Cisco Nexus 9000 Series NX-OS Release Notes, Release 10.2(4)M

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Introduction

This document describes the features, issues, and exceptions of Cisco NX-OS Release 10.2(4)M software for use on Cisco Nexus 9000 Series switches.

The new Cisco NX-OS Software Release and Image-naming Convention information is available here — Cisco NX-OS Software Strategy and Lifecycle Guide.

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:

Date	Description
April 25, 2024	Added CSCwh50989 and CSCwe53655 to the Open Issues section.
June 2, 2023	Updated the Resolved Issues section.
May 05, 2023	Added PTP in Unsupported Features on N9K-C92348GC section.
April 09, 2023	Added caveat CSCwe67205 to the Open Issues section.
February 3, 2023	Updated Table 11 with N9K-C9336C-FX2 and N9K-C9336C-FX2-E switches.
January 25, 2023	Updated the Unsupported Features on N9K-C92348GC section.
October 27, 2022	Cisco NX-OS Release 10.2(4)M became available.

New and Enhanced Software Features

There are no new features introduced in Cisco NX-OS Release 10.2(4)M.

The enhanced features listed below are existing features introduced in earlier releases but enhanced to support new platforms in Cisco NX-OS Release 10.2(4)M.

Enhanced Features	
Feature	**Description**
Periodic ARP Refresh on MAC Delete	Added a new command to configure the interval and frequency on the L3 VLAN interface, so that ARP process tracks the MAC deletes and sends ARP refreshes for the corresponding adjacency in the configured interval for the configured frequency (count). For more information, see Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 10.2(x).
Scale Enhancements	For Cisco NX-OS Release 10.2(4)M Scale Enhancements, see Cisco Nexus 9000 Series NX-OS Verified Scalability Guide, Release 10.2(4)M.
Nexus Cloud - Telemetry	Cisco NX-OS Release 10.2(4)M provides onboarding of supported Nexus Switches to

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Enhanced Features	
Feature	**Description**
	Nexus Cloud. This enables telemetry collection from the Nexus Switches.

Hardware Features

There are no new hardware features introduced in Cisco NX-OS Release 10.2(4)M.

For details on transceivers and cables that are supported by a switch, see the Transceiver Module (TMG) Compatibility Matrix.

Unsupported Features on N9K-C92348GC

Beginning with Cisco NX-OS Release 10.1(1), the following features are not supported on N9K-C92348GC:

- VXLAN
- SW/HW Telemetry
- NetFlow/Analytics
- iCAM
- PTP
- NX-SDK
- DME, Device YANG, OpenConfig YANG, gRPC, NETCONF, RESTCONF

Note: NXAPI CLI and XML Agent (NETCONF over SSH) are supported on this platform.

Release Image

In Cisco NX-OS Release 10.2(4)M, the following two 64-bit images are supported:

- The 64-bit Cisco NX-OS image filename that begins with " nxos64-cs" (for example, nxos64-cs.10.2.4.M.bin). This image is supported on all Cisco Nexus 9000 series fixed switches as well as 9000 Modular switches with FM-E/FM-E2/FM-G.
- The 64-bit Cisco NX-OS image filename that begins with " nxos64-msll" (for example, nxos64-msll.10.2.4.M.bin). This image is supported on Cisco Nexus 9000 -R and -R2 series modular switches.

The 32-bit image is no longer supported.

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Open Issues

Bug ID	Description
CSCwa77878	Headline: Default MTU shown in running-config when non-default value configured under network-qos class-map. Symptom: When configuring non-default values (dpp, pause, and so on) under class-map in network-qos policy-map, default MTU "mtu 1500" is shown in show running-config and cannot be deleted by "no mtu 1500". Default value should not be shown in show running-config. Workaround: None. Note that this is just showing default value in running-config and no impact to switch functionality.
CSCwc08911	Headline: Nexus 9000 :: dot1dBasePortIfIndex (.1.3.6.1.2.1.17.1.4.1.2) OID is not initiated properly on device reload. Symptom: The OID dot1dBasePortIfIndex (.1.3.6.1.2.1.17.1.4.1.2) is not available on Nexus 9000 series switch. Workaround: • (config)# no snmp-server load-mib dot1dbridgesnmp • Try killing the snmpd process: "run bash sudo killall snmpd" (requires "feature bash-shell")
CSCwc45694	Headline: TapAgg: 9300-GX - vlan tag is missing on captured packets with reload ascii. Symptom: On 9300-GX series switch, ASCII reload vlan tag is missing on the egress interface when TapAgg is configured to redirect traffic. Workaround: Remove and reapply "mode tap-aggregation" configuration under the interface.
CSCwc95871	Headline: Cisco Nexus 9200/9300 EOR switches: Unable to config switch mode trunk on FX breakout interface after replacing EX LC. Symptom: When N9500 line card module is removed and new line card is replaced, re-application of interface config on some breakout interfaces such as second breakout interface is not possible. Workaround: Reload the whole system to refresh interface dme running-config to re-apply breakout config and old running config for the new line card.
CSCwd20332	Headline: Ethernet port is breaking out without even giving breakout configs. Symptom: Interface breakout commands are not cleaned up on write erase + reload and POAP abort. Workaround: POAP abort is a negative scenario, circumvent the entire POAP abort by using the system no poap command. POAP can be aborted at any other stage such as, during breakout, during v4 DHCP phase, during v6 DHCP phase, and so on, and this issue does not occur.
CSCwe67205	Headline: Credit Loss Recovery is not triggered for FC interface with no transmit credits. Symptom: A Fibre Channel interface that stays at 0 transmit credits is not recovered by the Credit Loss Recovery agent. Workaround: If the interface has **switchport ignore bit-errors** configured, then remove it with the **no switchport ignore bit-errors** interface configuration command.
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.

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
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.

Resolved Issues

Bug ID	Description
CSCuq79793	Headline: IPv6 ND processes NA with Link-layer address 0000.0000.0000 as valid. Symptom: IPv6 ND installs a neighbor entry for an IPv6 host that sends an NA with the Link-layer address field populated with mac address 0000.0000.0000. Workaround: None
CSCvx84922	Headline: Interim ACL rule programmed during non-atomic update is not functioning as expected on all Nexus 9000 Cloudscale ASICs. Symptom: An issue with non-atomic updates of Access Control Lists (ACLs) on Cisco Nexus 9000 Series switches may result in traffic being permitted instead of denied during the brief time interval required for the device to update an ACL. Workaround: None. This issue only affects the brief time interval required for the non-atomic update of the ACL and the expected ACL behavior is enforced after that.
CSCvx93145	Headline: Topology information is not propagated from ISIS to MPLS TE when authentication is configured for ISIS. Symptom: The following symptoms are seen: • MPLS TE topology (show mpls traffic-eng topology) contains no information on other expected nodes, including those that are present in ISIS topology. • Similar logs are seen in " show isis event-history te" . Workaround: Configure ISIS authentication on per-interface level and remove it from the router isis section.
CSCvz01927	Headline: ARP process crash Symptom: ARP process crash Workaround: Do not run the show ip arp vrf XXX commands too often to reduce the associated risk.
CSCvz17681	Headline: Snapshot creation permission is denied. Symptom: Snapshot creation may fail with " Error:13(Permission denied)” when different users with different roles were used to create snapshots previously. Workaround: None
CSCvz38944	Headline: Nexus 9000 DHCPv6 Relay breaks after IPv6 snooping is removed. Symptom: Original Symptom from DHCPv6 Client perspective is not receiving an IPv6 Address from the DHCPv6 server. CPU will only show the DHCPv6 solicit/Re-bind packets; Relay-FWD is NOT originated by the Nexus 9000. Workaround: Shut/no-shut of the SVIs don’t seem to fix the issue. However, reload fixes the issue.

