 UP / UP 3 !Reply from 10.21.0.10, (D) Eth1/35 Vlan200 UP / UP+ There can be multiple hops duplicated Workarounds: There is no efficient workaround available currently.
CSCwa79726	Headline: Spanning Tree Protocol Dispute syslog should be more informative Symptoms: When a Nexus switch generates a syslog indicating that a Spanning Tree Protocol Dispute has been detected, the syslog looks like this:2022 Jan 28 15:25:03 switch %STP-2-DISPUTE_DETECTED: Dispute detected on port port-channel1 on VLAN0010.Identifying the source of the Spanning Tree Protocol BPDUs causing this Dispute scenario can be difficult if the Dispute scenario intermittently occurs. Workarounds: At present, identifying the Bridge ID and source MAC address of the offending Spanning Tree BPDU must be done through an Ethanalyzer control plane packet capture during the time of the issue.
CSCwa79883	Headline: executing tac-pac/ show tech-support with network operator role is requesing password on 10.2.1 NXOS Symptoms: executing tac-pac/ show tech-support with network operator role is requesing password on 10.2.1 NXOS Workarounds: do not execute tac-pac/ show tech-support with network operator role. In 9.3(x), " Only the network administrator can escalate privileges to the root. As per the new security measures, a network operator (priv-1 user) is not allowed to collect show tech. Therefore, the enable command does not help to escalate the privileges." https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/security/configuration/guide/b-cisco-nexus-9000-nx-os-security-configuration-guide-93x/b-cisco-nexus-9000-nx-os-security-configuration-guide-93x_chapter_0101.html
CSCwa84429	Headline: PACL redirect cause multicast traffic to flood Symptoms: Multicast traffic flooded To all the interfaces after hitting the ACL redirect . Workarounds: None
CSCwa85286	Headline: Nexus 9000 Sporadic unknown unicast flood; L2FM errors Symptoms: The following l2fm errors are seen on the switch that holds the orphan port:2022 Feb 03 13:49:49.617315: E_DEBUG l2fm [23344]: l2fm_mcec_rmdb_delete(222): Deleting MAC 0000.0800.0600 vlan 100 from RMDB2022 Feb 03 13:49:49.617289: E_DEBUG l2fm [23344]: l2fm_handle_mac_move_generic_l2_entry(15255): Ignoring entry if_index 0x1a000800, vl 100 mac 0000.0800.0600 state 32022 Feb 03 13:49:49.617131: E_DEBUG l2fm [23344]: l2fm_macdb_insert(9307): unexpected! entry 0000.0800.0600 already exists in SW. skip HW install2022 Feb 03 13:49:49.617095: E_DEBUG l2fm [23344]: l2fm_macdb_insert(8968): temp_str = slot 0 fe 0 mac 0000.0800.0600 vlan 100 flags 0x400107 hints 0 E8 NL lc : if_index 0x1a000800 old_if_index 0No L2FM errors on the remote switchl2fm l2dbg macdb on the switch that holds the orphan shows every second:Feb 3 13:49:49 2022:150665 0x1a000800 0 REFRESH_DETECT 3 0 0xffff1 --Feb 3 13:49:51 2022:87218 0x1a000800 0 REFRESH_DETECT 3 0 0xffff3 --Feb 3 13:49:52 2022:148802 0x1a000800 0 REFRESH_DETECT 3 0 0xffffFeb 3 13:49:49 2022:150654 0x1a000800 0 UPDATE 3 0 0x11 --Feb 3 13:49:51 2022:87207 0x1a000800 0 UPDATE 3 0 0x13 --Feb 3 13:49:52 2022:148791 0x1a000800 0 UPDATE 3 0 0x1l2fm l2dbg macdb on the remote switch shows:Feb 3 12:18:03 2022:230534 0x1a000800 3 INSERT 2 0 0xffff --Feb 3 12:48:03 2022:203921 0x1a000800 3 DELETE 2 0 0xffff --Feb 3 12:48:03 2022:203958 0x1a000800 3 MCEC_DEL_RCVD 2 0 0xffff --Feb 3 12:48:03 2022:238528 0x1a000800 3 INSERT 2 0 0xffff --Feb 3 13:18:03 2022:205338 0x1a000800 3 DELETE 2 0 0xffff --Feb 3 13:18:03 2022:205379 0x1a000800 3 MCEC_DEL_RCVD 2 0 0xffff --Feb 3 13:18:03 2022:236985 0x1a000800 3 INSERT 2 0 0xffff Workarounds: Add static ARP entry for the source of the traffic

