Cisco Nexus 9000 Series NX-OS Release Notes, Release 9.3(5)

This document describes the features, issues, and exceptions of Cisco NX-OS Release 9.3(5) software for use on Cisco Nexus 9000 Series switches.

For more information, see Related Content.

Date	Description
August 18, 2020	Added CSCvv25573 to Open Issues.
August 14, 2020	Updated FEX entry in the Software Features for the Cisco Nexus 9300-FX3 Platform Switches.
July 28, 2020	Updated the New Software Features section and Software Features for the Cisco Nexus 9300-FX3 Platform Switches.
July 21, 2020	Cisco NX-OS Release 9.3(5) became available.

Contents

New Software Features

Feature	Description
25G FCoE	Added support for 25G FCoE on Cisco Nexus 93180YC-FX, 93180YC-EX, and 93360YC-FX2 platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS FC-NPV and FCoE-NPV Configuration Guide, Release 9.3(x).
Alias Option for Sensor Path for Model-Driven Telemetry	Added the Alias Option for Sensor Path for Model-Driven Telemetry for Cisco Nexus 9000 Series switches and line cards. For more information, see the Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 9.3(x).
ARP Suppression with Reflective Relay	Supports the coexistence of these features for Cisco Nexus 9364C, 9300-EX, 9300-FX/FX2/FXP, and 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
Authentication through MAC Authentication Bypass Only	Added the ability to configure MAB as the default authentication method for all traffic on dot1x-enabled ports. Added support for Cisco Nexus 9000 Series switches and line cards. For more information, see the Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3(x).
BGP PIC Core	Support added for BGP Prefix Independent Convergence (PIC) Core. Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 9.3(x).
Breakout Support	Added 2x50G breakout support on Cisco Nexus 93600CD-GX platform switches. 4x10G, 4x25G, and 2x50G breakout support on the Cisco Nexus 9364C-GX switch on ports 1-24. For more information, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.3(x).
Cisco NX-OS Software Image Compaction	Added support for compacting the software image during copy operations. Added support for Cisco Nexus 9300 platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 9.3(x).
Cisco NX-OS Upgrade History	Added support for maintaining the software upgrade history across upgrades. Added support for Cisco Nexus 9000 Series switches and line cards. For more information, see the Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 9.3(x).

Feature	Description
Configuration Replace for FEX Interfaces	Added support for FEX interface configuration modifications. Added support for Cisco Nexus 9000 Series switches and line cards. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x).
Configuration Replace for Port Profiles	Added support for port profiles. Added support for Cisco Nexus 9000 Series switches and line cards. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x).
Configure Jobs Mode Option for Configuration Replace	Added support for the configure jobs mode. Added support for Cisco Nexus 9000 Series switches and line cards. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x).
Consistency Checker	ACL Consistency Checker: Added support on Cisco Nexus 93240YC-FX2, 93180YC-EX switches; Cisco Nexus 9500 platform switches with 9636Q-R, 9636C-R, 9636C-RX, and 96136YC-R line cards, and Cisco Nexus 9300-GX platform switches. Layer 2 Switchport Consistency Checker: Added support for all option in show consistency-checker l2 switchport interface command on Cisco Nexus 9200, 9300-EX, and 9300-FX platform switches and Cisco Nexus 9500 platform switches with -EX, -FX, and -R line cards. Multicast Consistency Checker: Verifies the programming consistency of these Layer 2 components IGMP snooping, MFDM, MFIBPI, MFIBPD, Hardware tables; and these Layer 3 components PIM, MRIB, IGMP snooping, MFDM, MFIBPI, MFIBPD and Hardware tables. SVI/subinterface Consistency Checker: Added support for Layer 3 setting of SVI and Sub-interfaces on Cisco Nexus 9200, 9300-EX, and 9300-FX platform switches and Cisco Nexus 9500 platform switches with -EX, and -FX line cards; and Cisco Nexus 9300-GX platform switches. Segment Routing Consistency Checker: Added support for the **show consistency-checker segment-routing mpls label** and **show consistency-checker segment-routing mpls** commands on Cisco Nexus 9200, 9300-EX, and 9300-FX platform switches and Cisco Nexus 9500 platform switches with -EX, and -FX line cards; and added support for Cisco Nexus 9316D-GX, 93600CD-GX, 9364C-GX devices. VLAN Consistency Checker: Added support for the interface option in the show consistency-checker stp-state vlan and show consistency-checker membership vlan commands on Cisco Nexus 9200, 9300-EX, and 9300-FX platform switches and Cisco Nexus 9500 platform switches with -EX, -FX, and -R line cards. For more information, see the Cisco Nexus 9000 Series NX-OS Troubleshooting Guide, Release 9.3(x).

Feature	Description
Device Led Conversion (DLC)	Added support for conversion of a traditional license to a Smart License. Supported for all Cisco Nexus 9000 Series switches and line cards. For more information, see the Cisco NX-OS Licensing Guide.
DHCPv6	Added support for DHCPv6 Option 79 (client link layer address) in DHCPv6 relayed packets for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3(x).
DSCP Wildcard Mask	Added support for creating an ACL that matches or filters traffic based on a DSCP bit mask. Added support for Cisco Nexus 9504 with 9464PX line card. For more information, see the Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide, Release 9.3(x).
Dual RD Support for Multi-Site	Enables route reorigination with dual route distinguishers (RDs). It is enabled automatically for Cisco Nexus 9332C, 9364C, 9300-EX, and 9300-FX/FX2/FXP platform switches and Cisco Nexus 9500 platform switches with -EX/FX line cards that have VXLAN EVPN Multi-Site enabled. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
Dual-Homed FEX	Added support for Cisco Nexus 9300-FX2 platform switches. Note: The following third-party equipment is not supported for dual-homed FEX for Cisco Nexus 9300-FX2/FX3 platform switches and straight-through FEX for Cisco Nexus 9300-FX3 platform switches: B22-HP, B22-IBM, B22-Dell, and B22-Fujitsu. For more information, see the Cisco Nexus 2000 Series NX-OS Fabric Extender Configuration Guide for Cisco Nexus 9000 Series Switches, Release 9.3(x).
Dynamic ACL	Added the ability to restrict access to the dot1x blocked list of MAB clients. This feature is supported for Cisco Nexus 9236C, 9336C-FX2, 93108TC-EX, and 93180YC-EX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3(x).
Enhanced ISSU	Added support for Cisco Nexus 92348GC-X, 9332C, 9364C, and 9300-FX/FX2/FXP switches. For more information, see the Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 9.3(x).

Feature	Description
Enhanced Policy-Based Routing (ePBR)	Provides traffic redirection and service chaining across the standalone and fabric topologies. It leverages the policy-based routing solution and achieves service chaining without adding additional headers. This feature allows you to define traffic selection, redirection of traffic to the service endpoint, and various fail-action mechanisms on the endpoints. It is supported on Cisco Nexus 9300-EX and 9300-FX/FX2 platform switches and Cisco Nexus 9500 platform switches with -EX/FX line cards. For more information, see the Cisco Nexus 9000 Series NX-OS ePBR Configuration Guide, Release 9.3(x).
ePBR Multi-Hop	Maintains the symmetry when fail-action bypass is configured for all of the services in the service chain. This feature is supported on Cisco Nexus 9300-EX and 9300-FX/FX2 platform switches and Cisco Nexus 9500 platform switches with -EX/FX line cards. For more information, see the Cisco Nexus 9000 Series NX-OS ePBR Configuration Guide, Release 9.3(x).
ePBR with Probes	ePBR creates SLA and Track objects based on the probe types configured on the policies and supports various probes and timers such as ICMP, TCP, UDP, DNS, HTTP. ePBR monitors the health of the end points by provisioning IP SLA probes and object tracks to track the IP SLA reachability when you apply the ePBR probe configuration. This feature is supported on Cisco Nexus 9300-EX and 9300-FX/FX2 platform switches and Cisco Nexus 9500 platform switches with -EX/FX line cards. For more information, see the Cisco Nexus 9000 Series NX-OS ePBR Configuration Guide, Release 9.3(x).
ePBR with User-Defined Probes	ePBR with User-Defined Probes-–Enables you to define tracks separately and assign the track ID to each service endpoint in ePBR. If no user-defined track is assigned to an endpoint, ePBR creates a track using the probe method for the endpoint. If no probe method is defined at the endpoint level, the probe method configured for the service level is used. This feature is supported on Cisco Nexus 9300-EX and 9300-FX/FX2 platform switches and Cisco Nexus 9500 platform switches with -EX/FX line cards. For more information, see the Cisco Nexus 9000 Series NX-OS ePBR Configuration Guide, Release 9.3(x).
ERSPAN destination	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x).
ERSPAN Type III	Added support for ERSPAN type III header for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x).

Feature	Description
Event Log Auto-Collection and Backup	Added updates to the auto-collection YAML file and additional options for the bloggerd log-snapshot command. Added support for Cisco Nexus 9000 Series switches and line cards. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x).
FC NPV	Added support for the Cisco Nexus 93360YC-FX2 switch. For more information, see Cisco Nexus 9000 Series NX-OS FC-NPV and FCoE-NPV Configuration Guide, Release 9.3(x).
FC/FCoE Switch Mode Features	Enhanced Device Alias: Added support for enhanced device alias mode. Enhanced Zoning: Added enhanced zoning capabilities that comply with the FC-GS-4 and FC-SW-3 standards. Both standards support the basic zoning and the enhanced zoning functionalities. Fabric-Device Management Interface (FDMI): Added the ability to manage devices such as Fibre Channel host bus adapters (HBAs) through in-band communications. This addition complements the existing Fibre Channel name server and management server functions. FC/FCoE Long Distance: Added support for long distance on the 32-Gbps Fibre Channel Inter-Switch Link (ISL). FCoE over vPC in Switch Mode: Added the ability to configure FCoE over vPCs to increase bandwidth and increased load-balancing to the Ethernet fabric on Cisco Nexus N9K-93180YC-FX devices. Smart Zoning: Adds the ability to implement hard zoning of large zones with fewer hardware resources. These features are supported on Cisco Nexus 93180YC-FX switches. For more information, see the Cisco Nexus 9000 Series NX-OS SAN Switching Configuration Guide, Release 9.3(x).
FCoE NPV	Added support for Cisco Nexus 93360YC-FX2 switches. For more information, see Cisco Nexus 9000 Series NX-OS FC-NPV and FCoE-NPV Configuration Guide, Release 9.3(x).
Flex Link	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide, Release 9.3(x).
gNMI Get/Set	Added support for the Get and Set Remote Procedure Call (RPC). Added support for Cisco Nexus 9000 Series switches and line cards. For more information, see the Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 9.3(x).

Feature	Description
iCAM Memory Monitoring	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS iCAM Configuration Guide, Release 9.3(x).
In-Service ACL Refresh for ITDv6	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Intelligent Traffic Director Configuration Guide, Release 9.3(x).
Interface Statistics	Added support for the Cisco Nexus 9000v. For more information, see the Cisco Nexus 9000v (9300v/9500v) Guide, Release 9.3(3).
IP Source Guard (IPSG)	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3(x).
IPv6 Egress ACL	Added support for Cisco Nexus 9504 and 9508 platform switches with -R and -RX line cards. For more information, see the Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3(x).
IPv6 First Hop Security (FHS)	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3(x).
IPv6 Flow Label Hashing	Added support for additional options such as IPv6 flow and TTL for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.3(x).
IPv6 MLD Snooping	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 9.3(x).
ISSU for uRPF	Added support for standard ISSU on Cisco Nexus 9300-EX and 9300-FX/FX2/FXP platform switches configured with uRPF. For more information, see the Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 9.3(x).
ITD	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Intelligent Traffic Director Configuration Guide, Release 9.3(x).

Feature	Description
ITD Destination NAT	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Intelligent Traffic Director Configuration Guide, Release 9.3(x).
ITD Fail Action Node with Include ACL	Added support for Include ACL with weighted fail action node-per-bucket and added new least-bit and mask position support for Include ACL. Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Intelligent Traffic Director Configuration Guide, Release 9.3(x).
ITD with User-Defined Probes	Added support for user-defined track objects (system health monitoring). Added support for Cisco Nexus 93108TC-EX and 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Intelligent Traffic Director Configuration Guide, Release 9.3(x).
ITDv6	Added support for Cisco Nexus 9300-GX platform switches and Cisco Nexus 9500 platform switches with 97160YC-EX and 9732C-FX line cards. For more information, see the Cisco Nexus 9000 Series NX-OS Intelligent Traffic Director Configuration Guide, Release 9.3(x).
Layer 3 Tenant Routed Multicast (TRM)	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
MACsec	Added support for Cisco Nexus 9500 platform switches with 9732C-FX and 9788TC-FX line cards. For more information, see the Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3(x).
MacSecPortLoopback Test	Added support for the bootup diagnostic test MacSecPortLoopback for Cisco Nexus 9504, 9508 and 9516 with 9736C-FX and 9736Q-FX line cards. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x).
MLD Snooping	Added support for 9300-GX platform switches and 9500 platform switches with 9400 and 9600 line cards. For more information, see the Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 9.3(x).
Modify Format of Repeated Syslog Messages	Added support for an updated indicator in repeated syslog messages. Added support for Cisco Nexus 9000 Series switches and line cards. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x).

Feature	Description
MPLS QoS	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Label Switching Configuration Guide, Release 9.3(x).
MPLS Stripping	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Label Switching Configuration Guide, Release 9.3(x).
Multicast Service Reflection	Enables you to translate externally received multicast destination addresses to addresses that conform to your organization's internal addressing policy. This feature is supported on Cisco Nexus 9300-EX and 9300-FX/FX2/FXP platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 9.3(x).
Multiple LLDP Neighbors per Physical Interface	Added support for up to three LLDP neighbors per interface. Added support for LLDP on interface port channels. Added support for Cisco Nexus 9000 Series switches and line cards. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x).
Multiple VRFs for Tunnel Decapsulation	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.3(x).
NAT	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.3(x).
NDcPP: OCSP for Syslog	Added OCSP support for syslog servers. This feature is supported on all Cisco Nexus 9000 Series switches and line cards. For more information, see the Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3(x).
NETCONF OpenConfig Notifications	Added support for NETCONF OpenConfig Notifications. Added support for Cisco Nexus 9200, 9300-EX, 9300-FX/FX2/FXP, 9300-GX, and 9500 with 9400, 9700-EX, and 9700-FX line cards. For more information, see the Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 9.3(x).
NETCONF/gRPC	Added support for NETCONF/gRPC. Added support for Cisco Nexus 9200, 9300-EX, 9300-FX/FX2/FXP, 9300-GX, and 9500 with 9400, 9700-EX, and 9700-FX line cards. For more information, see the Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 9.3(x).

Feature	Description
NX-API Idle Timeout-Enables	Enables you to configure the amount of time before an idle NX-API session is invalidated. For more information, see the Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 9.3(x).
NX-API REST Data Paths	See the "New and Changed Information" section of the Cisco Nexus 3000 and 9000 Series NX-API REST User Guide and API Reference for a detailed list of the updates.
OpenConfig Model Additions	Added updates for the OpenConfig YANG data modeling language. For more information, see the Cisco Nexus OpenConfig YANG Reference for examples of configuring and retrieving state data.
Optics Support	Added support for 10G BASE-T SFP+ on Cisco Nexus 93180YC-EX, 93180YC-FX, 93240YC-FX2, and 93360YC-FX2 switches. For more information, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.3(x).
PACL Redirects	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3(x).
PFC Watchdog Interval	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide, Release 9.3(x).
PIM6 for SVI	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 9.3(x).
Policy-Based Routing (PBR)	Added support for PBR on Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 9.3(x).
Private VLANs (PVLANs)	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide, Release 9.3(x).
Proportional Multipath for VNF for Segment Routing	Added the ability to advertise the VNF of a service network in the EVPN address family. This feature is supported on Cisco Nexus 9300-EX, 9300-FX/FX2, 9300-GX, and 9500 switches with 9700-EX, and 9700-FX line cards. For more information, see the Cisco Nexus 9000 Series NX-OS Label Switching Configuration Guide, Release 9.3(x).

