Cisco Nexus 9000 Series NX-OS Release Notes, Release 10.3(2)F

© 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 10.3(2)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 to the Open Issues section.
July 27, 2023	Updated Table 1. Cisco Nexus 9400 Switches
June 19, 2023	Added CSCwa83084 in the Resolved Issues section
May 05, 2023	Added PTP in Unsupported Features in the N9K-C92348GC section
April 09, 2023	Added CSCwe67205 in the Open Issues section
February 16, 2023	Moved CSCvs79768 from Open to Resolved Issues section
February 9, 2023	Added CSCwe20605 in the Open Issues section
January 31, 2023	Updated Table 5. Cisco Nexus 9800 Supervisor Module
January 25, 2023	Updated the Unsupported Features in the N9K-C92348GC section
December 19, 2022	Cisco NX-OS Release 10.3(2)F became available

New and Enhanced Software Features

The following tables provide information about new and enhanced software features in Release 10.3(2)F.

New Features

Product Impact	Feature	Description
Ease of use	SRTE for Recursive VPN Routes	The SRTE for Recursive VPN Routes feature allows BGP to request policy from SRTE with GW-IP as the endpoint, wherein, SRTE returns the BSID for the matching policy. For more information, see Cisco Nexus 9000 Series NX-OS Label Switching Configuration Guide, Release 10.3(x).

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

Cisco Confidential

Product Impact	Feature	Description
	Long Distance support on FCoE	Added support for long distance, up to 10 kilometers, on FCoE ISLs on Cisco Nexus C93180YC-FX platform switches. For more information, see Cisco Nexus 9000 Series NX-OS SAN Switching Configuration Guide, Release 10.3(x).
Feature Set	Q-in-VNI with L2 Protocol Tunneling	Q-in-VNI with Layer 2 Protocol Tunneling (L2PT) is now used to transport control and data packets across a VXLAN EVPN fabric for multi-tagged traffic. For more information, see Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 10.3(x).
	PFM-SD support for IPFM deployments	The PIM flooding mechanism with source discovery (PFM-SD) feature eliminates the necessity for rendezvous points (RPs) while sending the multicast data streams. For more information, see Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 10.3(x).
	BGP: RPKI Support	Beginning with this release, the Cisco Nexus switches running BGP can connect to the Resource Public Key Infrastructure (RPKI) to validate the origin-AS of BGP paths. For more information, see Cisco Nexus 9000 Series NX-OS Security Configuration Guide, and Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 10.3(x).
Performance and Scalability	BFD for SRTE	The BFD for SRTE feature allows the switch, on which one or more SRTE policies are configured, to proactively detect if the active path or paths of an SRTE policy have failed. For more information, see Cisco Nexus 9000 Series NX-OS Label Switching Configuration Guide, Release 10.3(x).
	TRM Data MDT	This feature leverages S-PMSI (data MDT) to optimize the TRM multicast forwarding on the VXLAN EVPN fabric. For more information, see Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 10.3(x).
Security	EVPN null route	This feature enables a VTEP within the network to send Type 2 and Type 5 routes tagged with a specific community (defined for null routes) to drop traffic on the remote VTEPs. For more information, see Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, and Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 10.3(x).

Enhanced Features

The enhanced features listed below are existing features introduced in earlier releases, but enhanced to support new platforms in Cisco NX-OS Release 10.3(2)F.

Product Impact	Feature	Description
Diagnostics and Serviceability	ITD Consistency Checker	ITD consistency checker is now supported on Cisco Nexus 9300-EX, 9300-FX, 9300-FX2, 9300-FX3, 9300-GX, and 9300-GX2 platform switches. For more information, see Cisco Nexus 9000 Series NX-OS Troubleshooting Guide, Release 10.3(x).

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

Cisco Confidential

Product Impact	Feature	Description
	MPLS Consistency Checker	Beginning with this release, proactive consistency checker supports MPLS route consistency check. For more information, see Cisco Nexus 9000 Series NX-OS Troubleshooting Guide, Release 10.3(x).
Ease of Setup/ Deployment	gRPC Tunneling	Beginning with this release, gRPC tunnel supports dial-out approach. For more information, see Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 10.3(x).
	Expanded support for OpenConfig IS-IS model	The OC IS-IS LSP Database is now supported on NX-OS. This feature also allows you to query the details of the LSP database. For more information, see Cisco Nexus OpenConfig YANG, Release 10.3x.
Ease of Use	Additional LLDP TLVs for ecosystem integrations	The existing lldp tlv-select command that specifies TLVs now has additional optional parameters such as 802.1 link aggregation, 802.1 vlan name, and 802.3 maxframe size. For more information, see Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 10.3(x).
Feature Set	DSCP-based SR-TE flow steering	The DSCP-based SRTE flow steering feature is now supported on Cisco Nexus 9500 platform switches with Cisco Nexus 9700-FX and 9700-GX line cards. For more information, see Cisco Nexus 9000 Series NX-OS Verified Scalability Guide, Release 10.3(2)F; Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 10.3(x); and Cisco Nexus 9000 Series NX-OS Label Switching Configuration Guide, Release 10.3(x).
	Flow-based traffic steering	The flow-based traffic steering feature is now supported on Cisco Nexus 9700-FX and 9700-GX line cards. For more information, see Cisco Nexus 9000 Series NX-OS Label Switching Configuration Guide, Release 10.3(x).
	Storm Control on L3 interfaces	Traffic storm control is now supported on Layer 3 interfaces. For more information, see Cisco Nexus 9000 NX-OS Security Configuration Guide, Release 10.3(x).
	PBR - Default IPv4/IPv6 nexthop VRF Selection Support	Default IPv4/IPv6 NH VRF selection for PBR is now supported on Cisco Nexus 9000 Series platform switches. For more information, see Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 10.3(x).
	VPLS Stripping	EoMPLS header stripping is now supported on Cisco Nexus 9300-FX, 9300-FX2, 9300-FX3, 9300-GX, and 9300-GX2 platform switches. For more information, see Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 10.3(x).
	GM/GPS/GNSS support on N9K-C93180YC-FX3	PTP Primary Leader (GM) functionality with GPS and GNSS inputs is now supported on Cisco Nexus C93180YC-FX3 platform switches. SyncE license is required for using this functionality. For more information, see Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 10.3(x).
	vPC Fabric Peering	vPC Fabric Peering is now supported only for IPv6 underlay on Cisco Nexus 9300-

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

Product Impact	Feature	Description
		EX, 9300-FX, 9300-FX2, 9300-FX3, 9300-GX, and 9300-GX2 platform switches. For more information, see Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 10.3(x).
	Seamless integration of EVPN with L3VPN (MPLS SR)	Seamless integration of EVPN with L3VPN (MPLS SR) is now supported on Cisco Nexus 9500 platform switches with Cisco Nexus 9700-FX and 9700-GX line cards. For more information, see Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 10.3(x).
	Flexible NBM modes with Multi-tenancy VRF	Beginning with Cisco NX-OS Release 10.3(2)F, NBM mode pim-active and NBM mode pim-passive can coexist on the same switch. For more information, see Cisco Nexus 9000 Series NX- OS IP Fabric for Media Solution Guide, Release 10.3(x).
	NBM support on sub-interfaces	Sub-interface type is now supported in NBM mode pim-active and NBM mode pim-passive. For more information, see Cisco Nexus 9000 Series NX-OS IP Fabric for Media Solution Guide, Release 10.3(x).
	Multicast NAT support on sub-interfaces for IPFM flows	Multicast service reflection (Multicast NAT) is now extended to sub-interfaces on all host and fabric ports for NBM mode pim-active and NBM mode pim-passive. For more information, see Cisco Nexus 9000 Series NX-OS IP Fabric for Media Solution Guide, Release 10.3(x).
	NAT Enhancement	Beginning with Cisco NX-OS Release 10.3(2)F, egress service reflection (egress multicast NAT, and multicast to unicast NAT) supports Post-NAT Source IP to be IP Address of an egress interface. This enhancement is supported for regular multicast, and for NBM. For more information, see Cisco Nexus 9000 Series NX-OS IP Fabric for Media Solution Guide, Release 10.3(x).
	PTP with Media profile support on Cisco Nexus 9408 platform	PTP with IEEE 1588v2, SMPTE 2059-2 and AES67 profiles are now supported on Cisco Nexus 9408 platform switch. For more information, see Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 10.3(x) and Cisco Nexus 9000 Series NX-OS Verified Scalability Guide, Release 10.3(2)F.
	Enhanced Convergence for vPC BGW CloudSec Deployments	You can now configure a separate loopback interface for CloudSec-enabled vPC BGW. Furthermore, we recommend the use of separate loopback interfaces for source and anycast IP addresses under NVE for better convergence in MLAG deployments. For more information, see Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 10.3(x).
Licensing	Support SLP on Non-Management VRF	Smart Licensing using Policy is now supported on non-management VRF for smart transport and CSLU mode of transport. For more information, see Cisco Nexus 9000 and 3000 Series NX-OS Smart Licensing Using Policy User Guide.
	Support for Source Interface for call home	You can now optionally specify a source interface to send Smart Call Home messages over HTTP.

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

Cisco Confidential

Product Impact	Feature	Description
		For more information, see Cisco Nexus 9000 and 3000 Series NX-OS Smart Licensing Using Policy User Guide.
	CSSM to display PI hostname	The CSSM now displays the host name of the Product Instance (PI) instead of UDI. For more information, see Cisco Nexus 9000 and 3000 Series NX-OS Smart Licensing Using Policy User Guide.
	Licensing support for Cisco Nexus 9408 switches	Smart Licensing Using Policy is now supported on Cisco Nexus 9408 platform switches. For more information, see Cisco Nexus 9000 and 3000 Series NX-OS Smart Licensing Using Policy User Guide.
Scalability	Scale Enhancements	For Cisco NX-OS Release 10.3(2)F Scale Enhancements, see Cisco Nexus 9000 Series NX-OS Verified Scalability Guide, Release 10.3(2)F.
Security	Primary key enablement within configuration mode	Until this release, you could only configure the primary key within the configuration mode. Beginning with Cisco NX-OS Release 10.3(2)F, you can also use DME payload to configure the master key. For more information, see Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 10.3(x).
	Source CoPP ACLs on Nexus 9504/9508 with -R line cards	Source IP based filtering in CoPP is now supported on Cisco Nexus 9504 and 9508 switches with -R line cards. For more information, see Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 10.3(x).
	MAB, Critical Authentication, and Multi-auth support	MAC authentication bypass, critical authentication, and multi-authentication is now supported on Cisco Nexus 9508 switches with N9K-X9788TC-FX and N9K-X97160YC-EX line cards. For more information, see Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 10.3(x).
	Consent token for bash access	This feature allows you to use the consent token secure mode to enable shell access on NX-OS. However, this feature works only on Trust Anchor Module (TAM) based devices. For more information, see Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 10.3(x).