© 2022 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwa88247	Headline: show tech detail/tac-pac never collecting " show tech-support usd-all" Symptoms: " show tech-support usd-all" might not be collected as part of " show tech detail" / " tac-pac" . The " show tech" file will instead display:`show tech-support usd-all`Another show tech is running, please try again later`show tech-support forwarding l3 unicast detail`... Workarounds: None
CSCwa90548	Headline: Anycast BGW vlan-floodlist mis-programmed Symptoms: *BUM traffic broken in one direction when forwarded between two EVPN sites,* traffic arrives to the BGW from the DCI, but is not correctly forwarded towards the leaf switches Workarounds: None
CSCwa90917	Headline: Nexus 9000 PKI Authentication Failure Symptoms: Unable to login to Nexus 9000 using certificate-based login. Workarounds: None
CSCwa93094	Headline: N9336C-FX2 reports false minor temperature alarm with back-to-front airflow Symptoms: N9336C-FX2 reports lower temp on exhaust side than intake with back-to-front(port-side exhaust) airflow. Workarounds: None
CSCwa95441	Headline: Power supply identified as UNKNOWN Symptom: PSU model is shown as UNKNOWN or Absent when a power cord is unplugged. `show environment power`Power Supply:Voltage: 12 VoltsPower Actual Actual TotalSupply Model Output Input Capacity Status (Watts) (Watts) (Watts)------- ---------- ---------- ---------- ---- -- ---------- -- ----------1 UNKNOWN 0 W 0 W 0 W Shutdown <<<<<2 N2200-PAC-400W-B 96W 113W 400W OkConditions:Unplugging a power cord although PSU is being inserted-platform: N9K-C92348GC-X- PSU: N2200-PAC-400W-B Workaround: Plug in or reconnect the power cord / source.
CSCwa96115	Headline: Callhome process crash with proxy configuration Symptoms: Callhome process crashes when it is configured with proxy configuration as shown below. The trigger for crash is issuing 'show run callhome' command when the DUT is trying to reach to CSSM via callhome. Workaround: None
CSCwa98589	Headline: CC_PC_MEMBERSHIP: Consistency Check: FAILED due to port-channel mis-programing Symptoms: [+]Error message " %COCHK-2-CC_RUN_STATUS: CC_PC_MEMBERSHIP: Consistency Check: FAILED" has been observed after reloading the switch Workarounds: None
CSCwa99850	Headline: Significant PTP correction observed during PTP path failover Symptoms: In network based on Nexus9k we occasionally observe high PTP correction - around 1-2k ns - during the failover of the path towards the GM clock.the issue happens when the primary path gets broken and PTP switches to alternative one.During the transition period some of the N9k briefly use their local clocks as time reference. Workarounds: Try increasing the frequency of ptp announce/sync messages and reduce the timeout values to configurable minimum. This should shorten the duration for which N9k uses it's local clock for reference.
CSCwb05591	Headline: show lldp neigh | json return incorrect information when no neighbor is present Symptoms: " show lldp neigh | json" return below when no neighhor is present:ERROR: No neighbour informationwhich is not json format and cause issue in nxapi and also any onbox python script Workarounds: None

© 2022 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwb06912	Headline: Nexus 9300 GX and GX2 output discards when egress interface goes down Symptoms: * interface goes down* at this point " output discards" briefly increase on multiple interfaces belonging to the same ASIC slice Workarounds: None
CSCwb08528	Headline: Mac learned on orphan port not getting sync with peer switch over Peer-Link Symptoms: Server's MAC Address learned on Leaf1's orphan port was not getting synced across peer-link on Leaf2 causing teaming issue at the server end. Workarounds: Put the ports in fex-fabric mode and move it back to mode trunk or reload the switch.
CSCwb11593	Headline: HSRP 1000 Groups - After ISSU from H to I, unable to scale to 1000 groups Symptoms: Max scalable HSRP group reduces to 490 rather than 1000 Workarounds: None
CSCwb13774	Headline: Nexus 9000 -FX All Traffic Dropped on MACSEC Secured Interfaces After " show tech macsec/detail/usd-all" Symptoms: A Nexus 9000 " -FX" Series Switch with MACSEC secured links can experience a full loss of traffic on said links whenever the following CLI command is executed:slot X quoted " show hardware internal tah macsec details hw fp-port #" This CLI is contained in various " show tech-support" bundles, and as such, will most likely be encountered when collecting tech-supports. This only occurs with XPN Cipher-Suites after PN has exceeded 2^32. Workarounds: Flap the impacted interface(s).
CSCwb16315	Headline: N9k LLDP DCBX negotiation issue. Symptoms: - When lldp dcbx is configured auto on N9k and the remote device supports only CEE, sometimes N9k is sending dcbx ieee and it is causing issue.- When we hardcode lldp dcbx CEE on N9k and remote device supports IEEE/CEE, N9k is not sending DCBX CEE TLV. Workarounds: If the remote device supports only dcbx CEE, we can hardcode CEE on N9k.
CSCwb21884	Headline: 9300-FX - Traffic is being dropped on the interfaces after enabling tcam knob " egr-l2-qos 6" Symptoms: + L3 protocols Adjacency is lost+ BFD is in down state+ ARP is resolved from both sides of the connection+ Ping between directly connected interfaces fails with ACL_DROP reason in ELAM Workarounds: Remove this TCAM configuration and reload the switch.
CSCwb22718	Headline: FEX ports show hardware inconsistencies for VLAN programming Symptoms: Traffic drops are seen on ingress for some interfaces that make part of FEX fabric port of Nexus 9000 parent switch. Workarounds: None
CSCwb23075	Headline: Closing SSH session before commands complete can fill up /var/volatile/tmp. Symptoms: You will see this syslog:%SYSMGR-2-TMP_DIR_FULL: System temporary directory usage is unexpectedly high at 100%.`show system internal flash`Filesystem 1K-blocks Used Available Use% Mounted onnone 9265152 1494784 7770368 17% //dev/loop0 65792 65792 0 100% /usr_roaufs 9265152 1494784 7770368 17% /usrproc 0 0 0 - /procnone 0 0 0 - /sysnone 204800 72640 132160 36% /varnone 5120 3112 2008 61% /etcnone 102400 1764 100636 2% /nxos/tmpnone 81920 4 81916 1% /nxos/xlognone 81920 10552 71368 13% /nxos/dme_logsnone 51200 5920 45280 12% /var/volatile/lognone 5120 48 5072 1% /var/homenone 307200 307200 0 100% /var/volatile/tmp <<<<<< /var/volatile/tmp will be full./var/volatile/tmp/ will be filled with " csm_sh_run_acfg" files.CORE# run bashbash-4.3$ cd /var/volatile/tmp/bash-4.3$ ls -lahtotal 11Mdrwxrwxrwx 35 root root 4.3K Jan 28 09:27 .drwxr-xr-x 5 root floppy 100 Apr 29 2020 ..-rw-rw-rw- 1 root root 0 Jan 27 10:58 acfg_maintenance_profile_dst_file_vdc1-rw-rw-rw- 1 root root 0 Jan 27 10:58 acfg_maintenance_profile_src_file_vdc1-rw-rw-rw- 1 root root 941 Jan 27 10:58 acfg_rollback_vdc_1_dst_excl_cfg_exec-rw-rw-rw- 1 root root 113 Jan 27 10:58 acfg_rollback_vdc_1_src_excl_cfg_exec-rw-rw-rw- 1 root root 5.1M Jan 24 13:16

