Cisco Nexus 9000 Series NX-OS Release Notes, Release 10.2(1)F

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

This document describes the features, issues, and exceptions of Cisco NX-OS Release 10.2(1)F 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 Open Issues.
May 05, 2023	Added PTP in Unsupported Features on N9K-C92348GC section.
April 09, 2023	Added caveat CSCwe67205 in Open Issues table.
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 5, 2021	Added details about 'Thousand Eyes (TE) Integration' feature in the 'New and Enhanced Software Features' section.
August 24, 2021	Cisco NX-OS Release 10.2(1)F became available.

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

New and Enhanced Software Features

New Features	
Feature	**Description**
Smart Licensing Using Policy	Smart Licensing Using Policy (SLP) is an enhanced version of Smart Licensing, which provides a licensing solution that does not interrupt the operations of your network and to enable a compliance relationship to account for the hardware and software licenses you purchase and use. SLP solution provides a seamless experience with various aspects of licensing such as purchase, use, report license usage to CSSM through Resource Utilization Measurement (RUM) report, and reconciliation. The only enforcement type supported is Unenforced or Not Enforced on Cisco Nexus 9000 and 3000 platform switches. For more information see, *Cisco Nexus NX-OS Smart Licensing Using Policy Guide, Release 10.2(x)*.
EVPN Hybrid IRB Mode	Introduced support for EVPN Hybrid IRB mode. This feature allows NX-OS VTEP devices operating in symmetric IRB mode to seamlessly integrate with asymmetric IRB VTEPs within the same fabric. For more information, see *Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 10.2(x).*
Dense Wavelength-Division Multiplexing (DWDM) configuration	Introduced Dense Wavelength-Division Multiplexing (DWDM) configuration in Cisco Nexus 9000 Series switches. For more information, see *Cisco Nexus 9000 Series NX-OS Interface Configuration Guide, Release 10.2(x)*.
Thousand Eyes (TE) Integration	Introduced Thousand eyes integration support with Cisco Nexus 9000 Series switches. For product overview look at: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/at-a-glance-c45-2431016.html It is a must to install the following general SMU when TE integration is performed: nxos.CSCvz52812-n9k_ALL-1.0.0-10.2.1.lib32_n9000.tar nxos64.CSCvz52812-n9k_ALL-1.0.0-10.2.1.lib32_64_n9000.tar For SMU installation please refer to the following guide: https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/102x/configuration/system-management/cisco-nexus-9000-series-nx-os-system-management-configuration-guide-102x/m-performing-software-maintenance-upgrades-10x.html

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(1)F.

Enhanced Features	
Feature	**Description**
PBR: Default IPv4 Next Hop	Provides a mechanism to support inter-VRF routing. One of the ways to achieve inter-VRF routing is to specify the VRF where the next-hops to be resolved as part of set statement itself. This can be achieved through “set ip/ipv6 vrf next-hop” command. For more information, see *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 10.2(x).*

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Enhanced Features	
Feature	**Description**
Enable/disable 'lacp suspend-individual' without port-channel 'shutdown'	The [no] lacp suspend-individual configuration is allowed on port-channels which are in admin up state. This feature is supported on all Cisco Nexus 9000 platform switches. For more information, see *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 10.2(x).*
2 Stage Commit	Introduced show configuration command that displays the staged configurations. Also provides a 2 stage CLI commit wherein a confirm-commit model configurations get stored in a cli staging area and does not affect the switch running configuration until user issues a 'commit' cli. For more information, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 10.2(x)*.
BFD	Added support for 2048 BFD sessions on Cisco Nexus 9300-EX, 9300-FX, 9300-FX2, 9300-FX3, 9300-GX platform switches. For more information, see *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 10.2(x).*
Cisco-av-pair	Beginning with Cisco NX-OS Release 10.2(1)F, the shell:roles attribute in cisco-av-pair can be mentioned at beginning or at the end. LDAP does not support 'snmpv3' attributes. For more information, see *Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 10.2(x)*.
QoS -PFC Forwarding	Added support for Querying Interface Queuing Counters in Querying Interface and VLAN Counters and Statistics. For more information, see *Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide, Release 10.2(x)*.
Support for IS-IS support in DME for stats and oper data	Added support for Querying IS-IS Statistics in IS-IS Operational Commands. For more information, see *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 10.2(x).*
Querying SVI Counters (SVI counters for unicast, mcast, broadcast packets and bytes counter)	Added support for Querying SVI Counters in Querying Interface and VLAN Counters and Statistics. For more information, see *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 10.2(x).*
Hierarchical PKI with Multiple CAs	Provides a facility to download CA bundles that could include several intermediate and root CAs. For more information, see *Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 10.2(x).*
Model based Operations - gNOI/NETCONF/RESTCONF	This feature adds trusted secure services and crypto ca import CLI for model based operations. For more information, see *Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 10.2(x).*
Exclusive Terminal Lock	Provides CLIs to lock the terminal to allow one user to access the configure terminal commands. It prevents other users from changing the NX-OS running configuration. For more information, see *Cisco Nexus 9000 Series NX-OS Security Configuration*

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Enhanced Features	
Feature	**Description**
	Guide, Release 10.2(x).
LACP PXE	Beginning with Cisco NX-OS 10.2(1)F release, the [no] lacp suspend-individual pxe configuration supports PXE boot and prevents L2 loop due to server misconfiguration. This configuration allows only one port-channel member to be in individual (I) state for both regular port-channels and across vPC peers. This feature is supported on all Cisco Nexus 9000 platform switches. For more information, see *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 10.2(x).*
SFLOW BGP Extension	This feature adds configuring sFlow Extended BGP (Gateway) to the switch. For more information, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 10.2(x)*.
Tap-agg feature and NDB license	Beginning with Cisco NX-OS 10.2(1)F release, tap aggregation is a licensed feature that requires you to configure feature tap-aggregation so that you can configure the tap aggregation-related CLIs. This feature is supported on all Cisco Nexus 9000 series platform switches. For more information, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 10.2(x)*.
L3 Netflow export on L2 physical interface	Beginning with Cisco NX-OS 10.2(1)F release, you can define Layer 3 flow monitors on Layer 2 interfaces to cpature Layer 3 flow information on Layer 2 interfaces. For more information, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 10.2(x)*.
MH-BFD over VXLAN	Added support for BFD multihop over VXLAN on Cisco Nexus 9000 Series switches. For more information, see *Cisco Nexus 9000 NX-OS Interfaces Configuration Guide, Release 10.2(x).*
OSPF SnmpTrap DMEization	This feature provides support for DMEization for OSPFv2. For more information, see *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 10.2(x).*
DME Configuration - Multicast	This feature provides support for Configuring Fabric Multicast (ngmvpn). For more information, see *Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 10.2(x).*
ERSPAN over IPv6	Added support for ERSPAN over IPv6 on Cisco Nexus 9300 – EX, FX, FX2, FX3, GX family switches. For more information, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 10.2(x)*.
NDB: Optimise ERSPAN implementation	Added support for inline ERSPAN header stripping from the incoming ERSPAN packets on NX-OS switch or NDB switch. For more information, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 10.2(x)*.
Disable secure channel identifier (SCI)	Beginning with Cisco Nexus Release 10.2(1)F, Secure Channel Identifier (SCI) can be disabled from MACSec security tag (SecTAG) on Cisco Nexus 9000 Series switches. The new CLI is " no include-sci" . For more information, see *Cisco Nexus 9000 Series NX-OS Security Configuration*