Hardware Features

The following hardware is supported in Cisco NX-OS Release 10.3(2)F:

- The Cisco Nexus 9408 (N9K-C9408) is a 4-rack unit (RU) 8-slot LEM-based modular switch, which is configurable with up to 128 200-Gigabit QSFP56 (256 100-Gigabit by breakout) ports or 64 400-Gigabit ports. This switch supports port-side intake airflow. The switch requires four AC power supply for operation and offers 2+2 power grid redundancy.
- This switch includes the following high-power optics and MACsec:
  - The N9K-X9400-16W LEM offers full MACsec (128 ports) for a full load chassis with no limitation for 200G optics.

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

Cisco Confidential

- The N9K-X9400-8D LEM offers full MACsec (64 ports) for a full load chassis but with a limit of 400G high power optics within 32pcs among 8 slots (maximum of 32 ports of 20-W optics irrespective of MACsec), and the high-power optics can go in any of the 400G ports.

The following table provides information about spares support:

Product	Chassis Height (Rack Units)	Power Supply Options	Fan Options	Module Options	Accessory Kits
N9K-C9408	4 RU	AC port-side intake (NXA-PAC-2KW-PI)	Port-side intake (N9K-C9400-FAN-PI)	CPU Card (N9K-C9400-SUP-A) Switch Card (N9K-C9400-SW-GX2A) LEM 8p 400G (N9K-X9400-8D) LEM 16p 200G (N9K-X9400-16W)	Accessory Kit (N9K-C9400-ACK) Rack mount kit (N9K-C9400-RMK) LEM Blank (N9K-C9400-BLK)

For more details about Cisco Nexus 9408 Switches, see Cisco Nexus 9408 NX-OS Mode Switch Hardware Installation Guide.

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

For more details about supported features on Cisco Nexus 9408 Switches, see Nexus Switch Platform Support 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, and RESTCONF

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

Release Image

In Cisco NX-OS Release 10.3(2)F, 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.10.3.2.F.bin). This image is supported on all Cisco Nexus 9000 series fixed platforms and Cisco Nexus 9800 platform switches.

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

- The 64-bit Cisco NX-OS image filename that begins with " nxos64-msll" (for example, nxos64-msll.10.3.2.F.bin). This image is supported on Cisco Nexus 9000 -R and -R2 series modular switches.

The 32-bit image is no longer supported.

Open Issues

Bug ID	Description
CSCvz06811	Headline: Nexus Data Broker switch floods IGMPv3 membership queries out of all input ports. Symptoms: IGMP membership queries are flooded out of monitoring ports. IGMP storms (due to queries) are forwarded from Nexus Data Broker Switch to production network. Workarounds: Filter the IGMP with an access list.
CSCwd86261	Headline: NFM crash causes the N9K-C9336C-FX2 to reboot unexpectedly. Symptoms: Unexpected reload of the switch without any special configurations or new exporters. Workarounds: None
CSCwd84893	Headline: F3 PIXM CBL is wrongly programming on vPC secondary after VLAN change. Symptoms: Wrong programming of F3 PIXM CBL on vPC secondary after change of VLAN. Workarounds: Perform any one of the following workarounds: • Remove and reconfigure wrong VLAN entry command Physical interface shut/no shut
CSCwd68210	Headline: After upgrading Cisco Nexus 9500, Cisco Nexus 9000, and Cisco Nexus 3000 Switch 100Gig Interface does not come up. Symptoms: Interface doesn't come up after upgrading Nexus 9500 from Cisco NX-OS Release 9.3(4) to 9.3(8). SFP used is the QSFP-100G-CWDM4-S Link between Nexus 9000: N9K-X9736C-FX and leaf: N3K-C36180YC-R. Workarounds: None
CSCwd75778	Headline: Unable to connect to grpc port 50051 in non-default vrf. Symptoms: Unable to connect to grpc port 50051 in non-default vrf with MPLS path. Telnet to port 50051 also fails. Workarounds: None
CSCwd83094	Headline: LACP rate configuration causes the config replace operation to fail. Symptoms: If the existing port is in a port-channel and admin up, and the desired configuration on the same port needs to change 'lacp rate,' then this causes the config replace operation to fail and the following error is seen in the output of 'show config-replace log exec' command: <snip>'interface Ethernet1/1'`lacp rate fast`ERROR: Command validation failed. Cannot set lacp rate. Port is not admin down in port-channel. Workarounds: Shut down the conflicting port before attempting config replace again.
CSCwd85017	Headline: Multicast Traffic drop. Symptoms: Remote host/receiver tunes into a wrong UDP port number.

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

Bug ID	Description
	Workarounds: None
CSCwd85841	Headline: NX-OS SNMP does not respond to CISCO-ENTITY-FRU-CONTROL-MIB for N9K-C9508-FAN-PWR. Symptoms: No response to snmp OID 1.3.6.1.4.1.9.9.117.1.2.1.1.2 for 9K-C9508-FAN-PWR modules. Workarounds: None
CSCwd87170	Headline: snmpbulkget to ciscoEntityFRUControlMIB creates invalid unicode in show snmp internal event-his pktdump. Symptoms: Unicode Symbols are seen in SNMP packet buffer dump, when performing FRUget snmpbulkget. Workarounds: Perform Snmpbulkget with two instances rather than more than two instances.
CSCwd88006	Headline: Nexus 95XX sends " epld_upgrade" SNMP trap. Symptoms: Nexus 95XX sends " epld_upgrade" SNMP trap. Workarounds: None
CSCwd75851	Headline: /nxos/xlog is filled 100% with repeated " copy run start" and log files are not rolled over. Symptoms: When config changes are done through automation and multiple sessions trying to save the config changes simultaneously and repeatedly, a syslog is seen. Workarounds: Avoid simultaneous config sessions and excessive/repeated config save operation.
CSCwd86342	Headline: SPAN traffic received from Cisco Nexus 9300 is dropped on Cisco Nexus 3548. Symptoms: On Cisco Nexus 9000 SPAN is configured and the SAPN destination interface is configured to Cisco Nexus 3548. On Cisco Nexus 3548, traffic is received and dropped. The drops are verified using the show hardware internal errors module 1 command. However, SPAN/ERSPAN traffic that Cisco Nexus 3548 should have received traffic is not seen. Workarounds: To resolve the issue, replace Cisco Nexus 9000 with Catalyst or add Catalyst switch in between Cisco Nexus 9000 and Cisco Nexus 3000.
CSCwd41247	Headline: samcproxy is deadlocked with multiple Instances. Symptoms: Configuration or simple tasks such as turning on a locator LED do not complete. Multiple instances of samcproxy running are seen, and one is in a deadlocked state. There may also be other miscellaneous faults on the domain, due to samcproxy being in a bad state. Workarounds: Contact Cisco TAC for a workaround that requires debug shell access.
CSCwd77505	Headline: MAC Address Not Learned on Peer 6332 FI. Symptoms: The host experiences a failover event or the VM is migrated to a different host, and the network connectivity to that VM is lost. Workarounds: Contact Cisco TAC for workarounds.
CSCwd84165	Headline: Unexpected FI Reboot due to FCPC Hap Reset. Symptoms: During normal operation, an unexpected reboot of a Fabric Interconnect occurs. From the NX-OS CLI, following system reset reason is seen: `show system reset-reason` ----- reset reason for Supervisor-module 1 (from Supervisor in slot 1) ---

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

Bug ID	Description
	1) At 273479 use cs after [DATE] Reason: Reset triggered due to HA policy of Reset Service: fcpc hap reset Workarounds: The FI reboots on its own.
CSCwd90085	Headline: SNMPD Hap Reset causes unexpected outages. Symptoms: Fabric Interconnect goes down without warning and the 'snmpd hap reset' is present in the output of the show system reset-reason command. Workarounds: Fabric Interconnect often reboots after it goes down, bringing the paths back up after the reset is completed.
CSCwe20605	Headline: Cisco Nexus 9300-FX3: Encrypted tunnel (VxLAN Cloudsec) traffic is getting dropped. Symptoms: After upgrading Cisco Nexus 9300-FX3 to Cisco NX-OS Release10.3(2)F image, few or all of the encrypted tunnel traffic is dropped. VxLAN cLoudsec or tunnel encryption statistics do not update. Workarounds: The workaround is as follows: 1. Remove tunnel-encryption from DCI uplinks. 2. Copy running-config startup-config. 3. Reload the switch. Post reload, configure tunnel-encryption on DCI uplinks.
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.
CSCwh50989	Headline: Custom COPP causing transit traffic to be punted to the CPU on Nexus 9300-GX2 Symptom: 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. Workaround: Custom COPP policy using src/dst match mitigates punt for transit traffic.

Resolved Issues

Bug ID	Description
CSCvs79768	Headline: Cisco Nexus 9000 Micron_5100_MTFD " Bootflash Read-Only State"; Kernel I/O errors found. Symptoms: Write operations on switch fail and an error is seen. Workarounds: None
CSCwa31486	Headline: Cisco Nexus 9300 BFD session over SVI/L2 sends packets out on incorrect L2 port. Symptoms: BFD session on SVI/L2 does not come up.