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
CSCvz69242	Headline: SNMP error in FIPS mode when modifying roles using username command. Symptom: Unable to change admin password or create new user in FIPS mode. Configuration fails with the following error message: SNMP : User with MD5/DES is not supported in FIPS mode. Workaround: User Role password and new user creation to begin with SNMP using sha-256 model, followed by username command.
CSCvz75894	Headline: Nexus 9500-R/Nexus 3600-R hardware application counters may get corrupted. Symptom: Nexus 9500-R/Nexus 3600-R running Cisco NX-OS 9.3(x) version of converged code may experience hardware counter corruption causing specific application counters to show incorrect information. Workaround: Reload clears the issue, but it can resurface.
CSCvz79573	Headline: Netstack MPLS OAM Fragmentation Issue. Symptom: IP fragment that matched the ACL for MPLS OAM packets. Workaround: Not have IP fragments that have data not matching the destination port of 3503.
CSCvz86703	Headline: In Cisco NX-OS Release 9.3(8), ip radius-source interface is not working. Symptom: mab/dot1x fails as ip-source interface is not crafting the correct source address. Workaround: None
CSCvz93622	Headline: Layer 3 VNI SVI is down indicating "VLAN/BD is down" after upgrade. Symptom: After disruptive upgrade from Cisco NX-OS Release 9.3(5) to 9.3(8), the layer 3 vni svi on a leaf/Border Leaf/Border Gateway may stay down, indicating "VLAN/BD is down", leading to connectivity issues. Workaround: Shut/No-shut the L3 VNID SVI. Note that a reload might not fix it as the next reload might also result in L3VNID SVI to remain in down/down.
CSCwa05191	Headline: Interface track configured under sub-interface does not work after reload. Symptom: Interface track is configured under sub-interface. When the switch comes back from reload, interface track does not work. For example, when interface track is configured under sub-interface where HSRP is configured, even after the tracked interface is up, HSRP still recognizes the tracked interface as down. Workaround: Do not use sub-interface. With parent interface (no sub interface) or SVI, this configuration should work correctly.
CSCwa32356	Headline: NX-OS Switch may experience an unexpected reset of snmpd. Symptom: In rare circumstances, an SNMPd process crash can happen, causing the whole switch to reload. The crash has been confirmed to be caused by memory corruption, with unknown circumstances. NX-OS versions in "known fixed releases" contain a fix that prevents this corruption from causing issues. Workaround: None
CSCwa41394	Headline: Nexus 9000 - "copy run start" fails due to NTP. Symptom: Nexus 9000 config save fails due to NTP config having concurrent resource locks. The following syslog is seen when the copy fails: %SYSMGR-3-CFGWRITE_SRVFAILED: Service "ntp" failed to store its configuration (error-id 0xFFFFFFFF) Workaround: Disable the feature ntp and re-enable it. However, if the issue persists, a reload is required to clear the PSS.

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
CSCwa56558	Headline: MTS leak between lldp dcx sap and Qosmgr SAP after enabling feature lldp Symptom: `show system internal mts buffers summary` or `detail`seeing 100+ stuck MTS buffers on pers_q between lldp dcx sap and Qosmgr SAP Workaround: Disable feature LLDP.
CSCwa58073	Headline: Nexus 9000 - " copy run start" fails after enabling " feature bfd" due to DME failure. Symptom: After inserting a module in the switch and saving the configuration before the module is removed or made offline (followed by a reload), if a user tries to enable BFD and execute copy run start, it fails. Workaround: To clear the DME inconsistency, reload ASCII or clear NX-API retries.
CSCwa61442	Headline: OSPF Process Crash due to Heartbeat Failure. Symptom: A Nexus switch might experience an OSPF process crash due to a heartbeat failure. Workaround: After the process crash, OSPF should come back up. However, it's possible that the switch later faces the same condition. Ensure that your network is stable to minimize the number of LSUs that need to be processed.
CSCwa73467	Headline: Adding member to port channel (pc) is rejected if userCfgdFlags doesn't have admin_layer in nc pld, but pc has it. Symptom: 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" . Workaround: There are 2 workarounds; any one can be chosen. • Re-create port-channel interface (remove and add it back) without switchport explicit config. • In the netconf payload, add admin_layer to the userCfgdFlags of member port.
CSCwa85286	Headline: Sporadic unknown unicast flood; L2FM errors. Symptom: L2FM errors are seen on the switch that holds the orphan port. Workaround: Add static ARP entry for the source of the traffic.
CSCwa91783	Headline: The show interface command displays abnormally high traffic rates. Symptom: A Nexus 9000 switch may show abnormally high input or output traffic rates on its interface, in the order of tens of terabits per second. This is observed in “show interface" as well as SNMP polling. This does not cause any problems beyond incorrect counters. Workaround: The problem may return after " reload" and even " reload ascii" . No reliable workaround available.
CSCwa93094	Headline: Nexus 9336C-FX2 reports false minor temperature alarm with back-to-front airflow. Symptom: Nexus 9336C-FX2 reports lower temperature on the exhaust side than intake, with back-to-front (port-side exhaust) airflow. Workaround: None
CSCwa99850	Headline: Significant PTP correction observed during PTP path failover. Symptom: In a network based on Nexus 9000, 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 Nexus 9000 switches briefly use their local clocks as time reference. Workaround: Increase the frequency of PTP announce/sync messages and reduce the timeout values to configurable minimum. This should shorten the duration for which Nexus 9000 uses its local clock for reference.

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
CSCwb08528	Headline: MAC learned on orphan port does not sync with peer switch over Peer-Link. Symptom: Server's MAC Address learned on Leaf1's orphan port is not getting synced across peer-link on Leaf2, causing teaming issue at the server end. Workaround: 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. Symptom: Max scalable HSRP group reduces to 490 rather than 1000. Workaround: None
CSCwb14542	Headline: Unexpected HSRP MAC refresh interval. Symptom: The configured HSRP mac-refresh interval on parent interface doesn't get applied to HSRP MGO follow groups configured on sub-interface, and the follow groups still send hellos with the default mac-refresh interval of 60 sec. This can be seen in the show hsrp detail command output. Workaround: Re-configure the mac-refresh command on parent interface after all the HSRP groups are configured.
CSCwb22718	Headline: LACP HIF port suspend causes traffic disruption Symptom: Traffic drops are seen on ingress for some interfaces that are part of FEX fabric port of the Nexus 9000 parent switch. Workaround: None
CSCwb30246	Headline: Nexus 9500-R/Nexus 3600-R CoPP incorrectly matches fragmented UDP packet with UDP PTP port payload as PTP packet. Symptom: PTP CoPP class shows drops. Workaround: None
CSCwb40813	Headline: Nexus 9300 syslogs incorrectly error "TCP NAT allocated region index exceeded." Symptom: There is a syslog message that reads "TCP NAT allocated region index exceeded" even though there is one more entry available for installation. Workaround: Configure one more entry in the customer environment.
CSCwb43500	Headline: PFSTAT crash @memmove_avx_unaligned_erms. Symptom: "pfstat" process crash observed. Workaround: None