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Enhanced Features	
Feature	**Description**
	Guide, Release 10.2(x).
OSPFv3 IPSec ESP Encryption	Added support for configuring OSPFv3 encyrption at router level, area level, interface level, and virtual links. Also, provides support for configuring ESP IPSec. For more information, see *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 10.2(x).*
OSPFv3 ESP DMEization	Added support for DMEization of OSPFv3 at router level, areal level, interface level, virtual links, and ESP. For more information, see *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 10.2(x).*
Enhanced ISSU support on FC NPV and FCoE NPV mode	Added enhanced ISSU support on FC NPV and FCoE NPV mode. For more information, see *Cisco Nexus 9000 Series NX-OS FC-NPV and FCoE-NPV Configuration Guide, Release 10.2(x).*
VXLAN EVPN Downstream VNI and VXLAN IPv6 Underlay support for Nexus 9300v and Nexus 9500v platforms	Added VXLAN EVPN Downstream VNI and VXLAN IPv6 Underlay support for Nexus 9300v and Nexus 9500v platforms. Removed Nexus 9300v and 9500v platforms support for MPLS Segment Routing (SRv4). For more information, see *Cisco Nexus 9000v (9300v/9500v) Guide, Release 10.2(x).*
Disable USB ports	Introduced a new CLI, " port usb disable" to disable USB ports on Cisco NX-OS switches. For more information, see *Cisco Nexus 9000 Series NX-OS Interface Configuration Guide, Release 10.2(x)*.
ESR: ITD NAT Statistics	Beginning with Cisco NX-OS Release 10.2(1)F, ITD supports NAT statistics. For Cisco Nexus N9K X9636C-RX and N9K X96160YC-R line cards, ITD statistics is not supported. For more information, see *Cisco Nexus 9000 Series NX-OS Intelligent Traffic Director Configuration Guide, Release 10.2(x)*.
PMN PIM passive ENAT	PMN supports Multicast-to-Unicast NAT in both PIM active and PIM passive modes. *For more information, see Cisco Nexus 9000 Series NX-OS IP Fabric for Media Solution Guide, Release 10.1(x).*
PMN MU NAT	The Multicast Service Reflection feature supports Multicast-to-Unicast translation only in egress mode. *For more information, see Cisco Nexus 9000 Series NX-OS IP Fabric for Media Solution Guide, Release 10.1(x).*
ITD and ePBR - OTM and SLA APIs	Beginning with Cisco NX-OS Release 10.2(1)F, ITD can use APIs to manage tracks created to monitor the interface and nodes status. ITD can use SLA APIs to create and delete sla_id for nodes. For more information, see *Cisco Nexus 9000 Series NX-OS Intelligent Traffic Director Configuration Guide, Release 10.2(x).*
gNMI Enhancements	Added support for the subscribe option mode for gNMI payload. For more information, see *Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 10.2(x).*

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Enhanced Features	
Feature	**Description**
Single 64-bit Image Support and 64-bit and 32-bit to 64-bit ISSU	Added 64-bit image support for Cisco Nexus 9000 series switches ending with - EX, -FX, -FX2, -FX3, -GX modules. 32-bit image support are provided for Cisco Nexus 9000 series with – R line cards. For more information, see the Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 10.2(x).
DHCPv6 SMART Relay	Introduced DHCPv6 Smart Relay on Cisco Nexus 9000 Series switches. For more information, see *Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 10.2(x)*.
Secure Channel Identifier (SCI) Optionality	Added MACsec support on Cisco Nexus N9K-X9716D-GX. For more information, see *Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 10.2(x).*
Dynamic Access Control Lists (DACLs)	From Cisco NX-OS Release 10.2(1)F, you can download per-user dynamic access control lists (DACLs) from the Cisco ISE Server as policy enforcement after authentication using IEEE 802.1X. For more information, see *Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 10.2(x).*
No-Reload option for SMU installation	Provides No-Reload option payloads for SMU installation. For more information, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 10.2(x)*.
show itd brief DMEization	Added support for Querying ITD Runtime Information. For more information, see *Cisco Nexus 9000 Series NX-OS ITD Configuration Guide, Release 10.2(x).*
show epbr policy DMEization	Added support for Querying ePBR Runtime Information. For more information, see *Cisco Nexus 9000 Series NX-OS ePBR Configuration Guide, Release 10.2(x).*
Platform Telemetry of PSU, Fans, and Sensors.	This feature provides support for platform telemetry of PSU, fans, and sensors. For more information, see *Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 10.2(x).*
ITD and ePBR service options	This feature provides ITD and ePBR service options for IPv4 and IPv6 policies. For more information, see *Cisco Nexus 9000 Series NX-OS ITD Configuration Guide, Release 10.2(x).*
FT/FTE for SR Encapsulation	Added support for MPLS SR encapsulation. For more information, see *Cisco Nexus 9000 Series NX-OS Label Switching Configuration Guide, Release 10.2(x).*
Netflow Extension to support FT	This feature adds limitations for FX packet events and supports FT/FTE V9 feature. For more information, see *Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 10.2(x).*
EVPN Distributed NAT	This feature enables NAT on the leaf and spine in the VXLAN topology.

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Enhanced Features	
Feature	**Description**
	For more information, see *Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 10.2(x).*
Inter VRF PBR	Added support for IPv4 or IPv6 next-hop address for policy-based routing, to load balance traffic across next-hop addresses, to enable next-hop ordering, and to drop packets instead of using default routing when the configured next hop becomes unreachable. For more information, see *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 10.2(x).*
Honour specified port number	Added support to specify port numbers for SCP or SFTP and other protocols such as HTTPS, TFTP, and FTP. Enables you to copy files from/to an Nexus switch where the existing copy protocols are running on custom ports. For more information, see *Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 10.2(x).*
Multicast Flow Path Visibility for TRM Flows	Added Multicast Flow Path Visibility support for TRM L3 mode and underlay multicast. The Multicast Flow Path Visibility feature enables you to export all multicast states in a Cisco Nexus 9000 Series switch. For more information, see *Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 10.2(x).*
POAP User-agent	Provides provisioning details by verifying the HTTP GET function and validates the data from non-Cisco devices on to the Cisco's HTTP server so that the correct provisioning script is identified and used in provisioning. For more information, see *Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide, Release 10.2(x).*
Multicast NAT: Multicast to Unicast	Added support for Multicast-to-Unicast NAT translation in egress mode. For more information, see *Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 10.2(x).*
Tenant Routed Multicast (TRM) with IPv6 Overlay	Added support for TRM IPv6 in the overlay. For more information, see *Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 10.2(x).*
TRM with vPC BGW and with Anycast BGW	Added TRM with vPC BGW and with Anycast BGW support on Cisco Nexus 9300-GX family switches. For more information, see *Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 10.2(x).*
ESR: Support Flexible End Point Deployment (A-A) and multisite	With this feature the interface on which the ePBR policy is applied can be on a different VRF than the VRF of each service in each of the service chains. Also, the ePBR supports port-channel sub-interfaces as the end-point interfaces. For more information, see *Cisco Nexus 9000 Series NX-OS ePBR Configuration Guide, Release 10.2(x).*
Multicast NLB and GRE Consistency Check	Added support for Multicast NLB and GRE Consistency Checker. For more information, see *Cisco Nexus 9000 Series NX-OS Troubleshooting Guide, Release 10.2(x).*

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Enhanced Features	
Feature	**Description**
Global Boundary Multicast Configuration	Added support for Global Boundary Multicast configuration. For more information, see *Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 10.2(x).*
MACsec and MKA support	Added support for MACsec and MKA on N9K-X9716D-GX module. Functionalities such as fallback, EAPOL, Macsec over breakout, and. global MACsec shutdown are also supported. For more information, see *Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 10.2(x).*
ESR: PBR on Port-channel subinterface	Added ITD support for policy-based routing with Layer 3 portchannel ingress subinterfaces. For more information, see *Cisco Nexus 9000 Series NX-OS ITD Configuration Guide, Release 10.2(x).*
OTM Commands DMEization	The following OTM commands are DMEized in Cisco NX-OS Release 10.2(1)F: 1) track <*object-id*> list threshold weight threshold weight {up < *weight-val* > [down <*weight-val*>]} object <*object-id*> weight <*weight-val*> [no] threshold weight {up <*weight-val* > [down <*weight-val*>]} 2) track <*object-id*> list threshold percentage threshold percentage {up <*percentage -val* > [down <*percentage -val*>]} [no] threshold percentage {up <*percentage -val*> [down <*percentage -val*>]} 3) track <*object-id*> {list {boolean <*bool-val*>}} 4) object <*object-id*> [not] no object <*object-id*> [not] 5) vrf member {<*vrf_name*> | <*vrf-known-name*>} no vrf member [<*vrf_name*> | <*vrf-known-name*>]

New Hardware Features

There are no new hardware features introduced in Cisco NX-OS Release 10.2(1)F.

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

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

- 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

Cisco Nexus 9000 Series switches require 32-bit or 64-bit NX-OS image depending on the Cisco Nexus 9000 platforms.