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

Cisco Confidential

Bug ID	Description
	Workarounds: None
CSCwa58073	Headline: Cisco Nexus 9000 - 'copy run start' fails after enabling 'feature bfd' due to DME failure. Symptoms: Switch had a module inserted and configuration saved before module was removed or made offline, followed by a reload. When enabling BFD and executing copy run start, the configuration is not stored. Workarounds: To clear the DME inconsistency, reload ascii or clear nxapi retries.
CSCwa83084	Headline: CSLU and smart transport do not support non-management VRF. Symptoms: Currently, smart licensing CSLU and smart transport methods do not support non-management VRF. Only management VRF is supported. For the use cases that rely on non-management VRF Callhome transport to connect to an OnPrem server with NX-OS versions < Cisco NX-OS Release 10.2(1), you need to have connectivity through VRF management to the OnPrem server, post upgrade to ≥ Cisco NX-OS Release 10.2(1), as it requires CSLU, and only VRF management is supported. For versions ≥ Cisco NX-OS Release 10.2(1), SMART and CSLU transport only support VRF management. There is no command to customize the VRF for the two transport modes. Workarounds: Use management VRF path for connectivity.
CSCwc92177	Headline: ip arp stats always shows zero for received total value. Symptoms: Total under Received in show ip arp statistics vrf all field shows 0 even when the any other received field is counted. Workarounds: None. However, this does not have any impact on switch functionality.
CSCwd21451	Headline: SNMP walk on any OID does not return expected results. Symptoms: SNMP walk on any OID does not return with expected results. Workarounds: None
CSCvf09329	Headline: VRF is NULL message in Syslog. Symptoms: The following message is consistently seen in the syslog: May 16 15:59:36 <leaf> <132> May 16 15:59:36 <leaf> %LOG_LOCAL0-4-SYSTEM_MSG [E4204936][transition][warning][sys] %IGMP-4-L3VM_LIBAPI_FAILED: VRF is NULL - failed in l3vm_if_get_context_info() We can also see the following logs in the output of " show ip igmp internal event-history objst" because of this issue: 2017 Jun 22 16:22:36.897419 igmp [10528]: TID 11503:igmp_is_if_on_objstore:2032: IGMP-OBJST: Failed to get context info from l3vm for Tunnel18 2017 Jun 22 16:02:33.533493 igmp [10528]: TID 11503:igmp_is_if_on_objstore:2032: IGMP-OBJST: Failed to get context info from l3vm for Tunnel18 2017 Jun 22 15:22:29.838229 igmp [10528]: TID 11503:igmp_is_if_on_objstore:2032: IGMP-OBJST: Failed to get context info from l3vm for Tunnel18 2017 Jun 22 15:12:50.360132 igmp [10528]: TID 11503:igmp_is_if_on_objstore:2032: IGMP-OBJST: Failed to get context info from l3vm for Vlan12 Workarounds: None
CSCwc35394	Headline: Coop adjacency is down between leaf and one of the spines | ISIS Fabric Link State down Symptoms: Coop adjacency is down between leaf switches and one of the spines. Workarounds: Choose any one of the following workarounds:

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

Cisco Confidential

Bug ID	Description
	• Shut down all interfaces of spine (connected to other fabric nodes, that is, spines and leafs in fabric/pod) and no shutdown them. • Decommission and then commission the spine.
CSCwc74517	Headline: ESG to vzAny PBR wrongly redirecting L2 unknown unicast packet. Symptoms: If a PBR contract is either provided or consumed by vzANy and at the same time consumed or provided by an ESG, unknown unicast l2 traffic in that ESG might be wrongly redirected to PBR devices if the BD is in FLOOD mode. Workarounds: Use BD in hw-proxy.
CSCwc91496	Headline: HAL Fanout port for rleaf HREP tunnel may not updated after next-hop change. Symptoms: Multicast or broadcast from local leaf switches to remote leaf switches can be dropped after a next-hop change on IPN. This drop is caused by the failure of the head-end replication for remote leaf switches when a spine switch transmits BUM traffic. Workarounds: Trigger the hardware reprogramming to bounce the IPN port or to update the routing information, which changes the next hop.
CSCwd03377	Headline: Line Card module reset with PTPLC crash. Symptoms: Line card modules reset with a PTPLC crash. Workarounds: Disable PTP or reload the card that does not have the follower port (once in every 5 days).
CSCwd46678	Headline: Cisco Nexus 9000 Back Pressure Correction to Prevent PSU Fan Reverse Direction. Symptoms: Reported power supply exhaust fan was observed spinning in wrong direction in Cisco Nexus 9000 switch. Workarounds: Increasing PSU fan speed can prevent back-pressure from occurring.
CSCwd56718	Headline: PBR dynamic mac, mac keeps flapping after failover causing disruption. Symptoms: PBR dynamic mac, mac keeps flapping after failover causing disruption. Workarounds: If only one switch in vPC peer is active, then no issues are seen.
CSCwd75707	Headline: Parser Dropping IP-in-IP packet associated with IP Traffic on Ingress Leafs. Symptoms: Parser Dropping IP-in-IP packet associated with IP Traffic on Ingress Leafs. Workarounds: None
CSCwc87548	Headline: Underrun errors transmitted when upgrading from 40 to 100 Gbps on an EOR Cisco Nexus 9000. Symptoms: When the SFP is replaced to support 100G (QSFP-100G-SR4) or by changing the speed of the port (QSFP-40/100-SRBD), transmitting of underrun packets begins. However, output errors counter will not increase locally. Only CRC start to increase on neighbor device is seen. These ports are configured on a layer 2 port channel (no vPC). While working at 40G, no CRC are seen. Workarounds: Downgrade to 40 Gbps.
CSCwb83283	Headline: Memory leak due to port profile. Symptoms: Memory leak port profile process crashes and generates core files. Workarounds: None
CSCuw91064	Headline: 'show ip access-list' output does not update/display statistics.

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

Cisco Confidential

Bug ID	Description
	Symptoms: Statistics do not get updated in the output of the show ip access-list <acl-name> command. Workarounds: To populate the statistics field, apply ACL to a single SVI; remove SVI (no int vlan 10) and recreate SVI.
CSCvx75284	Headline: Host mobility does not work between DCs if leaves are vPC. Symptoms: Host mobility does not work in fabric. Workarounds: Manually clear the ARP entry on the leaves where host was in the past, reduce the ARP aging. After ARP times out routing will point correctly.
CSCwc08583	Headline: vPC " peer is alive for" counter does not increase. Symptoms: vPC " peer is alive for" counter does not increase when IPv6 is configured for keep-alive. This counter moves for " msec" but keeps as 0 for " seconds" . Workarounds: Use IPv4 instead.
CSCwc83796	Headline: Nexus 5000 Crashes in EIGRP process when modifying IP Prefix-list. Symptoms: A Nexus 5000 switch may experience a crash in the EIGRP process when making changes to the ip prefix-list configurations. Workarounds: None
CSCwc95886	Headline: BGP additional paths not advertised as expected when eBGP Peer Is configured in VPNv4 address family. Symptoms: BGP additional paths are not advertised to peers as expected. Workarounds: Remove eBGP neighbors from VPNv4 address family to advertise additional paths as expected.
CSCwc30665	Headline: IGMPv3 Leave from one receiver briefly affects receivers on other ports. Symptoms: While some receivers send IGMPv3 Leave for a multicast group, it results in other active receivers losing multicast traffic for a brief duration of time. Source and Receivers are in the same VLAN. Workarounds: If there are more than two groups sharing the same OIF and an IGMP Leave is received for one of the groups, then the drop will not be seen as the OIF is not deleted.
CSCuz51618	Headline: Memset, memcpy, strncpy causing overflow. Symptoms: A device can crash because of a stack overflow/corruption in the SNMPd process. Workarounds: None
CSCvq83799	Headline: Enhancement - CLI to specify Callhome Source interface. Symptoms: Enhancement request: Ability to specify source-interface with callhome config. Workarounds: None
CSCvt99338	Headline: BGP peer template is not removed in software and still seen in show ip bgp peer-template. Symptoms: Removing a BGP template from the configuration does not remove it in software. The BGP template in question will not be seen in the output of the show running-config command. However, it will still be present in software as seen with the show bgp peer-template command. Workarounds: Do not use BGP templates.
CSCvw48958	Headline: FEX HIF - Support disabling of auto-negotiation on optical 1G ports.

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

Cisco Confidential

Bug ID	Description
	Symptoms: Support disabling of auto-negotiation on 2232PP, 2248PQ and 2348UPQ FEX devices for optical 1G ports. Workarounds: None
CSCvw54690	Headline: VXLAN EVPN - BGP fails to import EVPN route when VNI is up. Symptoms: A flap of a VXLAN EVPN neighbor may cause the NVE peer to not come up due to the route not being installed in the uRIB. Workarounds: Reset BGP neighbor or clear the route may recover from the broken state using clear bgp all * orclear ip route *.
CSCvw60409	Headline: HSRP vmac is not cleared and remains as static entry after shutting down SVI. Symptoms: On Cisco Nexus 9000 switch running HSRP, when SVI is shut down on active HSRP switch, HSRP vmac is not cleared and remains as static entry. This may cause traffic disruption. Workarounds: Remove HSRP configurations from SVI and then shut down SVI. switch(config-if)# no hsrp 1 ipv4 switch(config-if)# no hsrp 1 ipv6
CSCvw68515	Headline: BGP-3-BFD_SES_ADD: error Failed to create too big mts msg - Multihop BFD is not installed. Symptoms: BFD session does not establish, and the following error message is seen: %BGP-3-BFD_SES_ADD: error Failed to create too big mts msg Workarounds: None
CSCvw75391	Headline: Cisco Nexus 9000 TRM L2/L3 mixed mode anchor DR does not form OILs after recovery from maintenance mode. Symptoms: OIL for Mroutes missing the VLANs where the receivers are present. Workarounds: Reload or restart BGP.
CSCvx07403	Headline: Some prefixes are not advertised to eBGP peer. Symptoms: Following symptoms are seen: • Prefixes are not advertised to eBGP neighbors. • eBGP peers have lower than default timers as well as a low value for 'advertisement-interval' ------- address-family ipv4 unicast advertisement-interval 1 ------- Workarounds: The clear ip bgp * soft command restores all prefixes that are advertised. Remove the advertisement-interval 1 configuration parameter.
CSCvx23049	Headline: Nexus 9000 clear ip bgp * failed to clear BGP routes after removing retain-route-target all. Symptoms: On VXLAN Multi-Site border gateway, route from newly added/removed tenant-vrf is not removed. Workarounds: Do not configure retain route-target all on VXLAN back-to-back BGW. Follow the VXLAN configuration guidelines.
CSCvx27433	Headline: BGP Core due to BMP configuration. Symptoms: After a migration to Cisco NX-OS Release 9.3(6), BGP crashes multiple times due to