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
CSCwb51700	Headline: Netconf Connections are not responding from Nexus. Symptom: The Netconf feature may stop working after some time. Even after restart, the same problem can occur again. Workaround: Recover - Once the switch is in the bad state, do not execute 'no feature netconf / feature netconf'. Use the following command to restart the Netconf process into the normal state: ----- n9k# conf t n9k# feature bash n9k# run bash sudo su - bash> kill -9 `pidof netconf` -----
CSCwb53272	Headline: Nexus 9000 TOR OID dot1dBasePortIfIndex value after port 64 is displayed incorrectly. Symptom: OID: dot1dBasePortIfIndex .1.3.6.1.2.1.17.1.4.1.2 The OID displays the interface index based on VLAN. By default, VLAN1 is used. • 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. • 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. Workaround: None
CSCwb53950	Headline: Specific N9K-9736C-FX Ports do not Link Up with FM-G modules installed. Symptom: Certain ports fail to link up on various FX-based modules in Cisco Nexus 9500 and show up as not connected. Workaround: Use N9K-C9504-FM-E modules instead or move the transceiver to a non-BV port (1-28).
CSCwb56624	Headline: After corrected HSRP duplicated group id, Nexus 9000 cannot learn specific HSRP VIP MAC address anymore. Symptom: Two Nexus 9000 (vPC configured) connected with 2 other devices (using orphan port), when misconfigured with the duplicate HSRP group id and corrected, the secondary vPC peer device Nexus 9000 cannot ping through HSRP VIP anymore. Workaround: The issue can be resolved by performing any of the following workarounds: • Flap vPC peer-link • Reload the N9k1 switch
CSCwb56686	Headline: Nexus 9000/FX3 standalone/FEX mode port stop is forwarding traffic after flap. Symptom: Interfaces might stop forwarding traffic even when remaining up. During the issue fifo overflow interrupt counter keeps increasing - this can be verified by the following commands: # slot X quoted " sh ha int tah interrupts" | grep fifoov 0 1 46319490 N Y roc_hea_prx_int_ff_0:overflow # slot X " sh ha int tah interrupts " | grep prx | grep ov 0 1 46319510 N Y roc_hea_prx_int_ff_0:overflow All traffic is not forwarded including control plane traffic as LLDP, STP, BFD, and so on. Workaround: Only possible recovery is to reload the device.

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
CSCwb57686	Headline: Nexus 9000 VTEP BUM Traffic has forwarding issues following an interface flap under certain conditions. Symptom: Multiple symptoms may be seen as follows: • BUM Traffic not sent out through Interfaces in the OIL • BUM Traffic may get duplicated on remote end Workaround: Bounce the interface. Note: After bounce, if the interface comes back up in a specific fashion as below, the issue may persist: • From UP to Down > Initializing > UP > Down > Initializing > UP or • From UP to Down > initializing > suspended > UP
CSCwb58274	Headline: NTP control packets are being processed when using ntp access-group serve-only. Symptom: 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 the NTP control packets. Workaround: None
CSCwb58876	Headline: Fabric-peering N9K-CXXX-FX2 switches may not process BPDUs from another switch. Symptom: Multiple symptoms may be seen as follows: • STP disputes on a downstream STP Root switch that is connected to vPC pair using fabric-peering. • The show spanning-tree detail command on the Nexus doesn't increment for the " received" BPDU Counter stats. • Ethanalyzer on Nexus 9000 shows the incoming STP BPDUs with the correct dot1q tag and with Root information (includes better priority for the VLAN in question). Workaround: 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.
CSCwb60501	Headline: Nexus routing unicast packets destined to broadcast link layer address routes packet to next hop. Symptom: A Nexus switch receiving unicast packets destined for broadcast link layer address (ffff:ffff:ffff) routes packet to next hop instead of dropping on the Cloudscale management interface. Workaround: None
CSCwb64677	Headline: Nexus 9000: Mirroring does not work if source-interface SPORT values are equal to or more than 31. Symptom: Seeing non-allowed VLANs on a SPAN session. Traffic is mirrored on the incorrect source interface or not configured interface but does not mirror the traffic from configured source interface. Workaround: None
CSCwb64912	Headline: BGP can see traceback/crash with aggregate-address command in EVPN setup. Symptom: BGP process may see traceback and potentially process crash. Workaround: Do not use aggregate-address.

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
CSCwb66026	Headline: MAC ACL containing multicast MAC cannot be applied to the port. Symptom: When attempting to apply a MAC ACL to an L2 port that is matching on a reserved multicast MAC address, the following error is seen on the configuration attempt, as well as a syslog reporting the issue: mac access-list L2_ACL 60 deny any 0100.5e00.0000 0000.007f.ffff N9K-C93600CD-GX-1(config-if)# mac port access-group test ACLQOS_ERROR: ACL entry creation failed N9K-C93600CD-GX-1(config-if)# sh logging log | last 10 2022 Apr 20 02:21:29 513E-A-19-N9K-C93600CD-GX-1 %ACLQOS-SLOT1-2-ACLQOS_FAILED: ACLQOS failure: ACL entry create API failed Status: 0xb reason dchal api generi Workaround: None
CSCwb66035	Headline: is-dci is set to TRUE for fabric interface. Symptom: BUM traffic is dropped which can impact ARP, multicast and broadcast packets. Hosts on siteA cannot perform ARP resolution to SiteB. Workaround: Make sure remote BGWs multisite IP address are not reachable via the fabric link when fabric link is bringing itself up. The is-DCI consults the routing table for the remote multisite BGWs peer IP to verify whether the link is DCI link or not.
CSCwb69140	Headline: Nexus 9500 Power-Denied when Capacity is more than the Total Power allocated (Budget) Symptom: • I/O module in Power-Denied state despite sufficient installed Capacity is more than the Total Allocated Power (Budget). • Attempt to configure a power redundancy mode such as N+1 (ps-redundant) or N+N (insrc-redundant) is rejected despite having sufficient Capacity installed. Workaround: Add Power Supply(s) to increase capacity aligned with the power redundancy mode used.
CSCwb70215	Headline: Adding/removing the interface from the Layer 2 port-channel causes a multicast issue. Symptom: When an interface is removed/added to an existing Layer 2 port-channel between Cisco Nexus and Cisco ASR 9000, the multicast traffic start dropping in Cisco Nexus Software: 9.3(7) Hardware: N9K-C93180YC-EX. Workaround: • Reload the switch. • Shut/no shut the port-channel. • Remove ip igmp snooping vxlan. • Remove VXLAN configuration under the VLAN.
CSCwb73211	Headline: NX-OS PTP TS missing logging information and sufficient PTP correction history. Symptom: PTP TS does not have sufficient information for problem analysis. Workaround: Collect 'show logging logfile | grep -i ptp' individually.
CSCwb73231	Headline: Nexus 9000/Nexus 3100/Nexus 3500 may be sending out of spec PTP messages with SourcePortID equal to zero. Symptom: Nexus PTP messages rejected by third-party PTP device. Workaround: Do not use port 1 for PTP.

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
CSCwb73581	Headline: Config replace fails when trying to modify a route map if route-map name uses delimiter characters. Symptom: Config replace fails while trying to make changes to " match community" statement under a route-map. Workaround: To resolve the failing route-maps, create community-lists with new unique names and associate them to the failing route-maps.
CSCwb74307	Headline: RPF for PIM Bidir with phantom RP is not changed on shutting the interface. Symptom: PIM Bidir has wrong OIF entry when interface toward RP is shut. It is not updated and showing the interface that is shut. Workaround: Clear ip mroute * vrf " name of vrf" .
CSCwb78090	Headline: Only a limited amount of odd or even VLANs can be added to an MST instance. Symptom: Apply odd or even VLANs to an MST instance but only a certain amount of VLANs is applied after committing the change. For example, if you apply all odd VLANs from 1 to 3967, only the odd VLANs from 1 to 3497 are applied. The show system internal dme running-config all dn sys/stp/inst/mstent command shows that the VLANs such as VLAN 3499 were pushed to the MST instance in DME. However, the show spanning-tree vlan 3499 command will show that the VLAN is still in the default instance 0. Workaround: Limit the amount of alternating VLANs that are added to each instance. This can be done by adding consecutive VLANs to an instance such as 1-500. Alternatively, you can utilize more instances such as the following config: instance 1 vlan 1,3,5,7,9,11,13,15,17,19 CUT FOR BREVITY instance 1 vlan 2001,2003,2005,2007,2009,2011,2013,2015,2017,2019 instance 2 vlan 2021,2023,2025,2027,2029,2031,2033,2035,2037,2039 CUT FOR BREVITY instance 2 vlan 3961,3963,3965,3967
CSCwb81409	Headline: Nexus 9000-FX3: SyncE process crashes due to MTS drop (with PTP configured). Symptom: SyncE hap reset/crash logs are seen, and core generated. Workaround: None
CSCwb83283	Headline: Memory leak due to port profile. Symptom: Memory leak port profile process crashes and generates core files. The memory usage for port-profile process increments every day. Workaround: None
CSCwb85986	Headline: Nexus 9000 FEX – Traffic loss is seen when parent switch reloads and comes online. Symptom: Traffic through Active-Active FEX (vPC) is lost for about 20 secs when one of the parent Nexus 9000 reloads and comes online. Workaround: None
CSCwb86276	Headline: tnl ecmp mac is mis-programming on ECMP churn. Symptom: With GX-based 9500 LC, intermittent traffic impact may be seen due to ECMP churn. Workaround: Flap impacted interfaces/reload impact modules.