Feature	Description
Proportional Multipath for VNF for VXLAN	Introduced the following enhancements for Cisco Nexus 9364C, 9300-EX, and 9300-FX/FX2 platform switches: • Added the ability to have only eBGP or iBGP filter the ECMP paths, rather than using mixed paths. • Added the maximum-paths local *number* command, which allows multiple local paths to be chosen as the BGP best path. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
PTP and Timestamp Tagging (TTAG)	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x).
PTP Event Notifications	Added support for configuring event-based notifications for PTP error scenarios. This feature is supported on: • Cisco Nexus 92348GC-X, 9332C, 9364C, 9300-EX, 9300-FX/FX2/FXP, and 9300-GX platform switches. • Cisco Nexus 9500 platform switches with 97160YC-EX, 9732C-EX, 9732C-FX, 9736C-EX, 9736C-FX, and 9788TC-FX line cards. • Cisco Nexus 9504 and 9508 platform switches with 9636C-R, 9636C-RX, and 9636Q-R line cards. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x).
PTP Monitoring	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x).
Python 3 on NX-OS	Added support for all Cisco Nexus 9000 Series switches and line cards. For more information, see the Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 9.3(x).
Q-in-VNI	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
QinQ-QinVNI	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).

Feature	Description
Seamless Integration of EVPN (TRM) with MVPN (Draft Rosen)	Enables packets to be handed off between a VXLAN network (TRM or TRM Multi-Site) and an MVPN network. A Cisco Nexus 9504 or 9508 platform switch with an 9636C-RX line card with VXLAN TRM and MVPN enabled can serve as a handoff node. This central node performs the necessary packet forwarding, encapsulation, and decapsulation to send the traffic to the respective receivers. It is the PE for the MVPN network and the VTEP for the VXLAN network. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
Seamless Integration of EVPN with L3VPN (MPLS SR)	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
Secure VXLAN EVPN Multi-Site using CloudSec	Ensures data security and data integrity for VXLAN-based Multi-Site fabrics. Using the cryptographic machinery of IEEE MACsec for UDP packets, this feature provides a secure tunnel between authorized VXLAN EVPN endpoints. It is supported for Cisco Nexus 9300-FX2 platform switches only. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
Segment Routing MPLS	Added support for Layer 2 EVPN on Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Label Switching Configuration Guide, Release 9.3(x).
Selective Q-in-Q with Multiple Provider VLANs	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.3(x).
Selective Q-in-VNI	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
Selective Q-in-VNI + Advertise PIP on a VTEP	Supports the advertise-pip command with selective Q-in-VNI on a VTEP. This feature is supported for Cisco Nexus 9300-EX, 9300-FX/FX2/FXP, and 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
Selective Q-in-VNI and VXLAN VLAN on Same Port	Supports selective Q-in-VNI and VXLAN VLANs on the same port. By adding the vlan *vlan-range* option to the system dot1q-tunnel transit command, you can specify the provider VLANs and allow other VLANs to be used for regular VXLAN traffic. This feature is supported for Cisco Nexus 9300-EX, 9300-FX/FX2/FXP, and 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).

Feature	Description
Selective Q-in-VNI with Multiple Provider VLANs	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
SPAN Truncation	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x).
SRv6 Static Per-Prefix TE	Added the ability to advertise multiple prefixes as a part of the same VRF through the route map. This feature is supported on Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Label Switching Configuration Guide, Release 9.3(x).
SRv6 Traffic Engineering	Introduced this feature for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS SRv6 Configuration Guide, Release 9.3(x).
Standard ISSU with FC/FCoE	Added support for Cisco Nexus 93180YC-FX and 93360YC-FX2 switches. For more information, see the Cisco Nexus 9000 Series NX-OS FC-NPV and FCoE-NPV Configuration Guide, Release 9.3(x).
SVI and Subinterface Ingress/Egress Unicast Counters	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.3(x).
Syslog for Exceeding Logging Message Size Threshold	Added support for logging message files to a location that is persistent across system reloads. Added support for all Cisco Nexus 9000 Series switches and line cards. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x).
Time-to-Live for ECMP Hashing	Added support for additional options such as UDF and TTL for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.3(x).
Type-6 Encryption of MACsec Keys	Added support for all Cisco Nexus 9000 Series switches and line cards that support MACsec. For more information, see the Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3(x).

Feature	Description
UDP for IP Helper Address	Added the ability to enable route configuration to relay broadcasts destined for all UDP ports, except DHCPv4 port numbers 67 and 68. This feature is supported on Cisco Nexus 9200, 9332C, 9364C, 9300-EX, 9300-FX/FX2/FXP platform switches, and Cisco Nexus 9500 platform switches with -EX/FX line cards. For more information, see the Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3(x).
Unidirectional Ethernet (UDE)	Added support for Cisco Nexus 9500 platform switches with 97160YC-EX line cards. For more information, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.3(x).
vPC Fabric Peering	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
VXLAN EVPN Loop Detection and Mitigation	Detects Layer 2 loops in a single VXLAN EVPN fabric or a Multi-Site environment. This feature operates at the port/VLAN level and disables the VLAN(s) on each port where a loop is detected. In this way, it ensures that the network remains up and available. This feature is supported for Cisco Nexus 9332C, 9364C, 9300-EX, 9300-FX/FX2/FXP, and 9300-GX platform switches and Cisco Nexus 9500 platform switches with -EX/FX line cards. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
VXLAN EVPN Multi-Site	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
VXLAN EVPN with Downstream VNI	Provides the following solutions for Cisco Nexus 9332C, 9364C, 9300-EX, and 9300-FX/FX2/FXP platform switches, Cisco Nexus 9500 platform switches with -EX/FX line cards. • Enables asymmetric VNI communication across nodes in a VXLAN EVPN network • Provides customers access to a common shared service outside of their domain (tenant VRF) • Supports communication between isolated VXLAN EVPN sites that have different sets of VNIs For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).

Feature	Description
VXLAN over Parent Interface that Carries Subinterfaces	Adds the ability for subinterfaces on VXLAN uplinks to carry non-VXLAN L3 IP traffic for Cisco Nexus 9332C, 9364C, 9300-EX, 9300-FX/FX2/FXP, and 9300-GX platform switches and Cisco Nexus 9500 platform switches with -EX/FX line cards. This feature is supported for VXLAN flood and learn and VXLAN EVPN, VXLAN EVPN Multi-Site, and DCI. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
VXLAN Static Tunnels	Added support for Cisco Nexus 9300-GX platform switches. In Cisco NX-OS Release 9.3(5), this feature allows the Cisco Nexus switch to send packets to the hosts or other switches over the tunnel. In Cisco NX-OS Releases 9.3(3) and 9.3(4), VXLAN static tunnels support communication only from the local host to the remote host. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
YANG Support for Multiple Keys	YANG Support for Multiple Keys added. Supported for all Cisco Nexus 9000 Series switches and line cards. For more information, see the Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 9.3(x).

Software Features for the Cisco Nexus 9300-FX3 Platform Switches

Feature	Description
FEX	• 802.1X • Dual-homed FEX • Straight-through FEX Note: The following third-party equipment is not supported for dual-homed FEX for Cisco Nexus 9300-FX2/FX3 platform switches and straight-through FEX for Cisco Nexus 9300-FX3 platform switches: B22-HP, B22-IBM, B22-Dell, and B22-Fujitsu. For more information, see the Cisco Nexus 2000 Series NX-OS Fabric Extender Configuration Guide for Cisco Nexus 9000 Series Switches, Release 9.3(x).
Fundamentals	• Erase configuration • USB support for POAP For more information, see the Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide, Release 9.3(x).
iCAM	• iCAM Scale Monitoring For more information, see the Cisco Nexus 9000 Series NX-OS iCAM Configuration Guide, Release 9.3(x).

Feature	Description

Interfaces	• 802.1Q Tunnel Port
	• Autonegotiation on native 25G ports
	• BFD Multihop
	• ECMP load balancing
	• ECMP resilient hashing
	• ECMP symmetric hashing
	• EtherType for Q-in-Q
	• FEC information
	• GRE inner headers
	• GTP Tunnel Load Balancing
	• Interface port channel
	• IP event dampening
	• IP load sharing
	• IP TCP MSS
	• IP tunnels
	• IPv6 flow label
	• LACP System MAC
	• Link debounce time
	• Management Interface Configurable MTU
	• Multiple IP-in-IP/GRE tunnel interfaces
	• Multiple VRF Support on Tunnel Decap
	• MTU Configuration on Interfaces in Switch Profiles
	• Port-channel symmetric hashing
	• Selective Q-in-Q with multiple provider VLANs
	• SVI and Subinterface Ingress/Egress Unicast Counters
	• TCP aware NAT
	• vPCs
	  ○ Dual vPCs
	  ○ vPC non-dis role change
	  ○ vPC Object Tracking
	  ○ vPC Peer Gateway
	  ○ vPC Peer Switch
	  ○ vPC Role Preempt (ND - no traffic loss on STP root switch)

Feature	Description
ITD	• In-Service ACL Refresh for ITDv6 • ITD Destination NAT • ITD Fail Action Node with Include ACL • ITD with User-Defined Probes • ITDv6
Label Switching	• Ingress and Egress Label Stats with Stats Knob • Layer2 EVPN over Segment Routing MPLS • Layer3 VPN over Segment Routing • Local label allocation • MPLS Adjacency Statistics • MPLS QoS • MPLS Queuing • MPLS stripping with VLAN tagging • NetFlow for MPLS • Port Channel and ECMP Load balancing based on MPLS Label Information • Segment routing • sFlow • sFlow collector over segment routing • vPC-based multihoming For more information, see the Cisco Nexus 9000 Series NX-OS Label Switching Configuration Guide, Release 9.3(x).
Layer 2 Switching	• Flex Link • PVLANs • PVLANs over vPCs and port channels • Reflective Relay • STP Extensions • SVI • Traffic storm control For more information, see the Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide, Release 9.3(x).

Feature	Description
Licensing	• Device Led Conversion (DLC) • Honor mode syslog • Smart software licensing For more information, see the Cisco NX-OS Licensing Guide.
Multicast Routing	• IPv6 MLD snooping • MLD snooping • Multicast on GRE tunnels • Network Load Balancing • PIM and PIM6 • PIM6 for SVI • PIM BiDir For more information, see the Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 9.3(x).

Feature	Description

QoS	• Classification/Marking
	  ○ ACL Classification
	  ○ Bank (MAC level)
	  ○ COS
	  ○ DSCP
	  ○ Label Sharing
	  ○ MAC
	  ○ No-DROP
	  ○ Precedence
	  ○ QoS-grp
	  ○ ROCE/RTP
	  ○ Set action/MARKING
	  ○ TCAM Carving
	• Policer
	  ○ Egress Policer
	  ○ Ingress Policer
	  ○ Policer - 1R2C
	  ○ Policer - 2R3C
	• Queuing
	  ○ 4-Q and 8-Q policy support
	  ○ AFD
	  ○ Bandwidth (Percentage/Remaining Percent)
	  ○ Congestion control - ECN
	  ○ Congestion control - WRED
	  ○ ETRAP
	  ○ Forward NON-ECN
	  ○ Ingress Queueing
	  ○ Interface Level Queuing
	  ○ Micro-Burst Monitoring
	  ○ Queue Limits - Dynamic (0 to 10 alpha)
	  ○ Queue Limits - Static
	  ○ Shaper - bps/gbps/kbps/mbps/pps
	  ○ Strict Priority (Level from 1 to 8)

Feature	Description
Programmability	• Ansible 2.4 • BASH • Cloud Scale Telemetry • Direct Streaming from DME to Native YANG • Docker Containers • Flow Monitor for VRF Filtering • gRPC • Guest Shell • Model-Driven Telemetry • Native Data Source • NETCONF RFC 6241 • NX-API CLI • NX-API Client Authentication • NX-API • NX-SDK • OpenConfig YANG • Perl Modules • Puppet • Salt Stack • Streaming Syslog and Filtered Syslog • Streaming of YANG Models • Streaming Telemetry • Synchronization • Telemetry gNMI OpenConfig • Telemetry Multi-Threading For more information, see the Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 9.3(x).

Feature	Description

Security	• ACLs
	  ○ ACL log Rate Limits
	  ○ ACL TCAM Regions
	  ○ ACL with UDF
	  ○ LOU
	  ○ MAC ACL
	  ○ MGMT ACL
	  ○ PACL
	  ○ RACL
	  ○ VACL
	• CoPP
	• DHCPv4/v6
	• First-Hop Security
	• IP ACL - object groups
	• IPv6 First-Hop Security - IPv6 RA Guard
	• IPv6 wildcard masks
	• MACsec
	• MACsec EAPOL
	• Option 82 String Identifiers
	• SSH
	• uRPF
	For more information, see the Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3(x).

Software Upgrade	• Optionality • vPC topology For more information, see the Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 9.3(x).

Feature	Description

System Management	• ASIC Register Health Check
	• Configuration Replace
	• DCBX/DCBXP
	• EEM
	• Extended Event Log Storage
	• FEX ports as SPAN sources in the ingress direction
	• LLDP
	• MIBs
	• NetFlow
	• Online diagnostics
	• PTP, PTP Offload
	• SNMP
	• System message logging
	• Syslog messages - link level pause frames
	• Timestamp Tagging (TTAG)
	• SPAN and ERSPAN
	  ○ SPAN
	  ○ ERSPAN (Type II and Type III, RFC-compliant header 3 option)
	  ○ ERSPAN destination
	  ○ SPAN/ERSPAN ACL
	  ○ SPAN/ERSPAN UDF support
	  ○ SPAN/ERSPAN Rate Limits
	  ○ SPAN + sFlow
	• SyncE - Support for ITU-compliant precision frequency over Ethernet ports and the PHY-level frequency distribution of known common precision frequency references.
	NOTE: GNSS and GPS are not supported on the Cisco Nexus 93180YC-FX3S switch for Cisco NX-OS Release 9.3(5).
	• Telecom Profile G.8275.1 and Telecom Profile G.8273.2 - Support for ITU-T Telecom Profiles for PTP as defined in the ITU-T recommendation.
	NOTE: Time of Day and PTP GM are not supported on the Cisco Nexus 93180YC-FX3S switch for Cisco NX-OS Release 9.3(5).
	For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x).

Feature	Description
Troubleshooting	• ACL Consistency Checker • Multicast Consistency Checker • Optimized Memory Utilization • Slow Drain Detection and Congestion Isolation • VXLAN Consistency Checker For more information, see the Cisco Nexus 9000 Series NX-OS Troubleshooting Guide, Release 9.3(x).

Feature	Description
Unicast Routing	• 64-way ECMP • ACL Logging • ACL statistics • ARP / GRAT ARP / Proxy ARP • BFD support for both IPv4 and IPv6 • BGP (VRF Aware) • BGP Fast Failover • BGP Next-Hop Address Tracking • BGP scan timer, & Best path algorithm • Bidirectional Flow Detection (BFD) for ipv4 and v6 Static routes • Default Interface Configuration • DHCP • DHCP Relay • Duplicate Address Detection • Dynamic Port Breakout • ECMP Routing and Port-Channel Load-Balancing Hash • EIGRP (IPv4 and IPv6 - VRF Aware) • Enable/disable fast External Fallover • Fast reboot • FIB Dest MISS statistics • Flexible ACL Carving • Generic Routing Encapsulation (GRE) Tunneling • Graceful Restart Helper • HA & Fast Convergence • Hot-Standby Router Protocol (HSRP) for IPv6, including link-layer address as well as global IPv6 address support • Ingress/Egress ACL • Internet Control Message Protocol (ICMPv6) • IPv6 RACLs • IPv6 stateless address autoconfiguration • ISIS - VRF Aware • Low Memory Handling • Neighbor discovery • OSPF HA & Fast Convergence

Feature	Description
VXLAN	• BGP EVPN filtering • IPv6 in the underlay • Layer 3 Tenant Routed Multicast (TRM) • MultiAuth with CoA • Nested VXLAN (Host Overlay over Network Overlay) • NGOAM • PIM BiDir • Port VLAN routing • Proportional Multipath for VNF • PVLANs with VXLAN • Q-in-VNI • QinQ-QinVNI • RP Everywhere • Sampled Flow Export • Seamless Integration of EVPN with L3VPN (MPLS SR) • Selective Q-in-VNI • Tenant Routed Multicast (TRM) • TRM with Multi-Site with External Connectivity on BGW • TRM with Multi-Site • TRM with vPC border leafs • VLAN-mapping switching • vPC Fabric Peering • VXLAN BGP EVPN • VXLAN BiDir • VXLAN Bud Node • VXLAN Cross Connect • VXLAN DHCP Relay • VXLAN EVPN Multi-Site • VXLAN Flood and Learn • VXLAN Multi-Site with vPC • VXLAN QoS • VXLAN Static Tunnels • VXLAN Tunnel Egress QoS Policy

New Hardware Features

Feature	Description
Cisco Nexus 93180YC-FX3S	The Cisco Nexus 93180YC-FX3S switch (93180YC-FX3S) is a 1-rack unit (RU), fixed-port switch designed for deployment in data centers. This switch has the following ports: • 48 x 1/10/25-Gbps fiber ports and 6 x 40/100-Gbps QSFP28 ports. • Due to hardware limitation native FC on 93180YC-FX3S is not supported (although the LS 1800 FX3 ASIC is FC capable). • One management port (one 10/100/1000BASE-T port) • One console port (RS-232) • One USB port For more information, see the Cisco Nexus 93180YC-FX3S NX-OS Mode Switch Hardware Installation Guide.