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

Cisco Confidential

Bug ID	Description
	SIG 6 and triggers the HAP policy, leading to a reload of the switch. Workarounds: Disable BMP server configuration.
CSCvx38173	Headline: VM Mobility issues seen when inter-site connections between multisite flaps. Symptoms: Mobility issues seen when inter-site link between multisite flaps. Workarounds: Clear the stale MAC entries at Site A immediately after the inter-site link failure.
CSCvx56128	Headline: VRF stuck in delete is pending because BGP is not dropping the MTS_OPC_L3VM. Symptoms: After VRF gets deleted from router configuration, under rare circumstances, it can get stuck in a deletion state. This prevents the users from re-configuring the VRF and using it. Workarounds: Reload the box or use a different VRF name.
CSCvy09592	Headline: IPv6 BGP link-local neighbor does not come up after BGP neighbor and interface flapping. Symptoms: When the BGP ipv6 link-local neighbor is up, shut down the BGP neighbor and interface. Then bring up the interface. The bgp link-local neighbor does not come up. Workarounds: Flap the interface again to bring up the BGP neighbor or restart the BGP process.
CSCvy13764	Headline: BGP: RFC7854 BMP Peer RD is not set. Symptoms: Received BMP messages do not contain "Peer RD" for VRF monitored peers. Workarounds: None
CSCvy52393	Headline: Cisco Nexus 9000 reloads; reason unknown. Symptoms: Following are the symptoms: • The Cisco Nexus 9000 should have a version that has the fix for the bugs CSCvm44989 and CSCvu78592. • The Reload Reason should be the following: show logging onboard internal reset-reason Reset Reason for this card:Image Version : 9.3(7)Reset Reason (LCM): Unknown (0) at time Reset Reason (SW): Reset Requested by CLI command reload (9) at time Reset Reason (HW): Unknown (0) at time • The IOFPGA registers show this outputs: show logging onboard internal cardcl<Time of the crash>crdcl_get_board_reset_reason: reason:0x00000000<Time of the crash>IOFPGA POWER DEBUG = 83000004<Time of the crash>IOFPGA RESET CAUSE = 00000000 Workarounds: This is hardware/power related issue. Need to check power source and power supplies connections. If issue persists a hardware replacement might be required. Open a TAC case for review.
CSCwd03152	Headline: VLAN Mapping issue and STP inconsistency with single leg vPC. Symptoms: Cisco Nexus 9000 switches running on Cisco NX-OS Release 9.3(9) in vPC connecting to downstream access switch with single link. Switch is running VXLAN, and vPC port channels have PV mapping configuration. STP state of configured vPC port channel, even though port is in shut state, will be in forwarding state. The translated VLAN is in downstream access; VLAN will be in broken state due to wrong BPDUs being received. Workarounds: Enable both links from vPC primary and secondary towards access switch.
CSCvz14651	Headline: BGP outputs need to be aligned correctly when 4 Byte ASN is used. Symptoms: show bgp l2vpn evpn summary output is mis-aligned when 4 Byte ASN is used. Workarounds: None
CSCvz22694	Headline: Type 2 l2vpn evpn routes are not advertised to Multisite Peer under certain conditions. Symptoms: Two symptoms will be seen;1) Type 2 Routes that are supposed to be blocked by a route-map will be incorrectly advertised to BGW Peer2) Type 2 Routes that are supposed to be

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

Bug ID	Description
	advertised by a route-map permit statement, will NOT be advertised to multisite peer (incorrect behavior). Workarounds: None Clearing/restarting BGP might NOT fix the problemReload also will NOT fix this problemIf feasible, removing route-map applied on the BGP peer will fix this issue.
CSCvz40618	Headline: local-as configured on BGP neighbor switches to template local-as after reload. Symptoms: When the local-as is configured in a template inherited by the neighbor as well as configured in the neighbor, the local-as configured in the neighbor is used:router bgp 65000 address-family ipv4 unicast template peer test_template local-as 45000 no-prepend replace-as remove-private-as all address-family ipv4 unicast neighbor 1.1.1.2 inherit peer test_template remote-as 65001 local-as 65002 no-prepend replace-as no remove-private-as all address-family ipv4 unicastswitch# show ip bgp neighbors 1.1.1.2BGP neighbor is 1.1.1.2, remote AS 65001, local AS 65002, ebgp link, Peer index 3However, when the switch is reloaded, the local-as in the template is used but no change was made to the config:switch# show ip bgp neighbors 1.1.1.2BGP neighbor is 1.1.1.2, remote AS 65001, local AS 45000, ebgp link, Peer index 3 Workarounds: Remove and re-configure the local-as in the neighbor:switch(config-router)# neighbor 1.1.1.2switch(config-router-neighbor)# default local-as 65002switch(config-router-neighbor)# local-as 65002 no-prepend replace-as
CSCvz53721	Headline: VxLAN BGP EVPN - incorrect processing of RD vs origin_id on receiving side. Symptoms: Reflected BGP L2VPN EVPN prefixes are incorrectly processed causing RD and origin_id mismatch. Senders sends out BGP update containing multiple RD under one origin_id.This cause BGP best path algorithm results to choose wrong or suboptimal path due to router-id preference. Workarounds: None
CSCvz59009	Headline: Cisco Nexus 9000 - BGP next-hop filtering affect FIB table for Static route Symptoms: On Nexus 9000 series switches after static route have the next-hop denied under BGP next-hop filtering, the static route have a valid next-hop in RIB but not valid in FIB.As a side effect, a BGP neighbor learns via this static route, is not established, because route to NH considered as unreachable in kstack. As BGP use kstack, BGP cannot use this NH for establish TCP session to peer. Workarounds: Remove and add again the static route or use pinned static route
CSCvz67451	Headline: Bootflash lifetime usage threshold syslog has in correct usage value in show command Symptoms: The following syslog will appear when the switch reaches a lifetime usage value of 95% on the bootflash. PLATFORM-2-BOOTFLASH_LIFETIME_MAJOR: Bootflash lifetime usage crossed 95%. Collect 'show hardware internal bootflash log' and consult with product support team.When the recommended command is checked the output has been observed to have inaccurate usage percentages. These percentages make it difficult to determine if the syslog is correct and if the switch is seeing an issue. Workarounds: None
CSCvz75734	Headline: Cisco Nexus 9000 EVPN route installs incorrect/random next hop. Symptoms: evpn route imported into vrf with bogus next-hop on a VTEP causing traffic to black-hole. Workarounds: delete " soft-reconfiguration inbound" CLI from template and restart bgp process.
CSCvz89475	Headline: Cisco Nexus 9300-FX2/FX3 send untranslated packets via twice NAT when one HW entry is already installed. Symptoms: With twice nat configuration with pool and overload, packets with untranslated destination address (pool address as destination) are seen in out to in direction. Workarounds: Configuring " ip nat translation creation-delay 0" can help in this situation by

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

Bug ID	Description
	minimizing the time window for which untranslated packets are received. The problem can still be seen and hence not a foolproof workaround.
CSCvz99747	Headline: VLAN id configured, unable to generate auto RD error when applying VNI config. Symptoms: The following error is seen but the configuration is applied anyways:switch(config)# apply profile testMessage reported by command :: rd autoNo VLAN id configured, unable to generate auto RD Workarounds: None. The error can be ignored because it doesn't affect the switch operation.
CSCwa25046	Headline: BGP neighbor flapping when routes churn with soft-reconfig Symptoms: All bgp neighbor flap randomly Workarounds: remove soft-reconfig
CSCwa33163	Headline: show ip route route uptime refreshed for all next hops when one next hop goes down Symptoms: Show ip route route uptime is reset for all NHs when NH goes down Workarounds: None, this is cosmetic issue
CSCwa50172	Headline: oc bgp: afi-safis container is missing for bgp neighbor with by inherit a template Symptoms: When we request the l2vpn evpn neighbor state, using the query path as /network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/afi-safis/afi-safi/state/prefixes, the response returned has missing afi-safi's container corresponding to the neighbor that inherited the template. Workarounds: configure the address-family under neighbor, for example: neighbor 99.99.99.99 inherit peer POD update-source loopback0 address-family ipv4 unicast address-family ipv6 unicast address-family l2vpn evpn
CSCwa77148	Headline: OSPF neighbor name is not shown when name-server is configured with VRF Symptoms: OSPF neighbor ID is not resolved when name-server is configured under with use-vrf command.# show ip ospf neighbors OSPF Process ID 10 VRF default Total number of neighbors: 1 Neighbor ID Pri State Up Time Address Interface 192.168.1.1 1 FULL/ - 1d00h 10.1.1.2 Eth1/3 <====name should be shown on 192.168.1.1 Workarounds: configure name-server without use-vrf argument and make sure name server is reachable via default VRF.
CSCwa77878	Headline: Default MTU shown in running-config when non-default value configured under network-qos class-map Symptoms: When configuring non-default values (dpp, pause, etc) under class-map in network-qos policy-map, default MTU " mtu 1500" is shown in show running-config and not be deleted by " no mtu 1500". Default value should not be shown in show running-config. Workarounds: None. Note that this is just showing default value in running-config and no impact to switch functionality.
CSCwa92834	Headline: Enhancement to tweak the PLL value through non hidden cli Symptoms: Link flap between Nexus 93180 and Cat 9200 switch due to jitter tolerance in the signal. Workarounds: CLI command. contact TAC for details.
CSCwb11701	Headline: Cisco Nexus 9000: One or more VRF stuck in " Delete Holddown" due to BGP RNH route cleanup issue Symptoms: One or more VRF stuck in " Delete Holddown" because RNHs are not deleted`show bgp internal af vrf`L3VM down MTS drop pending : YesCleanup skip reason : RNH pending Also, one or more routes in BGP event-history is stuck trying to resolve RNH roughly every

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

Cisco Confidential

Bug ID	Description
	100ms:`show bgp event-history events`2022 Feb 14 07:59:52.546118: E_DEBUG bgp [32680]: RNH: Request needs to be retried for rnh 0.0.0.0/0 flags 0x06 not added (urib), suspending2022 Feb 14 07:59:52.439910: E_DEBUG bgp [32680]: RNH: Request needs to be retried for rnh 0.0.0.0/0 flags 0x06 not added (urib), suspending2022 Feb 14 07:59:52.339621: E_DEBUG bgp [32680]: RNH: Request needs to be retried for rnh 0.0.0.0/0 flags 0x06 not added (urib), suspending Workarounds: The tested workaround is to delete ALL stale or missing VRF under bgp via " no vrf NAME" where NAME should be replaced by every missing VRF
CSCwb22718	Headline: LACP HIF port is suspended causing traffic disruption. Symptoms: Traffic drops are seen on ingress for some interfaces that make part of FEX fabric port of Nexus 9000 parent switch. Workarounds: None
CSCwb41711	Headline: DHCP snooping source MAC address validation drops DHCP relay messages Symptoms: DHCP snooping enabled Nexus switch drops DHCP Discover messages generated by the DHCP relay agent device due to mismatched packet source MAC address and DHCP Client MAC Address field. Workarounds: disable DHCP snooping MAC address validation.no ip dhcp snooping verify mac-address
CSCwb64912	Headline: bgp can see traceback/crash with aggregate-address CLI in evpn setup Symptoms: BGP process may see traceback and potentially process crash2022 Jul 18 21:01:56.697 N9K-C9364D-GX2A-SPN-01 %BGP-3-ASSERT: bgp- [24765] ../routing-sw/routing/bgp/converged/bgp_attr_converged.c:182: Assertion `0' failed.2022 Jul 18 21:01:56.698 N9K-C9364D-GX2A-SPN-01 %BGP-3-ASSERT: bgp- [24765] -Traceback: bgp=0x55aefb018000 0x55aefb342c8f 0x55aefb342e80 0x55aefb4fee19 0x55aefb344c58 0x55aefb34505b 0x55aefb2cad5f 0x55aefb2f3e6a 0x55aefb2f92e0 0x55aefb4fc5a4 0x55aefb10dbd3 librsw_kstack.so=0x7f7bdb580000 librsw_kstack.so+0xb4* Workarounds: Do not use aggregate-address
CSCwc19848	Headline: OBFL no partitions mounted on eMMC device Symptoms: OBFL diagnostic failure was observed on Cisco Nexus 9000 (N9K-C9364C) following ISSU. %DEVICE_TEST-2-OBFL_FAIL: Module 1 has failed test OBFL 1 time on device OBFL due to error OBFL no partitions mounted on eMMC device - Unable to test. Workarounds: Reload the switch 2 times to repartition and reformat obfl.
CSCwc38530	Headline: BGP with MD5 authentication not forming between switches using non-default vrf with long name Symptoms: When trying to form BGP with MD5 authentication between two directly connected switches in VRF with 32-character name, BGP is not coming up. Workarounds: Workaround is as follows: • 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 Symptoms: ACLQoS errors output missing in TS detail and ACLQoS TS Workarounds: Collect missing output separately.
CSCwc43123	Headline: CLI CR failing with logging server configs Symptoms: If the current running config has non-default facility logging server 10.10.10.10 5 use-