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
CSCwb86325	Headline: Packets larger than 1500 are software switched in DSVNI deployments, regardless of SVI MTU. Symptom: Routed packets that are taking a DSVNI / Asymmetric route are being punted to the CPU if the packet-size exceeds 1500 bytes. Punted packets are observed in ethanalyzer. Workaround: None
CSCwb89150	Headline: NX-OS/ARP - vPC peer does not learn ARP when ARP reply has a different SRC MAC in ETH and ARP header. Symptom: For servers that are sending ARP reply with different SRC MAC in ETH header and SRC MAC in ARP header, ARP entry is installed in one of the vPC peers, and, consequently, in L2 route and advertised to the EVPN. This situation can cause traffic blackholing in case traffic arrive on a vPC peer that does not have ARP entry installed. Workaround: Force server to send ARP reply with same MAC in ETH and ARP header.
CSCwb90448	Headline: Traceback: satctrl crash post FX3 FEX conversion with optical fiber uplink. Symptom: The following symptom is seen: Wind River Linux <snip> (none) ttyS0 none) login: admin login[5632]: root login on `ttyS0' Loading parse tree (LC). Please be patient... fex-1# [21.352638] NX-OS starts punching watchdog Jun 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] Workaround: Apply 'write erase' before the FEX conversion configuration: term dont-ask write erase no boot nxos copy running-config startup-config boot fex delete bootflash:poap_replay*.cfg reload

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
CSCwb91752	Headline: Segmentation Fault Signal 11 is seen on service LLDP. Symptom: LLDP core file is generated # show core VDC Module Instance Process-name PID Date(Year-Month-Day Time) --- ------ -------- --------------- -------- ------------------------ 1 1 1 lldp xxxx 202x-xx-xx xx:xx:xx LLDP packet length error is seen. Workaround: None

CSCwb92400	Headline: Changes in the way how " show hardware internal buffer info pkt-stats" is collected in show techs.
	Symptom: Currently, `show tech-support` outputs are collecting buffer stats only for module 1 and instance 0:
	`show hardware internal buffer info pkt-stats module 1 instance 0`
	`show hardware internal buffer info pkt-stats input module 1 instance 0`
	Above outputs will not present all information if 'show tech' output is collected on switch with LC module that has more than one instance.
	Workaround: None

CSCwb93820	Headline: Nexus 9000/TRM: Invalid host entry in hardware after mcast source move between sites. Symptom: Traffic destined to IP address of multicast sources can be forwarded by CPU or drop after multicast sources are moved between EVPN sites. Issue happens on transit sites that have neither directly connected sources nor receivers. This is due to invalid HW entry in host route table that has destination IP redirect to CPU set, which can be verified by CLI. Workaround: Move host again between sites or stop multicast traffic and wait until S,G entry expires.
CSCwb97155	Headline: EOR drops VXLAN packet with incorrect checksum. Symptom: A VXLAN packet with inner ip header checksum 0x0000 will be dropped by EOR with no vxlan feature enabled. Workaround: None
CSCwb99044	Headline: Need to remove mandate of L2VNI with " dci-advertise-pip" . Symptom: NVE peering goes down across multisite. Workaround: Create dummy l2vni for NVE peering to work.
CSCwb99717	Headline: VLAN Tags are suppressed when the traffic hits the redirect ACL. Symptom: When the dot1Q traffic match IP-ACL redirect condition, VLAN tag is removed from the traffic header. Workaround: Apply the following configuration: interface eth X no mode tap- aggregation mode tap- aggregation After reloading the switch, the issue recurs.

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
CSCwc00066	Headline: Nexus 9000: Interface disables CDR after shut/no shut due to lack of checks when TX LOL is gone. Symptom: CDR is disabled for an optic. Workaround: Reload to restore CDR status- It is unconfirmed if removal and re-insertion restores CDR status.
CSCwc03573	Headline: Nexus reload at OSPF update. Symptom: Nexus C93180YC-FX has OSPF sessions flaps. OSPF process crashes while doing name-lookup. Workaround: This crash occurs when name-server is slow or unreachable and along with this network (OSPF adjacency) is not stable. Workaround is to remove the name-lookup command from OSPF configurations.
CSCwc05498	Headline: Flow exporter not working after changing the destination ip and/or vrf. Symptom: The netflow exporter does not send any packets towards the collector, although the output of " show flow exporter" command shows increase in number of packets sent. Workaround: • 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.
CSCwc06034	Headline: Twinax link bringup delays on N9K-C93108TC-FX3P. Symptom: N9K-C93108TC-FX3P switches may experience delays in bringing up ports using twinax cables. Workaround: There is no workaround other than trying a different media type, such as fiber optics with ordinary transceivers instead of twinax.
CSCwc08227	Headline: Nexus 9000/vxlan - incorrect destination MAC for nve peers. Symptom: Traffic passing BGW can observe a packet drop destined for specific NVE peers over specific interfaces. Packets are dropped by peer device (spine or VTEP - in case BGW/Spine) because they are destined to the incorrect MAC address. Workaround: Flap of destination interface or flap NVE or reload of the device.
CSCwc08583	Headline: The vPC " peer is alive for" counter does not increase. Symptom: The vPC " peer is alive for" counter does not increase when IPv6 is configured for keep-alive. The counter increases for " msec" but not for " seconds" (keeps as 0). Workaround: Use IPv4 instead.
CSCwc10388	Headline: Nexus 9000 running Cisco NX-OS Release 7.0(3)I7(x) allows SNMPv3 Noauth security level configuration. Symptom: Nexus 9000 with Cisco NX-OS Release 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" . Workaround: None

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
CSCwc11728	Headline: CR Verify-Only validation is failed with error : Syntax error while parsing 'port-type fabric'. Symptom: CR " verify-only" is failed with the error : Syntax error while parsing 'port-type fabric'. Workaround: None
CSCwc12120	Headline: Nexus 9000 : continuous nfm crashes after upgrade to Cisco NX-OS Release 10.2(3) because of NetFlow. Symptom: Nexus 9000 series switch crashes continuously after upgrade to software release 10.2(3). Workaround: • Hold with upgrading the device / downgrade the device. • Remove NetFlow configuration prior to device upgrade.
CSCwc12930	Headline: Nexus 9000: Traffic is not forwarded due to interface mis-programming. Symptom: When a Nexus 9000 Interface receives a packet from the server/any device which is directly connected to Nexus it drops the packet. Here the entire traffic is dropped for all the VLANs that will be used under an interface. The parent switch (Nexus 9000) is affected due to FEX port which is associated with the switch interface, and, in turn, that interface will also be affected. Workaround: There are 2 options: • To Bounce the Impacted Interface. • To Reload the Device.
CSCwc14067	Headline: Nexus 9000 EOR - Received icmpv6 NS packet with Own mac address after SUP Switchover. Symptom: After supervisor switchover, Nexus receives alerts for icmpv6 Own mac address in the NS packet. The icmpv6 NS comes from own Nexus ipv6 address to VIP VRRPV3 address for target VIP VRRPV3 address. Workaround: Perform any one of the following workarounds: • Delete the VRRPv3 IPv6 VIP6 on issue VLAN and reconfigure it. • Reload the switch.
CSCwc14167	Headline: Shutting down L3 subinterface removes HSRP RMAC on other L3 subinterfaces. Symptom: Shutting down L3 subinterface removes HSRP RMAC on other L3 subinterfaces. Workaround: None
CSCwc14383	Headline: On EOR incorrect standby sup status results in patch installer failure. Symptom: Patch install operations may fail on Nexus 9500. Workaround: Reinsert secondary SUP to the device.
CSCwc14617	Headline: SNMP Query for ARP/IPv6 ND results in missing entries. Symptom: snmpwalk against mib 1.3.6.1.2.1.4.35.1.4 with IPv6 interface results in some entries not being returned. Issue is most noticeable when there is an IPv6 interface without IPv4. All ARP and IPv6 ND entries after this entry are lost. Workaround: None