Release Versioning Strategy

Cisco Nexus 9000 Series switches and the Cisco Nexus 3000 Series switches, use the same NX-OS binary image also called the “unified" image. The binary image covers all variations of the Cisco Nexus 9000 Series switches and Cisco Nexus 3000 Series switches. Cisco NX-OS Release 9.2(1) was the first release that adopted unified version numbering. With unified version numbering, the platform designator is obsolete.

Moving forward for the previously identified platforms, we will be adopting the simplified 3-letter versioning scheme. For example, a release with X.Y(Z) would mean:

X - Unified release major

Y - Major / Minor release

Z - Maintenance release (MR)

Where the Z = 1 is always the first FCS release of a Major/Minor release.

An example of a previous release number is: 7.0(3)I7(4). In this format, the ‘I’ is the platform designator.

Note: In order to accommodate upgrade compatibility from an older software version that is expecting a platform designator, when the install all command is entered or the show install all impact command is entered, the version string appears as 9.3(5)I9(1). The “I9(1)” portion of the string can be safely ignored. It will later appear as 9.3(5).

Note: The Cisco Nexus 34180YC and 3464C platform switches are not supported in Cisco NX-OS Release 9.3(5).

Open Issues

Bug ID	Description

Bug ID	Description
CSCvq33024	Headline: TRM Multisite: traffic drop on BGW after restarting ngmvpn Symptoms: TRM traffic loss for 1-2 seconds. Workarounds: None
CSCvt28463	Headline: N9K-93XX-GX: Delayed link up between Gearbox Ports to bear valley on Peer for 40G AOC ports Symptoms: 40G AOC connection from N9K-C9364C-GX to N9K-C9364C (port 49 to 64) or N9K-C9336C-FX2 (port 1 to 6, 33 to 36) might see a longer link up time. Workarounds: Use port 1 to 48 on N9K-C9364C or port 7 to 32 on N9K-C9336C-FX2, or use other 40G optics than AOC.
CSCvt49337	Headline: N9K-C9364C-GX: 100G (1/50 AOC1M, 1/56 PSM4) steady state flap after 61st/multiple reload Symptoms: When tested with a reload loop, on one of the reloads the link flaps in steady state. Workarounds: Flap the port to recover.
CSCvu07720	Headline: Lpe16002BM6 negotiates to 8G when speed changed to auto when port in 'Link failure or not-connected' Symptoms: 16G Lpe16002B-M6 adapter is connected to a port with 32G SFP on N93360YC-FX2 switch. When the speed is set to 'auto', the port auto-negotiates to 8G instead of auto-negotiating to 16G. Workarounds: The port should be brought up in "fixed 16G" on N93360YC-FX2 switch instead of "Auto".

Bug ID	Description
CSCvu67445	Headline: N9k/Cloud Scale - Flood list missing po member port - broadcast traffic loss Symptoms: Broadcast may not Tx an Ethernet port for VLAN's allowed for one of the port-channel member links. ARP request or any other form of ethernet broadcast may not reach destination. This would lead to no connectivity for affected hosts. Consistency check will report failure for VLAN membership: Example: show consistency-checker membership vlan 442 Checking hardware for Module 1 Unit 0 No FEX interfaces to validate Consistency Check: FAILED >>> Vlan:442, Hardware state consistent for: Ethernet1/41 Ethernet1/49 Ethernet1/50 Ethernet1/53 Vlan:442, Hardware state inconsistent for: Ethernet1/54 </snip> Workarounds: Enter shut/no shut (flap) the affected interface. Do not use the "port-channel port load-defer" command.
CSCvu72682	Headline: buffer-stuck on mac-block (macsec-enabled) while one-port auto-neg to 100M Symptoms: Link up but no Tx packets when speed is auto negotiated to 100M on any interface of the same port group (MacId), where macsec is/was configured previously. Seen on Cisco Nexus 9300-FX platform switches only. Workarounds: If 100M speed is desired -> Remove the MACsec configuration from all interfaces on the port group (MacId) and reload --OR -- If MACsec is not configured explicitly -> Reload with Bootup Diag Level set to Minimal. --OR -- If MACsec configuration is desired -> Reload with different peer AN speed. Note: Use the show interface hardware-mappings command to check if the ports are part of the same port group (MacId).

Bug ID	Description
CSCvu80471	Headline: VXLAN vPC VTEP - Extended traffic loss when vPC peer reloads before NVE source hold timer expiry Symptoms: Traffic loss for hosts behind VPC in a VXLAN setup. NVE interface remains down after source hold-down timer expiry: # show nve interface nve1 det <> Source Interface hold-down-time: 180 >>> default time Source Interface hold-up-time: 30 Remaining hold-down time: 67 seconds. <<< after countdown finishes, goes to 0 From the same device, we can see the following in the log: %ETHPORT-5-IF_DOWN_NONE: Interface port-channel1 is down (None) <<< Virtual peer-link goes down %USER-2-SYSTEM_MSG: NVE: send reinit to bring down nve1 - nve <<< NVE goes down %NVE-5-NVE_INTF_STATE: nve1: NVE Interface state changed to down From here, VXLAN traffic will stop and all the devices behind vPC will have traffic black-holed for an extended duration Workarounds: Do not upgrade/reload on vPC Peer switch (SW2) before NVE source hold-down timer has expired on SW1.
CSCvv06363	Headline: Type 5 not propagated after Remove/add of "evpn multisite border-gateway" on Site BGW Symptoms: In a TRM use case, with the removal of multisite config and configuration replace - traffic loss is seen. Workarounds: clear bgp ipv4 mvpn <BGP router ID of remote BGW> soft out
CSCvv25573	Headline: DHCP request sent towards the server has router ID in option 54 instead of server ID Symptoms: Host doesn’t receive IP address from DHCP server Workarounds: SMU available in software download page for permanent fix.

Resolved Issues

Bug ID	Description

Bug ID	Description
CSCvk44504	Headline: Cisco Nexus 9000 Series Switches NX-OS Mode Fibre Channel over Ethernet NPV DoS Vulnerability Symptoms: A vulnerability in the Fibre Channel over Ethernet (FCoE) N-port Virtualization (NPV) protocol implementation in Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition. The vulnerability is due to an incorrect processing of FCoE packets when the fcoe-npv feature is uninstalled. An attacker could exploit this vulnerability by sending a stream of FCoE frames from an adjacent host to an affected device. An exploit could allow the attacker to cause packet amplification to occur, resulting in the saturation of interfaces and a DoS condition. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link:https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-npv-dos This advisory is part of the March 2019 Cisco FXOS and NX-OS Software Security Advisory Bundled Publication, which includes 25 Cisco Security Advisories that describe 26 vulnerabilities. For a complete list of the advisories and links to them, see Cisco Event Response: March 2019 Cisco FXOS and NX-OS Software Security Advisory Bundled Publication. http://tools.cisco.com/security/center/viewErp.x?alertId=ERP-70757 Workarounds: Please refer to the Security Advisory.
CSCvm11554	Headline: PTP High correction on slave when master have SVI which have IGMP Connected Group Membership Symptoms: When SVI on a PTP master switch receives an IGMP membership report and creates IGMP entries, PTP High correction issues occur. %PTP-2-PTP_HIGH_CORR: Slave port Eth1/X High correction -125750482(nsec) This issue is applicable only to Cisco Nexus 9500-R platforms. Workarounds: A or B A. - Remove PIM config from PTP VLAN SVI B. - Use other VLAN to PTP instead of VLAN used for multicast
CSCvp46147	Headline: Need Support for Multiple LLDP Neighbors over Same Interface Symptoms: LLDP Neighbor TLV fields may change over time or show unexpected information. This can cause issues with accounting tools that are expecting specific values in a given LLDP TLV field Workarounds: Currently the only workaround is to enforce a single LLDP neighbor/device on a given physical connection to the Cisco Nexus switch, which can be accomplished by disabling LLDP everywhere except for the physical port on the Cisco Nexus LLDP neighbor.

Bug ID	Description
CSCvq44103	Headline: 25g AOC/LR/SR Cable type is shown as unknown Symptoms: Cable type is shown as "unknown" for 25G SFP- LR, SR, and AOC cables. However, for copper 25G cables 'cable type' is displayed as CA-L, CA-N and CA-S accordingly. Workarounds: There is no workaround for this problem.
CSCvq45166	Headline: Control-plane traffic might be affected by high rate of NetFlow record packets on inband Symptoms: Control-plane traffic, like LACP might be affected (dropped) due to a high rate of new short-lived flows learned on NetFlow enabled interface Workarounds: HW rate-limiter for NetFlow might need to be configured to drop NFM traffic more aggressively, like 60000 instead of default 120k:* hardware rate-limiter netflow 60000Validate configuration with:* show hardware rate-limiter netflow
CSCvq81656	Headline: N9K-C9336C-FX2 front port ingress direction silent drop packet Symptoms: The link connection is up but port could not receive any traffic. All incoming packets dropped by ingress buffer Workarounds: None

Bug ID	Description
CSCvq95342	Headline: Intermittent VNI in DOWN state due to vni-add-await-buffer Symptoms: VNI in down state due to vni-add-await-buffer Non working: 07-29 17:39:15.012963 |22524 |113 |nve1 |vni-add-await |vni-add-await-buffer | |07-29 17:39:15.011930 |22524 |113 |nve1 |vlan-vni-add |vni-init | |07-29 17:39:15.011843 |22524 |0 |nve1 |cfg-mem-vni-mcast-cmd |vni-init | |07-29 17:39:15.308433 |22584 |114 |nve1 |vni-add-await |vni-add-await-buffer | |07-29 17:39:15.307472 |22584 |114 |nve1 |vlan-vni-add |vni-init | |07-29 17:39:15.307380 |22584 |0 |nve1 |cfg-mem-vni-mcast-cmd |vni-init |07-29 17:26:52.314255 |51089 |115 |nve1 |vni-add-await |vni-add-await-buffer | |07-29 17:26:52.313145 |51089 |115 |nve1 |vlan-vni-add |vni-init | |07-29 17:26:52.313063 |51089 |0 |nve1 |cfg-mem-vni-mcast-cmd |vni-init | |07-29 17:26:53.014215 |51110 |102 |nve1 |vni-add-await |vni-add-await-buffer | |07-29 17:26:52.621671 |51110 |0 |nve1 |cfg-mem-vni-mcast-cmd |vni-init | |07-29 17:26:53.022930 |51112 |103 |nve1 |vni-add-await |vni-add-await-buffer | |07-29 17:26:52.932304 |51112 |0 |nve1 |cfg-mem-vni-mcast-cmd |vni-init | |07-29 17:26:53.641801 |51113 |105 |nve1 |vni-add-await |vni-add-await-buffer | |07-29 17:26:53.354901 |51113 |0 |nve1 |cfg-mem-vni-mcast-cmd |vni-init | | Expected: 06-13 19:04:35.705995 |51024 |108 |nve1 |vni-add-comp |vni-add-complete | |06-13 19:04:35.705947 |51024 |108 |nve1 |l2rib-add-complete |vni-add-complete | |06-13 19:04:35.703578 |51024 |108 |nve1 |vni-add-pend |vni-add-pending | |06-13 19:04:35.703571 |51024 |108 |nve1 |vni-add-await |vni-add-await-buffer | |06-13 19:04:35.702581 |51024 |108 |nve1 |vlan-vni-add |vni-init | |06-13 19:04:35.702454 |51024 |0 |nve1 |cfg-mem-vni-mcast-cmd |vni-init | |06-13 19:04:36.440637 |51026 |109 |nve1 |vni-add-comp |vni-add-complete | |06-13 19:04:36.440581 |51026 |109 |nve1 |l2rib-add-complete |vni-add-complete | |06-13 19:04:36.437700 |51026 |109 |nve1 |vni-add-pend |vni-add-pending | |06-13 19:04:36.437691 |51026 |109 |nve1 |vni-add-await |vni-add-await-buffer | |06-13 19:04:36.039712 |51026 |0 |nve1 |cfg-mem-vni-mcast-cmd |vni-init Workarounds: Remove the entry and recreate resolves the issue.
CSCvr75903	Headline: Sequence timeout seen at reload with VXLAN PBR -- SVI flap optimizations needed. Symptoms: The system might experience a sequence timeout that might cause the L2alredirect loopback test to fail, rpm verification to fail, or a DHCP snoop hardware programming failure. When hit on the vPC secondary, this situation might result in vPC VLANs getting suspended on primary. Workarounds: Once the issue is hit, you can shut/no-shut the MCT link in vPC primary or operational primary to bring up the suspended VLANS. Also, to avoid getting into this situation, you may use GIR (graceful insertion and removal) to isolate the 9500, upgrade the chassis, and after all modules are up, insert the switch in to the network.