© 2022 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
	auto_tmp_file_deletion_log.txt-rw-r--r-- 1 root root 512 May 28 2020 blkoops_pattern-rw-r--r-- 1 root root 1.2K May 28 2020 bootflash_sync.log-rw-rw-rw- 1 root root 92 May 28 2020 bootflash_virt_strg_pool_bf_vdc_1__rootfs.guestshell+.e2fsck.20200528214528-rw-r--r-- 1 root root 1.6K May 28 2020 boot_uptime.log-rw-rw-rw- 1 root root 7 Jan 27 17:22 cfg_status.log_1-rw-rw-rw- 1 root root 0 May 28 2020 cmp_slot_id.27-rw-rw-r-- 1 user1 network-admin 52K Jan 25 04:02 csm_sh_run_acfg_10034.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 06:02 csm_sh_run_acfg_10204.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 00:02 csm_sh_run_acfg_11012.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 24 17:02 csm_sh_run_acfg_11322.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 19:02 csm_sh_run_acfg_11366.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 08:02 csm_sh_run_acfg_12447.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 18:02 csm_sh_run_acfg_12578.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 10:02 csm_sh_run_acfg_12591.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 17:02 csm_sh_run_acfg_12906.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 28 05:02 csm_sh_run_acfg_12907.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 04:02 csm_sh_run_acfg_13445.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 24 21:02 csm_sh_run_acfg_13789.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 23:02 csm_sh_run_acfg_13960.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 03:02 csm_sh_run_acfg_1401.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 12:02 csm_sh_run_acfg_14868.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 22:02 csm_sh_run_acfg_15075.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 11:02 csm_sh_run_acfg_15264.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 28 09:02 csm_sh_run_acfg_15295.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 05:02 csm_sh_run_acfg_1591.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 01:02 csm_sh_run_acfg_16222.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 03:02 csm_sh_run_acfg_16357.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 21:02 csm_sh_run_acfg_17185.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 24 14:02 csm_sh_run_acfg_17390.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 08:02 csm_sh_run_acfg_17443.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 16:02 csm_sh_run_acfg_17462.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 15:02 csm_sh_run_acfg_17864.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 14:02 csm_sh_run_acfg_18089.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 05:02 csm_sh_run_acfg_18634.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 07:02 csm_sh_run_acfg_18784.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 28 02:02 csm_sh_run_acfg_19071.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 01:02 csm_sh_run_acfg_19608.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 24 18:02 csm_sh_run_acfg_19903.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 20:02 csm_sh_run_acfg_19960.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 09:02 csm_sh_run_acfg_21039.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 19:02 csm_sh_run_acfg_21166.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 11:02 csm_sh_run_acfg_21183.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 28 06:02 csm_sh_run_acfg_21493.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 05:02 csm_sh_run_acfg_22040.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 24 22:02 csm_sh_run_acfg_22409.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 00:02 csm_sh_run_acfg_22569.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 18:02 csm_sh_run_acfg_23287.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 13:02 csm_sh_run_acfg_23537.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 23:02 csm_sh_run_acfg_23677.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 12:02 csm_sh_run_acfg_23848.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 23:02 csm_sh_run_acfg_2402.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 02:02 csm_sh_run_acfg_24817.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 04:02 csm_sh_run_acfg_24973.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 22:02 csm_sh_run_acfg_25782.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 24 15:02 csm_sh_run_acfg_25951.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 09:02 csm_sh_run_acfg_26032.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 17:02 csm_sh_run_acfg_26148.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 16:02 csm_sh_run_acfg_26553.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 15:02 csm_sh_run_acfg_26707.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 24 16:02 csm_sh_run_acfg_2710.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 06:02 csm_sh_run_acfg_27227.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 08:02 csm_sh_run_acfg_27376.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 18:02 csm_sh_run_acfg_2762.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 28 03:02 csm_sh_run_acfg_27659.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 02:02 csm_sh_run_acfg_28200.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 24 19:02 csm_sh_run_acfg_28488.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 21:02