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
CSCwc17000	Headline: SSH x509v3 Certificate with TACACS unsupported could allow escalation of privilege level. Symptom: For the Cisco NX-OS Software product family a SSH x509v3 certificate used with a Personal Identification Verification (PIV) card is not supported with TACACS Remote Authentication. The Authentication, Authorization, and Accounting (AAA) functionality does not properly return invalid for this configuration. This could allow a user to escalate their privilege level to that of an administrator. Workaround: The aaa authorization ssh-certificate default group <group> command should be removed as this is not a valid configuration.
CSCwc19270	Headline: N93108TC-FX3P in FEX mode displays incomplete port speed capabilities. Symptom: N93108TC-FX3P 100M port speed is not included in port capabilities output. Workaround: None
CSCwc19305	Headline: BGP Idle due to neighbor configured with " disable-connected-check" . Symptom: If the disable-connected-check feature is configured on the neighbor, EBGP multi-hop sessions will not be established. Workaround: By removing the disable-connected-check feature from the configuration and adding ebgp-multihop #, the session will complete the process.
CSCwc19848	Headline: OBFL no partitions mounted on eMMC device. Symptom: OBFL diagnostic failure is observed on Nexus 9000 (N9K-C9364C) following ISSU. Workaround: Reload the switch twice to re-partition and re-format OBFL.
CSCwc21224	Headline: aclqos crashes due to hap reset @ tlv_aligned_array_get_next_tlv. Symptom: Switch crashes due to an " aclqos" process crash, as seen in " show version" or " show module internal exceptionlog" . Workaround: None
CSCwc21801	Headline: NBM PIM_Passive: retry for the link-down flows. Symptom: In NBM PIM-Passive mode, if NBM flows have link in down state then NBM used to raised fault MO and the controller can fix the link down issue and delete and stitch again. On the latest releases, behavior is changed and NBM will not raise fault and will auto-try to stitch the flows whenever the link comes up. With the new behavior, if the RPF or the OIF is down on receiving the API request, PMN will create the static-db data-structure with fault? Interface down?. But this will not be published in Fault MO. When the interface comes back up later, PMN walks through the static flow-db and adds the interface in MRIB. This is true for both RPF and OIF. When the interface goes down later, PMN withdraws the interface from MRIB and again sets the fault reason in static flow-db. Workaround: Use the nbm pim-passive mode.
CSCwc21903	Headline: Device yang JSON ON_CHANGE snapshot is returned in flattened, rather than aggregated format. Symptom: In Cisco NX-OS Release 10.2(3)F, the on_change snapshot for yang paths became flattened instead of aggregated. In Cisco NX-OS Release 10.2(2)F, the format was aggregated. Events remained the same. Workaround: Use GPB as encoding.

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
CSCwc24060	Headline: Nexus 9000: Inner tag removed when traffic is crossing vPC peer-link. Symptom: Dot1q tunneled traffic has its inner tag removed/stripped when crossing the Peer-link of the vPC pair. Workaround: Disabling and enabling the " system dot1q-tunnel transit vlan <vlan-id>" (for the provider VLANs) seems to solve the forwarding issue.
CSCwc26955	Headline: LACP egress is set to incorrect traffic class Symptom: LACP tx direction may drop LACP PDU randomly due to incorrect TC values set. Such control plane flow is always expected as TC0. However, in current release it's TC7. Workaround: Shut down or remove monitor session.
CSCwc30146	Headline: IPv6 packet does not include L3 header when calculating MTU. Symptom: The MTU violation, when forwarding IPv6 packets, is flagged only when the packet-size exceeds the length of the payload carried by the IPv6 header. The expected behavior is to report the violation when the length of the L3 Header and payload put together exceeds the configured MTU. Workaround: None
CSCwc30202	Headline: NX-OS images boot despite being corrupted. Symptom: It's possible for a switch to boot a corrupted NX-OS image. This may lead to various problems in the subsequent behavior of the switch, the most noticeable of which may be various standard features such as BGP or interface-vlan missing in the parser and being impossible to configure. Workaround: Verify the image's MD5 checksum before upgrading.
CSCwc34293	Headline: N9K-C9336C-FX2 Multicast Tx SPAN doesn't work. Symptom: N9K-C9336C-FX2 Multicast Tx SPAN doesn't work. Configure multicast Tx span source, but there is no output on span dst. Workaround: None
CSCwc35610	Headline: PSU actual input & output power are " 0" after upgrade to 9.3.9. Symptom: Output of CLI -" show environment power" results actual input and output as " 0" , though box will be working fine. No Power failure alert in logging. Workaround: None
CSCwc36081	Headline: Log rotation within /var/volatile/tmp inside modules. Symptom: On Nexus 9000 Cloudscale ASIC switches, we will observe the following syslog: SYSMGR-SLOT1-2-TMP_DIR_FULL: System temporary directory usage is unexpectedly high at 100% Workaround: Address the flapping link issue to stop the increment of the temporary log file. Reload the switch to clear the log condition.
CSCwc36651	Headline: EEM " event fib route" is not working. Symptom: We are not able to generate/triggered syslog with EEM " event fib route" feature. Workaround: None

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwc37654	Headline: Nexus 9300 NAT breaks short-lived passive data FTP sessions with non-zero NAT creation-delay. Symptom: Short-lived passive FTP data session fails. Workaround: None
CSCwc38530	Headline: BGP with MD5 authentication not forming between switches using non-default vrf with long name. Symptom: When trying to form BGP with MD5 authentication between 2 directly connected switches in VRF with 32-character name, BGP is not coming up. Workaround: • Shorten VRF name from at least one side (even by 1 character). • Remove MD5 authentication.
CSCwc40726	Headline: Nexus aclqos event-history error output is missing in aclqos TS and TS detail. Symptom: ACLQoS errors output missing in TS detail and ACLQoS TS. Workaround: Collect missing output separately.
CSCwc41076	Headline: Nexus 9000 - Packet loss during initializing FEX HIF after FEX comes online. Symptom: In AA FEX topology, when the NIF(vpc leg) is shut/no shut on the Primary SW(HSRP) and the FEX comes online again, arp reply to the host connected to the FEX from the SW is dropped on the SW until HIF on the FEX is up on the SW. Workaround: None
CSCwc42251	Headline: LLDP crashes when configuring it on the device. Symptom: When trying to configure LLDP it crashes. The LLDP feature is enabled but doesn't seem to be running. Disabling and re-enabling the feature lldp command in the configuration does not work. Workaround: None
CSCwc43123	Headline: CLI CR is failing with logging server configurations. Symptom: If the current running configuration has non-default facility, the CR fails in the configuration that has default options. Workaround: To recover, configure using CLI so that the default configuration parameters are programmed.
CSCwc43397	Headline: Memory leak in NGINX process. Symptom: Nexus switch memory usage might be constantly increasing due to NGINX process. Workaround: None
CSCwc44309	Headline: Nexus 9300 single NAT w/o AU breaks passive data FTP session flow after successful initial start. Symptom: Passive FTP session data transfer fails to complete. Workaround: None
CSCwc48758	Headline: CoPP fails to apply, and no syslog is generated when PPF session fails. Symptom: Under rare circumstances, CoPP may fail to apply on system boot (PPF timeout). Workaround: Use the show copp status command to validate that CoPP is applied.