Bug ID	Description
CSCvr76803	Headline: Netstack core seen in non-destructive ISSU using FQDN for NTP Symptoms: FQDN for NTP server and ND ISSU on T2 ToR Workarounds: Do not use FQDN for NTP Servers. Use IP Address.
CSCvr79758	Headline: receive-only path overwrites BRIB path in ephemeral DME database Symptoms: When querying rest API, some BGP paths are missing. Workarounds: Remove the "always" keyword from the "soft-reconfiguration inbound " command.
CSCvs12578	Headline: Security: service NTP SIGABRT due to heartbeat failure Symptoms: The NTP process gets busy at times, while processing older version NTP packets and might miss sending heartbeat messages. The NTP process gets restarted and continues as before. This doesn't impact the time synchronization functionality of NTP in any manner. Workarounds: None
CSCvs19744	Headline: N9K: LLFC returns 'Ingress buffer allocation fail' error after ASCII reload on 52nd port Symptoms: You will see an LLFC buffer allocation error like the following: 2019 Nov 22 17:47:59 Sug-3-chart2 %$ VDC-1 %$ %IPQOSMGR-2-QOSMGR_LLFC_APPLY_FAILURE: Unable to apply flow-control configuration on interface: Ethernet1/52 due to 'Ingress buffer allocation fail'. Workarounds: None.
CSCvs20278	Headline: SVI is down while VLAN has active port after port flapping Symptoms: SVI is down while VLAN has active port Workarounds: Workaround #1 Remove the affected SVI VLAN and add it back Workaround #2 Reload can solve this issue.
CSCvs28295	Headline: MPLS entries present after no feature-set mpls command Symptoms: After entering the "no feature-set mpls" command, the output of the "show for adjacency mpls stats" command is not empty. Workarounds: Reload the box.
CSCvs41360	Headline: 93600CD-GX: Extra Flaps seen after Multiple reloads/flaps on different Optics on Gearbox Ports Symptoms: One Extra Flap seen after Multiple reloads/flaps on different Optics on ports 1-24 of 93600CD-GX. Similar extra flap seen after Multiple reloads/flaps on QSFP-100G-PSM4 and QSFP-100G-FR of N9K-9364C-GX. Workarounds: None

Bug ID	Description
CSCvs52421	Headline: Memory utilization for nginx process is growing over time Symptoms: Memory utilization for nginx process is increasing over time. Workarounds: Remove all subinterfaces from running config.
CSCvs62874	Headline: interface port-channel all command fails when sub interfaces are present Symptoms: interface port-channel all fails Workarounds: There is no workaround. nginx process restarts by itself.
CSCvt04531	Headline: Traffic drop seen when silent member FOP is shut. Symptoms: To see this issue, the port channel members should be in same ASIC instance and shut on one of PC mbr. Due to that mbr_chk idx in Vif state does not reflect until PC MOD trigger from PCM. To solve this, it needs to be changed mbr_chk_idx next fop of PC mbr. Workarounds: No workaround.
CSCvt06466	Headline: N9K-C9364C-GX: 100G CRC (1/50,53, AOC 1M/5M) after 61st/16th reload Symptoms: During reload loop we observed that one of the lanes on a couple of ports on a particular board (port 53) that one of the lanes of the port shows low SNR compared to other lanes of that same port. Due to this low SNR, CRC is seen on that lane. Issue is seen only with one board and only when AOC cable is connected. Workarounds: Flap the port to recover.
CSCvt20782	Headline: NVE interface remains up while associated loopbacks are down Symptoms: NVE interface remains up while associated loopbacks are down Workarounds: If the switch is manually reloaded or for an upgrade, you can either shutdown the north bound BGP sessions or shutdown the BGP process entirely until after the switch reloads and the multisite recovery timer expires. Then turn up BGP.
CSCvt26282	Headline: DCNM configured VXLAN SVI's unable to be shutdown. Symptoms: When attempting to shutdown (either from DCNM or CLI) a SVI which was configured via DCNM results in failure to do so along with the following log message: "ERROR: Profile conflicts with manual config" Workarounds: None

Bug ID	Description
CSCvt35218	Headline: Cisco Nexus process crash in syslog, callhome server due to SNMP leak Symptoms: A Cisco Nexus switch might experience a process crash as a result of a memory leak involving SNMP. %SYSMGR-2-SERVICE_CRASHED: Service "callhome server" (PID #) hasn't caught signal # (core will be saved). or %SYSMGR-2-SERVICE_CRASHED: Service "syslogd" (PID #) hasn't caught signal # (core will be saved). Workarounds: Configure "snmp-server contact [sysContact]".
CSCvt38574	Headline: Changing prefix-list in route-map doesn't change number of prefixes received in BGP summary Symptoms: In BGP, whenever you replace an existing prefix-list in the route-map with a new prefix-list, it doesn't change the number of prefixes received from a neighbor until you restart the BGP process itself. Workarounds: 1) Graceful BGP restart helps to resolve the issue. 2) Choose a different name for new prefix-list.
CSCvt43179	Headline: IPv6 BGP neighborship fails to come up (Idle state) on N9K-C93180YC-FX Symptoms: Below syslogs are seen on the device: %BGP-3-SOCKBIND: bgp- [1592] Cannot bind local socket for peer 2000:x:x:x Cannot assign requested address Workarounds: Shut/Unshut L3 IPv6 interface
CSCvt49643	Headline: Revert CSCvi89490 Symptoms: If exact the same as existing type-2 EVPN route received but with decreased sequence number, we would not send it to l2rib component. There should be no functionality impact with this change. Workarounds: None
CSCvt56182	Headline: Cisco NX-OS 9.3(3) to 9.3(5): ND ISSU on LXC TOR causing transient traffic drop Symptoms: Cisco NX-OS 9.3(3) to 9.3(5): ND ISSU on LXC TOR causing transient traffic drop when we have the BFD enabled as the BFD is going down and coming up during the ND ISSU Workarounds: Remove the BFD and re-add.
CSCvt61537	Headline: Upgrade from 7.0(3)IA7(2) to I7(5a) results in incorrect PSS convert for breakout Symptoms: Upgrade will fail from 7.0(3)I7(5a) to any other release with following error: Pre-upgrade check failed. Return code 0x0000000C (if_index type mismatch). Workarounds: Reload ASCII in 7.0(3)I7(5a) corrects the issue.

Bug ID	Description
CSCvt69760	Headline: sysmgr failed and stuck while writing to /mnt/pss Symptoms: sysmgr crashed while collecting sysinfo core. Workarounds:
CSCvt75268	Headline: IPv6 routes use wrong VLAN as next hop Symptoms: After creating an SVI, all of the IPv6 routes with the next hop in that SVI (including host routes and the route to the SVI's own address) will show an incorrect interface in "show ipv6 route ...". The interface shown in the output might have been disabled or deleted previously. This doesn't affect IPv4. Example: 2a00:1:2:10:::10/128, ubest/mbest: 1/0, attached *via 2a00:1:2:10:::10, Vlan10, [190/0], 00:26:24, hmm interface Vlan20 ipv6 address 2a00:1:2:10:::10/64 Workarounds: Deleting and re-creating the SVI typically fixes the issue.
CSCvt78821	Headline: Global | Nexus 9k 7.0(3)I7(5a) Layer 2 Multicast traffic delivery issues Symptoms: After a Cisco NX-OS upgrade in a C9508 from 7.0(3)I5(2) code to 7.0(3)I7(5a) code, Layer 2 Multicast traffic is not being forwarded to Layer 2 access ports belonging to IGMP snooping groups in a specific VLAN. This occurs when there is an SVI configured in the shutdown state in that specific VLAN with ip pim sparse-mode in the switch. Workarounds: Delete ip pim sparse-mode in SVI.
CSCvt79015	Headline: Port-channel load balancing issue when PBR load-share in use Symptoms: The issue is specific to N9K-C93180YC-EX devices only; When PBR sets several next-hops with "load-share" keyword, and in case the traffic has to be sent out (load-shared) over several port-channel interfaces further, an issue might be observed with load-balancing of the traffic over the physical member interfaces on these port-channel interfaces. Workarounds: NA
CSCvt87601	Headline: VXLAN Spine MAC Address Learning Ignored - IGN_LRN_RVTEP_MISS Symptoms: MAC address learning ignored on VXLAN Flood and Learn Spine switch Workarounds: Flap NVE interface on both Spine and Leaf switches

Bug ID	Description
CSCvt88547	Headline: MAC ACL + MAC packet classification could not let IPv6 NS/NA pass through Symptoms: With the configuration of MAC ACL + MAC packet classification, the port will deny IPv6 NS/NA packets. It caused the IPv6 traffic could not go through the port. Example configuration: mac access-list test statistics per-entry 10 permit any any 0x86dd <<<<< ethertype of IPv6 interface Ethernet2/1 switchport mac port access-group test mac packet-classify no shutdown Workarounds: mac access-list test statistics per-entry 10 permit any any 0x86dd 20 permit any any vlan X <<<<< use this entry to permit all the traffic
CSCvt91055	Headline: PTP unicast packets sent out with wrong destination MAC on Master ports after reloading Symptoms: PTP unicast packets might be seen to be sent out with wrong destination MAC on Master ports after reloading of the Cisco Nexus 9000 switch. Reentering the "slave ipv4" command on the affected PTP Master interfaces restores the PTP unicast operation on the corresponding links. Workarounds: Use physical IP addresses of the L3 interfaces for PTP unicast operation instead of loopbacks.
CSCvt91791	Headline: SNMP traps can't be disabled Symptoms: Disabling some SNMP traps might be seen not working: N9K# show run all | i i entity_mib_change snmp-server enable traps entity entity_mib_change N9K# conf t N9K(config)# no snmp-server enable traps entity entity_mib_change N9K(config)# exit N9K# show run all | i i entity_mib_changesnmp-server enable traps entity entity_mib_change N9K# Workarounds:

Bug ID	Description

CSCvt94027	Headline: Python script not able to log out console user
	
	Symptoms: Python script cannot stop ethanalyzer and terminate console vty session.
	
	The following logs are seen:
	
	%VSHD-2-VSHD_SYSLOG_EOL_ERR: EOL function security_clear_vty from library libsecuritycli.so exited due to Signal 11
	
	Workarounds: -Don't use EEM to call python to clear line, instead just use Python.
	-Replace "action 1.0 cli source check_keepalive.py" with "action 1.0 cli python check_keepalive.py"
	
	<pre>switch# show file scripts/test.py
	#!/usr/bin/env python
	import re
	import time
	import cisco
	import syslog
	from cli import *
	
	cli('clear line ttyS0')
	switch#
	switch# source background test.py
	pid 31599
	switch#
	
	User Access Verification
	switch login:
	User Access Verification
	switch login:</pre>

Bug ID	Description
CSCvt97441	Headline: RX power shows -26.98 dBm when remote device TX shows -5.11 dBm Symptoms: Topology : N9K1 E1/1-----1G fiber link-----E1/1 N9K2 When rx cable is removed from E1/1 on N9K1, link will be down after debounce timer expired and the TX laser will be toggled on N9K1 which is expected. However after the TX laser on N9K1 re-enabled the RX power on N9K2 shows -26.98 dBm and link up failed. We need to know if this is expected behavior and if it is related with 802.3ae. N9K1 2020 Apr 17 02:59:32.424715 Switch %ETHPORT-5-IF_DOWN_LINK_FAILURE: Interface Ethernet1/1 is down (Link failure) Switch# show int e1/1 transceiver details Ethernet1/1 transceiver is present type is 1000base-SX name is CISCO part number is FTLF8519P3BNL-CS revision is A serial number is FNS173628EM nominal bitrate is 1300 MBit/sec cisco id is 3 cisco extended id number is 4 cisco part number is 10-2626-01 cisco product id is GLC-SX-MMD SFP Detail Diagnostics Information (internal calibration) ---------- Current Alarms Warnings Measurement High Low High Low ---------- Temperature 35.28 C 90.00 C -10.00 C 85.00 C -5.00 C Voltage 3.29 V 3.59 V 3.00 V 3.50 V 3.09 V Current 6.41 mA 15.00 mA 1.00 mA 12.00 mA 2.00 mA Tx Power -5.11 dBm 0.00 dBm -13.56 dBm -3.00 dBm -9.50 dBm Rx Power -26.98 dBm -- 2.99 dBm -21.54 dBm 0.00 dBm -16.98 dBm Transmit Fault Count = 0 ---------- Note: ++ high-alarm; + high-warning; -- low-alarm; - low-warning N9K 22020 Apr 17 02:59:42.312164 switch %ETHPORT-5-IF_DOWN_LINK_FAILURE: Interface Ethernet1/1 is down (Link failure) switch# show int e1/1 transceiver details Ethernet1/1 transceiver is present type is 1000base-SX name is CISCO part number is SFBR-5716PZ revision is 001 serial number is AGJ1935RB6B nominal bitrate is 1300 MBit/sec cisco id is 3 cisco extended id number is 4

Bug ID	Description
CSCvt98187	Headline: Permanent traffic loss from hosts in IPSG table when port-security is also combined on the interface Symptoms: Hosts connected to Cisco Nexus 9000 Series switch might experience complete traffic loss when connected to interfaces where both IP Source Guard and port-security is configured. Workarounds: Don't use both features at the same time.
CSCvu03290	Headline: Nexus 9372 tahusd crash due to transceiver speed mismatch Symptoms: A Nexus 9372 switch could experience a crash in the Tahoe User Space Driver (tahusd) while trying to bring up a 40G port using a 100G transceiver: N9K# sh int trans <snip>Ethernet1/6 transceiver is present type is QSFP-100G-LR4-S name is CISCO-FINISAR part number is FTLC1151RDPL-C2 revision is A serial number is FNS23290AKK nominal bitrate is 25500 MBit/sec per channel Link length supported for 9/125um fiber is 10 km cisco id is 17 cisco extended id number is 220 cisco part number is 10-3146-02 cisco product id is QSFP-100G-LR4-S <snip> N9K# conf t Enter configuration commands, one per line. End with CNTL/Z. N9K(config)# int Eth1/6 N9K(config-if)# no shut 2020 Apr 28 18:23:12 N9K %$ VDC-1 %$ %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "tahusd" (PID 31341) hasn't caught signal 6 (core will be saved). 2020 Apr 28 18:23:15 N9K %$ VDC-1 %$ %SYSMGR-SLOT1-2-HAP_FAILURE_SUP_RESET: Service "tahusd" in vdc 1 has had a hap failure 2020 Apr 28 18:23:15 N9K %$ VDC-1 %$ %SYSMGR-SLOT1-2-LAST_CORE_BASIC_TRACE: fsm_action_become_offline: PID 18307 with message Could not turn off console logging on vdc 1 error: mts req-response with syslogd in vdc 1 failed (0xFFFFFFFF) . 2020 Apr 28 18:23:42 N9K %$ VDC-1 %$ Apr 28 18:23:42 %KERN-2-SYSTEM_MSG: [3979.796087] usd process 31341, uuid 1356 (0x54c) failed to send heartbeat - kernel 2020 Apr 28 18:23:56 N9K %$ VDC-1 %$ %SYSMGR-SLOT1-2-LAST_CORE_BASIC_TRACE: core_client_main: PID 5482 with message filename = 0x102_tahusd_log.31341.tar.gz . 2020 Apr 28 18:23:57 N9K %$ VDC-1 %$ %MODULE-2-MOD_DIAG_FAIL: Module 1 (Serial number: SAL2003WZEJ) reported failure due to Service on linecard had a hap-reset in device DEV_SYSMGR (device error 0x54c) Workarounds: Avoid using 100G transceivers in ports that only support 40G.

Bug ID	Description
CSCvu04347	Headline: device rebooted due to Kernel panic - not syncing: WATCHOG HIT Symptoms: device rebooted `show system reset-reason` ----- reset reason for module 1 (from Supervisor in slot 1) --- 1) At 721544 usecs after Tue Mar 31 14:43:18 2020 Reason: Watchdog Timeout Service: Version: 9.3(3) Stack trace observed as below: <6>[6772598.222919] klm_requiem wrote crashinfo for process sysinfo pid 28841 at 6326277809. <0>[6902207.050788] NMI due to FPGA WATCHDOG <7>[6902207.095740] cctrl DBG: cctrl_ow_write dev_type 5 data 4f <6>[6902207.097727] obfl_set_mmc_rr initialized on mmcblk0p2 blksize=512, cpu=0 <6>[6902207.097730] obfl_set_mmc_rr: tv sec is 5e82e686, usec is b0a52 rr=32 rr_str= <6>[6902207.101437] writing reset reason succeeded with retval=0 on cpu=0 <7>[6902207.103818] cctrl DBG: cctrl_ow_write dev_type 5 data 4f <6>[6902207.103820] CCTRL PANIC DUMP<6>[6902207.103821] ========== <6>[6902207.103823] WDT last punched at 1585636990 <6>[6902207.103826] REG(0x60) = 3c <6>[6902207.103830] REG(0x64) = 0 <6>[6902207.103833] REG(0x300) = baadbeef <6>[6902207.103837] REG(0x304) = baadbeef <6>[6902207.103838] ========== <0>[6902207.111842] nxos_panic: Kernel panic - not syncing: WATCHOG HIT <0>[6902207.111842] <6>[6902207.204726] CPU: 0 PID: 0 Comm: swapper/0 Tainted: P O 4.1.21-WR8.0.0.28-standard #1 <6>[6902207.313233] Hardware name: Default string Default string/Default string, BIOS 5.11 08/30/2019 <6>[6902207.417572] 0000000000000000 ffff88047fc08d40 ffffffff9282b128 ffffffff923ee210 <6>[6902207.508866] ffffffff92e3f7f0 ffff88047fc08dc0 ffffffffb9234ffc ffff88046c5707f8 <6>[6902207.600160] ffffffff00000008 ffff88047fc08dd0 ffff88047fc08d70 0000000000000010 <6>[6902207.691454] Call Trace: Workarounds:
CSCvu05601	Headline: Remote VTEP loopback is programmed incorrectly in hardware on receipt of a default route Symptoms: Multisite Encapsulation is not working on a VXLAN Border Gateway Workarounds: If a host route(/32 route) is received or a summary route for the remote NVE Peer's loopback IP address, issue won't happen

Bug ID	Description
CSCvu05955	Headline: N9k: PFC mode config wiped out from port-channel interface with no member ports after reload Symptoms: Switch configured with the "priority-flow-control mode off" command on uplink port-channels. If the port-channel member ports are removed for some reason and switch is reloaded, the "priority-flow-control mode off" command gets wiped out from the port-channel but is still present on the physical port. If you re-add the "priority-flow-control mode off" command to the port-channel, the CLI accepts the config but doesn't get applied without any error. The members can't be re-added back into the port-channel due to config incompatibility. Workarounds: Add the interface into port-channel using the force option and then re-enter the "priority-flow-control mode off" command to the port-channel.
CSCvu07795	Headline: [ ] is removed from show run when configuring interface description for mgmt 0 Symptoms: When configuring interface description for mgmt 0 enclosing in brackets (for example, [for_management]),brackets are removed in show running-config(for_management for the example above). Workarounds: No functional impact due to this symptom. Current workaround is not using [ ]
CSCvu08122	Headline: Cannot modify NTP server configs for 192.0.x.x address due to DB and PSS inconsistency Symptoms: Additional NTP servers cannot be configured in the 192.x.x.x range NTP server configuration removal via config-replace fails for address in 192.x.x.x range Workarounds: Configure static hostname-to-address mappings for the ntp servers using "ip host <hostname> <ntp address>" command N9K(config)#ip host NTPServer1 192.0.1.1 N9K(config)#ip host NTPServer2 192.0.1.2 N9K(config)#ntp server NTPServer1 use-vrf management N9K(config)#ntp server NTPServer2 use-vrf management Note: Cannot use underscore in hostname NN9K(config)# ntp server NTPServer_1 ? ^ % Invalid command at '^' marker.