© 2022 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
	csm_sh_run_acfg_28638.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 10:02 csm_sh_run_acfg_29632.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 20:02 csm_sh_run_acfg_29755.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 28 07:02 csm_sh_run_acfg_30062.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 06:02 csm_sh_run_acfg_30757.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 12:02 csm_sh_run_acfg_30795.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 24 23:03 csm_sh_run_acfg_31320.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 01:02 csm_sh_run_acfg_31420.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 17:02 csm_sh_run_acfg_3181.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 19:02 csm_sh_run_acfg_32142.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 14:02 csm_sh_run_acfg_32393.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 28 00:02 csm_sh_run_acfg_32534.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 16:02 csm_sh_run_acfg_3330.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 13:02 csm_sh_run_acfg_350.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 07:02 csm_sh_run_acfg_3846.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 09:02 csm_sh_run_acfg_3992.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 28 04:02 csm_sh_run_acfg_4303.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 03:02 csm_sh_run_acfg_4821.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 24 20:02 csm_sh_run_acfg_5113.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 10:02 csm_sh_run_acfg_5124.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 22:02 csm_sh_run_acfg_5258.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 11:02 csm_sh_run_acfg_6257.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 21:02 csm_sh_run_acfg_6462.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 28 08:02 csm_sh_run_acfg_6687.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 02:02 csm_sh_run_acfg_7791.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 20:02 csm_sh_run_acfg_8509.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 25 15:02 csm_sh_run_acfg_8732.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 26 13:02 csm_sh_run_acfg_8765.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 07:02 csm_sh_run_acfg_8848.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 28 01:02 csm_sh_run_acfg_8909.txt-rw-rw-r-- 1 user1 network-admin 52K Jan 27 14:02 csm_sh_run_acfg_9273.txt Workarounds: Wait until the output has completed before ending SSH sessions. If using an automated process to run show commands ensure that the script checks for the output to be complete before ending the SSH session.
CSCwb23471	Headline: N9K diagnostic interval timer shown as " 0" when configured " config profile" Symptoms: diagnostic interval timer showing as " 0" show run all | egrep " diagnostic monitor interval" diagnostic monitor interval module 1 test NVRAM hour 0 min 5 second 0diagnostic monitor interval module 1 test RealTimeClock hour 0 min 5 second 0diagnostic monitor interval module 1 test BootFlash hour 0 min 30 second 0diagnostic monitor interval module 1 test SystemMgmtBus hour 0 min 0 second 30diagnostic monitor interval module 1 test OBFL hour 0 min 30 second 0diagnostic monitor interval module 1 test ACT2 hour 0 min 30 second 0diagnostic monitor interval module 1 test Console hour 0 min 0 second 30diagnostic monitor interval module 1 test FpgaRegTest hour 0 min 0 second 30diagnostic monitor interval module 1 test Mce hour 1 min 0 second 0diagnostic monitor interval module 1 test ASICRegisterCheck hour 0 min 0 second 20diagnostic monitor interval module 1 test L2ACLRedirect hour 0 min 1 second 0 Workarounds: None
CSCwb25169	Headline: account validation failure, is your account locked /var/volatile/tmp/dnf Symptoms: TACACS username : test+ After some time since switch is discovered in NDB with user test we are starting observing following logs:2022 Mar 16 09:21:13 switch %AUTHPRIV-5-SYSTEM_MSG: pam_unix(sudo:account): account test has expired (account expired) - sudo2022 Mar 16 09:21:14 switch %AUTHPRIV-1-SYSTEM_MSG: test: account validation failure, is your account locked? ; TTY=pts/14 ; PWD=/var/sysmgr/vsh ; USER=root ; COMMAND=/bin/rm -rf /var/volatile/tmp/dnf-test-yvyffro4/dnf.librepo.log /var/volatile/tmp/dnf-test-yvyffro4/dnf.log /var/volatile/tmp/dnf-test-yvyffro4/dnf.rpm.log /var/volat - sudo+ Above logs are happening almost every one second.+ TACACS server is not showing any authentication request being sent from the switch as for remote authentication we are creating temporary local user if there is no local one created with same credentials+ That temporary user is expiring after some time if there is no re-authentication done.+ This problem will start exactly at midnight after 2 days since switch is discovered in NDB. Of course if within those 2 days there is no " ssh" login to the box with same TACACS account which was used for discovery. This would extend existing account for another two days.

© 2022 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
	Workarounds: To prevent those logs from happening: Problem will not occur if there is local user created with same credentials Problem will be temporarily mitigated (for around 2 days) if ssh to the switch will be performed with credentials which were used for discovery in NDB
CSCwb25442	Headline: In 2x50G breakout mode, DOM info missing for lane 2 Symptoms: On Nexus 9000-R switches, DOM may be missing for lane 2 on breakout ports when running 50g-2x breakout mode. Workarounds: n/a
CSCwb27720	Headline: ACE configured with missing object-group does not generate any warning Symptoms: ACL might not block traffic as expected due to missing configuration of addrgroup or port-group, and there are no warning messages. Workarounds: Configure the missing addrgroup(s) or port-group(s).
CSCwb28510	Headline: Unexpected reload on Nexus 9000 reported by monitorc on a UP/DOWN event when sflow is enabled Symptoms: The issue was seen for first time on N9K-C93180YC-FX running in 9.3(6) the unexpected reload generated a core file from monitorc process even when there were no monitor sessions configured but the decodes pointed to sflow feature reporting an interface UP/DOWN events Workarounds: None
CSCwb30246	Headline: N9500-R/N3600-R CoPP incorrectly matches fragmented UDP packet with UDP PTP port payload as PTP pkt Symptoms: PTP CoPP class shows drops. Workarounds: N/A
CSCwb31043	Headline: L3 Multicast forwarding fails if " src-dst ip-vlan" hash is in use Symptoms: Multicast receivers get duplicate traffic from the sources or no traffic at all;It seems that the issue occurs only if the ingress Po is L3 Workarounds: Default the load-balancing hash (no port-channel load-balance src-dst ip-vlan);Disabling port-channel members (on the ingress or egress POs) might also work
CSCwb31158	Headline: Nexus 9000 FX3 Crashes Upon " no shutdown" of 25G Interface Symptoms: Running " no shutdown" on a 25G copper interface will trigger a crash in the tahusd process. Workarounds: None
CSCwb32907	Headline: Fix to correct incorrect duty cycle value. Symptoms: NXOS currently writing duty cycle 99% when set to max duty cycle at 100%. Creating SW fix to correct incorrect PWM value to hard code actual 100% duty cycle. Workarounds: None
CSCwb38210	Headline: invalid UDP checksum when Nexus UDP relay replicating broadcast packets to direct broadcast packets Symptoms: When UDP relay feature is configured under N9K, single broadcast packet (255.255.255.255) is replicated/regenerated into multiple (as configured) directed broadcast packets with " invalid UDP checksum" .The directed broadcast packet with invalid UDP checksum is going to be punted to CPU in some Cisco platforms (like Catalyst) which drops the packets due to invalid UDP checksum. Workarounds: none.
CSCwb42598	Headline: VXLAN Unicast Traffic dropped after ECMP paths were reduced Symptoms: VXLAN Unicast Traffic dropped after ECMP paths were reducedVTEP sends traffic to next-hop that has no path to the destination VTEP Workarounds: Reload the switch or LC