Open Issues

Bug ID	Description
CSCvz39258	Headline: Incorrect error message while appling IPv6 RA Guard Policy Symptoms: While configuring IPV4 RA Guard Policy, if TCAM is not carved for IPV4 PACL [ifacl] region, general error message printed " Could not attach policy:" instead of more specific error message " Could not attach policy: IFACL TCAM not available,configure before enabling feature" Workarounds: Verify if TCAM memory for ifacl region is carved. If not then carve TCAM for this region using this guide to carve TCAM. https://www.cisco.com/c/en/us/support/docs/switches/nexus-9000-series-switches/119032-nexus9k-tcam-00.html
CSCvx86007	Headline: Intermittent Link Flaps observed with QSFP-100G-PSM4 Symptoms: Repeating flaps are seen on the links between Jericho linecard and Tahoe linecard, using CISCO-LUXTERA QSFP-100G-PSM4 rev B or C. The links recovers from the flap shortly and is stable for some time afterwards. Workarounds: NA
CSCvy62175	Headline: N9k Lacrosse Platforms - 100Gig link not coming up due to FEC Symptoms: An operational 100Gig link on the switch goes down without any trigger after a flap and doesn't come up. The link could be using AOC cable or SR4 Optics. Replacing the Optics or cable doesn't help.When FEC is disabled on both ends using " no fec off" , the link comes up. Workarounds: Multiple workarounds:- Move to connection to an unused port on the switch- Disable FEC on both ends if acceptable- A reload of the switch can resolve the issue.
CSCvz06811	Headline: Nexus Data Broker switch floods IGMPv3 membership queries out of all input ports Symptoms: IGMPv3 membership queries are flooded out of input ports Workarounds: none
CSCvz35213	Headline: BFD per-link causes flaps with multiple discriminators Symptoms: BFD per-link may be unstable when one of the port-channel members is stuck in " XCVR not inserted" . Workarounds: Attempt to bring the stuck interface up.

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCvz38543	Headline: N9k Type-7 to Type-5 LSA translation is not happening when Link-ID is in host IP range Symptoms: Issue is seen when type 7 LSA will be received with Link ID as host IP range. Workarounds: None
CSCvz38944	Headline: N9k DHCPv6 Relay breaks after IPv6 snooping is removed Symptoms: Original Symptom from DHCPv6 Client perspective would be not receiving an IPv6 Address from the DHCPv6 server. CPU will only show the DHCPv6 solicit/Re-bind packets; Relay-FWD would NOT be originated by the n9k Workarounds: Reload fixes the issue(shut/no-shut of the SVIs Dont seem to fix the problem)
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.
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
CSCuv49114	Headline: ipAddressPrefix MIB returning wrong object Symptoms: ipAddressPrefix MIB when being polled will return " ipAddressPrefixEntry" instead of " ipAddressPrefixOrigin" Workarounds: NA
CSCvu64601	Headline: High memory usage after streaming high volume of telemetry data for more than 6 days Symptoms: A Nexus switch streaming high volume telemetry data may experience high memory usage which may eventually cause data collections to be dropped. Workarounds: To prevent this issue from happening, configure higher sample-interval

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
	time value for subscriptions.If the issue is seen already on a Nexus switch, the problem can be resolved by disabling the telemetry feature via " no feature telemetry" and apply the configurations back.
CSCvy45581	Headline: only one path returns event notifications for on-change sub with 2 xpaths that have same parent Symptoms: There are couple issues with on-change notifications when subscribing to 2 xpaths in the same request (that belong to same parent).- Event notifications are not received for the second xpath subscribed.- For every single event, two notifications are received for the first xpath subscribed. I sent an on-change subscription with xpaths as: ?/System/intf-items/phys-items/PhysIf-list\[id=eth1\/4\]/phys-tems/operSt/System/intf-items/phys-items/PhysIf-list\[id=eth1\/4\]/phys-tems/operDescr Initial snapshot sent the notifications for both the operSt and operDescr paths followed by a sync_response. When an event is triggered for both the above paths, notification is received only for the operSt (the first xpath in the request) and not for the operDescr. Also, 2 notifications are received for every single event on operSt. Please refer to 'gnmi-console-logs' for more details. Workarounds: subscribe from different channel
CSCvy53526	Headline: Nexus 9000 : IP SLA log feature is not working Symptoms: Nexus 9000 : IP SLA log feature is not working2021 Jun 1 15:24:43 N95-1 %ETHPORT-5-IF_UP: Interface Ethernet2/47 is up in Layer32021 Jun 1 15:24:55 N95-1 %SLA_SENDER-3-SNMP: rttMonCtrlAdminTag = (null)2021 Jun 1 15:26:05 N95-1 %SLA_SENDER-3-SNMP: rttMonCtrlAdminTag = (null)On 7.0(3)I7.X,2021 Jun 2 06:09:18 N9K-1 %SLA_SENDER-3-SNMP: rttMonCtrlAdminTag = (null)2021 Jun 2 06:09:18 N9K-1 %SLA_SENDER-3-IPSLATHRESHOLD: IP SLAs(10): Threshold Occurred for timeout>>>>Down2021 Jun 2 06:10:03 N9K-1 %SLA_SENDER-3-SNMP: rttMonCtrlAdminTag = (null)2021 Jun 2 06:10:03 N9K-1 %SLA_SENDER-3-IPSLATHRESHOLD: IP SLAs(10): Threshold Cleared for timeout >>>>UP Workarounds: None
CSCvy63631	Headline: N9k: Can not delete ipv6 static bfd routes from running-config Symptoms: Can not remove ipv6 static routes from running-configIt is very straightforward: Switch(config)# show run | in " ipv6 route static bfd Vlan12 2001:xxxx:xx:xxxx:xx:xxx:0:xx" ipv6 route static bfd Vlan12 2001:xxxx:xx:xxxx:xx:xxx:0:xxSwitch(config)# Switch(config)# Switch(config)# no ipv6 route static bfd Vlan12 2001:xxxx:xx:xxxx:xx:xxx:0:xx Switch(config)# show run | in " ipv6 route static bfd Vlan12 2001:xxxx:xx:xxxx:xx:xxx:0:xx ipv6 route static bfd Vlan12 2001:xxxx:xx:xxxx:xx:xxx:0:xx <<<<!!!!!!!!! Workarounds: Remove config from the box and edit it. And reboot the box with the new config.
CSCvy75027	Headline: vPC VTEP use fabric anycast mac to promote ipv6 neighbor with VRRPv3 L3 External Connectivity Symptoms: Fabric Anycast Gateway MAC is used as ipv6 ND Link-layer address with src mac of the VRRPV3 MAC.For exampleEthernet II, Src: VRRP MAC , Dst: HOST MAC..... ICMPv6 Option (Target link-layer address) Type: Target link-layer address (2) Length: Link-layer address: Fabric Anycast Gateway MACIf L2 switch is connect behind VXLAN EVPN Layer 3 External Connectivity Link, you will see packet is flooded to both Master/Standby Nexus and cause duplicate due to VRRP MAC was learnt but the packet use Fabric Mac as dst MAC. Workarounds: flap the VXLAN EVPN Layer 3 External Connectivity Link will make the traffic works for a while. Clear the IPV6 ND will reproduce the issue again