Bug ID	Description
CSCvu09425	Headline: When mapping a VLAN to VNI, the VLAN is suspended resulting in a line card aclqos client crash Symptoms: %NVE-5-NVE_INTF_STATE: nve1: NVE Interface state changed to down %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "aclqos" (PID 2195) hasn't caught signal 11 (core will be saved). %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "aclqos" (PID 5813) hasn't caught signal 11 (core will be saved). %ETHPORT-5-IF_SEQ_ERROR: Error ("Linecard aclqos client crash") communicating with MTS_SAP_SPM for opcode MTS_OPC_ETHPM_PORT_LOGICAL_BRINGUP (RID_PORT: Ethernet1/53) %ETHPORT-3-IF_ERROR_VLANS_SUSPENDED: VLANs 311 on Interface Ethernet1/53 are being suspended. (Reason: Linecard aclqos client crash) %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "aclqos" (PID 6175) hasn't caught signal 11 (core will be saved). %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "aclqos" (PID 6860) hasn't caught signal 11 (core will be saved). %SYSMGR-SLOT1-2-HAP_FAILURE_SUP_RESET: Service "aclqos" in vdc 1 has had a hap failure %SYSMGR-SLOT1-2-LAST_CORE_BASIC_TRACE: fsm_action_become_offline: PID 20094 with message Could not turn off console logging on vdc 1 error: mts req-response with syslogd in vdc 1 failed (0xFFFFFFFF) Workarounds: No workaround to make functionality work. To avoid cores remove BFD configuration on NS ports and its VLANs.
CSCvu11175	Headline: N9K/FEX: Sup bound traffic coming from FEX HIF dropped in LCND Symptoms: If Cisco Nexus 9000 switch with straight through FEX has port-channels removed under HIFs and re-added with different port-channel number, traffic coming from host and destined to switch CPU(such as ARP/ICMP etc) will be dropped Workarounds: Use original port-channel number
CSCvu13827	Headline: The "show system error-id list" CLI command results in a VSH crash on FEX Symptoms: The following steps cause the issue: attach fex 117 show system error-id list This causes VSH to crash and generate a core. The FEX doesn't reload and the core does not impact the functionality of the FEX. Workarounds: Not available
CSCvu14542	Headline: Longevity: kernel panic on EOR fabric module after DUT running I+A MR CCO for ~5days5hours Symptoms: Kernel panic may occur on Cisco Nexus 9500 non-CloudScale LCs/FMs after upgrade to 9.3(4). Workarounds: No known workarounds are available for this issue as of now.

Bug ID	Description
CSCvu14934	Headline: N9K: TRM/VXLAN, Non-Multi-Site setup, Type-7 routes are not imported into BRIB Symptoms: MVPN BGP Type-7 routes are not imported into BRIB. This is due to the fact that the Incoming route targets are not matching to what BL expects Workarounds: + Remove send-community extended on the VRF Lite neighbor so that the extended community- VRI(VRF Route import) is not received + use aggregate-address x.x.x.x/x summary-only
CSCvu15037	Headline: Cisco Nexus 9000 Cloud Scale devices drop 25G broadcast traffic as output discard with queue-limit Symptoms: A Cisco Nexus 9000 switch with the Cloud Scale ASIC will drop multi-destination/BUM (Broadcast/Unknown Unicast/Multicast) traffic received through a 25G interface as an output discard if the system's egress queuing policy has a queue-limit defined for the traffic's queue. Since the affected traffic is multi-destination in nature, output discards will increment on all interfaces that are forwarding the ingress VLAN in question. As this issue affects all multi-destination traffic, this issue can manifest itself with multiple different symptoms. Some common ones include: +++ 25G-connected hosts are not able to obtain IP addresses via DHCP +++ 25G-connected hosts are not able to establish network connectivity through ARP resolution +++ 25G-connected hosts are not able to receive multicast traffic via IGMP Workarounds: Removing the queue-limit from relevant queues in the system-wide egress queueing policy will prevent multi-destination traffic placed in that queue from being dropped if it is received on a 25G interface.
CSCvu15867	Headline: FEX ports go through STP LRN state regardless of the default Edge config Symptoms: FEX ports are by default Edge ports. FEX ports transition through LRN state. Workarounds: None
CSCvu17177	Headline: N9K - "ttag" is not configured under an interface in running-config but still enabled in hardware. Symptoms: TTAG header is added to packets, where we can see there is an extra 8 bytes added with the first 2 bytes representing the IP protocol header as 8905, which indicates the TTAG header is added to a packet when running-config says it should be. Workarounds: Reconfigure "ttag"/"no ttag" on the impacted interface.

Bug ID	Description
CSCvu20429	Headline: Storm control commands broadcast/muliticast added to interface configs after non disruptive ISSU Symptoms: After multiple non disruptive ISSUs, the following commands were added to the interface configuration causing complete connectivity issues. For instance, non-disruptive ISSU was carried as below versions and all L2/L3 interfaces were added with below commands. I7.0(3)I4(1) > 7.0(3)I7(7)> 7.0(3)I7(8) interface Ethernet1/17 link transmit reset-skip no link dfe adaptive-tuning storm-control broadcast level pps 0 <- added after the upgrade storm-control multicast level pps 0 <- added storm-control unicast level pps 0 <- added switchport virtual-ethernet-bridge <- added Workarounds: Reconfigure the same commands on effected ports and then remove it as indicated below. configure terminal interface e1/17 storm-control broadcast level pps 0 storm-control multicast level pps 0 storm-control unicast level pps 0 switchport virtual-ethernet-bridge config t int eth 1/17 no storm-control broadcast level pps 0 no storm-control multicast level pps 0 no storm-control unicast level pps 0 no switchport virtual-ethernet-bridge Or Write erase and reapply the original configurations.
CSCvu20547	Headline: N9K active sup reload due to tempSensor policy trigger even though temp is not high Symptoms: Cisco Nexus 9500 active SUP switchover due to major temperature alarm for the outlet sensor even though temp is not high. Workarounds: NA

Bug ID	Description
CSCvu20805	Headline: SNMP slow response seen after reload Symptoms: SNMP slow response seen after reload With the below configuration: snmp-server community <community> use-ipv4acl snmp-acl snmp-acl should permit check once for every OID. However, after reload, we see the permit checks are performed twice. Before reload: (from "debug snmp all") 2020 May 7 05:25:45.988578 snmpd: check_acl_permit : Call npacl_apply_filter for acl:snmp-acl:4194305 2020 May 7 05:25:45.989459 snmpd: check_acl_permit : Exit npacl_apply_filter 2020 May 7 05:25:45.993292 snmpd: check_acl_permit : Call npacl_apply_filter for acl:snmp-acl:4194305 2020 May 7 05:25:45.994174 snmpd: check_acl_permit : Exit npacl_apply_filter After reload: 2020-05-04 16:56:25.227101 us: [101] check_acl_permit : Call npacl_apply_filter for acl:snmp-acl:4194308 2020-05-04 16:56:25.227515 us: [101] check_acl_permit : Exit npacl_apply_filter 2020-05-04 16:56:25.227526 us: [101] check_acl_permit : Call npacl_apply_filter for acl:snmp-acl:4194305 2020-05-04 16:56:25.227938 us: [101] check_acl_permit : Exit npacl_apply_filter Workarounds: Remove and reconfigure the snmp aclno snmp-server community <community> use-ipv4acl snmp-aclsnmp-server community <community> use-ipv4acl snmp-acl
CSCvu23201	Headline: NX-OS BGP: rare BGP updates corruption Symptoms: Very rarely BGP update messages can get corrupted Workarounds: disable enhanced error processing via CLI router bgp <as number> ; no enhanced-error
CSCvu23546	Headline: tahusd crash due to link flapping Symptoms: N9K-C93108TC-EX in some cases, tahusd crash while device got physical link flapping. Workarounds: none
CSCvu29529	Headline: Not able to create (s,g) entry for non-directly connected source. Symptoms: N9k does not create (s,g) when (*,g) is already populated on the switch Workarounds: Possible workaround is to create a loopback interface with an IP address with a less specific mask covering non-directly connected sources

Bug ID	Description
CSCvu29761	Headline: Leaking of OSPF Hello packet received in P2P link Symptoms: OSPF Hello packets received on a P2P interface are forwarded to other OSPF enabled P2P link. This leads to an INIT state visible on remote devices, towards a device they should never peer with. This issue is not limited to OSPF hello packets, but applies to LL MC packets. Workarounds:
CSCvu30354	Headline: WR-ERSPAN-DEST: terminating traffic is getting acl_drop Symptoms: ACL_DROP seen on ERSPAN termination for monitored packets Workarounds: None
CSCvu31888	Headline: Unexpected reload of sysmgr process Symptoms: When the user tries to perform a copy of the running configuration, the process failed and crashes Workarounds: No workaround
CSCvu34684	Headline: bcm-crash after configuring/adding VLAN Symptoms: Creating or allowing VLAN causing bcm_usd to crash on Cisco Nexus 9000. Workarounds: Reload switch.
CSCvu36208	Headline: OSPFv3 packets are punted to CPU from STP ALT-BLK ports Symptoms: OSPF reported the bad address in the system log as below: N9K# sh logging log | i ' Bad source address fe80::171:102:250:4 - ours on Vlan28' 2020 May 18 10:05:57 N9K %OSPFV3-4-SOURCE_ERR: ospfv3-1 [29849] (default) Bad source address fe80::171:102:250:4 - ours on Vlan28 2020 May 18 10:06:14 N9K %OSPFV3-4-SOURCE_ERR: ospfv3-1 [29849] (default) Bad source address fe80::171:102:250:4 - ours on Vlan28 2020 May 18 10:06:32 N9K %OSPFV3-4-SOURCE_ERR: ospfv3-1 [29849] (default) Bad source address fe80::171:102:250:4 - ours on Vlan28 Workarounds: NA

Bug ID	Description
CSCvu37853	Headline: Cisco Nexus 9000 TAHUSD crash with a HAP failure on Cisco NX-OS 9.2(3) Symptoms: 1/ inside the module level executing - "show hardware internal tah mcast l2ptr hashindex 40972 asic 0" 2/ show cores VDC Module Instance Process-name PID Date(Year-Month-Day Time) --- ------ -------- --------------- -------- ------------------------- 1 3 1 tahusd 9187 2020-05-25 13:18:41 1 1 1 tahusd 9186 2020-05-25 13:19:59 3/ Module crash with the following reason ********* Exception info for module 1 ******** exception information --- exception instance 1 ---- Module Slot Number: 1 Device Id : 134 Device Name : System Manager Device Errorcode : 0x0000054c Device ID : 00 (0x00) Device Instance : 00 (0x00) Dev Type (HW/SW) : 05 (0x05) ErrNum (devInfo) : 76 (0x4c) System Errorcode : 0x401e008a Service on linecard had a hap-reset Error Type : FATAL error PhyPortLayer : 0x0 Port(s) Affected : Error Description : tahusd hap reset DSAP : 0 (0x0) UUID : 1 (0x1) Time : Mon May 25 13:20:04 2020 (Ticks: 5ECB9BD4 jiffies) 4/ I/O modules models: N9K-X9732C-EX and N9K-X97160YC-EX Workarounds: N/A

CSCvu40117	Headline: N9K-C93600CD-GX TOR GOLD process crash || "device_test" SIGABRT
	
	Symptoms: Switch experiences a process crash of "device_test". A core is saved and the switch remains operating (no reload seen). This crash does not appear to impact the switch (still under investigation).
	
	<pre>
	YYYY Month XX HH:MM:SS SWITCH_A %SYSMGR-2-SERVICE_CRASHED: Service "device_test" (PID 28882) hasn't caught signal 6 (core will be saved).
	</pre>
	
	Workarounds: TBA

Bug ID	Description
CSCvu41437	Headline: 3rd Party QSFP ports are down Symptoms: 3rd party QSFP ports are not coming up after upgrade to Cisco NX-OS 7.0(3)I7(7) or 7.0(3)I7(8) Workarounds: None
CSCvu49145	Headline: JSON request for "show l2route mac all" or "show l2route evpn mac all" respond w/ empty flag field. Symptoms: JSON request for "show l2route mac all" or "show l2route evpn mac all" respond w/ empty flag field. Workarounds: Issue not seen in Cisco NX-OS 7.0(3)I7(8)
CSCvu49698	Headline: Need to revert SqiVNI catchall to allow native VLAN config Symptoms: In QinVNI environment - configuration: interface X/Y switchport trunk native vlan 4003 switchport vlan mapping all dot1q-tunnel 1002 Should encapsulate all C-VLANs except native VLAN without having to specify them explicitly. Release 9.3.4 reject ?all? keyword: Error Invalid params : ERROR: (switchport vlan mapping all dot1q-tunnel 1002) Native VLAN config cannot coexist with dot1q all please remove native VLAN config under interface po3005 before configuring dot1q all This is incorrect behavior. Workarounds: Explicitly specify VLAN to be encapsulated - if possible
CSCvu52350	Headline: Sysmgr failed on active sup when standby sup reloaded Symptoms: Sysmgr crashed on active SUP when standby SUP was reloading Workarounds: None

Bug ID	Description
CSCvu53480	Headline: N9K VXLAN EVPN - static route VRF leaking issue upon recursive lookup Symptoms: In a VXLAN fabric, route leaked in between VRF may not contain the tunnel information, leading to traffic sent without VXLAN header in the fabric. This issue is related to recursive lookup, where NH for the destination IP is reachable over the fabric. The issue is only present when the route to reach the recursive NH is a static route leaked from the VRF where the NH resides. The presence of this static route may be justified by the fact that the NH can move around the fabric/VTEPs. Workarounds: Several workarounds are available: + Instead of using route leaking with RT import/export, leak the route using static route in the VRF where the source resides (VRF A), pointing towards next-hop in VRF B: vrf context A ip route <dst_ip>/32 <nh_ip> vrf B + Use hmm tracking to advertise the route in VRF where the destination resides only where the NH is reachable over hmm.
CSCvu55046	Headline: EX_EOR : ACL commands not working after upgrade from 9.3.2 or 9.3.4 Symptoms: After upgrade EoR from Cisco NX-OS 9.3.2 to 9.3.4 then we see below error log when adding ACE in ACL Sat Jun 6 19:27:52 2020:type=update:id=10.79.102.146@pts/2:user=admin:cmd=install all nxos bootflash:/nxos.9.3.4.bin (SUCCESS) switch(config-acl)# 40 permit ip 3.3.3.3/32 4.4.4.4/32 Error: Exceeds maximum number of v4/v6 ACEs for RTP Workarounds: if the issue is seen on 9.3.3, reload the switch by entering the "reload ascii" commandif the issue is seen on 9.3.4, write erase & reload
CSCvu65527	Headline: BGP packets sent with invalid label after SR route change Symptoms: If there is an MPLS-labeled route, and another route appears for the same prefix that doesn't require an MPLS label to be imposed before the previous route is withdrawn, packets sent by the BGP process or by "telnet x.x.x.x 179" to that destination still have the old MPLS label on them. Since there is no LSP, they are dropped. Pings or packets to any other ports are not affected. Workarounds: A switch reload might be needed for this problem.
CSCvu69707	Headline: Add event history error log with invalid character by show lldp entry Symptoms: Add event history error log with invalid character by show lldp entry Workarounds: none