© 2022 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwb43500	Headline: PFSTAT crash @memmove_avx_unaligned_erms Symptoms: " pfstat" process crash observed Workarounds: None
CSCwb49879	Headline: GRE tunnel interface description configured with more than 31 characters is not displayed Symptoms: When a GRE tunnel interfaces description is configured with 31 characters length, it will not be displayed when commands below are executed.#sh run int #sh run description | in Tunnel interface Tunnel1 no ip redirects ip address --------- tunnel source loopback1 tunnel destination -------- description A_WAN det1-wn-p001-cnx Tu1014 (GRE-PHL1/DET1/1/Inet) mtu 1400 bandwidth 100000 no shutdownSwitch1# sh interface description | in TunnelTunnel1 up GRE/IP -- Workarounds: Run 9.3.3 or 9.3.4Configure GRE tunnel int description using 31 characters or less
CSCwb51700	Headline: Netconf Connections not responding from nexus Symptoms: The Netconf feature may stop working after some time. Even after restart, the same problem can occur again. Workarounds: There is no workaround. Recover once the switch is in the bad state, please do not execute 'no feature netconf / feature netconf'. Do the below command to restart the Netconf process into the normal state:- ----n9k# conf tn9k# feature bashn9k# run bash sudo su -bash> kill -9 `pidof netconf`-----
CSCwb53249	Headline: Nexus 9500 EOR Broadcom asic cannot forward ARP unicast if configured with SVI. Symptoms: Nexus 9500 EoRs T2 asic can forward broadcast but not ARP unicast request packet (no reply)Also cannot find drop counters at any interface and CoPP.show policy-map interface control-plane <<< no dropShow interface <<< no dropWe can see the unicast arp request punt to CPU , but not forward out. Workarounds: Remove SVI or upgrade OS to fixed release
CSCwb53272	Headline: N9K TOR OID dot1dBasePortIfIndex value after port 64 is displayed incorrectly Symptoms: OID: dot1dBasePortIfIndex .1.3.6.1.2.1.17.1.4.1.2The OID displays the interface index based on VLAN. By default, VLAN1 is used.1. All 108 ports are in L2 mode, polling result of dot1dBasePortIfIndex shows only the first 64 ports and port-channel, but without ports 65-108.2. Configured the first 64 ports into routed mode, leave 65-108 ports in L2 mode, the index value of 65-108 is incorrect, for example, The value of eth1/65 & eth1/108 corresponds to port 1/1 to port 1/44. Workarounds: None
CSCwb56624	Headline: After corrected HSRP duplicated group id, N9K can not learn specific HSRP VIP MAC address anymore. Symptoms: Two Nexus 9000 (vPC configured) are connected with two other devices (using orphan port). When misconfigured the duplicate HSRP group id and correct it , the secondary vPC peer device N9K cannot ping through HSRP VIP anymore. Workarounds: the issue can be resolved by doing any of the workaround below: a. flap vPC peer-link b. reload N9K1 switch
CSCwb57686	Headline: Nexus 9000 VTEP BUM Traffic forwarding issues following an interface flap under certain conditions Symptoms: Multiple Symptoms may be seen such as below: a) BUM Traffic not sent out via Interfaces in the OIL b) BUM Traffic may get duplicated on remote end Workarounds: Bounce the interface. Note that if after bounce, the interface comes back up in a specific fashion as below(the issue may persist). 1) From UP to Down > Initializing > UP > Down > Initializing > UP or 2) From up to down > initializing > suspended > UP
CSCwb57916	Headline: Kernel panic when grep commands are run with route scale Symptoms: Kernel Panic due to wrong char passed in the MTS sap options Workarounds: None

© 2022 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwb58274	Headline: NTP control packets are being processed when using ntp access-group serve-only Symptoms: The NTP control packets arriving to the Nexus switch are processed against the " SERVE-ONLY" ACL.As per the documentation SERVE-ONLY ACL should not process NTP control packets. Workarounds: None
CSCwb58876	Headline: Fabric-peering N9K-CXXX-FX2 switches may not process BPDU's from another switch. Symptoms: Multiple Symptoms may be seen such as below: 1) STP disputes on a downstream STP Root switch that is connected to vPC pair using fabric-peering. 2) show spanning-tree detail command on the Nexus doesn't increment for the " received" BPDU Counter stats 3) Ethanalyzer on Nexus 9k shows the incoming STP BPDUs with the correct dot1q tag and with Root information(includes better priority for the Vlan in Question) Workarounds: Shutting down the vpc domain although this is an intrusive step as all downstream vPC port-channels will go down on this step.A reload may NOT correct this behavior.
CSCwb59812	Headline: The BUM traffic is dropped on Spines n9k-9508 Symptoms: BUM traffic not forwarded properly on Spines of model n9k-9508 . The traffic might be forwarded only to some of the interfaces in the OIL that are in same ASIC/Slice as the incoming interface . Workarounds: Put the incoming and the outgoing interfaces of the Spine handling the BUM traffic on the same ASIC/SLICE.
CSCwb62002	Headline: CloudScale VPCM bulk fail retry mechanism Symptoms: Nexus Cloudscale box in VPC that appears to have stale configurations. ie. FEX configurations that are present from VPC perspective but are no longer in the running configuration. Workarounds: Flapping vpc interface on device that sees stale vPC state Reload the device in which the stale vPC state is present
CSCwb64677	Headline: Nexus 9000: Mirroring is not working if source-interface SPORT values >= 31 Symptoms: Seeing non-allowed VLANs on a SPAN session. Traffic would be mirrored on the incorrect source interface or not configured interface and not mirrors the traffic from configured source interface. Workarounds: None
CSCwb66341	Headline: `show tech macsec` should not be allowed if `feature macsec` is not enabled Symptoms: Switch allows " sh tech macsec" even if macsec is not enabled. Workarounds: None
CSCwb69140	Headline: N9500 Pwr-Denied when Capacity > Total Power allocated (Budget) Symptoms: I/O module in Pwr-Denied state despite sufficient installed Capacity > Total Allocated Power (Budget) Workarounds: Add Power Supply(s) to increase capacity aligned with the power redundancy mode used
CSCwb70215	Headline: Adding/remove the interface from the layer2 port-channel cause a multicast issue Symptoms: when we remove/add interface to an existing layer 2 port-channel between nexus and ASR9k , the multiact traffic start dropping IN nexus SW : 9.3(7) HW : N9K-C93180YC-EX Workarounds: Reload the switch Shut/no shut the port-channel Remove ip igmp snooping vxlan Remove vxlan configuration under the vlan .
CSCwb73211	Headline: NXOS PTP TS missing logging information and sufficient PTP correction history Symptoms: PTP TS does not have sufficient information for problem analysis. Workarounds: Collect 'show logging logfile | grep -i ptp' individually.