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCvy90363	Headline: 9500-R :: Feature ptp causes the spine switch to intercept unicast ARP replies in VxLAN fabric Symptoms: The L2 adjacent host are not able to resolve each others ARP accross VxLan fabric.The broadcasted ARP reply is flooded correctly and reaches all hosts, however the unicast ARP reply is lost inside of the fabric.In fact the ARP replies are redirected to SPINE CPU instead of being forwarded.Other unicast communication works fine (eg. when we configure static ARPs) Workarounds: So far three possible workarounds were identified0. Disable 'featue nv overlay' on Spine. This will avoid this problem and also will ensure better hashing of packets over ECMP links.1. Enable " arp suppression" or.2. Remove " feature ptp" from the SPINES. After doing so " reload" or " reload ascii" is required to restore connectivity
CSCvo17797	Headline: Fan interrupts led to platform crash Symptoms: platform crash and reload Workarounds: none
CSCvo80791	Headline: N9000 fails to process correctly fragmented traffic Symptoms: Pings may fail when sent from bash shell if exceeding MTU of interface. Workarounds: Send pings with size that does not exceed the MTU of the egress interface.
CSCvu67445	Headline: N9k/Cloud Scale - Flood list missing po member port - broadcast traffic loss Symptoms: Broadcast may not Tx an Ethernet port for VLAN's allowed for one of the port-channel member links.ARP request or any other form of ethernet broadcast may not reach destination. This would lead to no connectivity for affected hosts.Consistency check will report failure for VLAN membership:Example:show consistency-checker membership vlan 442hecking hardware for Module 1 Unit 0No FEX interfaces to validateConsistency Check: FAILED >>> Vlan:442, Hardware state consistent for: Ethernet1/41 Ethernet1/49 Ethernet1/50 Ethernet1/53 Vlan:442, Hardware state inconsistent for: Ethernet1/54</snip> Workarounds: Enter shut/no shut (flap) the affected interface.Do not use the " port-channel port load-defer" command.
CSCvv09729	Headline: Cisco Nexus 92348 back pressure results in PSU fan spinning wrong direction Symptoms: The power supply exhaust fan may spin in the wrong direction on the Cisco Nexus 92348. Workarounds: None
CSCvv93710	Headline: TRM-MS Sanity Failure: Remove/Add EVPN Multisite Global Config on BGW Symptoms: BGP may skip a routing update when the bestpath changes but all attributes of the new bestpath are the same as that of the old one. This will result in the old bestpath's peer not receiving an update to the new bestpath leading to potential black-holing of traffic. A secondary consequence is that the new bestpath's peer will *NOT* receive a withdrawal of the old bestpath leaving stale information in that peer Workarounds: Issuing a " clear bgp <afi> <safi> soft out" to affected peers will address the issue
CSCvx23114	Headline: Breakout interface flaps on certain ports associated with Cisco Nexus 9504/9508/9516 switch

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
	Symptoms: Breakout interfaces may flap unexpectedly on the certain port for no apparent reason. Workarounds: If breakout configuration is required - consider using other interfaces on the switch/linecard.
CSCvx36083	Headline: Improve IPv4 pim address list hello option length validation Symptoms: If pim hello address list option is received with invalid length, including length 0, the hello is rejected. It is more appropriate and safer to just ignore the option. Workarounds: At least one vendor is wrongfully sending the option with length 0. Configuring secondary IPv4 addresses may be a workaround, depending on the vendor's implementation.
CSCvx59546	Headline: SNMP not reporting accurate stats for Macsec pktrate/octrate Objects Symptoms: SNMP is not reporting accurate stats for the following:CISCO-SECY-EXT-MIBcseSecyIfRxUncontrolledPktRate,cseSecyIfRxControlledPktRate,cseSecyIfTxUncontrolledPktRate,cseSecyIfTxControlledPktRatecseSecyIfRxControlledOctetRatecseSecyIfTxControlledOctetRatecseSecyIfRxUnControlledOctetRatecseSecyIfTxUnControlledOctetRate Workarounds: Use these insteadCISCO-SECY-EXT-MIBcseSecyIfRxControlledOctetcseSecyIfTxControlledOctetcseSecyIfRxUnControlledOctetcseSecyIfTxUnControlledOctet
CSCvx72007	Headline: 9.3.7: URPF in Strict Mode dropping valid packets on ingress interface Symptoms: 9.3(7) switch serving as the gateway to a host with unicast RPF configured on the gateway interface.Host still has Arp/IPv6 neighbor adjacency in it's table.Switches neighbor/arp entries have aged out for given host.Switch doesn't attempt to resolve for the neighbor when a packet is received for an unresolved neighbor.Despite a longest prefix match being present in the RIB/FIB, packet is still dropped as (/128 || /32) Workarounds: None
CSCvx89804	Headline: N9K using QSFP-40G-LR4-S and WSP-Q40GLR4L may cause High TX Alarm/Port Flapping Symptoms: After upgrade to 9.3(5), 9.3(6) or 9.3(7) and using the QSFPs- QSFP-40G-LR4[-S] or WSP-Q40GLR4L may see High Tx Alarm and/or link flap. Workarounds: None.
CSCvx89951	Headline: vfprintf snmp related crash on nexus9k Symptoms: +Service "snmpd" hasn't caught signal 11 seen+Core files generated for snmpd Workarounds: tbd
CSCvy04038	Headline: N9k Cloud Scale ASIC RWX drops not reported in ELAM Brief Report Symptoms: ELAM Brief report not indicating RWX drops Workarounds: Check ELAM report detail under following drop vector:*.STA_rwb_drop_vector_capture_access

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCvy07815	Headline: issues seen when gnmi/grpc connection with ipv6 default address connectivity Symptoms: Inband GRPC connections, from front panel ports, to the loopback interface using IPv6 for transport fail. The loopback is not answering, i.e. connection refused, inbound IPv6 connections on the configured GRPC port.switch# show run grpc<snip>feature grpcgrpc use-vrf defaultgrpc certificate mytrustpointgrpc port 15000switch# show run interface lo0<snip>interface loopback0 ip address 1.1.1.1/32 ipv6 address 2001:1:1:1::1/32From management station:[user@localhost ~]$ telnet 2001:1:1:1::1 15000Trying 2001:1:1:1::1...telnet: connect to address 2001:1:1:1::1: Connection refused[user@localhost ~]$ Workarounds: Before enabling GRPC for IPv6 transport, make sure that the Management interface is up/up and has IPv6 configured on it.switch# show run grpc ^% Invalid command at '^' marker.switch# switch# show run int mgmt 0<snip>interface mgmt0 vrf member management ip address 10.31.121.31/26 ipv6 address 2001::1/64switch(config)# feature grpcswitch(config)# grpc use-vrf defaultswitch(config)# grpc certificate mytrustpointswitch(config)# grpc port 15000From the management station:[user@localhost ~]$ telnet 2001:1:1:1::1 15000Trying 2001:1:1:1::1...Connected to 2001:1:1:1::1.Escape character is '^]'.^]telnet> qConnection closed.[user@localhost ~]$
CSCvy11663	Headline: N9K EOR TxBitRate and/or RxBitRate on LC from FM are incorrect Symptoms: The TxBitRate and/or RxBitRate from `show system internal interface counters peak` command will show a higher value (2-3x) greater on an LC than the traffic that it is actually receiving from the FM. When looking at the FM perspective using the same CLI command, the TxBitRate and RxBitRate for the corresponding internal interfaces are all correct. Workarounds: Issue is cosmetic.If you want stats for the module do not run with " peak" command.Use " show system internal interface counters module X"
CSCvy11949	Headline: Nexus switch may crash if CLI " show vdc" is entered after a downgrade of the NX-OS version Symptoms: A Nexus switch may experience an unexpected reload of the VDC service if the command " show vdc" is executed.%SYSMGR-2-SERVICE_CRASHED: Service " vdc_mgr" (PID 31023) hasn't caught signal 11 (core will be saved).%SYSMGR-2-HAP_FAILURE_SUP_RESET: Service " vdc_mgr" in vdc 1 has had a hap failure Workarounds: Once we observe this issue need to do " write erase and reload" as workaround.
CSCvy13764	Headline: bgp: RFC7854 BMP Peer RD not set Symptoms: Received BMP messages do not contain " Peer RD" for VRF monitored peers. Workarounds: No workaround.
CSCvy15010	Headline: Cannot generate RSA keypair for AAA user accounts Symptoms: Getting following error message when trying to generate RSA keypair from NXOS CLI for a AAA user account:Nexus9K(config)# username nxosadmin keypair generate rsa 2048 forceNexus9K(config)# oes not exist.Could not generate ssh key Workarounds: N/A
CSCvy16482	Headline: Packet drops when port-security is enabled on vPC with fabric peering Symptoms: Packets are lost/drops for a host that is connected behind a vPC leg of a