Bug ID	Description
CSCvu72035	Headline: BFD must teardown packets with TTL other than 255 in a directly connected neighbor async mode Symptoms: BFD session keeps up even when we received a BFD packet with TTL <255 Workarounds: Not available or not applicable
CSCvu75595	Headline: Route Leak - VXLAN EVPN - Attached-Export not flushed with host mobility Symptoms: IP host mobility is not working in inter-vrf leaking scenario in VXLAN EVPN setup. VRF-X : host A resides behind Leaf1 VRF-Y : route leaking using RT import from VRF-X Move host A behind Leaf4 and now routing is broken in VRF-Y, attached-export entry is still seen: 10.26.11.202/32, ubest/mbest: 1/0, attached *via 10.26.11.202%VRF-X, Vlan1820, [190/0], 00:11:49, attached-export >>>>>> problem as this entry should be removed once host moved from Leaf1 via 10.222.22.201%default, [200/0], 00:00:08, bgp-65004, internal, tag 65004, segid: 300011 (Asymmetric) tunnelid: 0xade16c9 encap: VXLAN Workarounds: clear ip route entry in VRF-Y on Leaf1 where host was previously active: # clear ip route vrf VRF-Y 10.26.11.202/32 Clearing 10.26.11.202/32 IP Route Table for VRF "VRF-Y" '*' denotes best ucast next-hop '**' denotes best mcast next-hop '[x/y]' denotes [preference/metric] '%<string>' in via output denotes VRF <string> 10.26.11.202/32, ubest/mbest: 1/0 *via 10.222.22.201%default, [200/0], 00:00:11, bgp-65004, internal, tag 65004, segid: 300011 tunnelid: 0xade16c9 encap: VXLAN
CSCvu79156	Headline: Unable to disable auto-negotiation on 100mb RJ-45 ports Symptoms: A Nexus 9000 Series Switch with RJ-45 copper ports may be unable to disable auto-negotiation by entering the `no negotiate auto` command when the port speed is set to 100M. Auto-negotiation is mandatory for RJ-45 ports when the speed is set to 1/10G, but should be optional when the speed is set to 100M. Workarounds: None
CSCvu82423	Headline: Remote VTEP forms PIM adjacency in underlay with router connected to L2-only VXLAN fabric Symptoms: Remote VTEP forms PIM adjacency in underlay with router connected to L2-only VXLAN fabric Workarounds: - Replace IP Unnumbered with IP addresses. OR - Configure SVI interfaces and L3VNI in fabric.

Bug ID	Description
CSCvu86704	Headline: ARP failed in Kstack causing BGP to go IDLE state Symptoms: ARP failed in Kernel causing BGP to go IDLE state bash-4.3$ ip netns exec test-vxlan arp Address HWtype HWaddress Flags Mask Iface 10.10.10.1 (incomplete) Vlan66 Workarounds: Always delete the VRF context <>with one direct route present (like a dummy loopback/SVI in the respective VRF); 1. no vrf context <> follow-up steps can be: 1. no interface VLAN 2. no redistribute static 3. no member VNI 4. no vlan x

Bug ID	Description

CSCvu86996	Headline: N9K reloading continuously because of kernel panic after upgrade.
	
	Symptoms:
	
	N9k started rebooting continuously after upgrade from 7.0(3)I7(4) to 9.3(3)
	
	`show system reset-reason`
	----- reset reason for module 1 (from Supervisor in slot 1) ---
	<snip>
	3) At 488602 usecs after Sat Jun 13 03:54:21 2020
	Reason: Kernel Panic
	Service:
	Version: 9.3(3)
	4) At 485109 usecs after Sat Jun 13 03:47:42 2020
	Reason: Kernel Panic
	Service:
	Version:
	
	`show logging onboard module 1 stack-trace`
	---------- 	
	Module: 1
	---------- 	
	
	**********
	STACK TRACE GENERATED AT Sat Jun 13 04:11:27 2020 EDT
	**********
	
	Panic#1 Part2
	<3>[212.138832]
	<3>[212.138832] cctrl_handle_io_isr Got LC Presence intr 9
	<6>[212.138873] LEM OIR detected..
	<6>[212.138873] Slot(1) got interrupt
	<6>[212.138874] Slot(2) got interrupt
	<6>[212.138874] Slot(3) got interrupt
	<6>[212.138875] Slot(4) got interrupt
	<6>[212.138875] Slot(6) got interrupt
	<6>[212.138875] Slot(7) got interrupt
	<6>[212.138876] Slot(8) got interrupt
	<3>[212.138887]
	<snip>
	
	Workarounds: None

Bug ID	Description
CSCvu91224	Headline: Modify IPv6 LPM 4096 cause Cisco Nexus 9508 IPv6 forwarding issue Symptoms: After modify Ipv6 LPM to max value, the N9K not forwarding the packet even the routing table & forwarding table are fine. hardware profile multicast max-limit lpm-entries 0 hardware profile ipv6 lpm-entries maximum 4096 Multicast Heavy mode N9K# show system routing mode Configured System Routing Mode: Multicast Heavy Scale Applied System Routing Mode: Multicast Heavy Scale Workarounds: NA
CSCvu97672	Headline: sup switchover causes ECMP OIF of CNH missing in hardware Symptoms: When reloading the active sup, CNH ECMP outgoing interface disappears from HW but stays in SW with some probability. Workarounds: clear ip route x.x.x.x
CSCvv02345	Headline: Ports don't come up after NX-OS upgrade from any release to I7.8, 9.3.3, 9.3.4 Symptoms: Ports fail to come up after NXOS upgrade from any release to I7.8, 9.3.3,9.3.4 %USER-2-SYSTEM_MSG: BCMXXXXX UCODE Download Failure at PHY ID 0 - tahusd Workarounds: Contact TAC.

Known Issues

Behavior Changes for Cisco Nexus 9504 and 9508 Switches with -R Line Cards

Bug ID	Description
N/A	Interface: The output format for the exec command CLI show vpc orphan-ports has changed from the 7.0(3)F3(4) release to the 9.3(5) release.
N/A	FEX: MTU 9216 is the default value for FEX fabric ports-channels.
N/A	FEX: MTU 9216 is the only allowed value to be configured on FEX fabric port-channels. Configuring any other value will throw an error.

Bug ID	Description
CSCvp87914	FEX: If the MTU value on a FEX fabric port-channel was set to 9216 before upgrading to Cisco NX-OS Release 9.3(5), the show running config command will not display the MTU config as it is the new default in Cisco NX-OS Release 9.3(5). Due to this, the show running-config diff command displays the difference which is expected.
N/A	Programmability: Release 9.3(5) brings in a new kernel and new processes.
N/A	Programmability: Interface counter statistics are grouped together in the XML/JSON output. The output for the show interface-counters command in JSON format has changed.
N/A	Programmability: NX-API does not support insecure HTTP by default.
N/A	Programmability: NX-API does not support weak TLSv1 protocol by default.
N/A	Security: Stronger ciphers are used in this release.
N/A	Security: A new command, no service password-recovery is supported.
N/A	Security: Only one version out of v4 and v6 versions of the uRPF command can be configured on an interface. If one version is configured, all the mode changes must be done by the same version. The other version is blocked on that interface. Cisco Nexus 9300-EX, 9300-FX, and 9300-FX2 platform switches do not have this limitation and you can configure v4 and v6 version of urpf cmd individually.

General Known Issues

Bug ID	Description
CSCvt99828	Setting the value of "none" for the property authName, basically stands for a zero value, which is not allowed, and shouldn't be used. Allowable values other than "none" should be used as inputs to this property.
CSCvt99859	The allocate-label option-b command is disabled and not shown in the configuration unless MPLS Layer 3 VPN is enabled. This is achieved by entering the feature mpls l3vpn command.
CSCvt93823	An NVE interface is required to be in shut state before making changes to the source-interface for NVE. Trying to do the default operation on NVE interface brings it out of the shut state as it performs a no shut first. This causes the operation to fail as there is an attempt to modify the source-interface in the no shut mode. Fixing this might require changes to how the default keyword behaves fundamentally. This can affect other types of interfaces, as well, as they too can be operated on using the default keyword. For this reason, if there is a need to remove the configuration for the NVE interface, enter the shut command on the NVE interface. Then enter the no interface nve 1 command, followed by reconfiguring the NVE interface with the new configuration.

Bug ID	Description
CSCvu48474	Due to an ASIC limitation, FC-FEC cannot be configured on the native (non-retimer) ports (ports 25-36) of N9K-C93600CD-GX when broken out to 2x50G. Only RS-FEC and FEC off are supported. To be consistent, the retimer port (ports 1-24) capabilities are also being limited to RS-FEC and FEC off when broken out to 2x50G. There is no plan to enable FC-FEC on the retimer ports for this reason, so this CDET is being closed.
CSCvu02712	Intermittent CRC errors are seen on Cisco Nexus N9K-C9236C retimer ports (1-8 and 29-36), when connected to Cisco Nexus N9K-C93600CD-GX 100G native ports (25-28) and broken out to 4x25G. The issue is not seen in non-breakout 100G mode. Workarounds: Avoid these connections. Ports 9-28 on the Cisco Nexus N9K-C9236C can be used instead.
CSCvt41915	ISIS route is deleted from kernel when ip unnumbered config is deleted and added back in quick succession (within say 30 seconds) Recovery: ip unnumbered config deletion and addition should be done within the 60-second window to be safe. If issue is hit, recovery is to flap the interface with the shut command followed by the no shut command.

Bug ID	Description
CSCvr20128	The issue happens for pinned static routes only. These routes don't get installed in the kernel. So, BGP sessions over these routes might not work. A ping from Bash will not work. Recovery: If the issue is seen, pinned static routes can be deleted and added back. Also, entering the clear ip route vrf <*vrf-name*> command can be done to recover from the issue. Further Problem Description: 1. The issue happens for pinned static routes only. Pinned static routes is a feature borrowed from Catalyst 6000 IOS platforms and not many customers use it on Cisco Nexus 9000. 2. There are 3 flavors of the issue a. Pinned static route could have a next hop which is not in the subnet of the IP address configured on the interface. In this case, the kernel cannot install the route irrespective of when Netstack sends the route programming request because, the next hop is not in the same subnet of the interface IP address. b. Pinned static route could have some next hops. But on the interface, there is no global IPv6 address configured. It has only a link-local address configured. In this case also, the kernel cannot install the route irrespective of when Netstack sends the route programming request because the next hop is not in the same subnet of the interface IP address. c. Pinned static route could have a next hop which is in the same subnet of the IP address configured on the interface. In this case, the kernel can install the route only if Netstack sends a route programming request after it programs the IP address to the kernel. While programming the route, the kernel determines that the next hop is already programmed. This is a very specific case of pinned static routes.
CSCvc95008	On Cisco Nexus 9300-EX, 9348GC-FXP, 93108TC-FX, 93180YC-FX, 9336C-FX2, 93216TC-FX2, 93360YC-FX2, 93240YC-FX2, 92348GC-X, C93108TC-EX-24, C93108TC-FX-24, C93180YC-EX-24, C93180YC-FX-24, 9316D-GX, 9364C-GX, and 93600CD-GX switches, when 802.1q EtherType has changed on an interface, the EtherType of all interfaces on the same slice will be changed to the configured value. This change is not persistent after a reload of the switch and will revert to the EtherType value of the last port on the slice.
CSCvr92708	CoPP violations can be seen under class-map copp-system-p-class-l2-default and access-group copp-system-p-acl-mac-undesirable in an MVPN setup on a PE device. This can cause an impact to MVPN control plane functionality for packets such as MSDP and PIM register messages, in case of a large number of MVPN PE devices and MDT groups. You can create a custom CoPP policy with an increased "cir" value until no CoPP violation is seen for that class.

Bug ID	Description
CSCvr95514	Per-VRF Configuration of MDT MTU size is not supported on MVPN PE devices on N9K-X9636C-R/RX, N3K-C36180YC-R, N3K-C3636C-R platforms. While, Tunnel MTU size is not configurable interface MTU for the core facing interface can be configured to control port-level MTU. MDT tunnel is capable of carrying up to jumbo MTU size of 9192 (excluding tunnel header), provided interface MTU for the core-facing interface also supports jumbo MTU.
CSCvr92710	CMIS standards prescribe delays at each state as mentioned by the QSFP-DD firmware on those optics. If you are using those optics with delays, you will see a higher link-up time.
CSCvr14625	CMIS standards prescribe delays at each state as mentioned by the QSFP-DD firmware on those optics. If you are using those optics with delays, you will see a higher link-up time.
CSCvr13930	The Cisco Nexus 9300-GX ASIC does not support FC-FEC on the second lane of 50x2 breakout port. This is due to an ASIC limitation. The second link cannot come up when 50x2 breakout is done. Workarounds: You must configure RS-FEC with 50x2 breakout.
CSCvr11900	Multicast routes used by Data MDT are not deleted immediately on MVPN PE (where Encapsulation takes place) after all the customer (VRF) traffic stops which use the same Data MDT. They may stay up for 15 minutes and then get deleted.

N/A	When large files, for example NX-OS, images are copied to USB, the following message is printed:
	
	`2019 Jul  2 15:49:47 Molti_A %$ VDC-1 %$ Jul  2 15:49:46 %KERN-3-SYSTEM_MSG: [ 8032.291555] INFO: task vsh.bin:9418 blocked for more than 120 seconds. – kernel`
	`2019 Jul  2 15:49:47 Molti_A %$ VDC-1 %$ Jul  2 15:49:46 %KERN-3-SYSTEM_MSG: [ 8032.291560]       Tainted: P           O    4.1.21-WR8.0.0.28-standard #1 - kernel`
	`2019 Jul  2 15:49:47 Molti_A %$ VDC-1 %$ Jul  2 15:49:46 %KERN-3-SYSTEM_MSG: [ 8032.291561] "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message. - kernel`
	
	As long as these messages correspond to a copy operation to USB, this message can be ignored.

N/A	In the NX-API sandbox, whenever XML or JSON output is generated for the show run command or the show startup command, the output contains additional characters. For example, </nf:source> <============nf: is extra <namespace> : extra characters are seen with XML and JSON from NX-API.
N/A	When you upgrade a Cisco Nexus 9000 device to Cisco NX-OS Release 9.3(5), if a QSFP port is configured with the manual breakout command and is using a QSA, the configuration of the interface Ethernet 1/50/1 is no longer supported and will need to be removed. To restore the configuration, you must manually configure the interface Ethernet 1/50 on the device.
N/A	Due to the airflow design, back-to-front fans require the fan to be run at full speed all the time. You might also see fan speeds increase from 40% to 70% post-upgrade. This applies to the following PIDs: N9K-C9272Q, N9K-C9236C, N9K-C93180YC-FX, N9K-C93180TC-FX, N9K-C9364C, N9K-C9336C-FX2, N9K-C9332C. This change is made as of Cisco NX-OS Release 7.0(3)I7(3). If your PID is not listed, please contact Cisco TAC for additional verification.
N/A	PTP is not supported on the 96136YC-R line card or for line cards on the Cisco Nexus 9504 switch.