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

Cisco Confidential

Bug ID	Description
	vrf default facility local1CR will fail with following in the candidate config which has default options logging server 10.10.10.10s witch# show config-replace log verifyOperation : Config-replace to user configCheckpoint file name : .replace_tmp_24763Scheme : tmpCfg-replace done By : adminCfg-replace mode : atomicVerbose : disabledStart Time : Tue, 21:30:53 12 Jul 2022Start Time UTC : Tue, 21:30:53 12 Jul 2022----------End Time : Tue, 21:31:09 12 Jul 2022End Time UTC : Tue, 21:31:09 12 Jul 2022Status : FailedVerification patch contains the following commands:----------!!Configuration To Be Added Missing in Running-config==========!logging server 10.10.10.10Undo Log----------End Time : Tue, 21:32:00 12 Jul 2022End Time UTC : Tue, 21:32:00 12 Jul 2022Status : Success Workarounds: To recover, configure using CLI so that default config parameters are as follows: programmedlogging server 10.10.10.10 5 use-vrf default facility local7
CSCwc43397	Headline: Memory leak in nginx process Symptoms: Nexus switch memory usage might be constantly increasing due to nginx process. <pre>PID NAME |TOTAL |TEXT |HEAP |STACK |DATA |MALLOC/MMAP |SHARED |READONLY |IO |20060 nginx_f | 415544 227664 218399 |30864 7532 432 |218712 218700 217532 | 216 128 35 | 1068 1032 301 | 748 196 79 | 163844 4 1 | 84 72 19 | 0|20098 nginx_f | 413796 225916 216739 |30864 7532 432 |216964 216952 215784 | 216 128 123 | 1068 1032 301 | 748 196 79 | 163844 4 1 | 84 72 19 | 0|PID NAME |TOTAL |TEXT |HEAP |STACK |DATA |MALLOC/MMAP |SHARED |READONLY |IO |20098 nginx_f | 450752 262816 253658 |30864 7484 403 |253920 253900 252732 | 216 128 123 | 1068 1032 301 | 748 196 79 | 163844 4 1 | 84 72 19 | 0|20060 nginx_f | 450760 262744 253586 |30864 7484 403 |253928 253828 252660 | 216 128 123 | 1068 1032 301 | 748 196 79 | 163844 4 1 | 84 72 19 | 0|%PLATFORM-2-MEMORY_ALERT: Memory Status Alert : CRITICAL. Usage 86% of Available Memory</pre> Workarounds: None
CSCwc44309	Headline: Cisco Nexus 9300 switch single NAT w/o AU breaks passive data FTP session flow after successful initial start Symptoms: Passive FTP session data transfer fails to finish. Workarounds: None
CSCwc48758	Headline: CoPP fails to apply, and no syslog is generated when PPF session fails Symptoms: Under some rare circumstances CoPP may fail to apply on system boot (PPF timeout). This caveat has been filed to track better handling for when this condition occurs. Workarounds: Use 'show copp status' to validate CoPP is applied
CSCwc56079	Headline: High PTP correction on -R line cards on 2 PTP GMs failover Symptoms: - On the Cisco Nexus 9000 fabric, high PTP correction is seen on -R-series based line cards on Nexus 9500 (more than ~600 ns) during PTP GM fail over with different GM ID. Workarounds: None
CSCwc59914	Headline: Unable to apply PACL when TCAM template is enabled Symptoms: 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: switch# show hardware access-list tcam region. Ingress PACL [ing-ifacl] size = 256switch# show system internal access-list globals ...----------

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

Bug ID	Description
	---------- INSTANCE 0 TCAM Region Information:---------- ----------Ingress:-------- Region TID Base Size Width ---------- ----------... Ingress PACL 1 0 256 1switch# show hardware access-list resource utilization slot 1=======INSTANCE 0x0---------- -- ACL Hardware Resource Utilization (Mod 1) ---------- ---------- Used Free Percent Utilization---------- Ingress PACL 2 254 0.78 Ingress PACL IPv4 0 0.00 Ingress PACL IPv6 0 0.00 Ingress PACL MAC 0 0.00 Ingress PACL ALL 2 0.78 Ingress PACL OTHER 0 0.00 Workarounds: Remove the TCAM template configuration and configure TCAM region using the " hardware access-list tcam region ing-ifacl 256" command.
CSCwc65941	Headline: Increasing input overruns on the management interface on Nexus 9000 Symptoms: Observed increasing in input overruns on management interface (mgmt0) on Cisco Nexus 9000 when receiving LLDP packets from catalyst (WS-C2960X-48T) switch. Workarounds: Disable the LLDP configurations on catalyst switch for the mgmt0 attached port.
CSCwc66335	Headline: Cisco Nexus 9000 - SRCTEP Peer Entry Missing in HW Symptoms: BUM traffic received on VTEP dropped with INFRA_ENCAP_SRC_TEP_MISS reason This is due to the Source VTEP entry for peer missing in hardware. The peer entry will be present in NVE & IPFIB though. Workarounds: None
CSCwc67943	Headline: Nexus 9000 TRM - SA-AD not being triggered from the Turn-around router Symptoms: Nexus 9000 TRM - SA-AD not being triggered from the Turn-around router. Workarounds: None
CSCwc70139	Headline: L2ACLredirect failures are not resulting in kernel panic Symptoms: L2ACLredirect failures are not resulting in kernel panic Workarounds: Apply the following EEM for force reload: event manager applet gold_l2acl override __L2ACLRedirect action 1 syslog priority emergencies msg L2ACL_test_failed_reloading action 2 reload force
CSCwc73361	Headline: MPLS Labels not being advertised to neighbor switches after reboot on Nexus 9336C. Symptoms: Network topology configured with Segment Routing + MPLS network for L3VPNS on 4 X Nexus 9336C switches (NX-OS mode). OSPF as the IGP and to advertise the MPLS labels. Labels are learnt once its configured. Once any one of the Nexus devices are rebooted, the label from the switch is no longer advertised by the switch that was rebooted to any other neighbor Nexus devices. The same occurs for any switch that is rebooted. OSPF database opaque external type 7 prefix is not generated or advertised to other neighbor switches by the switch which was rebooted. Workarounds: When a command is entered under the Segment Routing configuration section. For example: global block range or a prefix, something triggers the labels to be advertised via OSPF and the type 7 prefix is visible in the OSPF database and subsequently installed in the MPLS forwarding table of the remaining three switches. Workaround: Remove p2p config from loopback interface.
CSCwc74073	Headline: Copper interfaces in N9K-X9788TC-FX do not come up when using N9K-C9504-FM-G. Symptoms: None of the RJ45 interfaces of line card N9K-X9788TC-FX come up. Workarounds: None

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

Bug ID	Description
CSCwc78473	Headline: 9500 delaying sending BPDU's every 60 seconds. Symptoms: A Nexus 9500 switch might delay sending out spanning-tree BPDU's every 60 seconds. This issue is under investigation. Workarounds: None
CSCwc80086	Headline: Cisco Nexus 9000 sysmgr crashed due to incorrect core pattern in 7.0(3)I7(x) version result in LC/FM reload. Symptoms: 1.Cisco Nexus 9000 EOR with BCM linecard or N9K-C9508-FM will be crashed due to sysmgr:show coresVDC Module Instance Process-name PID Date(Year-Month-Day Time)---- ------ -------- --------------- -------- -------------------------1 2 1 sysmgr 6481 2022-08-09 16:58:271 24 1 sysmgr 6516 2022-08-19 06:30:111 24 1 sysmgr 6534 2022-08-20 04:58:482. System uptime is nearly two years.Kernel uptime is 810 day(s), 7 hour(s), 6 minute(s), 15 second(s)3. In worst case, OBFL will be failed after the crash and RMA needed.4) OBFL FError code ------------------> DIAG TEST FAIL(Failed to open)Total run count -------------> 1Last test execution time ----> Mon Aug 22 16:23:34 2022First test failure time -----> Mon Aug 22 16:23:34 2022Last test failure time ----> Mon Aug 22 16:23:34 2022Last test pass time ---------> n/aTotal failure count ---------> 1Consecutive failure count ---> 1Last failure reason ---------> Failed to open OBFL file (/mnt/plog/gold_file) for write.Next Execution time ---------> n/a4. These logs can be seen previous the line card reboots: %SYSMGR-SLOT1-3-BASIC_TRACE: bury_child: PID 15933 with message failed to write kernel trace to /var/sysmgr/tmp_logs/kernel-trace.6468. return value -1 . %SYSMGR-SLOT1-3-SYSMGR_CRASHED: Sysmgr (PID 6468) has terminated on receiving signal 6 %MODULE-2-MOD_DIAG_FAIL: Module 1 (Serial number: XXXXXXXXXXX) reported failure due to Service on line card had a hap-reset in device DEV_SYSMGR (device error 0x0) Workarounds: There is no workaround. Cisco NX-OS upgrade is required to avoid another line card/module reboot for the same reason.
CSCwc81130	Headline: Log reported that N9K-C92348GC's PSU went down and up in 1-3 sec Symptoms: Syslog reported that N9K-C92348GC's PSU went down and up in 1-3 sec Workarounds: This is a cosmetic error and PSU keeps providing power to the switch.
CSCwc81429	Headline: PHY ports stay linked up when peer is powered off Symptoms: On Cisco Nexus N9K-X9788TC2-FX, N9K-C93108TC2-FX platform, when the peer goes for a reload, on some occasions the link is not going Workarounds: None
CSCwc83656	Headline: stormcontrol interfaces may see intermittent flap Symptoms: GX2 Interfaces may see flap if sudden burst of traffic is seen across the interface Workarounds: errdisable recovery interval <>
CSCwc84291	Headline: KIM Process MTS Buffers Stuck Symptoms: - KIM Process has messages stuck in MTS queue - SAP no. 232 with recv_q stuck Workarounds: Reload the switch.
CSCwc86253	Headline: Notifications not generated for the path System/name Symptoms: 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. Workarounds: 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.