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
	vPC pair that is configured with fabric peering. The switch does not log port-security violations or error logs related to the drop. Drops can be confirmed through ELAM capture with drop reason SECURE_MAC_MOVE. Example:module-1(TAH-elam-insel7)# reportHEAVENLY ELAM REPORT SUMMARYslot - 1, asic - 0, slice - 0==========Incoming Interface: Eth1/60Src Idx : 0xed, Src BD : 666Outgoing Interface Info: met_ptr 0Packet Type: ARPDst MAC address: FF:FF:FF:FF:FF:FFSrc MAC address: CA:FE:CA:FE:CA:FE <<< This host is behind the vPC leg with port-securityTarget Hardware address: 00:00:00:00:00:00Sender Hardware address: CA:FE:CA:FE:CA:FETarget Protocol address: 192.0.2.15Sender Protocol address: 192.0.2..1ARP opcode: 1Drop Info:----------LUA:LUB:LUC:LUD: SECURE_MAC_MOVEFinal Drops: SECURE_MAC_MOVEvntag:vntag_valid : 0vntag_vir : 0vntag_svif : 0ELAM not triggered yet on slot - 1, asic - 0, slice - 1 Workarounds: Disable port-security on the vPC interface configuration of both vPC peers.
CSCvy23574	Headline: N9K-C9348 port bringup timing delay Symptoms: Various different server/host PID's reporting problems when reloads are needed for maintenance, patch upgrades, other. This delay may prevent the host from bringing up network applications needed for boot. Workarounds: Hard coding only the speed at either 1 Gi or 100 M prevents the issue.
CSCvy24198	Headline: L2FM process crash after l2fm_mcec_get_mac_handler Symptoms: The L2FM process crashes after the vPC comes online:%$ VDC-1 %$ %ASCII-CFG-2-CONF_CONTROL: System ready%$ VDC-1 %$ %VPC-2-PEER_KEEP_ALIVE_RECV_FAIL: In domain #, VPC peer keep-alive receive has failed%$ VDC-1 %$ %VPC-2-PEER_KEEP_ALIVE_RECV_FAIL: In domain #, VPC peer keep-alive receive has failed (message repeated 1 time)%$ VDC-1 %$ %VPC-2-PEER_KEEP_ALIVE_RECV_FAIL: In domain #, VPC peer keep-alive receive has failed (message repeated 1 time)...%$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service "l2fm" (PID 7824) hasn't caught signal 11 (core will be saved). Workarounds: Disconnect the vPC peer link and upgrade both peers separately. After they are both upgraded and the vPC is connected back, they should remain stable.
CSCvy29240	Headline: All ports stop passing unicast traffic Symptoms: No unicast traffic is passed through the switch, starting from one port, issue then replicates to other ports as well. Workarounds: ++ Reload.++ If detected in early stages, shut/no shut of the problematic port would work.
CSCvy31399	Headline: TAH "switchport mac-learn disable" does not fully work. CLI needs to be removed Symptoms: %L2FM-2-L2FM_MAC_FLAP_RE_ENABLE_LEARN: will be present in the logs even when mac-learn disable is configured under the interface in which the MACs are being moved on Workarounds: Change logging level to level 1 "logging level l2fm 1"
CSCvy32984	Headline: ND ISSU | Q-in-VNI | Double tag due to system dot1q tunnel-transit command Symptoms: dot1q tag is preserved after vxlan encapsulation for traffic received on a regular trunk port. Workarounds: If triggered, a reload of the affected device will stop this behavior. To

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
	prevent this behavior, perform a disruptive upgrade.
CSCvy33411	Headline: gnmi authentication with tacacs server fails if user is allowed only from a certain host Symptoms: gnmi requests fail with 'Authentication error' when a specific policy on ISE is configured to allow the tacacs user authenticate only from a certain host. Workarounds:
CSCvy33550	Headline: Unsupported CLI `ip dhcp relay subnet-broadcast` needs to be completely removed from N9K (NOP) Symptoms: Unsupported cli is still present (though hidden) on n9k -> ip dhcp relay subnet-broadcast Workarounds: None. Remove unsupported CLI 'ip dhcp relay subnet-broadcast' from the configuration.CSCvc32697 Was previously filed for this issue but the CLI was not completely removed from code, only hidden. The CLI needs to be made a NO-OP
CSCvy33584	Headline: N9K: nginx session flood if switch removed from DCNM with tracker enabled Symptoms: As soon as switch is removed from DCNM, it becomes slow to respond and the sysinfo service crashes. Contrary to the log message, a core file may not be saved.%SYSMGR-2-SERVICE_CRASHED: Service " sysinfo" (PID 29474) hasn't caught signal 6 (core will be saved).Switch# run bashbash-4.3$ ps aux | grep nginx(Thousands of nginx_f worker sessions are printed in the format below)svc-nxa+ 5892 0.0 0.0 296772 5692 pts/14 Ss+ 15:21 0:00 nginx_f worker bash-4.3$ copy /volatile/nginx.log /bootflash/bash-4.3$ exitSwitch# show file bootflash:/nginx.log(Thousands of these entries are generated)_pterm_create_vsh_session:291 pid:5879 User sa-dcnm does not exists!pterm_get_vsh:810 pid:5879 couldn't create a vsh session Workarounds: Disable the DCNM tracker feature in DCNM, before deprovisioning the switch.If the switch is already in this state, destroy the guestshell and reload the switch:Switch# guestshell destroySwitch# reload
CSCvy34356	Headline: Nexus 9000 series running NX-OS 10.1(2) does not upgrade Golden EPLD region to new version. Symptoms: On NxOS 10.1(X) upgrade of the EPLD Golden regions is sometimes unsuccessful. The device does not display any error when issuing the install command, instead it keeps booting from the Golden region with old EPLD version. Workarounds: Upgrade EPLD on an earlier release of EPLD image that has same version as NX-OS 10.1(2) and then perform upgrade to NX-OS 10.1(2). Refer to the Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes for the specific releases.
CSCvy36107	Headline: Improve pause timeout messages Symptoms: Improve the current Nexus 9000 pause timeout messages so they are understandable and can be associated with the pause timeout feature.These are the current messages:<pre> 2021 Mar 26 11:58:30 n9k %TAHUSD-SLOT1-2-TAHUSD_SYSLOG_CRIT: Ethernet1/29, slowdrain xoff hit ON (total xoff-hits:9) 2021 Mar 26 11:58:40 n9k %TAHUSD-SLOT1-2-TAHUSD_SYSLOG_CRIT: Ethernet1/29, slowdrain xoff hit OFF (last xoff-time:10 seconds) 2021 Mar 29 10:56:09 n9k %TAHUSD-SLOT1-2-TAHUSD_SYSLOG_CRIT: Ethernet1/29, slowdrain xoff hit ON (total xoff-hits:10) 2021 Mar 29 10:56:19 n9k %TAHUSD-SLOT1-2-TAHUSD_SYSLOG_CRIT: Ethernet1/29, slowdrain xoff hit OFF (last xoff-time:10 seconds)</pre> Workarounds: None.

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCvy39404	Headline: Packet loss after reload of VXLAN BGP EVPN vPC VTEP with eBGP underlay Symptoms: Packet loss may be observed between hosts connected via vPC to vPC VTEPs in a VXLAN BGP EVPN fabric that uses eBGP as an underlay as one of the vPC VTEPs is coming online after a reload or power outage. Specifically, the packet loss starts after the vPC Delay Restore timer of the reloaded vPC peer expires. During this time, the NVE source loopback (that is, the loopback interface sourced with the "source-interface {interface}" command) is held in an Administratively Down state. The total duration of the packet loss will vary, but usually ranges from 60 seconds to several minutes depending on the precise vPC Delay Restore and NVE source loopback hold-down timers. Workarounds: You can proactively avoid this issue by ensuring the NVE source loopback hold-down timer is set to a value less than the vPC Delay Restore timer.
CSCvy39858	Headline: N9K-C9332C: Interfaces with 1Gbps transceivers do not go down when link signal is lost Symptoms: If a Nexus 9332C switch with GLC-SX-MMD transceivers inserted in Ethernet1/33 or Ethernet1/34 has either interface come up/up when link signal is received, the interfaces will not transition to a down state when link signal is lost on either interface. Workarounds: There is no known proactive workaround for this issue. To reactively work around this issue, you can administratively shut down the interface(s) on the affected device.
CSCvy40886	Headline: N9K IPv6 NTP ACL missing from the configuration after reload ascii Symptoms: An IPv6 NTP ACL is missing from the device configuraton after reload ascii. Workarounds: N/A.
CSCvy45479	Headline: Batch ACL config fail with duplicate ACE Symptoms: ACL configuration is not as expected Workarounds: 1. Remove duplicate ACE entries within each ACL in the custom startup configuration fileand/or2. Apply unique sequence number to each ACE within every ACL in custom startup configuration.
CSCvy50202	Headline: N9K-C9364C - 9.3(7) + lxc boot mode - Fan speed stuck at 100% Symptoms: + Fan speeds stuck at 100% Workarounds: non lxc boot mode does not exhibit this behavior.
CSCvy51761	Headline: Errdisable recovery - reinit-no-flap being enabled after upgrade from 9.2(x) --- > 9.3(x) Symptoms: - After upgrade from 9.2(4) version to 9.3(7) reinit-no-flap is enabled in case of errdisable recovery.- Trigger for reinit-no-flap being enabled in 9.3(7) version looks to be "errdisable recovery cause dcbx-no-ack" being enabled in 9.2(4).- "errdisable recovery cause dcbx-no-ack" cannot be removed after the upgrade to 9.3(7)- even if "reinit-no-flap" is shown in 9.3(7) as enabled the feature looks to be not working#show errdisable recovery reinit-no-flap enabled <------- dcbx-error enabled <-------vlan-membership-erro enabled pause-rate-limit disabled inline-power enabled sw-failure disabled #show run | inc errerrdisable recovery cause dcbx-no-ack#no errdisable recovery cause dcbx-no-ackCreate-only and naming props cannot be modified after creation, class=ethpmEvent, prop=event