© 2022 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwb73231	Headline: N9000/N3100/N3500 may be sending out of spec PTP messages with SourcePortID equal zero Symptoms: Nexus PTP messages rejected by 3rd party PTP device. Workarounds: Do not use port 1 for PTP.
CSCwb73581	Headline: config replace fails when trying to modify a route map if route-map name uses delimiter chars Symptoms: Config replace fails while trying to make changes to " match community" statement under a route-map. Workarounds: For the failing route-maps, if the community-lists are created with a new unique name and associated to these failing route-maps, it should resolve.
CSCwb74307	Headline: RPF for PIM Bidir with phantom RP not changed on shutting the interface Symptoms: PIM Bidir has wrong OIF entry when interface toward RP is shut. It is not updated and showing interface that is shut. Workarounds: clear ip mroute * vrf " name of vrf"
CSCwb78090	Headline: Only a limited amount of odd or even VLAN's can be added to an MST instance Symptoms: You apply odd or even VLAN's to an MST instance but only a certain amount are applied once you commit the change. For example, if you apply all odd VLAN's from 1 to 3967, only the odd VLAN's from 1 to 3497 are applied. The command " show system internal dme running-config all dn sys/stp/inst/mstent" will show that the VLAN's like VLAN 3499 were pushed to the MST instance in DME. However, " show spanning-tree vlan 3499" will show that the VLAN is still in the default instance 0. Workarounds: You will have to limit the amount of alternating VLAN's are added to each instance. This can be done by adding consecutive VLAN's to an instance like 1-500.Alternatively, you can utilize more instances like the following config:instance 1 vlan 1,3,5,7,9,11,13,15,17,19CUT FOR BREVITYinstance 1 vlan 2001,2003,2005,2007,2009,2011,2013,2015,2017,2019instance 2 vlan 2021,2023,2025,2027,2029,2031,2033,2035,2037,2039CUT FOR BREVITYinstance 2 vlan 3961,3963,3965,3967
CSCwb85986	Headline: Nexus 9000:FEX:traffic loss is seen when parent switch reloads and comes online Symptoms: Traffic through Active-Active FEX (VPC) is lost for about 20 secs when one of the parent N9Kreloads and comes online. Workarounds: None
CSCwb86325	Headline: Packets larger than 1500 are software switched in DSVNI deployments regardless of SVI MTU Symptoms: + Routed packets that are taking a DSVNI / " Asymmetric" route are being punted to the CPU if the packet-size exceed 1500 bytes+ Punted packets observed in ethanalyzer. Workarounds: None
CSCwb90448	Headline: Traceback: satctrl crash post FX3 FEX conversion with optical Fiber uplink Symptoms: Wind River Linux <snip> (none) ttyS0(none) login: adminlogin[5632]: root login on `ttyS0'Loading parse tree (LC). Please be patient...fex-1# [21.352638] NX-OS starts punching watchdogJun 6 17:09:52 %SYSMGR-2-SERVICE_CRASHED Service " satctrl" (PID 6786) hasn't caught signal 11 (core will be saved).Jun 6 17:09:52 %SYSMGR-2-HAP_FAILURE_SUP_RESET Service " satctrl" in vdc 1 has had a hap failure <<<<<<<<<<<<<<< process crash[76.556696] Restarting system - satctrl hap reset [16] Workarounds: Apply 'write erase' before the Fex conversion configuration:term dont-askwrite eraseno boot nxoscopy running-config startup-configboot fexdelete bootflash:poap_replay*.cfgreload
CSCwb91752	Headline: Segmentation Fault Signal 11 on service LLDP Symptoms: LLDP core file generated# show coreVDC Module Instance Process-name PID Date(Year-Month-Day Time)--- ------ -------- --------------- -------- ---------- ---1 1 1 lldp xxxx 202x-xx-xx xx:xx:xxAlso seen LLDP pkt length errorSyslog messages %LLDP-3-INVALID_LLDP_RECEIVED: Received an invalid LLDP on Ethx/x Reason: Bad LLDP pkt length %LLDP-3-INVALID_LLDP_RECEIVED: Received an invalid LLDP on Ethx/x Reason: Bad TTL Workarounds: None

© 2022 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwb91897	Headline: Buffer-Boost enabled in DME for Cloudscale boxes Symptoms: when customers move away from BRCM to CS boxes and when they copy the configs of Port-channel which has Buffer-boost with 1st gen LC all Cloudscale platforms accept buffer-boost and enable this in DME. This causes error in the Port-channel when trunk or any configs are being edited. Workarounds: 1) Default the port-channel and add configs again 2) Reload of the Nexus 9000 box
CSCwb97155	Headline: EOR drop vxlan packet with incorrect checksum Symptoms: A vxlan packet with inner ip header checksum 0x0000 will be dropped by EOR though with no vxlan feature enabled Workarounds: None
CSCwb99717	Headline: VLAN Tags is suppressed when the traffic hitting the redirect ACL Symptoms: When the dot1Q traffic match IP-ACL redirect condition, VLAN tag is removed from the traffic header. Workarounds: Apply this configuration: interface eth Xno mode tap- aggregationmode tap- aggregation Once you reload the switch, the issue will re-occur again.
CSCwc00066	Headline: Interface disables CDR after shut/no shut due to lack of checks when TX LOL is gone Symptoms: CDR is disabled for an optic Workarounds: - Reload to restore CDR status- It is unconfirmed if removal and re-insertion restores CDR status.
CSCwc03518	Headline: N3K-C3408-S crash due statsclient and port_client process crash with 100G link flaps. Symptoms: N3K device unexpected reload by Reset Requested due to Fatal Module Error, Service: port_client hap reset and statsclient hap reset. Workarounds: None
CSCwc03573	Headline: Nexus reload at OSPF update Symptoms: Nexus C93180YC-FX has OSPF sessions flaps. OSPF process crashes while doing name-lookup and Workarounds: This crash occurs when name-server is slow or unreachable and along with this network (OSPF adjacency) is not stable. Work around is to remove " name-lookup" command from OSPF configurations.
CSCwc05498	Headline: Flow exporter not working after changing the destination ip and/or vrf Symptoms: The netflow exporter is not sending any packtets towards the colletor - even though output of " show flow exporter" shows increasing number of packtets sent. Workarounds: Take the " flow monitor" off from the physical interfaces. Remove the " exporter" from the " flow monitor" configuration. Remove and re-create the " flow exporter" with the correct configuration.
CSCwc05779	Headline: MCN-79278 - Innolight QSFP-100G-ER4L-S - Nexus 3000 - Utopias - Transceiver Details Errors Symptoms: DOM output is not showing properly on Nexus 3400There may also be false positive syslogs for high temp/voltage... Workarounds: None
CSCwc06034	Headline: Twinax link bringup delays on N9K-C93108TC-FX3P Symptoms: N9K-C93108TC-FX3P switches may experience delays in bringing up ports using twinax cables.