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
CSCwc52078	Headline: Nexus 9000-GX – show hardware internal statistics all – does not work. Symptom: LC command – show hardware internal statistics all – does not work on GX-based devices. Workaround: Collect statistics using other show commands as follows: • show system internal tah hw counters • sh hardware internal tah counters asic X • sh hardware internal tah drop counters
CSCwc52574	Headline: Nexus 9000 - SRC VTEP Peer IP 0.0.0.0 in show nve peers. Symptom: SRC VTEP peer IP 0.0.0.0 is listed in `show nve peers`. Workaround: Flap NVE Interface to clear and recreate peer entries. Reload the affected switch.
CSCwc53865	Headline: Nexus 9000 – the show npv flogi-table command output has changed so that it is split across two lines. Symptom: The output of the show npv flogi-table command splits into two lines unlike 7.0(3)I7(9) and MDS versions. Workaround: The show npv flogi-table command output is restored to its previous format.
CSCwc55730	Headline: PIM-Process Crash. Symptom: %SYSMGR-3-HEARTBEAT_FAILURE: Service "pim" sent SIGABRT for not setting heartbeat for the last 7 periods. Last heartbeat was 210.94 secs ago. Workaround: None. PIM restarts after the crash.
CSCwc59914	Headline: Unable to apply PACL when TCAM template is enabled. Symptom: On a Nexus 93180YC-EX that has a TCAM template configured, the following error is seen when a PACL is applied to an interface: " ERROR: TCAM region is not configured. Please configure TCAM region and retry the command." However, the TCAM hardware/software outputs indicate that the ing-ifacl (PACL) region is configured and has space available. Workaround: Remove the TCAM template configuration and configure TCAM region using the hardware access-list tcam region ing-ifacl 256 command.
CSCwc60753	Headline: VRRP is stuck in INIT. Symptom: VRRP may be stuck indefinitely in INIT state after reload. Workaround: Shut / no shut the affected interface.
CSCwc64216	Headline: EIGRP ISSU 9.x/10.1.x to 10.2.x : CLI is not converted to address-family if multiple redistributions are configured. Symptom: EIGRP ISSU 9.x/10.1.x to 10.2.x : CLI is not converted to address-family if multiple redistributions are configured. Only the first redistribution will be converted to the new style/address-family, the other redistributions will remain under the old style CLI and will not be active. Workaround: Remove and add the missing redistributions.
CSCwc66335	Headline: Nexus 9000 - SRCTEP Peer Entry is missing in hardware. Symptom: BUM traffic received on VTEP is dropped with the INFRA_ENCAP_SRC_TEP_MISS reason. This is due to the Source VTEP entry for peer missing in the hardware. The peer entry will be present in NVE & IPFIB though. Workaround: None

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
CSCwc67943	Headline: Nexus 9000 TRM - SA-AD is not triggered from the Turn-around router. Symptom: Nexus 9000 TRM - SA-AD is not being triggered from the Turn-around router. Turn-around is sending (S,G) join and (S,G) prune towards the source, leading to the traffic never getting pulled on Turn-around router. Workaround: None
CSCwc74073	Headline: Copper interfaces in N9K-X9788TC-FX do not come up when using N9K-C9504-FM-G. Symptom: None of the RJ45 interfaces of line card N9K-X9788TC-FX come up. Workaround: None
CSCwc78473	Headline: Nexus 9500 delays sending BPDUs every 60 seconds. Symptom: A Nexus 9500 switch might delay sending out spanning-tree BPDUs every 60 seconds. Workaround: None
CSCwc80086	Headline: Nexus 9000 sysmgr crashes due to incorrect core pattern in Cisco NX-OS Release 7.0(3)I7(x) resulting in LC/FM reload. Symptom: • Nexus 9000 EOR with BCM line card or N9K-C9508-FM crashes due to sysmgr. • Debug core file shows below output: 0xb6953e3c write ---> /nobackup/tstewart/smartdecoder-tmp/tmp/ucd.M347b/sysroot.LvgUTO/lib/libc.so.6 0xb68f1a54 _IO_file_write ---> /nobackup/tstewart/smartdecoder-tmp/tmp/ucd.M347b/sysroot.LvgUTO/lib/libc.so.6 • System uptime is nearly two years. • Kernel uptime is 810 day(s), 7 hour(s), 6 minute(s), 15 second(s) • OBFL will be failed after the crash and RMA needed. Workaround: Contact Cisco TAC.
CSCwc81429	Headline: PHY ports stay linked up when peer is powered off. Symptom: On Cisco N9K-X9788TC2-FX, N9K-C93108TC2-FX platforms, when the peer box reloads, sometimes the link does not go down. Workaround: None
CSCwc84291	Headline: KIM Process MTS Buffers are stuck. Symptom: KIM Process has messages stuck in MTS queue. Workaround: Reloading the switch clears stuck MTS buffers.
CSCwc86152	Headline: Nexus 9300 sends single NAT untranslated packet due to fib miss and mandatory add-route. Symptom: Single NAT untranslated packets received by NAT inside host. Workaround: None
CSCwc86253	Headline: Notifications are not generated for the path System/name. Symptom: Subscription for on_change notifications for the path System/name doesn't send notifications via netconf, restconf, or gnmi. This yang path refers to the hostname of the switch, so notifications are not generated due to changes to the hostname of the switch. Workaround: The hostname of the switch is also represented via System/vdc-items/Vdc-list[id=1]/name on Nexus 9000 platforms, so the user can subscribe to this path to get the notifications for hostname changes.

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
CSCwc87567	Headline: Nexus 9000: VXLAN Multisite VPC - w/ dci-advertise-pip tenant VRF CPU generated traffic still uses VIP. Symptom: Nexus 9000: VXLAN Multisite VPC - with dci-advertise-pip configured CPU generated traffic within the tenant VRF still uses the shared NVE source loopback VIP. Packets will be punted to CPU and seen in ethanalyzer on remote Border gateway. ELAM reports UC_TENANT_MYTEP_BRIDGE_MISS and ROUTING_DISABLED. This is because the VIP is not listed as an NVE peer on the remote Bordergateway, only the PIPs are advertised with " dci-advertise-pip" . Workaround: None, if you need both VPC and dci-advertise-pip configured.
CSCwc88702	Headline: Nexus 9000 syslog " Failed to open file: No such file or directory - securityd" - post upgrade to 9.3(9)+. Symptom: Nexus 9000 generates following syslog message periodically after upgrade to 9.3(9) " %USER-3-SYSTEM_MSG: Failed to open file: No such file or directory - securityd" No other changes were made. Logs started to appear after upgrade. Workaround: None
CSCwc90986	Headline: Unable to configure " ip tacacs source-interface" when " feature password encryption aes" is configured. Symptom: When " feature password encryption aes" is configured on the device, the ip tacacs source-interface command cannot be configured. Command is accepted but not reflected in the configuration. Workaround: • Removing " feature password encryption aes" • Removing " feature tacacs+" • Configuring " feature tacacs+" and " ip tacacs source-interface"
CSCwc94630	Headline: Nexus 9000 - DHCPv6 IAPD Parse Fails due to Invalid Client ID Option. Symptom: Parsing of DHCPv6 IAPD options from a Request packet will fail due to invalid client ID option referenced. Workaround: Disable option 19 or 20 on DHCPv6 Client. However, if this is not possible (depending on the client), contact client vendor for further assistance.
CSCwc97662	Headline: 40G RWX programming is incorrect, can lead to MAC under-run. Symptom: Output errors seen in TX interface where the traffic profile is 100g -> 40g. Also, " TAHUSD_MAC_INTR_TX_UNDERRUN_MAC" is seen when using the " show hardware internal tah event-history front-port X lane 1" command. Workaround: None
CSCwc98298	Headline: Nexus 9300 NAT does not translate packets of random tcp flow. Symptom: Packets of random tcp flow might be sent untranslated in in-out direction. Workaround: None