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
	Workarounds: - Downgrade back to 9.2(x) and remove " errdisable recovery cause dcbx-no-ack" from running configuration, then reload.- Simple reload in 9.3(x) release looks to be not solving problem.
CSCvy55293	Headline: IPinIP packets dropped on the peer-link Symptoms: IP-in-IP tunnelled traffic may fail when forwarded from one leaf to another over vpc peer-link in a vxlan environment.There is no impact for GRE traffic Workarounds: Adjust routing preferences to forward such traffic locally on the switch instead of crossing peer-link.
CSCvy57340	Headline: FIPs mode enabled+ nxapi disabled: switch reload allows access to nginx/nxapi sandbox port 80,443 Symptoms: 1. Switch reports ports 80 and 443 are open despite feature nxapi disabledTDC1P1-Rack01-BMC-1# show sockets connection tcp | in '*(80)|*(443)' n 1[host]: tcp LISTEN 0 *(80) <<< port should be closed Wildcard 0 *(*)--[host]: tcp6 LISTEN 0 *(80) <<< port should be closed Wildcard 0 *(*)--[host]: tcp LISTEN 0 *(443) <<< port should be closed Wildcard 0 *(*)--[host]: tcp6 LISTEN 0 *(443) <<< port should be closed Wildcard 0 *(*)2. user admin with valid password can open browser to NXAPI Sandbox despite feature disabled3. with feature bash enabled, find that nginx process was restarted, despite feature nxapi disabledTDC1P1-Rack01-BMC-1# run bash sudo pgrep -l nginx12616 nginx14059 nginx_1_fe14138 nginx_1_fe Workarounds: In this scenario an ACL can be used on mgmt0 interface to prevent access to the 80 & 443 service. Example:!ip access-list DENY-NXAPI 10 deny tcp any any eq 443 20 deny tcp any any eq www 30 permit ip any any !interface mgmt0 ip access-group DENY-NXAPI in!Note: There are normally restrictions when using an ACL with NX-API when it is configured to use a VRF. See https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/101x/programmability/cisco-nexus-9000-series-nx-os-programmability-guide-release-101x/m-n9k-nx-api-cli-101x.html section " Restricting Access to NX-API" for more details. For the purposes of this defect and workaround those limitations are not applicable.
CSCvy62164	Headline: Crash in N9K Fatal Module Error when downgrade - service port_client hap reset Symptoms: During downgrade from 9.3.7 to 9.3.6, vPC peer switch reloads due to " port_client" service crash:Service: port_clientDescription: Port Client DaemonExecutable: /lc/isan/bin/port_client Workarounds: No workaround. The switch is reloaded when the issue is hit.
CSCvy67232	Headline: %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service " fcoelc" (PID 25997) hasn't caught signal 11 Symptoms: The service " fcoelc" crashes on a Cisco N9k that has a FCoE link. A core file will be generated due to the event.From NVRAM logs:%SYSMGR-SLOT1-2-SERVICE_CRASHED: Service " fcoelc" (PID 25997) hasn't caught signal 11 core will be savedConfiguration changes were applied on QoS prior to the crash. Also can observe errors related to QoS and the frames received:%ACLQOS-SLOT1-2-ACLQOS_UNEXPECTED_PFC_FRAMES: Ethernet1/29 received 2 unexpected PFC frames for COS 4%ACLQOS-SLOT1-2-ACLQOS_UNEXPECTED_PFC_FRAMES: Ethernet1/29 received 2 unexpected PFC frames for COS 5%ACLQOS-SLOT1-2-ACLQOS_UNEXPECTED_PFC_FRAMES: Ethernet1/29 received 2 unexpected PFC frames for COS 6%ACLQOS-SLOT1-2-ACLQOS_UNEXPECTED_PFC_FRAMES: Ethernet1/29 received 2 unexpected PFC frames for COS 7%SYSMGR-SLOT1-2-SERVICE_CRASHED: Service " fcoelc" (PID 25997) hasn't caught signal 11 (core will

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
	be saved). Workarounds: none
CSCvy67509	Headline: Watchdog timeout reason may not be saved due to race condition Symptoms: After watchdog timeout reset there are no kernel logs or stack-traces available to determine a reason of the timeout, and reset-reason indicates that kernel did not receive NMI:----- reset reason for module 1 (from Supervisor in slot 1) ---1) At 123456 usecs after Sun May 01 01:02:00 2021 Reason: Watchdog Timeout Service: HW check by card-client Version:" HW check by card-client" indicates that Kernel either didn?t receive NMI or kernel didn?t able to write the reset reason section. Workarounds: None
CSCvy68524	Headline: Aclqos crash on ravl_insert and ravl_free Symptoms: aclqos process crash2021 Jun 8 03:35:29.789 RMD03-NX_LB-01 %$ VDC-1 %$ %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service " aclqos" (PID 28000) hasn't caught signal 11 (core will be saved).2021 Jun 8 03:35:30.407 RMD03-NX_LB-01 %$ VDC-1 %$ %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service " aclqos" (PID 8248) hasn't caught signal 11 (core will be saved).2021 Jun 8 03:35:31.026 RMD03-NX_LB-01 %$ VDC-1 %$ %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service " aclqos" (PID 8469) hasn't caught signal 11 (core will be saved).2021 Jun 8 03:35:31.640 RMD03-NX_LB-01 %$ VDC-1 %$ %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service " aclqos" (PID 8477) hasn't caught signal 11 (core will be saved)May also see the TCAM resource exhaustion logs like below-2021 May 22 18:47:26.685 RMD03-NX_LB-01 %$ VDC-1 %$ %ACLQOS-SLOT1-2-ACLQOS_OOTR: Tcam resource exhausted: Ingress RACL [ing-racl]2021 May 22 18:47:26.713 RMD03-NX_LB-01 %$ VDC-1 %$ %RPM-2-PPF_SES_VERIFY: rpm [31668] PPF session verify failed in client aclqos(Line card 1/VDC NONE/UUID 366) with an error 0x41040069(Sufficient free entries are not available in TCAM bank)2021 May 22 18:48:47.213 RMD03-NX_LB-01 %$ VDC-1 %$ %ACLQOS-SLOT1-2-ACLQOS_OOTR: Tcam resource exhausted: Ingress RACL [ing-racl]2021 May 22 18:48:47.240 RMD03-NX_LB-01 %$ VDC-1 %$ %RPM-2-PPF_SES_VERIFY: rpm [31668] PPF session verify failed in client aclqos(Line card 1/VDC NONE/UUID 366) with an error 0x41040069(Sufficient free entries are not available in TCAM bank)2021 May 22 18:51:05.725 RMD03-NX_LB-01 %$ VDC-1 %$ %ACLQOS-SLOT1-2-ACLQOS_OOTR: Tcam resource exhausted: Ingress RACL [ing-racl]2021 May 22 18:51:05.749 RMD03-NX_LB-01 %$ VDC-1 %$ %RPM-2-PPF_SES_VERIFY: rpm [31668] PPF session verify failed in client aclqos(Line card 1/VDC NONE/UUID 366) with an error 0x41040069(Sufficient free entries are not available in TCAM bank)2021 May 22 20:28:43.847 RMD03-NX_LB-01 %$ VDC-1 %$ %ACLQOS-SLOT1-2-ACLQOS_OOTR: Tcam resource exhausted: Ingress RACL [ing-racl]2021 May 22 20:28:43.909 RMD03-NX_LB-01 %$ VDC-1 %$ %RPM-2-PPF_SES_VERIFY: rpm [31668] PPF session verify failed in client aclqos(Line card 1/VDC NONE/UUID 366) with an error 0x41040069(Sufficient free entries are not available in TCAM bank) Workarounds:
CSCvy72704	Headline: NX-API Object Store DN/Class Properties Inconsistent with CLI for Vlans that Previously Existed Symptoms: In object store / visore from NXAPI:BdOperName is blank, operSt shows downIf vlan 12 is removed and then added again with name TEST-VLAN (or any other name), we see the following in object store: BdOperName ----> blank (no output here in visore / object store)operStdown ----> why is this not active? nameTEST-VLAN ----> name is populated with the name that I gave, but why is BdOperName blank? ++ It does not matter what method is used to add / delete the vlan. The result is the same as listed above.++ Reloading the switch causes all the above fields to be populated correctly / as expected. Ie; BdState ==========Test Switch output: ==========BMO-EQNY4-NX02(config)# sh vl brVLAN Name Status Ports---- ----------