© 2022 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
	Workarounds: There is no workaround other than trying a different media type, such as fiber optics with ordinary transceivers instead of twinax.
CSCwc10388	Headline: Nexus 9000 running 7.0(3)I7(x) allows SNMPv3 Noauth security level configuration Symptoms: Nexus 9000 with 7.0(3)I7(x) allows user to configure snmp-server host with SNMPv3 'noauthnopriv' security level even though it is not supported in NX-OS. This configuration remains if upgraded to 9.3(x) as well. However, 9.3(x) does not allow the configuration and gives an error that the 'security level is not set'.N9k(config)# show run snmp!Command: show running-config snmp!Running configuration last done at: Mon Jun 6 19:00:12 2022!Time: Mon Jun 6 19:04:45 2022version 7.0(3)I7(7) Bios:version 05.44 snmp-server user admin network-admin auth md5 ! priv ! localizedkeysnmp-server host 192.168.1.1 traps version 3 noauth cisco123 <<<<<<<<<<< Workarounds: None
CSCwc12169	Headline: FX3S - High PTP Corrections and SyncE failures Symptoms: - High PTP Corrections- SyncE failures a. " SCM CFM GST PFM Failed" b. " Invalid" Workarounds: Powercycle
CSCwc14067	Headline: Nexus 9000 EOR - Received icmpv6 NS packet with Own mac address after SUP Switchover Symptoms: After supervisor switchover, Nexus receive alerts for icmpv6 Own mac address in the NS packet.The icmpv6 NS come from own Nexus ipv6 address to VIP vrrpv3 address for target VIP vrrpv3 address. Workarounds: 1) Delete the VRRPv3 IPv6 VIP6 on issue VLAN and reconfigure it. 2) Reload the switch
CSCwc19270	Headline: N93108TC-FX3P in FEX mode dsplayes incomplete port speed capabilities Symptoms: N93108TC-FX3P 100M port speed not included in port capabilities output. Workarounds: None
CSCwa71023	Headline: N3164 : No data (stack\core\NMI) generated for Watchdog Timeout Symptoms: Nexus 3164 reloads and the reset-reason is set as 'Watchdog Timeout'.No other information/data is available in logs to conclude what caused the watchdog timeout. Workarounds: There is no workaround at this time.
CSCwb34359	Headline: N3232C - ICMPv6 Traffic Incorrectly Forwarded to CPU Symptoms: A Nexus 3232C Series Switch will erroneously punt ICMPv6 traffic to the CPU, causing legitimate ICMPv6 traffic to be dropped in the Control-Plane Policer. Workarounds: None.
CSCwb38098	Headline: the RACL configuration in the port-channel still appear even the port-channel become L2 from L3 Symptoms: Only in the N3K-C3172TQ, I found that when a L3 port-channel which set a RACL is set to a L2 port-channel, the RACL cannot be removed in the show run. Workarounds: This is an express issue. If you want to set an ACL on the L2 port-channel, please set a PACL.
CSCwc00709	Headline: PBR over GRE feature broken on N3K platform Symptoms: as below guide for 9.3.X, N3K support " Configuring a Tunnel Interface Based on Policy Based Routing" https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3000/sw/interfaces/93x/configuration/guide/b-cisco-nexus-3000-nx-os-interfaces-configuration-guide-93x/b-cisco-nexus-3000-nx-os-interfaces-configuration-guide-93x_chapter_0101.html#reference_5E381C4134354D75B9AEA470A000C8AA when the PBR set next-hop ip with the tunnel local ip, the PBR IPv4 nexthop table doesn't install the tunnel IP as below:

© 2022 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
	route-map XXX permit 5 match ip address yyyyy set ip next-hop 10.x.x.x <<< tunnel local ip addN3K# show system internal rpm pbr ip nexthop detail PBR IPv4 nexthop table for vrf default10.y.y.y Usable via 10.a.a.a Ethernet1/x 843d.c6xx.xxxx <<<< abnormal, doesn't use the tunnel ip Index 0 Command 0x717267e4 Index 0 Command 0x7172685cnormal behavior should as below:N3K# show system internal rpm pbr ip nexthop detail PBR IPv4 nexthop table for vrf default10.y.y.y Usable, Punt via 10.x.x.x Tunnel1 0000.0000.0000 <<<<< normal behaviour Index 0 Command 0x6ef266e4 Index 0 Command 0x6ef2675c Workarounds: None
CSCwc08268	Headline: Nexus all (N3K/N9K) GLC-GE-100FX V03 Transceiver Compatibility Symptoms: When a Nexus 3000 or 3500 is using a SFP-100FX-GE Cisco version V03 the link will come up fine; however, no traffic will pass on the link. No CDP information is shared over the link. Testing with ICMP traffic also fails even though the switch shows the link in an "up" state. Workarounds: Utilize a SFP-100FX-GE Cisco version V02 transceiver if possible
CSCvx51159	Headline: Nexus 3548 - Boot times increased after upgrade to 9.3(6) Symptoms: After upgrade from 9.3(5) to 9.3(6), boot times have increase from 20-40 seconds. Workarounds: None
CSCwb58128	Headline: use-vrf management is missing from the "logging server" configuration line in running config Symptoms: "use-vrf management" is missing from `show runN3K(config)# logging server 192.168.10.10 3 use-vrf managementN3K(config)# logging server 192.168.10.20 3 use-vrf managementN3K(config)# show running-config | include logging logging server 192.168.10.10 3logging server 192.168.10.20 3 Workarounds: None
CSCwa31781	Headline: PTP: Syncing CPU Time to PTP time Symptoms: When no PTP GM is present in a given PTP Network, one of the Nexus 9000 Switch is made as GM. In This scenario, GM to get time from System CPU Time. Workarounds: None
CSCwb70210	Headline: Cisco FXOS and NX-OS Software CDP DoS and Arbitrary Code Execution Vulnerability Symptoms: A vulnerability in the Cisco Discovery Protocol feature of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code with root privileges or cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper input validation of specific values that are within a Cisco Discovery Protocol message. 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 execute arbitrary code with root privileges or cause the Cisco Discovery Protocol process to crash and restart multiple times, which would cause the affected device to reload, resulting in a DoS condition. 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). Workarounds: 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-nxos-cdp-dos-ce-wWvPucC9 The Cisco Product Security Incident Response Team (PSIRT) validates only the affected and fixed release information that is documented in this advisory.