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwc98328	Headline: Syslog message is not descriptive – %PORT-5-IF_DOWN_LINK_FAILURE - Link failure Link reset. Symptom: The following syslog message is seen in N9K-C93360YC-FX2 running Cisco NX-OS 10.2(3): 2022 Sep 12 11:34:30 N9KSW1 %PORT-5-IF_TRUNK_DOWN: %$VSAN 2%$ Interface fc1/96, vsan 2 is down (Gracefully shutdown) 2022 Sep 12 11:34:30 N9KSW1 %PORT-5-IF_DOWN_LINK_FAILURE: %$VSAN 2%$ Interface fc1/96 is down (Link failure Link reset) 'Link failure link reset' is not a proper failure description. Workaround: None
CSCwc99946	Headline: ePBR probe command issues - DCNM 11.5(3) NXOS 10.2.3 Symptom: Unable to configure EPBR service-level and service-endpoint probes using DCNM Freeform configuration, with configuration not going through and/or configuration compliance failures. Workaround: Manually configure the EPBR services and policies on the switch and turn off strict configuration compliance for the fabric.
CSCwd04388	Headline: DME consistency error seen with snmp-server engindId. Symptom: DME consistency error is observed when snmp-server engineID local is configured using lower case hexadecimal values as below. snmp-server engineID local a:a:a:a:a Workaround: Apply snmp-server engineID local configuration using upper case hexadecimal values.

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
CSCwd06720	Headline: Removing one object-group causes statistics for the whole ACL to be disabled. Symptom: The following symptom is seen: Config: object-group ip address DST_PRE1 10 host x.x.x.x object-group ip address DST_PRE2 10 host x.x.x.x object-group ip port DST_PORT1 10 eq 11004 object-group ip port DST_PORT2 10 eq 11005 ip access-list TEST_ACL_IN statistics per-entry 1020 permit tcp any addrgroup DST_PRE2 portgroup DST_PORT2 log 1030 permit tcp any addrgroup DST_PRE1 portgroup DST_PORT1 log interface Vlan10 no shutdown ip access-group TEST_ACL_IN in ip address x.x.x.x/x N9K1(config)# no object-group ip port DST_PORT1 N9K1# show access-lists TEST_ACL_IN expanded 1020 permit tcp any 10.0.0.1/32 eq 11005 log << there are no statistics displayed [match=x] Workaround: Remove entry from ACL for which the port object-group has been removed or not configured.

Known Issues

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 10.2(4)M 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

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

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

Prodcut ID	Description	Maximum Quantity		
		Cisco Nexus 9504	Cisco Nexus 9508	Cisco Nexus 9516
N9K-X9716D-GX	Cisco Nexus 9500 16-port 400-Gigabit Ethernet QSFP line card	4	8	N/A
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
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-FX	Cisco Nexus 9500 32-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-X9736C-EX	Cisco Nexus 9500 36-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 Nexus 9508
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

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Product ID	Description	Maximum Quantity	
		Cisco Nexus 9504	Cisco Nexus 9508
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
N9K-X9624D-R2	Cisco Nexus 9500 24-port 400 Gigabit QDD line card	Not supported	8

Table 4. 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-C9504-FM-G	Cisco Nexus 9500 4-slot 1.6Tbps 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-C9508-FM-G	Cisco Nexus 9500 8-slot 1.6Tbps cloud-scale fabric module	4	5
N9K-C9516-FM-E2	Cisco Nexus 9516 100-Gigabit cloud scale fabric module	4	5

Table 5. 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
N9K-C9508-FM-R2	Cisco Nexus 9508 400-Gigabit R-Series fabric module	4	6

Table 6. 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.

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Table 7. Cisco Nexus 9500 System Controller

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

Table 8. Cisco Nexus 9500 Fans and Fan Trays

Product ID	Description	Quantity
N9K-C9504-FAN	Fan tray for 4-slot modular chassis	3
N9K-C9504-FAN2	Fan tray that supports the Cisco N9K-C9504-FM-G fabric module	3
N9K-C9508-FAN	Fan tray for 8-slot modular chassis	3
N9K-C9508-FAN2	Fan tray that supports the Cisco N9K-C9508-FM-G fabric module	3
N9K-C9516-FAN	Fan tray for 16-slot modular chassis	3

Table 9. Cisco Nexus 9500 Fabric Module Blanks with Power Connector

Product ID	Description	Minimum	Maximum
N9K-C9504-FAN-PWR	Nexus 9500 4-slot chassis 400G cloud scale fan tray power connector	1	2
N9K-C9508-FAN-PWR	Nexus 9500 4-slot chassis 400G cloud scale fan tray power connector	1	2

Table 10. Cisco Nexus 9500 Power Supplies

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

Table 11. Cisco Nexus 9200 and 9300 Switches

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Cisco Nexus Switch	Description
N9K-C9316D-GX	1-RU switch with 16x400/100/40-Gbps ports.
N9K-C9364C-GX	2-RU fixed-port switch with 64 100-Gigabit SFP28 ports.
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-C9332C	1-RU fixed switch with 32 40/100-Gigabit QSFP28 ports and 2 fixed 1/10-Gigabit SFP+ ports.
N9K-C9332D-GX2B	1-Rack-unit (1RU) spine switch with 32p 400/100-Gbps QSFP-DD ports and 2p 1/10 SFP+ ports.
N9k-9348D-GX2A	48p 40/100/400-Gigabit QSFP-DD ports and 2p 1/10G/10G SFP+ ports.
N9k-9364D-GX2A	64p 400/100-Gigabit QSFP-DD ports and 2p 1/10 SFP+ ports.
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-C9336C-FX2-E	1-RU switch with 36 40-/100-Gb QSFP28 ports.
N9K-C9336C-FX2	1-RU switch with 36 40-/100-Gb Ethernet QSFP28 ports.
N9K-C93360YC-FX2	2-RU switch with 96 10-/25-Gigabit SFP28 ports and 12 40/100-Gigabit QSFP28 ports.
N9K-C93240YC-FX2	1.2-RU Top-of-Rack switch with 48 10-/25-Gigabit SFP28 fiber ports and 12 40-/100-Gigabit Ethernet QSFP28 ports.
N9K-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-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-C93108TC-FX	1-RU Top-of-Rack switch with 48 100M/1/10GBASE-T (copper) ports and 6 40-/100-Gigabit QSFP28 ports.

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Cisco Nexus Switch	Description
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-C9348GC-FXP *	Nexus 9300 with 48p 100M/1 G, 4p 10/25 G SFP+ and 2p 100 G QSFP.
N9K-C92348GC-X	The Cisco Nexus 92348GC-X switch (N9K-C92348GC-X) is a 1RU switch that supports 696 Gbps of bandwidth and over 250 mbps. 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-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-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.

***Note:** For N9K-C9348GC-FXP the PSU SPROM is not readable when the PSU is not connected. The model displays as " UNKNOWN" and status of the module displays as " shutdown."