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
	---------- ---------- ----------1 default active Eth1/212 TEST-VLAN active Eth1/2We can see the vlan is active and functioning correctly so why is BdState down? ++ This is causing problems for my customer because they use scripting to check on vlan status and this erroneous output gives false flags (vlan seems inactive when it is active). Workarounds: Reload the switch
CSCvy73232	Headline: N9k ITD-NAT and User defined PBR applied to same interface may cause inconsistencies in aclqos table Symptoms: ITD NAT Traffic sent to node with Incorrect DMACaclqos is mis-matched b/w ASIC instances Workarounds: If feasible, remove PBR from the SVI(copy run start) and affected nexus 9k would have to be reloaded with " reload ascii"
CSCvy74199	Headline: OSPFv2 Auth key need to be relaxed Symptoms: OSPFv2 authentication commands with some type-7 passwords are not accepted from release 9.3.5 onward." ip ospf message-digest-key 100 md5 7 <password>" " ip ospf authentication-key 7 <password>If password violates below rules then that will not be accepted. i.) First four characters are numbers.ii.) Password length should be a multiple of 4.iii.) Max length can be 32 characters.This is incompatible with older releases which followed below rule.i.) Input must contain an even number of characters and minimum length is 4ii.). The first two digits must be decimal numbers and the rest are hexThis will cause failure of the command on upgrade (ISSU, reload etc). Workarounds: Before upgrade change the keys to follow below rules:i.) Input must contain an even number of characters and minimum length is 4ii.). The first two digits must be decimal numbers and the rest are hex
CSCvy76019	Headline: N9K - Mgmt0 RJ45 copper port goes down, once SFP is inserted on SFP port Symptoms: Mgmt0 port on a Cisco Nexus 9000 Series switch goes down and doesn't come back up.1.connect both of the RJ45 and SFP based mgmt port.2. remove the cable on the SFP based mgmt port.3.shut/no shut the mgmt port. Workarounds: Setting the speed to 100 fixes the problem or removing the SFP from the SFP mgmt0 port brings up the RJ-45 port.
CSCvy88454	Headline: Packets forwarded with Incorrect MPLS labels when using N9k layer 2 evpn over segment routing Symptoms: Spines drop the Labeled Packets from Leaf switchesIncorrect Outer label for MPLS packetsIn some cases, multiple labels are also seen(more than 2) Workarounds: Once impacted by this defect, the only way to restore is by Removing SPAN/SFLOW(if feasible) and " copy run start" , reload
CSCvy89592	Headline: N9K/FX Series - Egress IFACL Label allocation Exhaustion/Failure is handled incorrectly Symptoms: When Egress IFACL label allocation is reached; BFD flaps or traffic gets policed on port where egress QOS policy (policer) is not configured. Workarounds: Do not apply policies on more than supported Hardware limitRemove the policy from an interface.
CSCvy94454	Headline: Multiple sh process cores being created

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
	Symptoms: Device will get multiple sh cores created:`show cores`VDC Module Instance Process-name PID Date(Year-Month-Day Time)--- ------ -------- ---------- -------- ----------1 1 1 sh 17791 2021-06-25 13:28:591 1 1 sh 17820 2021-06-25 13:29:071 1 1 sh 17804 2021-06-25 13:30:01 Workarounds: none
CSCvy97053	Headline: N9508 sub-interface Tx counters are not incrementing. Symptoms: N9508 sub-interface Tx counters are not incrementing. Workarounds: Downgrade to 9.2(x) version.
CSCvy99573	Headline: PBR not correctly programmed with scaled L2 egress port-channel Symptoms: With PBR redirected to a next hop adjacent via a L2 port-channel, the PBR can become mis-programmed and blackhole traffic.May be observed when initially configuring or when adding links to an already provisioned port-channel. Workarounds: Constrain port-channel to 31 ports or less
CSCvz02714	Headline: When having PVLAN promiscuous on trunk link BFD and ISIS not coming up Symptoms: Current config of 2 N9K-C93180YC-FX connected back to back with a trunk link with a combination of PVLAN, ISIS and BFD configuration.++ When the PO1 is configured as " Switchport mode trunk" , both the BFD and ISIS comes up.++ When the PO1 is configured as " switchport mode private-vlan trunk promiscuous" , BFD goes down and ISIS adjacency goes down.++ However, when we configure " OSPF" as a testing purpose, under the same SVI VLAN 14, it comes up fine.N9k-1 <--trunk--> N9k-2N9k-1interface port-channel1 switchport switchport mode private-vlan trunk promiscuous switchport private-vlan trunk allowed vlan 1,10,14,200-201,250,300,350,500 switchport private-vlan mapping trunk 250 251-257 switchport private-vlan mapping trunk 300 301-307 switchport private-vlan mapping trunk 14 15 switchport trunk native vlan 10 switchport trunk allowed vlan 1,10,14,200-201,250,300,350,500N9k-2interface port-channel1 switchport switchport mode private-vlan trunk promiscuous switchport private-vlan trunk allowed vlan 1,10,14,200-201,250,300,350,500 switchport private-vlan mapping trunk 250 251-257 switchport private-vlan mapping trunk 300 301-307 switchport private-vlan mapping trunk 14 15 switchport trunk native vlan 10 switchport trunk allowed vlan 1,10,14,200-201,250,300,350,500IS-IS process: ISIS VRF: defaultIS-IS adjacency database:Legend: '!': No AF level connectivity in given topologySystem ID SNPA Level State Hold Time Interface2081.1609.5018 4c71.0d24.1d67 2 INIT 00:00:45 Vlan14F340.12.19-93180FX-9FD# sh bfd neOurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int Vrf 10.127.94.35 10.127.94.34 1090519057/0 Down N/A(3) Down Vlan14 default Workarounds: a. Provision a dedicated L2 trunk port (non PVLAN) between the switches.b. Remove BFD itself entirely for the time being to have isis adjacency - no feature BFD
CSCvz07339	Headline: sysDescr doesnt return hardware type for Nexus9000 Symptoms: sysDescr doesn't return with snmp hardware type that includes " Nexus 9000" string. According to OID description we should return the system's hardware type. Example:Non-working one:SNMPv2-MIB::sysDescr.0 = STRING: Cisco NX-OS(tm) nxos.9.3.2.bin, Software (nxos), Version 9.3(2), RELEASE SOFTWARE Copyright (c) 2002-2019 by Cisco Systems, Inc. Compiled 10/28/2019 22:00:00Working one displaying hardware type:SNMPv2-MIB::sysDescr.0 = STRING: Cisco NX-OS(tm) n7000, Software (n7000-s2-dk9), Version 8.2(4), RELEASE SOFTWARE Copyright (c) 2002-2019 by Cisco Systems, Inc. Compiled 5/31/2019