Bug ID	Description
CSCwc86514	Headline: ISIS: FAILED TO PARSE PROP bgpAsNum of class isisOverload with 4-Byte Autonomous System Numbers Symptoms: Cisco Nexus C93180YC-EX-2(config-router) # set-overload-bit on-startup wait-for bgp 66600 unsupported number format for uint16_t: 66600: FAILED TO PARSE PROP bgpAsNum of class isisOverload Workarounds: None
CSCwc87567	Headline: Cisco Nexus 9000: VXLAN Multisite vPC - w/ dci-advertise-pip tenant VRF CPU generated traffic still uses VIP. Symptoms: N9k: VXLAN Multisite vPC - with dci-advertise-pip configured CPU generated traffic within the tenant VRF still use the shared NVE source loopback VIP.Packets will be punted to CPU and seen in ethanalyzer on remote Bordergateway.ELAM reports UC_TENANT_MYTEP_BRIDGE_MISS and ROUTING_DISABLED.This is because the VIP is not a listed as an NVE peer on the remote Bordergateway, only the PIPs are advertised with " dci-advertise-pip" . Workarounds: None if you need both vPC and dci-advertise-pip configured.
CSCwc88702	Headline: Cisco Nexus 9000 syslog " Failed to open file: No such file or directory - securityd" -post upgrade to 9.3(9)+ Symptoms: Nexus 9k 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. Workarounds: NA - Log appears to be cosmetic
CSCwc89454	Headline: Cisco Nexus 9000 - NBR_FLOOD_WAR reported unexpectedly for OSPFv3 Symptoms:*Cisco Nexus 9000 series switch running 10.3(1) software release (so far issue was seen with this software release, but others are possibly also affected) * device runs ospfv3 and peers with few other switches * few times a day NBR_FLOOD_WAR syslog is reported for different LSA_IDs and neighbors Workarounds: None
CSCwc90986	Headline: Unable to config " ip tacacs source-interface" when " feature password encryption aes" is configured Symptoms: When " feature password encryption aes" is configured on the device, " ip tacacs source-interface" command couldn't be configured. Command is accepted but not reflected in configuration. Workarounds: Removing " feature password encryption aes" Removing " feature tacacs+" Configuring " feature tacacs+" and " ip tacacs source-interface"
CSCwc93774	Headline: Cisco Nexus 9000: Netflow configured under " vlan configuration" range takes longer than expected Symptoms: When configuring netflow under " vlan configuration" for large range (ex: 1-999) as below, the command takes 15 minutes to complete:vlan configuration 1-999 ip flow monitor flow_name inputfor the half range 1-500 the command takes 5 minutes Workarounds: None
CSCwc94630	Headline: Cisco Nexus 9000 - DHCPv6 IAPD Parse Fails due to Invalid Client ID Option Symptoms: Parsing of DHCPv6 IAPD options from a Request packet will fail due to invalid client ID option referenced. Workarounds: Disable option 19 or 20 on DHCPv6 ClientThis may not be possible depending on the client. Please reach out to your client vendor for further assistance.

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

Bug ID	Description
CSCwc97099	Headline: EIGRP is not logging error when wrong subnet configured or detected w/ cabling issue or defect Symptoms: EIGRP on NxOS does not generate a syslog message indicating a cabling issue or config issue on the ip addressing of a link as IOS-based platforms do. An example of IOS message that is missing from NxOS is below:Aug 31 18:00:00 GMT: %DUAL-6-NBRINFO: EIGRP-IPv4 1: Neighbor 10.2.1.1 (TenGigabitEthernet1/1) is blocked: not on common subnet (10.1.1.1/30) Workarounds: None
CSCwc97662	Headline: 40G RWX programming is incorrect, can lead to MAC under-run. Symptoms: Output errors seen in TX interface where the traffic profile is 100g -> 40gAlso you will see " TAHUSD_MAC_INTR_TX_UNDERRUN_MAC" via " show hardware internal tah event-history front-port X lane 1" Workarounds: None
CSCwc97953	Headline: Cisco Nexus 9000 Switch reloads due to SNMP process crashes after SNMP server reloads Symptoms: A Cisco Nexus 9000 switch suffers an unexpected reload due to the SNMP process crashes due to signal 11 - A core file was saved.+ Following logs could be seen upon device's reload:`show logging nvram`<snip>%$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service " snmpd" (PID 9687) hasn't caught signal 11 (core will be saved). <<<%$ VDC-1 %$ %USER-2-SYSTEM_MSG: <<%SNMPD-2-CRITICAL>> SNMP log critical: snmp_pss_open_url :pss2_open create failed for url sync:/mnt/pss/snmp.d/engine_db with syserr:File exists - snmpd%$ VDC-1 %$ %USER-2-SYSTEM_MSG: <<%SNMPD-2-CRITICAL>> SNMP log critical : pss_restore_snmp_engine_boots : SNMP Could not open engine_db PSS file. Exiting. - snmpd Workarounds: Currently none. Issue under investigation.
CSCwc98298	Headline: Cisco Nexus 9300 NAT randomly does not translate tcp flow packets Symptoms: Packets of random tcp flow may be send untranslated in in-out direction. Workarounds: None
CSCwc98328	Headline: %PORT-5-IF_DOWN_LINK_FAILURE - Link failure Link reset - not descriptive Symptoms: The following syslog messages are being seen in a Nexus9000 C93360YC-FX2 running 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. See bugid CSCub82340 for more details. Workarounds: None.
CSCwc98656	Headline: 3rd party Transceiver is not identified correctly Symptoms: Some 3rd party optics may report ACU instead of AOCEthernet1/49 transceiver is present type is SFP-H10GB-ACU10M name is FINISAR CORP. part number is FCBG110SD1C10 revision is A serial number is WZSXXXX nominal bitrate is 10300 MBit/sec cisco id is 3 cisco extended id number is 4 Workarounds: None
CSCwc99335	Headline: Nexus:: ospfv2/v3 :: fix unexpected LSA retransmissions Symptoms: Nexus switch may unexpectedly retransmit LSAs even before re-transmit timer expires. Workarounds: None
CSCwc99946	Headline: ePBR probe command issues – Cisco NX-OS Release 10.2.3 Symptoms: User is not able to configure EPBR service-level and service-endpoint probes via DCNM

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

Bug ID	Description
	Freeform configuration, with configuration not going through and/or configuration compliance failures. Workarounds: Manually configure the EPBR services and policies on the switch and turn off strict config compliance for the fabric.
CSCwd04388	Headline: DME consistency error seen with snmp-server engindId Symptoms: DME Consistency Error is observed when snmp-server engineID local is configured using lower case hexadecimal values as below.snmp-server engineID local 0a:0a:0a:0a:0a Workarounds: Apply snmp-server engineID local configuration using Upper case hexadecimal values as shown below.snmp-server engineID local 0A:0A:0A:0A:0A
CSCwd05450	Headline: PVLAN and port flap issue Symptoms: vPC member port on Secondary vPC peer get flapped once we associate/add/configure a Secondary PVLAN to the Primary PVLAN, along with the vPC member port configured as Promiscuous PVLAN port. Workarounds: None
CSCwd06720	Headline: Removing one object-group will cause statistics for the whole ACL to be disabled Symptoms: Removing one port object-group will cause the statistics for the whole ACL to be disabled. 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/xN9K1(config)# no object-group ip port DST_PORT1N9K1# 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] Workarounds: Remove entry from ACL for which the port object-group has been removed or not configured.
CSCwd11687	Headline: Cisco Nexus 9000/XXX -R ARP reply packets dropped in Cisco Nexus 9000 received if it is received from peer-link Symptoms: ARP resolution issue on devices connected to Cisco Nexus 9000 devices with -R line cards. Unicast ARP reply packet are not forwarded from Cisco Nexus 9000 device SVI to the host across the peer-link and i tis insteand redirected to CPU of vPC peer and dropped Workarounds: Shut and no shut vPC peer-link
CSCwd13471	Headline: SNMP trap does not send out to specific server Symptoms: With below snmp config, after reload, snmp trap only sent to X.X.X.2 and X.X.X.3, does not sent to X.X.X.1.snmp-server host X.X.X.1 traps version 2c public snmp-server host X.X.X.1 use-vrf managementsnmp-server host X.X.X.1 source-interface mgmt0snmp-server host X.X.X.2 traps version 2c public snmp-server host X.X.X.2 use-vrf managementsnmp-server host X.X.X.2 source-interface mgmt0snmp-server host X.X.X.3 traps version 2c public snmp-server host X.X.X.3 use-vrf managementsnmp-server host X.X.X.3 source-interface mgmt0 Workarounds: Remove existing config and reconfigure hosts after reload of device or snmp process restart.
CSCwd15262	Headline: Netconf crash during a rpc call Symptoms: The service netconf in a nexus device could fail after performing a RPC %SYSMGR-2-SERVICE_CRASHED: Service " netconf" (PID xxxx) hasn't caught signal 11 (core will be saved).This crash could leave the netconf process unestable show system internal sysmgr service name netconfService " netconf" (" netconf" , xxx): UUID = 0xXXX, PID = XXXX, SAP = XXXX State: SRV_STATE_CLEANING_UP [unstable] >>>>>This could produce when executing " copy running-config startup-config" , following message appears:?Configuration update aborted:

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

Bug ID	Description
	services in transient state, wait for the system to stabilize" Workarounds: none for the moment will update if any
CSCwd19176	Headline: Flex stats output broken for port channel subinterface Symptoms: Subinterface counters are 0 under " show interface counters" even after " hardware profile svi-and-si flex-stats-enable" has been configured. This affects port-channel subinterfaces.switch(config)# show run | i hardwarehardware profile svi-and-si flex-stats-enableswitch(config)# show interface counters | begin Po100----------Port InOctets InUcastPkts----------Po100 16305 5Po100.1101 0 0 Workarounds: No workaround is currently available.
CSCwd23382	Headline: Log reported that N9K-C9508 's PSU went down and up in 1-3 sec Symptoms: Cisco Nexus 9000 EOR PSU flap issue on 9.3.9 version2022 Aug 8 18:53:45 N9K-C9508 %PLATFORM-2-PS_REMOVE: Power supply 1 removed (Serial number ARTxxxxxxxx)2022 Aug 8 18:53:45 N9K-C9508 %PLATFORM-2-PS_CAPACITY_CHANGE: Power supply PS1 changed its capacity. possibly due to On/Off or power cable removal/insertion (Serial number ARTxxxxxxxx)2022 Aug 8 18:53:46 N9K-C9508 %PLATFORM-5-PS_FOUND: Power supply 1 found (Serial number ARTxxxxxxxx)2022 Aug 8 18:53:46 N9K-C9508 %PLATFORM-2-PS_OK: Power supply 1 ok (Serial number ARTxxxxxxxx)2022 Aug 8 18:53:46 N9K-C9508 %PLATFORM-5-PS_STATUS: Power Supply 1 current-status is PS_OK2022 Aug 8 18:53:46 N9K-C9508 %PLATFORM-2-PS_FANOK: Fan in Power supply 1 ok Workarounds: None
CSCwd23976	Headline: Nexus C9364C-GX - Golden EPLD upgrade times out and resets with Fatal Module Error Symptoms: A Cisco Nexus 9000 C9364C-GX Chassis may experience a reload following a Golden EPLD upgrade. If the EPLD has already been upgraded and is not necessary, performing the unnecessary golden upgrade results in the device timing out and reloading with a Fatal Module Error. N9K-C9364C-GX# install epld bootflash:[epld-image] module all golden...The switch will be reloaded at the end of the upgradeDo you want to continue (y/n) ? [n] yProceeding to upgrade Modules. Starting Module 1 EPLD UpgradeModule 1: MI FPGA [Programming]: 100.00% (# of # sectors)EPLD process seems to have exited unexpectedly 2700Unable to communicate with the EPLD ProcessReloading Supervisor Module 1...Last reset at [USECS] usecs after [DATE] Reason: Reset Requested due to Fatal Module Error System version: [IMAGE] Service: Workarounds: There is no workaround known at this time.
CSCwd27172	Headline: Unexpected reload after poap process crashed Symptoms: A device reloads leaving a poap core file:2022 Oct 11 13:00:32 switch %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service " poap" (PID 847) hasn't caught signal 11 (core will be saved). Workarounds: Reduce the bootfile-url length to be less than 128 characters.
CSCwd29257	Headline: IPv6 OSPF ECMP route does not show both route as best Symptoms: IPv6 OSPF ECMP route does not show both route with " *" as best, only one shows with " *" as best, so route from one neighbor is showing up with " *" and route from another neighbor is not. Before: =======N9508-TYB-CORE-1# sh clock ; sho ipv6 route 2001:fb1::/48 12:49:50.040 GMT Thu Sep 08 2022 Time source is NTP IPv6 Routing Table for VRF " default" '*' denotes best ucast next-hop '**' denotes best mcast next-hop '[x/y]' denotes [preference/metric] 2001:fb1::/48, ubest/mbest: 1/0 *via fe80::202:133:156:2, Vlan40, [110/20], 17w6d, ospfv3-1, type-1, tag 64549 via fe80::202:133:156:3, Vlan40, [110/20], 17w6d, ospfv3-1, type-1, tag 64549After clearing the route:==========N9508-TYB-CORE-1# show ipv6 route 2001:fb1::/48IPv6 Routing Table for VRF " default" '*' denotes best ucast next-hop '**' denotes best mcast next-hop '[x/y]' denotes [preference/metric] 2001:fb1::/48, ubest/mbest: 2/0 *via fe80::202:133:156:2, Vlan40, [110/20], 00:00:02, ospfv3-1, type-1, tag 64549 *via

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

Bug ID	Description
	fe80::202:133:156:3, Vlan40, [110/20], 00:00:02, ospfv3-1, type-1, tag 64549 Workarounds: clear the IPv6 route: #clear ipv6 route 2001:fb1::/48
CSCwd33062	Headline: PIM source-register loopback not honored for data encapsulated register packets Symptoms: PIM register packets generated by the DR with data encapsulated that are forwarded towards the RP are not honoring the configured source-register configuration, and instead using the local interface/DR where the traffic was originally received as the outer headerIssue is not seen for null register packets that do not contain encapsulated data.On RP, the incorrect packet can be seen under:-show ip pim internal event-history data-register-receiveConf:ip pim register-source loopback 8 (IP 10.10.200.101)Incorrect SRC:2022 Oct 17 19:37:24.299268: E_DEBUG pim [19811]: Received DATA Register from 10.25.0.3 for (10.25.0.10/32, 239.105.0.1/32) (pktlen 478)Correct SRC used from register-source IP:2022 Oct 17 19:44:42.316602: E_DEBUG pim [19811]: Received DATA Register from 10.10.200.101 for (10.25.0.10/32, 239.104.0.1/32) (pktlen 478)Null-register logs on RP always show correct SRC:2022 Oct 17 19:47:48.882281: E_DEBUG pim [19811]: Received NULL Register from 10.10.200.101 for (10.25.0.10/32, 239.104.0.1/32) (pktlen 20) Workarounds: Removal of the associated interface and register-source from configuration and reapplying it solves the issue.Data-encap register will then honor the register-source. Workaround does not survive the reload
CSCwd41354	Headline: grpcnxsdk works thread is not released properly Symptoms: The observation is that there exists an ongoing gnmi 5 second sample subscription for ?System/ptp-items/ephoper-items/pastcorrections-items/PtpEphCorrection-list'.This path is particularly special that the gNMI SET cannot happen when this path is been queried.-The repetitive queries every 5 second of this path triggered a bug, which prevented the query itself from finishing.-Then a following gNMI SET is blocked due to this unfinished query-The client script timeout and sent more SET requests, which could only pile up and used up the max 16 session limit. Workarounds: None
CSCwd42595	Headline: Output of show spanning-tree root no longer shows " This bridge is root" for non-vPC VLANs Symptoms: When upgrading to 9.3(10) the output of command: show spanning-tree root does not indicate if the bridge is root for non-vPC VLANs. In the example below: Agg-Sw2-N9k-382(config-if)# sh span root Root Hello Max FwdVlan Root ID Cost Time Age Dly Root Port---------- ---------- ------- ----- --- --- -------- ---------VLAN0001 8193 0023.04ee.be0a 0 2 20 15 This bridge is rootVLAN0050 4146 64f6.9d5a.ef43 1 2 20 15 port-channel30VLAN0100 8292 0023.04ee.be0a 0 2 20 15 This bridge is rootVLAN0200 4296 0023.04ee.be0a 0 2 20 15 VLAN0300 4396 0023.04ee.be0a 0 2 20 15 Additionally, you may see on both vPC Peers that the Bridge ID is using the local system-mac in place of the vPC system-mac. As well as seeing cost and port as 0 in the output of show spanning-tree vlan: Agg-Sw2-N9k-382(config-if)# sh spanning-tree vlan 200VLAN0200 Spanning tree enabled protocol rstp Root ID Priority 4296 Address 0023.04ee.be0a Cost 0 Port 0 () Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Bridge ID Priority 4296 (priority 4096 sys-id-ext 200) Address 0035.1a9d.bb23 Hello Time 2 sec Max Age 20 sec Forward Delay 15 secInterface Role Sts Cost Prio.Nbr Type---------- --- ---- --- --------- -------- --------------------------------Po2 Desg FWD 1 128.8193 P2p Eth1/34 Desg FWD 1 128.133 P2p Workarounds: None
CSCwd45291	Headline: router ospfv3 summary-address under address-family ipv6 unicast shows incomplete prefix value. Symptoms: After upgrading from Cisco NX-OS Release 7.0(3)I7(4) to 9.3(9), router ospfv3 summary-address under address-family ipv6 unicast shows incomplete prefix value router ospfv3 2

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

Bug ID	Description
	router-id 1.1.1.1 area 0.0.0.155 nssa no-summary default-information-originate log-adjacency-changes address-family ipv6 unicast area 0.0.0.155 range 2a00:f000:8000::/36 cost 300 area 0.0.0.155 range 2a00:f000:9000::/36 cost 300 area 0.0.0.155 default-cost 1000 summary-address 2000:f000:3000::/3 summary-address 2000:f000:3000::/4 summary-address 2000:f000:8000::/1sh cli his un summary-address 2000:f000:3000::/38 sh run ospfv3 summary-address 2000:f000:3000::/48 sh run ospfv3 summary-address 2000:f000:8000::/128 Workarounds: None
CSCwd45954	Headline: IOFPGA not displaying during EPLD upgrade Symptoms: ** After EPLD Upgrade from 7.0(3)I7(3) to 9.3.9, few 9788TC modules showing expected behavior whereas 5-6 9788 TC not upgraded correctly.** First issue 5-6 module is not upgraded epld.- Golden command ? upgrade only IO x02 to x04- Module all- Upgrade IO downgrade x04 to 0x2 and MI upgrade as expected x06.** Second issue is " show install all impact" showing both MI and IO FPGA in 7.0(3)I7(3). Whereas in 9.3.9 only MI FPGA seen. Workarounds: None
CSCwd46673	Headline: [NXOS] Cisco Nexus 9000 Back Pressure Correction to Prevent PSU Fan Reverse Direction Symptoms: Power supply exhaust fan was observed spinning in wrong direction in Cisco Nexus 9000 product. Workarounds: Increase PSU fan speed to prevent back-pressure. Workaround currently ongoing.
CSCwd46964	Headline: Issue with configuring BFD RX interval; the BFD session seems to always use 50 ms as TX interval Symptoms: When configuring BFD RX Interval, The BFD echo packets seem to be still transmitted at 50 ms which is the Minimum TX Interval. It seems like the desired RX interval which is configured in the config under the interface is not considered using the below command bfd echo-rx-interval 250 Workarounds: The workaround seems to use the below command to specify the BFD TX intervalbfd interval 250 min_rx 250 multiplier 3
CSCwd52666	Headline: BGP can crash when srte color attribute arrives on device with soft reconfig. Symptoms: BGP can crash when srte color attribute arrives on device with soft reconfig. Workarounds: None
CSCwd53084	Headline: Cisco Nexus 9000: SNMP does not return any value Symptoms: snmp get/walk to Cisco Nexus 9000 might stop working and returning empty values or note that OID does not exist even if OID should be present and populated on the system Example snmpwalk -v2c -c cisco123 10.48,73.150 1.3.6.1.4.1.9.9.82.1.12.2.1.3iso.3.6.1.4.1.9.9.82.1.12.2.1.3 = No Such Instance currently exists at this OID Workarounds: Restart SNMP process. However, issue might return after restart again and new restart is needed
CSCwd54117	Headline: Ipv6 ssh not getting denied for default port 22 Symptoms: Customer running 9.3(8) reported. Observed in 9.3(7) and in 10.2.4[M] as well during lab recreate No command in nexus cli syntax to change ssh port number, changing ssh port number available in bash mode.F241.04.11-C93180YC-EX-2(config-if)# ssh6 1450:7a50:0:1::27The authenticity of host '1450:7a50:0:1::27 (1450:7a50:0:1::27)' can't be established. RSA key fingerprint is SHA256:1/e08z24dBWqwqfaBtXUqfBaCTrpsO7eKYdM+Vyfpp0.Are you sure you want to continue connecting (yes/no)? yes Warning: Permanently added '1450:7a50:0:1::27' (RSA) to the list of known hosts. Outbound-ReKey for 1450:7a50:0:1::27:22Inbound-ReKey for 1450:7a50:0:1::27:22User Access VerificationPassword:F241.04.11-C93180YC-EX-2# conf Enter configuration commands, one per line. End with CNTL/Z. F241.04.11-C93180YC-EX-2(config)# run