Known Issues

© 2022 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwi99525	On Cisco Nexus N2K-C2348TQ HIFs fail to utilize redundant Port-Channel links, to NIF, during link failover events.

Device Hardware

The following tables list the Cisco Nexus 9000 Series hardware that Cisco NX-OS Release 9.3(10) 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 card	4	8	16

Table 3. Cisco Nexus 9500 R-Series Line Cards

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

© 2022 Cisco and/or its affiliates. All rights reserved.

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 module	4	5
N9K-C9516-FM-E	Cisco Nexus 9516 50-Gigabit cloud scale fabric module	4	5
N9K-C9516-FM-E2	Cisco Nexus 9516 100-Gigabit cloud scale fabric module	4	5

Table 6. Cisco Nexus 9500 R-Series Fabric Modules

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

Table 7. Cisco Nexus 9500 Fabric Modules

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

© 2022 Cisco and/or its affiliates. All rights reserved.

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

© 2022 Cisco and/or its affiliates. All rights reserved.

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 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]

© 2022 Cisco and/or its affiliates. All rights reserved.

Product ID	Description	Quantity	Cisco Nexus Switches
			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 coloring)	2	9332PQ 9372PX 9372PX-E 9372TX 9372TX-E 9396PX 9396TX
NXA-PAC-650W-PE	650-W power supply with port-side exhaust (blue coloring)	2	92160YC-X 9236C 92300YC 93180YC-FX3S 92304QC 93108TC-EX 93180YC-EX
NXA-PAC-650W-PI	650-W power supply with port-side intake (burgundy coloring)	2	92160YC-X 9236C 92300YC 93180YC-FX3S 92304QC 93108TC-EX 93180YC-EX
NXA-PAC-750W-PE	750-W AC power supply with port-side exhaust airflow (blue coloring) [1]	2	9336C-FX2 93240YC-FX2 9332C 9336C-FX2
NXA-PAC-750W-PI	750-W AC power supply with port-side exhaust airflow (burgundy coloring) [1]	2	9336C-FX2 93240YC-FX2 9332C 9336C-FX2

© 2022 Cisco and/or its affiliates. All rights reserved.

Product ID	Description	Quantity	Cisco Nexus Switches
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 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

© 2022 Cisco and/or its affiliates. All rights reserved.

Product ID	Description	Quantity	Cisco Nexus Switches
			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 airflow (blue coloring)	2	9364C-GX
NXA-PAC-2KW-PI	2000-W AC power supply with port-side intake airflow (burgundy coloring)	2	9364C-GX
NXA-PDC-2KW-PE	2000-W DC power supply with port-side exhaust airflow (blue coloring	2	9364C-GX
NXA-PDC-2KW-PI	2000-W DC power supply with port-side intake airflow (burgundy coloring)	2	9364C-GX
N2200-PAC-400W	400-W AC power supply with port-side exhaust airflow (blue coloring)	2	92348GC-X
N2200-PAC-400W-B	400-W AC power supply with port-side intake airflow (burgundy coloring)	2	92348GC-X
N2200-PDC-350W-B	350-W DC power supply with port-side intake airflow	2	92348GC-X
N2200-PDC-400W	400-W DC power supply with port-side exhaust airflow (blue coloring)	2	92348GC-X

Table 15. Cisco Nexus 9200 and 9300 Switches

Cisco Nexus Switch	Description
N9K-C92160YC-X	1-RU Top-of-Rack switch with 48 10-/25-Gigabit SFP+ ports and 6 40-Gigabit QSFP+ ports (4 of these ports support 100-Gigabit QSFP28 optics).
N9K-C92300YC	1.5-RU Top-of-Rack switch with 48 10-/25-Gigabit SFP28 ports and 18 fixed 40-/100-Gigabit QSFP28 ports.
N9K-C92304QC	2-RU Top-of-Rack switch with 56 40-Gigabit Ethernet QSFP+ ports (16 of these ports support 4x10 breakout cables) and 8 100-Gigabit QSFP28 ports.
N9K-C92348GC-X	The Cisco Nexus 92348GC-X switch (N9K-C92348GC-X) is a 1RU switch that supports

© 2022 Cisco and/or its affiliates. All rights reserved.

Cisco Nexus Switch	Description
	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 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.

© 2022 Cisco and/or its affiliates. All rights reserved.

Cisco Nexus Switch	Description
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(10) 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.

© 2022 Cisco and/or its affiliates. All rights reserved.

- 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)

© 2022 Cisco and/or its affiliates. All rights reserved.

- 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)

© 2022 Cisco and/or its affiliates. All rights reserved.

- 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

© 2022 Cisco and/or its affiliates. All rights reserved.

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(10)

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.

© 2022 Cisco Systems, Inc. All rights reserved.