Bug ID	Description
N/A	The following features are not supported on the Cisco Nexus 9364C switch. ■ 100 G port cannot support breakout (HW limitation) ■ FEX ■ ISSU ■ Segment routing ■ Tetration (HW limitation)
N/A	The following feature is not supported on the Cisco Nexus 9332C: ○ uRPF
N/A	Only the following switches support QSFP+ with the QSFP to SFP/SFP+ adapter (40 Gb to 10 Gb): ■ N9K-C93120TX ■ N9K-C93128TX ■ N9K-C9332PQ ■ N9K-C9372PX ■ N9K-C9372PX-E ■ N9K-C9372TX ■ N9K-C9396PX ■ N9K-C93108TC-EX ■ N9K-C93108TC-FX ■ N9K-C93180YC-EX ■ N9K-C93180YC-FX
N/A	The Cisco Nexus 9300 platforms support for the QSFP+ breakout has the following limitations: ■ 1 Gb and 10 Gb can be supported using the QSFP-to-SFP Adapter on 40-Gb uplink ports on Cisco Nexus 9300 platform switches in NX-OS. ■ For the Cisco Nexus 9332PQ switch, all ports except 13-14 and 27-32 can support breakout.

Bug ID	Description
N/A	The following switches and line cards support the breakout cable (40 Gb ports to 4x10-Gb ports): ■ N9K-C9332PQ ■ N9K-X9436PQ line card ■ N9K-X9536PQ line card ■ N9K-C93180LC-EX-–last four ports are breakout capable (10x4, 24x4, 50x2) ■ N9K-C93180YC-EX ■ N9K-C93108TC-EX ■ N9K-X9732C-EX line card ■ N9K-X9732C-FX line card ■ N9K-X97160YC-EX line card ■ N9K-C93180YC-EX ■ N9K-C93108TC-EX ■ N9K-C93180YC-FX ■ N9K-C93108TC-FX ■ N9K-C9348GC-FXP
N/A	Nested VXLAN is supported on a Layer 3 interface or on a Layer 3 port-channel interface from Cisco NX-OS Release 9.3(5) onwards.
N/A	Limitations for ALE (Application Link Engine) uplink ports are listed at the following location: Limitations for ALE 40G Uplink Ports on Cisco Nexus 9000 Series Switches

Device Hardware

The following tables list the Cisco Nexus 9000 Series hardware that Cisco NX-OS Release 9.3(5) supports. For additional information about the supported hardware, see the *Hardware Installation Guide* for your Cisco Nexus 9000 Series device.

Table 1 Cisco Nexus 9500 Switches

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

Table 2 Cisco Nexus 9500 Cloud Scale Line Cards

Product ID	Description	Maximum Quantity		
		Cisco Nexus 9504	Cisco Nexus 9508	Cisco Nexus 9516
N9K-X97160YC-EX	Cisco Nexus 9500 48-port 10/25-Gigabit Ethernet SFP28 and 4-port 40/100 Gigabit Ethernet QSFP28 line card	4	8	16
N9K-X9732C-EX	Cisco Nexus 9500 32-port 40/100 Gigabit Ethernet QSFP28 line card	4	8	16
N9K-X9732C-FX	Cisco Nexus 9500 32-port 40/100 Gigabit Ethernet QSFP28 line card	4	8	16
N9K-X9736C-EX	Cisco Nexus 9500 36-port 40/100 Gigabit Ethernet QSFP28 line card	4	8	16
N9K-X9736C-FX	Cisco Nexus 9500 36-port 40/100 Gigabit Ethernet QSFP28 line card	4	8	16
N9K-X9788TC-FX	Cisco Nexus 9500 48-port 1/10-G BASE-T Ethernet and 4-port 40/100 Gigabit Ethernet QSFP28 line card	4	8	16

Table 3 Cisco Nexus 9500 R-Series Line Cards

Product ID	Description	Maximum Quantity	
		Cisco Nexus 9504	Cisco 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

Table 4 Cisco Nexus 9500 Classic Line Cards

Product ID	Description	Maximum Quantity		
		Cisco Nexus 9504	Cisco Nexus 9508	Cisco Nexus 9516
N9K-X9408C-CFP2	Line card with 8 100 Gigabit CFP2 ports	4	8	16
N9K-X9432C-S	Cisco Nexus 9500 32-port 40/100 Gigabit Ethernet QSFP28 line card	4	8	N/A
N9K-X9432PQ	Cisco Nexus 9500 32-port 40 Gigabit Ethernet QSFP+ line card	4	8	16
N9K-X9636PQ	Cisco Nexus 9500 36-port 40 Gigabit Ethernet QSFP+ line card	4	8	N/A
N9K-X9464PX	Cisco Nexus 9500 48 1/10-Gigabit SFP+ and 4-port 40-Gigabit Ethernet QSFP+ line card	4	8	16
N9K-X9464TX	Cisco Nexus 9500 48 port 1/10-Gigabit BASE-T Ethernet and 4-port 40-Gigabit Ethernet QSFP+ line card	4	8	16
N9K-X9464TX2	Cisco Nexus 9500 48 port 1/10-Gigabit BASE-T Ethernet and 4-port 40-Gigabit Ethernet QSFP+ line card	4	8	16
N9K-X9536PQ	Cisco Nexus 9500 36-port 40 Gigabit Ethernet QSFP+ line card	4	8	16
N9K-X9564PX	Cisco Nexus 9500 48 1/10-Gigabit SFP+ and 4 port 40-Gigabit Ethernet QSFP+ line card	4	8	16
N9K-X9564TX	Cisco Nexus 9500 48 port 1/10-Gigabit BASE-T Ethernet and 4 port 40-Gigabit Ethernet QSFP+ line card	4	8	16

Table 5 Cisco Nexus 9500 Cloud Scale Fabric Modules

Product ID	Description	Minimum	Maximum
N9K-C9504-FM-E	Cisco Nexus 9504 100-Gigabit cloud scale fabric module	4	5

N9K-C9508-FM-E	Cisco Nexus 9508 100-Gigabit cloud scale fabric module	4	5
N9K-C9508-FM-E2	Cisco Nexus 9508 100-Gigabit cloud scale fabric module	4	5
N9K-C9516-FM-E	Cisco Nexus 9516 50-Gigabit cloud scale fabric module	4	5
N9K-C9516-FM-E2	Cisco Nexus 9516 100-Gigabit cloud scale fabric module	4	5

Table 6 Cisco Nexus 9500 R-Series Fabric Modules

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

Table 7 Cisco Nexus 9500 Fabric Modules

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

Table 8 Cisco Nexus 9500 Fabric Module Blanks with Power Connector

Product ID	Description	Minimum	Maximum
N9K-C9508-FM-Z	Cisco Nexus 9508 Fabric blank with Fan Tray Power Connector module	N/A	2
N9K-C9516-FM-Z	Cisco Nexus 9516 Fabric blank with Fan Tray Power Connector module	N/A	2

Table 9 Cisco Nexus 9500 Supervisor Modules

Supervisor	Description	Quantity
N9K-SUP-A	1.8-GHz supervisor module with 4 cores, 4 threads, and 16 GB of memory	2
N9K-SUP-A+	1.8-GHz supervisor module with 4 cores, 8 threads, and 16 GB of memory	2
N9K-SUP-B	2.2-GHz supervisor module with 6 cores, 12 threads, and 24 GB of memory	2

N9K-SUP-B+	1.9-GHz supervisor module with 6 cores, 12 threads, and 32 GB of memory	2

NOTE: N9K-SUP-A and N9K-SUP-A+ are not supported on Cisco Nexus 9504 and 9508 switches with -R line cards.

Table 10 Cisco Nexus 9500 System Controller

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

Table 11 Cisco Nexus 9500 Fans and Fan Trays

Product ID	Description	Quantity
N9K-C9504-FAN	Fan tray for 4-slot modular chassis	3
N9K-C9508-FAN	Fan tray for 8-slot modular chassis	3
N9K-C9516-FAN	Fan tray for 16-slot modular chassis	3

Table 12 Cisco Nexus 9500 Power Supplies

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

Table 13 Cisco Nexus 9200 and 9300 Fans and Fan Trays

Product ID	Description	Quantity	Cisco Nexus Switches	
N9K-C9300-FAN1	Fan 1 module with port-side intake airflow (burgundy coloring)	3	9396PX (early versions)	
N9K-C9300-FAN1-B	Fan 1 module with port-side exhaust airflow (blue coloring)	3	9396PX (early versions)	
N9K-C9300-FAN2	Fan 2 module with port-side intake airflow (burgundy coloring)	3	93128TX	9396PX 9396TX
N9K-C9300-FAN2-B	Fan 2 module with port-side exhaust airflow (blue coloring)	3	93128TX	9396PX 9396TX

Product ID	Description	Quantity	Cisco Nexus Switches	
N9K-C9300-FAN3	Fan 3 module with port-side intake airflow (burgundy coloring)	3	92304QC 9272Q[1]	93120TX
N9K-C9300-FAN3-B	Fan 3 module with port-side exhaust airflow (blue coloring)	3	92304QC 9272Q[1]	93120TX
NXA-FAN-160CFM-PE	Fan module with port-side exhaust airflow (blue coloring)	3	9364C[1]	93360YC-FX2
NXA-FAN-160CFM-PI	Fan module with port-side intake airflow (burgundy coloring)	3	9364C[1]	93360YC-FX2
NXA-FAN-160CFM2-PE	Fan module with port-side exhaust airflow (blue coloring)	4	9364C-GX	
NXA-FAN-160CFM2-PI	Fan module with port-side intake airflow (burgundy coloring)	4	9364C-GX	
NXA-FAN-30CFM-B	Fan module with port-side intake airflow (burgundy coloring)	3	92160YC-X 9236C[1] 93108TC-EX 93108TC-FX[1] 93180LC-EX[1] 93180YC-EX 93180YC-FX[1]	9332PQ 9372PX 9372PX-E 9372TX 9372TX-E 9348GC-FXP[1]
NXA-FAN-30CFM-F	Fan module with port-side exhaust airflow (blue coloring)	3	92160YC-X 9236C[1] 93108TC-EX 93108TC-FX[1] 93180LC-EX[1] 93180YC-EX 93180YC-FX[1]	9332PQ 9372PX 9372PX-E 9372TX 9372TX-E 9348GC-FXP
NXA-FAN-35CFM-PE	Fan module with port-side exhaust airflow (blue coloring)	4	92300YC[1]	9332C[1] 93108TC-FX3P 93180YC-FX3S[2]

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

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

[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.

Table 14 Cisco Nexus 9200 and 9300 Power Supplies

Product ID	Description	Quantity	Cisco Nexus Switches	
NXA-PAC-500W-PE	500-W AC power supply with port-side exhaust airflow (blue coloring)	2	93108TC-EX 93180LC-EX	93180YC-EX 93180YC-FX
NXA-PAC-500W-PI	500-W AC power supply with port-side intake airflow (burgundy coloring)	2	93108TC-EX 93180LC-EX	93180YC-EX 93180YC-FX
N9K-PAC-650W	650-W AC power supply with port-side intake (burgundy coloring)	2	9332PQ 9372PX 9372PX-E 9372TX	9372TX-E 9396PX 9396TX
N9K-PAC-650W-B	650-W AC power supply with port-side exhaust (blue coloring)	2	9332PQ 9372PX 9372PX-E 9372TX	9372TX-E 9396PX 9396TX
NXA-PAC-650W-PE	650-W power supply with port-side exhaust (blue coloring)	2	92160YC-X 9236C	92304QC 93108TC-

Product ID	Description	Quantity	Cisco Nexus Switches	
			92300YC 93180YC-FX3S	EX 93180YC-EX
NXA-PAC-650W-PI	650-W power supply with port-side intake (burgundy coloring)	2	92160YC-X 9236C 92300YC 93180YC-FX3S	92304QC 93108TC-EX 93180YC-EX
NXA-PAC-750W-PE	750-W AC power supply with port-side exhaust airflow (blue coloring) [1]	2	9336C-FX2 93240YC-FX2	9332C 9336C-FX2
NXA-PAC-750W-PI	750-W AC power supply with port-side exhaust airflow (burgundy coloring) [1]	2	9336C-FX2 93240YC-FX2	9332C 9336C-FX2
NXA-PAC-1100W-PE2	1100-W AC power supply with port-side exhaust airflow (blue coloring)	2	93240YC-FX2 9332C 9316D-GX	9336C-FX2 93600CD-GX
NXA-PAC-1100W-PI2	1100-W AC power supply with port-side intake airflow (burgundy coloring)	2	93240YC-FX2 9332C 9316D-GX	9336C-FX2 93600CD-GX
NXA-PAC-1100W-PI	Cisco Nexus 9000 PoE 1100W AC PS, port-side intake	2	93108TC-FX3P	
NXA-PAC-1100W-PE	Cisco Nexus 9000 PoE 1100W AC PS, port-side exhaust	2	93108TC-FX3P	
NXA-PAC-1900W-PI	Cisco Nexus 9000 PoE 1900W AC PS, port-side intake	2	93108TC-FX3P	
N9K-PAC-1200W	1200-W AC power supply with port-side intake airflow (burgundy coloring)	2	93120TX	
N9K-PAC-1200W-B	1200-W AC power supply with port-side exhaust airflow (blue coloring)	2	93120TX	
NXA-PAC-1200W-PE	1200-W AC power supply with port-side exhaust airflow (blue coloring)	2	9272Q 93360YC-FX2	9364C

Product ID	Description	Quantity	Cisco Nexus Switches	
NXA-PAC-1200W-PI	1200-W AC power supply with port-side intake airflow (burgundy coloring)	2	9272Q 93360YC-FX2	9364C
N9K-PUV-1200W	1200-W Universal AC/DC power supply with bidirectional airflow (white coloring)	2	92160YC-X 9236C 92300YC 92304QC 9272Q[1] 93108TC-EX 93108TC-FX 93360YC-FX2 93180YC-FX3S	93120TX 93128TX 93180LC-EX 93180YC-EX 93180YC-FX 9364C
NXA-PDC-930W-PE	930-W DC power supply with port-side exhaust airflow (blue coloring)	2	9272Q 93108TC-EX 93180YC-EX 93360YC-FX2 93180YC-FX3S	93120TX 93180YC-FX 9364C 92160YC-X
NXA-PDC-930W-PI	930-W DC power supply with port-side intake airflow (burgundy coloring)	2	9272Q 93108TC-EX 93180YC-EX 93360YC-FX2 93180YC-FX3S	93120TX 93180YC-FX 9364C 92160YC-X
NXA-PDC-1100W-PE	1100-W DC power supply with port-side exhaust airflow (blue coloring)	2	93240YC-FX2 93600CD-GX 9316D-GX	9332C 9336C-FX2
NXA-PDC-1100W-PI	1100-W DC power supply with port-side intake airflow (burgundy coloring)	2	93240YC-FX2 93600CD-GX 9316D-GX	9332C 9336C-FX2
UCSC-PSU-930WDC	930-W DC power supply with port-side intake (green coloring)	2	92160YC-X 9236C 92304QC 9272Q 93108TC-EX	9332PQ 9372PX 9372PX-E 9372TX

Product ID	Description	Quantity	Cisco Nexus Switches	
			93120TX 93128TX 93180YC-EX	9372TX-E 9396PX 9396TX
UCS-PSU-6332-DC	930-W DC power supply with port-side exhaust (gray coloring)	2	92160YC-X 9236C 92304QC 9272Q 93108TC-EX 93120TX 93128TX 93180YC-EX	9332PQ 9372PX 9372PX-E 9372TX 9372TX-E 9396PX 9396TX
NXA-PHV-1100W-PE	1100-W AC power supply with port-side exhaust airflow (blue coloring)	2	93240YC-FX2	9336C-FX2
NXA-PHV-1100W-PI	1100-W AC power supply with port-side intake airflow (burgundy coloring)	2	93240YC-FX2	9336C-FX2
NXA-PAC-2KW-PE	2000-W AC power supply with port-side exhaust airflow (blue coloring)	2	9364C-GX	
NXA-PAC-2KW-PI	2000-W AC power supply with port-side intake airflow (burgundy coloring)	2	9364C-GX	
NXA-PDC-2KW-PE	2000-W DC power supply with port-side exhaust airflow (blue coloring	2	9364C-GX	
NXA-PDC-2KW-PI	2000-W DC power supply with port-side intake airflow (burgundy coloring)	2	9364C-GX	
N2200-PAC-400W	400-W AC power supply with port-side exhaust airflow (blue coloring)	2	92348GC-X	
N2200-PAC-400W-B	400-W AC power supply with port-side intake airflow (burgundy coloring)	2	92348GC-X	
N2200-PDC-350W-B	350-W DC power supply with port-side intake airflow	2	92348GC-X	
N2200-PDC-400W	400-W DC power supply with port-side exhaust airflow (blue coloring)	2	92348GC-X	

[1] Compatible with Cisco NX-OS Release 9.3(3) and later.