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
	23:00:00 Workarounds: None
CSCvz07646	Headline: lldp neighbor information dispeared if configured 'no lldp tlv-select power-management' Symptoms: If configure 'no lldp tlv-select power-management', 'show lldp neighbor' won?t show neighbor information and the below two counters in ?show lldp traffic? keep increasing.N9K-1(config)# show lldp neighborsERROR: No neighbour information <<<N9K-1(config)# show lldp traffic LLDP traffic statistics: Total frames transmitted: 252 Total entries aged: 4 Total frames received: 156 Total frames received in error: 124 <<< Total frames discarded: 124 <<< Total unrecognized TLVs: 0 Total flap count: 4 Workarounds: Configure ?lldp tlv-select power-management'
CSCvz08309	Headline: LXC Mode ND ISSU wont upgrade Micron500IT firmware Symptoms: LXC boot mode with ND ISSU wont upgrade Micron500IT firmware for FN72150 Workarounds: Use script mentioned in fn72150 upgrade it manuallyDisable LXC mode and do reload
CSCvz09834	Headline: N9500-R/N3600 CoPP policer counters are incorrect after upgrade to 9.3.7 Symptoms: CoPP policer counters across all classes are incorrect. Workarounds: N/A
CSCvz11134	Headline: N9500-R/N3600 ttl=1 mcast traffic impacts link-local mcast control-plane Symptoms: Flapping link-local mcast based neighbor-ship (OSPF). Workarounds: Eliminate TTL=1 traffic.
CSCvz17536	Headline: Traffic blackhole when both uplinks of compute to ToR are flapped Symptoms: Setup is CVIM running 3.4.4 with N9K ToR pairs running 9.3.7 Compute Nodes <--> Leaf pair <---> Spines <-----> ECX (Juniper) <--->CE (Juniper)When both uplinks from Compute to ToR pair are flapped , traffic is blackholed. Workarounds: Ping compute VTEP IP from ECX node or Leaf node OR restart VPP on compute node.
CSCvx70658	Headline: 100G SFP's starting with FBN S/N reported as 40G-SR4 Symptoms: FCOT read failures causing display issue of 100G SFP's as 40G-SR4's Workarounds: Reload
CSCvy66586	Headline: External Error Message for 36180-YC-R uses Fretta in message Symptoms: This is a document bug, or error message correction bug that has been brought to the technical teams attention. Workarounds: None
CSCvy90700	Headline: Mac address disabled on ports after removing VPC Peer-link from configuration

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
	Symptoms: After removing VPC peer-link from configuration router mac addresses from VPC peer will not be learnt agan.If using BFD you can see he following error under: sh bfd neighbors detail: sh bfd neighbors details OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int Vrf Type 10.3.200.254 10.3.200.253 1090519044/0 Down N/A(3) Down Vlan200 default SH Session state is Down and not using echo functionSession type: SinglehopLocal Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: NoneMinTxInt: 0 us, MinRxInt: 0 us, Multiplier: 0Received MinRxInt: 0 us, Received Multiplier: 0Holdown (hits): 0 ms (0), Hello (hits): 0 ms (0)Rx Count: 0, Rx Interval (ms) min/max/avg: 0/0/0 last: 0 ms agoTx Count: 0, Tx Interval (ms) min/max/avg: 0/0/0 last: 0 ms agoRegistered protocols: ospfDowntime: 0 days 0 hrs 1 mins 28 secs, Downcount: 0Last packet: Version: 0 - Diagnostic: 0 State bit: AdminDown - Demand bit: 0 Poll bit: 0 - Final bit: 0 Multiplier: 0 - Length: 24 My Discr.: 0 - Your Discr.: 0 Min tx interval: 0 - Min rx interval: 0 Min Echo interval: 0 - Authentication bit: 0 Hosting LC: 0, Down reason: No Diagnostic, Reason not-hosted: if_index type invalid <<<<<<<<<<< Workarounds: Reload the box can solve the issue.
CSCvy49381	Headline: QOSMGR_MEM_port_grp_mem_t memory leak in the ipqosmgr process Symptoms: Crash of ipqosmgr process due to a memory leak with core and process log files.%SYSMGR-2-SERVICE_CRASHED: Service " ipqosmgr" (PID 32142) hasn't caught signal 6 (core will be saved). Workarounds: Not known for now.
CSCvz36338	Headline: N9K-C9364C: 100g copper link with macseec config does not link up on port-flap intermittently Symptoms: With macsec config, link may not come up on 100G copper connection after repeated shut/no shut on ports 49-64. Workarounds: Reload the switch.

General/Known Issues

Bug ID	Description
CSCvz07339	Earlier the SysDescr did not return with snmp hardware type that includes " Nexus 9000" string. From Cisco NX-OS Release 10.2(1)F SysDescr MIB Information includes the Hardware Type (Nexus9000) and PID Information. An example is provided below. iso.3.6.1.2.1.1.1.0 = STRING: " Cisco NX-OS(tm) Nexus9000 C9348GC-FXP, Software (NXOS 64-bit), Version 10.2(1), Interim version 10.2(0.229), RELEASE SOFTWARE Copyright (c) 2002-2021 by Cisco Systems, Inc. Compiled 7/22/2021 21:00:00"
NA	Open Flow is not supported in Cisco Nexus 9000 Series switches.
NA	FM-G modules in slot-25 might fail to come up if N9K-X9736C-FX, N9K-X9736Q-FX line cards are in up state.
NA	Ingress packets above 626 bytes are truncated in a Span on Drop (SoD) scenario in Nexus 9300-GX Platform Switches.

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
NA	When you downgrade from Cisco NX-OS Release 10.2(1)F to an earlier version (for example – Cisco NX-OS Release 9.3(5)) you will receive a compatibility failure unless you delete DES from the snmp-server command. Cisco NX-OS Release 9.3(5) supports only AES. But when you remove DES from the snmp-server command, it changes the admin password that cannot be easily deciphered. You need to add a new user so that you can change the admin password, which then synchronizes it with the snmp-server password.
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(1)F 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 25
Table 2. Cisco Nexus 9500 Cloud Scale Line Cards 26
Table 3. Cisco Nexus 9500 R-Series Line Cards 26
Table 4. Cisco Nexus 9500 Cloud Scale Fabric Modules 26
Table 5. Cisco Nexus 9500 R-Series Fabric Modules 27
Table 6. Cisco Nexus 9500 Supervisor Modules 27
Table 7. Cisco Nexus 9500 System Controller 27
Table 8. Cisco Nexus 9500 Fans and Fan Trays 28
Table 9. Cisco Nexus 9500 Fabric Module Blanks with Power Connector 28
Table 10. Cisco Nexus 9500 Power Supplies 28
Table 11. Cisco Nexus 9200 and 9300 Switches 28
Table 12. Cisco Nexus 9200 and 9300 Fans and Fan Trays 30
Table 13. Cisco Nexus 9200 and 9300 Power Supplies 31
Table 14. Cisco Nexus 9500 Cloud Scale Line Cards 33
Table 15. Cisco Nexus 9500 R-Series Line Cards 34
Table 16. Cisco Nexus 9500 R2-Series Line Cards 34

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.

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Product ID	Description
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-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
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

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

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.

Table 7. Cisco Nexus 9500 System Controller

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

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

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

Cisco Nexus Switch	Description
N9K-C9316D-GX	1-RU switch with 16x400/100/40-Gbps ports.

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Nexus Switch	Description
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-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
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 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

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Cisco Nexus Switch	Description
	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
NXA-FAN-160CFM-PI	Fan module with port-side intake airflow (burgundy coloring)	3	9364C [1] 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	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	92300YC [1] 9332C [1] 93180YC-FX3S [2]

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

[2] 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.

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

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

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Product ID	Description	Quantity	Cisco Nexus Switches
			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 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

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Product ID	Description	Quantity	Cisco Nexus Switches
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
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-	5	5	5	5	5	5

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

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
FX						
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

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(1)F supports the Nexus Dashboard Insights 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 Nexus Insights documentation.

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

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(1)	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
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(1) 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.

© 2021-2023 Cisco and/or its affiliates. All rights reserved.

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.

© 2021-2023 Cisco Systems, Inc. All rights reserved.