Table 12. Cisco Nexus 9200 and 9300 Fans and Fan Trays

Product ID	Description	Quantity	Cisco Nexus Switches
NXA-FAN-160CFM-PE	Fan module with port-side exhaust airflow (blue coloring)	3	9364C [1] 93360YC-FX2 [2]
NXA-FAN-160CFM-PI	Fan module with port-side intake airflow (burgundy coloring)	3	9364C [1] 93360YC-FX2 [2]
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

1 For specific fan speeds see the Overview Section of the Hardware Installation Guide.

2 Due to the design of airflow, back-to-front FAN requires FAN speed to be run at full speed all the time. You may also see FAN speeds increase from 40% to 70% post-upgrade

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Product ID	Description	Quantity	Cisco Nexus Switches
NXA-FAN-30CFM-B	Fan module with port-side intake airflow (burgundy coloring)	3	93108TC-EX 93108TC-FX [1] 93180YC-EX 93180YC-FX [1] 9348GC-FXP [1]
NXA-FAN-30CFM-F	Fan module with port-side exhaust airflow (blue coloring)	3	93108TC-EX 93108TC-FX [1] 93180YC-EX 93180YC-FX [1] 9348GC-FXP
NXA-FAN-35CFM-PE	Fan module with port-side exhaust airflow (blue coloring)	4 6	92300YC [1] 9332C [1] 93180YC-FX3S [3] 93180YC-FX3 93108TC-FX3P 9336C-FX2-E 9316D-GX 93600CD-GX
NXA-FAN-35CFM-PI	Fan module with port-side intake airflow (burgundy coloring) Fan module with port-side exhaust airflow (blue coloring)	4 6 6	92300YC [1] 9332C [1] 93180YC-FX3S [2] 93180YC-FX3 93108TC-FX3P 9316D-GX 93600CD-GX 9336C-FX2-E
NXA-FAN-65CFM-PE	Fan module with port-side exhaust airflow (blue coloring)	3	93240YC-FX2 [1] 9336C-FX2 [1]
NXA-FAN-65CFM-PI	Fan module with port-side exhaust airflow (burgundy coloring)	3	93240YC-FX2 9336C-FX2 [1]

Table 13. 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 93180YC-EX

[3] 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.

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Product ID	Description	Quantity	Cisco Nexus Switches
			93180YC-FX
NXA-PAC-500W-PI	500-W AC power supply with port-side intake airflow (burgundy coloring)	2	93108TC-EX 93180YC-EX 93180YC-FX
NXA-PAC-650W-PE	650-W power supply with port-side exhaust (blue coloring)	2	92300YC 93180YC-FX3S 93108TC-EX 93180YC-EX 93180YC-FX3
NXA-PAC-650W-PI	650-W power supply with port-side intake (burgundy coloring)	2	92300YC 93180YC-FX3S 93108TC-EX 93180YC-EX 93180YC-FX3
NXA-PAC-750W-PE	750-W AC power supply with port-side exhaust airflow (blue coloring) 1	2	9336C-FX2 9336C-FX2-E 9332C 93240YC-FX2
NXA-PAC-750W-PI	750-W AC power supply with port-side intake airflow (burgundy coloring) 1	2	9336C-FX2 9336C-FX2-E 9332C 93240YC-FX2
NXA-PAC-1100W-PE2	1100-W AC power supply with port-side exhaust airflow (blue coloring)	2	93240YC-FX2 9332C 9316D-GX 9336C-FX2 9336C-FX2-E 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 9336C-FX2-E 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
NXA-PAC-1200W-PE	1200-W AC power supply with port-side exhaust airflow (blue coloring)	2	93360YC-FX2 9364C
NXA-PAC-1200W-PI	1200-W AC power supply with port-side intake airflow (burgundy coloring)	2	93360YC-FX2 9364C
N9K-PUV-1200W	1200-W Universal AC/DC power supply with bidirectional airflow (white coloring)	2	92300YC 93108TC-EX

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Product ID	Description	Quantity	Cisco Nexus Switches
			93108TC-FX 93360YC-FX2 93180YC-FX3S 93180YC-EX 93180YC-FX 9364C
NXA-PDC-930W-PE	930-W DC power supply with port-side exhaust airflow (blue coloring)	2	93108TC-EX 93180YC-EX 93360YC-FX2 93180YC-FX3S 93180YC-FX 9364C
NXA-PDC-930W-PI	930-W DC power supply with port-side intake airflow (burgundy coloring)	2	93108TC-EX 93180YC-EX 93360YC-FX2 93180YC-FX3S 93180YC-FX 9364C
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 9336C-FX2-E
NXA-PDC-1100W-PI	1100-W DC power supply with port-side intake airflow (burgundy coloring)	2	93240YC-FX2 93600CD-GX 9316D-GX 9332C 9336C-FX2 9336C-FX2-E
UCSC-PSU-930WDC	930-W DC power supply with port-side intake (green coloring)	2	93108TC-EX 93180YC-EX
UCS-PSU-6332-DC	930-W DC power supply with port-side exhaust (gray coloring)	2	93108TC-EX 93180YC-EX
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

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Product ID	Description	Quantity	Cisco Nexus Switches
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

Compatibility Information

Fabric Module and Line Card compatibility details are listed below.

Table 14. Cisco Nexus 9500 Cloud Scale Line Cards

Product ID	N9K-C9504-FM-G	N9K-C9508-FM-G	N9K-C9504-FM-E	N9K-C9508-FM-E	N9K-C9508-FM-E2	N9K-C9516-FM-E2
N9K-X9716D-GX	4	4	No	No	No	No
N9K-X9736C-FX	5	5	5	5	5	5
N9K-X97160YC-EX	4	4	4	4	4	4
N9K-X9788TC-FX	4	4	4	4	4	4
N9K-X9732C-EX	4	4	4	4	4	4
N9K-X9736C-EX	4	4	4	4	4	4
N9K-X9732C-FX	4 5 (n+1 redundancy)	4 5 (n+1 redundancy)	4 5 (n+1 redundancy)	4 5 (n+1 redundancy)	4 5 (n+1 redundancy)	4 5 (n+1 redundancy)

Table 15. Cisco Nexus 9500 R-Series Line Cards

Product ID	N9K-C9504-FM-R	N9K-C9508-FM-R
N9K-X9636C-RX	6	6
N9K-X9636Q-R	4 6 (n+2 redundancy)	4 6 (n+2 redundancy)
N9K-X9636C-R	5 6 (n+1 redundancy)	5 6 (n+1 redundancy)
N9K-X96136YC-R	6	6

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Table 16. Cisco Nexus 9500 R2-Series Line Cards

Product ID	N9K-C9508-FM-R2
N9K-X9624D-R2	6

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 Nexus Dashboard Insights

Cisco NX-OS Release 10.2(4)M supports the Nexus Dashboard Insights on Cisco Nexus 9200, 9300-EX, 9300-FX, 9300-FX2, and 9300-FX3 platform switches and 9500 platform switches with -EX/FX/GX line cards. For more information, see the Cisco Nexus 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 10.2(x). For information about an In Service Software Upgrade (ISSU), see the Cisco NX-OS ISSU Support Matrix.

Related Content

This document describes and provides links to the user documentation available for Cisco Nexus 9000. To find a document online, use one of the links in this section.

Document	Description
Cisco Nexus 9000 Series Switches	Cisco Nexus 9000 Series documentation
Cisco NX-OS Software Strategy and Lifecycle Guide	Cisco NX-OS Software Release and Image-naming Convention
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 NX-OS Software Upgrade and Downgrade Guide, Release 10.2(x)	Cisco Nexus 9000 Series Software Upgrade and Downgrade Guide
Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes, Release 10.2(4)	Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes
Cisco Nexus NX-API Reference	Cisco Nexus 3000 and 9000 Series NX-API REST SDK User Guide and API Reference
ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html	Cisco NX-OS Supported MIBs

© 2022-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Cisco Nexus 9000 Series Switch FEX Support Matrix	Supported FEX modules
Cisco NX-OS Licensing Guide and Cisco Nexus Smart Licensing Using Policy User Guide	Licensing Information

When you downgrade from Cisco NX-OS Release 10.2(4)M to an earlier release, the features that use the ACI+NX-OS Essentials, Advantage, and add-on licenses or the Hardware Streaming Telemetry license continue to work in honor mode in the downgraded version. In addition, the output of the show license usage command continues to include entries for these unsupported licenses.

For more information, see the 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.

© 2022-2023 Cisco Systems, Inc. All rights reserved.