Table 15 Cisco Nexus 9200 and 9300 Switches

Cisco Nexus Switch	Description
N9K-C92160YC-X	1-RU Top-of-Rack switch with 48 10-/25-Gigabit SFP+ ports and 6 40-Gigabit QSFP+ ports (4 of these ports support 100-Gigabit QSFP28 optics).
N9K-C92300YC	1.5-RU Top-of-Rack switch with 48 10-/25-Gigabit SFP28 ports and 18 fixed 40-/100-Gigabit QSFP28 ports.

Cisco Nexus Switch	Description
N9K-C92304QC	2-RU Top-of-Rack switch with 56 40-Gigabit Ethernet QSFP+ ports (16 of these ports support 4x10 breakout cables) and 8 100-Gigabit QSFP28 ports.
N9K-C92348GC-X	The Cisco Nexus 92348GC-X switch (N9K-C92348GC-X) is a 1RU switch that supports 696 Gbps of bandwidth and over 250 mpps. The 1GBASE-T downlink ports on the 92348GC-X can be configured to work as 100-Mbps, 1-Gbps ports. The 4 ports of SFP28 can be configured as 1/10/25-Gbps and the 2 ports of QSFP28 can be configured as 40- and 100-Gbps ports. The Cisco Nexus 92348GC-X is ideal for big data customers that require a Gigabit Ethernet ToR switch with local switching.
N9K-C9236C	1-RU Top-of-Rack switch with 36 40-/100-Gigabit QSFP28 ports (144 10-/25-Gigabit ports when using breakout cables)
N9K-C9272Q	2-RU Top-of-Rack switch with 72 40-Gigabit Ethernet QSFP+ ports (35 of these ports also support 4x10 breakout cables for 140 10-Gigabit ports)
N9K-C93108TC-EX	1-RU Top-of-Rack switch with 48 10GBASE-T (copper) ports and 6 40-/100-Gigabit QSFP28 ports
N9K-C93108TC-EX-24	1-RU 24 1/10GBASE-T (copper) front panel ports and 6 40/100-Gigabit QSFP28 spine facing ports.
N9K-C93108TC-FX	1-RU Top-of-Rack switch with 48 100M/1/10GBASE-T (copper) ports and 6 40-/100-Gigabit QSFP28 ports
N9K-C93108TC-FX-24	1-RU 24 1/10GBASE-T (copper) front panel ports and 6 fixed 40/100-Gigabit Ethernet QSFP28 spine-facing ports.
N9K-C93108TC-FX3P	1-RU fixed-port switch with 48 100M/1/2.5/5/10GBASE-T ports and 6 40-/100-Gigabit QSFP28 ports
N9K-C93120TX	2-RU Top-of-Rack switch with 96 1/10GBASE-T (copper) ports and 6 40-Gigabit QSFP+ ports
N9K-C93128TX	3-RU Top-of-Rack switch with 96 1/10GBASE-T (copper) ports and an uplink module up to 8 40-Gigabit QSFP+ ports
N9K-C9316D-GX	1-RU switch with 16x400/100/40-Gbps ports.
N9K-C93180LC-EX	1-RU Top-of-Rack switch with 24 40-/50-Gigabit QSFP+ downlink ports and 6 40/100-Gigabit uplink ports. You can configure 18 downlink ports as 100-Gigabit QSFP28 ports or as 10-Gigabit SFP+ ports (using breakout cables).
N9K-C93180YC-EX	1-RU Top-of-Rack switch with 48 10-/25-Gigabit SFP28 fiber ports and 6 40-/100-Gigabit QSFP28 ports
N9K-C93180YC-EX-24	1-RU 24 1/10/25-Gigabit front panel ports and 6-port 40/100 Gigabit QSFP28 spine-facing ports
N9K-C93180YC-FX	1-RU Top-of-Rack switch with 10-/25-/32-Gigabit Ethernet/FC ports and 6 40-/100-Gigabit QSFP28 ports. You can configure the 48 ports as 1/10/25-Gigabit Ethernet ports or as FCoE ports or as 8-/16-/32-Gigabit Fibre Channel ports.

Cisco Nexus Switch	Description
N9K-C93180YC-FX-24	1-RU 24 1/10/25-Gigabit Ethernet SFP28 front panel ports and 6 fixed 40/100-Gigabit Ethernet QSFP28 spine-facing ports. The SFP28 ports support 1-, 10-, and 25-Gigabit Ethernet connections and 8-, 16-, and 32-Gigabit Fibre Channel connections.
N9K-C93180YC-FX3S	1-RU, fixed-port switch with: • 48 25/50/100-Gigabit Ethernet SFP28 ports (ports 1-48). All of these ports are Unified Ports and can support 8/16/32-Gigabit FC. • 6 10/25/40/50/100-Gigabit QSFP28 ports (ports 49-54) • One management port (one 10/100/1000BASE-T port) • One console port (RS-232) • 1 USB port
N9K-C93216TC-FX2	2-RU switch with 96 100M/1G/10G RJ45 ports, 12 40/100-Gigabit QSFP28 ports, 2 management ports (one RJ-45 and one SFP port), 1 console, port, and 1 USB port.
N9K-C93240YC-FX2	1.2-RU Top-of-Rack switch with 48 10-/25-Gigabit SFP28 fiber ports and 12 40-/100-Gigabit Ethernet QSFP28 ports.
N9K-C9332C	1-RU fixed switch with 32 40/100-Gigabit QSFP28 ports and 2 fixed 1/10-Gigabit SFP+ ports.
N9K-C9332PQ	1-RU switch with 32 40-Gigabit Ethernet QSFP+ ports (26 ports support 4x10 breakout cables and 6 ports support QSFP-to-SFP adapters)
N9K-C93360YC-FX2	2-RU switch with 96 10-/25-Gigabit SFP28 ports and 12 40/100-Gigabit QSFP28 ports
N9K-C9336C-FX2	1-RU switch with 36 40-/100-Gb Ethernet QSFP28 ports.
N9K-C9348GC-FXP	Nexus 9300 with 48p 100M/1 G, 4p 10/25 G SFP+ and 2p 100 G QSFP
N9K-C93600CD-GX	1-RU fixed-port switch with 28 10/40/100-Gigabit QSFP28 ports (ports 1-28), 8 10/40/100/400-Gigabit QSFP-DD ports (ports 29-36)
N9K-C9364C	2-RU Top-of-Rack switch with 64 40-/100-Gigabit QSFP28 ports and 2 1-/10-Gigabit SFP+ ports. - Ports 1 to 64 support 40/100-Gigabit speeds. - Ports 49 to 64 support MACsec encryption. Ports 65 and 66 support 1/10 Gigabit speeds.
N9K-C9364C-GX	2-RU fixed-port switch with 64 100-Gigabit SFP28 ports.
N9K-C9372PX	1-RU Top-of-Rack switch with 48 1-/10-Gigabit SFP+ ports and 6 40-Gigabit QSFP+ ports
N9K-C9372PX-E	An enhanced version of the Cisco Nexus 9372PX-E switch.
N9K-C9372TX	1-RU Top-of-Rack switch with 48 1-/10GBASE-T (copper) ports and 6 40-Gigabit QSFP+ ports

Cisco Nexus Switch	Description
N9K-C9372TX-E	An enhanced version of the Cisco Nexus 9372TX-E switch.
N9K-C9396PX	2-RU Top-of-Rack switch with 48 1-/10-Gigabit Ethernet SFP+ ports and an uplink module with up to 12 40-Gigabit QSFP+ ports
N9K-C9396TX	2-RU Top-of-Rack switch with 48 1/10GBASE-T (copper) ports and an uplink module with up to 12 40-Gigabit QSFP+ ports

Table 16 Cisco Nexus 9000 Series Uplink Modules

Product ID	Description
N9K-M4PC-CFP2	Cisco Nexus 9300 uplink module with 4 100-Gigabit Ethernet CFP2 ports. For the Cisco Nexus 93128TX switch, only two of the ports are active. For the Cisco Nexus 9396PX and 9396TX switches, all four ports are active.
N9K-M6PQ	Cisco Nexus 9300 uplink module with 6 40-Gigabit Ethernet QSFP+ ports for the Cisco Nexus 9396PX, 9396TX, and 93128TX switches.
N9K-M6PQ-E	An enhanced version of the Cisco Nexus N9K-M6PQ uplink module.
N9K-M12PQ	Cisco Nexus 9300 uplink module with 12 40-Gigabit Ethernet QSPF+ ports.

Optics

To determine which transceivers and cables are supported by a switch, see the Transceiver Module (TMG) Compatibility Matrix.

To see the transceiver specifications and installation information, see the Install and Upgrade Guides.

Cisco Network Insights for Data Center

Cisco NX-OS Release 9.3(5) supports the Cisco Network Insights Advisor (NIA) and Cisco Network Insights for Resources (NIR) on Cisco Nexus 9200, 9300-EX, and 9300-FX platform switches and 9500 platform switches with -EX/FX line cards.

For more information, see the Cisco Network Insights documentation.

Upgrade and Downgrade

To perform a software upgrade or downgrade, follow the instructions in the *Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 9.3(x)*.

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

Exceptions

- Cisco Nexus 9200, 9300-EX, and 9300-FX Platform Switches
- Cisco Nexus 9300-FX3 Platform Switches

- Cisco Nexus 9300-GX Platform Switches
- Cisco Nexus 9500 Platform N9K-X9408PC-CFP2 Line Card and 9300 Platform Switches
- FEX Modules
- N9K-X96136YC-R Line Card
- N9K-X9736C-FX Line Card
- Nexus 9500 Cloud Scale

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

The following features are not supported for the Cisco Nexus 9200, 9300-EX, and 9300-FX platform switches:

- 64-bit ALPM routing mode
- Cisco Nexus 9272PQ and Cisco Nexus 92160YC platforms do not support the PXE boot of the Cisco NX-OS image from the loader.
- ACL filters to span subinterface traffic on the parent interface
- Egress port ACLs
- Egress QoS policer (not supported for Cisco Nexus 9200 platform switches). The only policer action supported is drop. Remark action is not supported on the egress policer.
- FEX (not supported for Cisco Nexus 9200 platform switches)
- GRE v4 payload over v6 tunnels
- IP length-based matches
- IP-in-IP (not supported on the Cisco Nexus 92160 switch)
- Maximum Transmission Unit (MTU) checks for packets received with an MPLS header
- NetFlow (not supported on Cisco Nexus 9200 platform switches)
- Packet-based statistics for Traffic Storm Control (only byte-based statistics are supported)
- PVLANs (not supported on Cisco Nexus 9200 platform switches)
- PXE boot of the Cisco NX-OS image from the loader (not supported for Cisco Nexus 9272PQ and 92160YC switches)
- Q-in-VNI (not supported on Cisco Nexus 9200 platform switches)
- Q-in-Q for VXLAN (not supported on Cisco Nexus 9200 and 9300-EX platform switches)
- Q-in-VNI (not supported on Cisco Nexus 9200 platform switches)
- Resilient hashing for port channels
- Rx SPAN for multicast if the SPAN source and destination are on the same slice and no forwarding interface is on the slice

- SVI uplinks with Q-in-VNI (not supported for Cisco Nexus 9300-EX platform switches)
- Traffic Storm Control for copy-to-CPU packets
- Traffic Storm Control with unknown multicast traffic
- Tx SPAN for multicast, unknown multicast, and broadcast traffic
- VACL redirects for TAP aggregation

Cisco Nexus 9300-FX3 Platform Switches

The following features are not supported for the Cisco Nexus 9300-FX3 Platform switches:

- ACL with DSCP Wildcard Mask
- ARP Suppression with Reflective Relay
- Dynamic ACL - Named ACL support for applying blacklist/limited VLAN access for devices
- ECMP Hashing based on GRE Inner IP Header
- Enhanced ISSU
- Enhanced Policy-Based Routing (ePBR)
- ePBR Multi-Hop
- ePBR with Probes
- ePBR with User-Defined Probes
- IPv6 MIB support (IP-MIB)
- Multicast Service Reflection (Ingress, PIM-border, Egress)
- Multiple LLDP neighbors per physical interface
- Secure VXLAN EVPN Multi-Site using CloudSec
- Selective Q-in-VNI + Advertise PIP on a VTEP
- Selective Q-in-VNI + VXLAN VLAN on the same port
- Standard ISSU
- Symmetric Hashing - ECMP (Inner DA)
- Unidirectional Ethernet (UDE)
- VXLAN EVPN with downstream VNI
- VXLAN over parent interface that also carries sub-interfaces

Cisco Nexus 9300-GX Platform Switches

The following features are not supported for the Cisco Nexus 9300-GX platform switches:

- 802.1x with VXLAN
- Asymmetric PFC
- Autonegotiation on all ports
- Enhanced ISSU
- FC-FEC for Cisco Nexus 9316D-GX and 93600CD-GX switches is not supported on the second lane of the 50x2 breakout port.
- FEX
- FTE
- IPv6 Underlay, TRM + Multi-Site
- ITD with VXLAN
- Multi Auth with COA
- Multicast NLB
- Multicast over GRE
- RTP Monitoring
- Standard ISSU
- TRM + Multi-Site
- VRF Aware FT
- VXLAN F&L
- VXLAN - PBR

Cisco Nexus N9K-X9408PC-CFP2 Line Card and 9300 Platform Switches

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

- 802.3x
- Breakout ports
- FEX (supported on some Cisco Nexus 9300 platform switches)
- Flows other than 40G
- Multichassis EtherChannel Trunk (MCT)
- NetFlow
- Port-channel (No LACP)
- PFC/LLFC

- Precision Time Protocol (PTP)
- PVLAN (supported on Cisco Nexus 9300 platform switches)
- Shaping support on 100g port is limited
- SPAN destination/ERSPAN destination IP
- Traffic Storm Control
- vPC
- VXLAN access port

FEX Modules

The following features are not supported for FEX modules:

- Active-Active FEX and straight-through FEX are not supported on the Cisco Nexus 92348GC switch.
- For Cisco Nexus 9500 platform switches, 4x10-Gb breakout for FEX connectivity is not supported.

Cisco Nexus N9K-X96136YC-R Line Card

The following features are not supported for Cisco Nexus 9500 platform switches with the N9K-X96136YC-R line card:

- Breakout
- PTP and gPTP

Cisco Nexus N9K-X9736C-FX Line Card

The following feature is not supported for Cisco Nexus 9500 platform switches with the N9K-X9736C-FX line card:

- Ports 29-36 do not support 1 Gbps speed.

Cisco Nexus 9500 Cloud Scale (EX/FX) Line Cards

The following features are not supported for Cisco Nexus 9500 platform switches with -EX/FX line cards:

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

Related Content

Cisco Nexus 3000 and 9000 Series NX-API REST SDK User Guide and API Reference: Cisco Nexus NX-API Reference

Cisco Nexus 9000 Series documentation: Cisco Nexus 9000 Series Switches

Cisco Nexus 9000 and 3000 Series NX-OS Switch License Navigator: Cisco Nexus 9000 and 3000 Series NX-OS Switch License Navigator

Cisco Nexus 9000 Series Software Upgrade and Downgrade Guide: Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 9.3(x)

Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes: Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes, Release 9.3(5)

Cisco Nexus OpenConfig YANG Reference, Release 9.3(x): Cisco Nexus OpenConfig YANG Reference, Release 9.3(x)

Cisco NX-OS Supported MIBs: ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html

Supported FEX modules: Cisco Nexus 9000 Series Switch FEX Support Matrix.

Licensing Information: Cisco NX-OS Licensing Guide

When you downgrade from Cisco NX-OS Release 9.3(5) to an earlier release, the features that use the ACI+NX-OS Essentials, Advantage, and add-on licenses or the Hardware Streaming Telemetry license continue to work in honor mode in the downgraded version. In addition, the output of the show license usage command continues to include entries for these unsupported licenses.

For more information, see the Cisco NX-OS Licensing Guide.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus9k-docfeedback@cisco.com. We appreciate your feedback.

Legal Information