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

Cisco Confidential

Bug ID	Description
	bashbash-4.3$ ssh 10.69.12.30 <<<<<<ipv4 ssh unsuccessful for default port 22kex_exchange_identification: Connection closed by remote hostbash-4.3$ ssh 10.69.12.30 -p 60066 <<<<<<ipv4 ssh successful for ssh port 60066The authenticity of host '[10.69.12.30]:60066 ([10.69.12.30]:60066)' can't be established. RSA key fingerprint is SHA256:1/e08z24dBWqwqfaBtXUqfBaCTrpsO7eKYdM+Vyfpp0.Are you sure you want to continue connecting (yes/no)? ^Cbash-4.3$ ssh 1450:7a50:0:1::27 <<<<<< ipv6 ssh successful for default port 22Outbound-ReKey for 1450:7a50:0:1::27:22Inbound-ReKey for 1450:7a50:0:1::27:22User Access VerificationPassword:bash-4.3$ ssh 1450:7a50:0:1::27 -p 60066 <<<<ipv6 ssh successful for port 60066 Outbound-ReKey for 1450:7a50:0:1::27:60066Inbound-ReKey for 1450:7a50:0:1::27:60066User Access VerificationPassword:bash-4.3$ Workarounds: None
CSCwd56801	Headline: difference between the running config and start-up config for MACSes Symptoms: there is a difference between the running config and start-up config for MACSec missed this command in startup-config :macsec keychain MACSEC_KEYCHAIN_1 policy system-default-macsec-policystartup-configinterface Ethernet1/1description 2p LABU32C101 E1/51 Remote-Leafmtu 9216no shutdownrunnig configinterface Ethernet1/1description 2p LABU32C101 E1/51 Remote-Leafmacsec keychain MACSEC_KEYCHAIN_1 policy system-default-macsec-policymtu 9216no shutdown+even after saved the copy r s , issue not resolved +issue does not appear on 9.3.9 and 9.3.10 Workarounds: None
CSCwd63552	Headline: There is mismatch between Scalability Doc and the threshold configured on the switch Symptoms: As per the Cisco Nexus 9000 Series NX-OS Verified Scalability Guide, Release 9.3(10): https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/scalability/guide-9310/cisco-nexus-9000-series-nx-os-verified-scalability-guide-9310.html. The switch supports 48000 STP instances however the devices trigger a log message when more than 14000 are in use %STP-2-VLAN_PORT_LIMIT_EXCEEDED: The number of vlan-port instances exceeded [Rapid-PVST mode] recommended limit of 14000 Workarounds: None
CSCwd66084	Headline: N9K-C9364C-GX Removing SFP-10G from one port will cause other ports in the same quad flap Symptoms: When the quad speed is 100G (when 100G optics are inserted in the port in the quad), Insert and then remove an SFP-10G will cause other ports which are in same quad flap. This issue only occurs when removing SFP-10G. The same issue is not seen when removing 40G SFP. Workarounds: None
CSCwd67745	Headline: Cisco Nexus 9000 - Switch crash with "tunnel-encryption" and "speed 10000" configured on the same interface. Symptoms: tahusd will crash resulting boot loop on switch startup when conditions are met. Workarounds: Do not manually set speed to 10000 or use QSA.
CSCwd47148	Headline: Smart licensing - Callhome HTTP proxy does not work when it is defined using IPv6 address. Symptoms: Communications with CSSM portal do not work when using IPv6 HTTP proxyDevice reports: %LICMGR-3-LOG_SMART_LIC_COMM_FAILED: (pid=xxxx) Communications failure with the Cisco Smart Software Manager (CSSM): Fail to send out Call Home HTTP message Workarounds: Instead of referencing the HTTP proxy using IPv6, use HOSTNAME and define static IPv6 host config. For example, Instead of:

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

Cisco Confidential

Bug ID	Description
	********** callhome ... transport http proxy server X:X::X:X port 8080 ********** use: ********** ipv6 host test.proxy.com X:X::X:X callhome ... transport http proxy server test.proxy.com port 8080 **********
CSCwe02448	Headline: Cisco N9K-C9808 – Fan Modules and Line Cards shut down due to Fans or PSUs not coming up. Symptoms: After completing NX-OS bootup, Fabric Modules and Line Cards are shut down due to multiple fans or power supplies not coming up. Workarounds: You can avoid this issue by upgrading NX-OS to Cisco NX-OS Release 10.3(2)F.
CSCwc89713	Headline: Few static BFD sessions are removed after reload. Symptoms: Few static BFD sessions are removed after reload. Workarounds: Default interface configuration and re-configure.

Device Hardware

The following tables list the Cisco Nexus 9000 Series hardware that Cisco NX-OS Release 10.3(2)F supports. For more information about the supported hardware, see the Hardware Installation Guide for your Cisco Nexus 9000 Series device.

Table 1. Cisco Nexus 9400 Switches

Product ID	Description
N9K-C9408	4-rack unit (RU) 8-slot LEM-based modular chassis switch, which is configurable with up to 128 200-Gigabit QSFP56 (256 100-Gigabit by breakout) ports or 64 400-Gigabit ports.

Note: N9K-C9400-SW-GX2A Sup card ports 2xSFP Eth10/1-2 are not supported in the current release [Cisco NX-OS Release 10.3(2)F].

Table 2. Cisco Nexus 9800 Switches

Product ID	Description
N9K-C9808	16-RU modular switch with slots for up to 8 line cards in addition to two supervisors, 8 fabric modules, 4 fan trays, and 3 power trays.

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

Table 3. Cisco Nexus 9800 Series Line Cards

Product ID	Description
N9K-X9836DM-A	Cisco Nexus 9800 QSFP line card (maximum of 8 line cards)

Table 4. Cisco Nexus 9800 Series Fabric Modules

Product ID	Description
N9K-C9808-FM-A	Cisco Nexus 9808 fabric module with maximum of 8 modules (7 fabric modules + 1 fabric module for redundancy)

Table 5. Cisco Nexus 9800 Supervisor Module

Product ID	Description	Quantity
N9K-C9800-SUP-A	Cisco Nexus 9800 Platform Supervisor Module	*

Table 6. Cisco Nexus 9800 Fans and Fan Trays

Product ID	Description	Quantity
N9K-C9808-FAN-A	Cisco Nexus 9800 8-slot chassis fan tray (1st Generation)	4

Table 7. Cisco Nexus 9800 Power Supplies

Product ID	Description	Quantity	Cisco Nexus Switches
NXK-HV6.3KW20A-A	Cisco Nexus 9800 6,300W 20A AC and HV Power Supply	9 (3 per tray)	Cisco Nexus 9808

Table 8. Cisco Nexus 9500 Switches

Product ID	Description
N9K-C9504	7.1-RU modular switch with slots for up to 4 line cards in addition to two supervisors, 2 system controllers, 3 to 6 fabric modules, 3 fan trays, and up to 4 power supplies.
N9K-C9508	13-RU modular switch with slots for up to 8 line cards in addition to two supervisors, 2 system controllers, 3 to 6 fabric modules, 3 fan trays, and up to 8 power supplies.
N9K-C9516	21-RU modular switch with slots for up to 16 line cards in addition to two supervisors, 2 system controllers, 3 to 6 fabric modules, 3 fan trays, and up to 10 power supplies.

Table 9. Cisco Nexus 9500 Cloud Scale Line Cards

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

Cisco Confidential

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 10. 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 11. 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

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

Product ID	Description	Minimum	Maximum
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 12. 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 13. 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 14. Cisco Nexus 9500 System Controller

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

Table 15. Cisco Nexus 9500 Fans and Fan Trays

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

Cisco Confidential

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 16. 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 17. 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 18. Cisco Nexus 9200 and 9300 Switches

Product ID	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.

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

Product ID	Description
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-C9348D-GX2A	48p 40/100/400-Gigabit QSFP-DD ports and 2p 1/10G/10G SFP+ ports
N9K-C9364D-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
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

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

Product ID	Description
N9K-C9348GC-FXP [1]	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 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.

Table 19. 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 Error! Reference source not found.[1] 93360YC-FX2
NXA-FAN-160CFM-PI	Fan module with port-side intake airflow (burgundy coloring)	3	9364C Error! Reference source not found.[1]Error! Reference source not found.**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.** 93360YC-FX2**Error! Reference source not found.Error! Reference source not found.**
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 Error! Reference source not found.[1] 93180YC-EX 93180YC-FX Error! Reference

[1] 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."

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

Product ID	Description	Quantity	Cisco Nexus Switches
			source not found.[1] 9348GC-FXP Error! Reference source not found.[1]
NXA-FAN-30CFM-F	Fan module with port-side exhaust airflow (blue coloring)	3	93108TC-EX 93108TC-FX Error! Reference source not found.[1] 93180YC-EX 93180YC-FX Error! Reference source not found.[1] 9348GC-FXP
NXA-FAN-35CFM-PE	Fan module with port-side exhaust airflow (blue coloring)	4 6	92300YC Error! Reference source not found.[1] 9332C Error! Reference source not found.[1] 93180YC-FX3S [2] 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 20. Cisco Nexus 9200 and 9300 Power Supplies

[1] For specific fan speeds see the Overview Section in 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.

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

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 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	2	92300YC

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

Product ID	Description	Quantity	Cisco Nexus Switches
	bidirectional airflow (white coloring)		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
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.

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 21. 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 22. 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.

Cisco Confidential

Table 23. 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 10.3(2)F supports the Nexus Dashboard Insights on Cisco Nexus 9200, 9300-EX, 9300-FX, 9300-FX2, 9300-FX3, 9400 and 9800 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 10.3(x). For information about an In Service Software Upgrade (ISSU), see the Cisco NX-OS ISSU Support Matrix.

Related Content

Document	Description
Cisco Nexus 9000 Series Switches	Cisco Nexus 9000 Series documentation
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 10.3(x)	Cisco Nexus 9000 Series Software Upgrade and Downgrade Guide
Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes, Release 10.3(2)	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.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	Licensing Information

When you downgrade from Cisco NX-OS Release 10.3(2)F to an earlier release, the features that use the ACI+NX-OS Essentials, Advantage, and add-on licenses or the Hardware Streaming Telemetry license

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

Cisco Confidential

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.