Cisco Nexus 9000 Series NX-OS Release Notes, Release 7.0(3)I2(1)

This document describes the features, caveats, and limitations for Cisco NX-OS Release 7.0(3)I2(1) software for use on the Cisco Nexus 9000 Series switches, the Cisco Nexus 31128PQ switch, and the Cisco Nexus 3164Q switch. Use this document in combination with documents listed in *Related Documentation*.

Note: Starting with Cisco NX-OS Release 7.0(3)I2(1), the Cisco NX-OS image filename has changed to start with "nxos" instead of "n9000."

Note: The Cisco Nexus 3000 code has merged with the Cisco Nexus 9000 code in Cisco NX-OS Release 7.0(3)|2(1). For a list of the Cisco Nexus 3000 changes in this release, see the *Cisco Nexus 3000 Series NX-OS Release Notes* and *Cisco NX-OS Release 7.0(3)I2(1) Overview.*

Table 1 shows the online change history for this document.

Table 1. Online History Change

Date	Description
September 4, 2015	Created the release notes for Release 7.0(3)I2(1).
September 8, 2015	■ Added 9332PQ and 9372PX-E to the *Supported FEX Modules* section. ■ Added a note to the *Supported FEX Modules* section stating “Cisco Nexus 9300 Series switches do not support FEX on uplink modules (ALE).”
September 9, 2015	■ Removed a statement from the *Configuring Private VLANs* section that said private VLANs do not support FEXes. ■ Clarified a statement about FEX in the *Unsupported Features* section. ■ Specified that the 9332PQ only supports 2300 FEX.
September 10, 2015	Changed PVLAN FEX support feature description to state that all FEXes are supported.
September 17, 2015	Added switchport isolated feature to the list of new features.

Date	Description
September 18, 2015	Removed the following from the release notes: ■ In a non-BGP eVPN environment, the SVI for L2/L3 boundary is expected to be on a non-VTEP routing block (a routerattached to a VTEP). ■ BGP eVPN neighbors are not supported over VPC interfaces.
September 21, 2015	Added N2K-C2348TQ-10GE to supported FEX.
September 28, 2015	Added Supported Cisco Software Releases section.
October 1, 2015	Specified that the N9K-C93120TX switch supports the QSFP+ with QSA adapter (40G to 10G QSA).
October 7, 2015	Updated the description of the switchport isolated feature.
October 13, 2015	■ Changed a note in *Limitations* to say: "The Nexus 9300 support for the QSFP+ breakout has the following limitations." ■ Stated that ISSU is not supported on Nexus 9000 Series switches in *Limitations*.
October 19, 2015	Removed N9K-C93120TX from the list of switches that support the breakout cable.
October 22, 2015	Removed "On the Nexus 9500 series, X9464PX and X9564 PX line cards are supported for FEX connectivity using the SPF+ ports."
December 1, 2015	Removed port profile support statement.
January 11, 2016	Added a link to the ALE limitations in the *Limitations* section.
March 4, 2016	■ Updated *Limitations*. ■ Updated *Supported FEX Modules*.

Date	Description
March 7, 2016	Specified switches that support the inner VLAN and outer VLAN mapping on a trunk port feature.
March 23, 2016	Removed the bullets stating that private VLANs support PVLAN across switches: ■ Through a regular trunk port-channel ■ Through a regular vPC-port
April 8, 2016	Added the following statement to *Limitations*: The N9K-X9408PC-CFP2 line card does not support port-channeling.
May 25, 2016	■ Added Cisco Nexus 9408 Line Card and 9300 Series Leaf Switches section ■ Added to FEX limitations: VTEP connected to FEX host interface ports is not supported. ■ Added to the Supported FEX Modules section: Note: For Cisco Nexus 9500 switches, 4x10G breakout for FEX connectivity is not supported. Native 10G or 40G should be used.
June 6, 2016	■ Updated Table 2 ■ Added link to Cisco Nexus 31128PQ Switch - Read Me First

Contents

Introduction

Cisco NX-OS software is a data center-class operating system designed for performance, resiliency, scalability, manageability, and programmability at its foundation. The Cisco NX-OS software provides a robust and comprehensive feature set that meets the requirements of virtualization and automation in mission-critical data center environments. The modular design of the Cisco NX-OS operating system makes zero-impact operations a reality and enables exceptional operational flexibility.

The Cisco Nexus 9000 Series uses an enhanced version of Cisco NX-OS software with a single binary image that supports every switch in the series, which simplifies image management.

System Requirements

This section includes the following sections:

- Supported Cisco Software Releases
- Supported Device Hardware
- Supported Optics
- Supported FEX Modules

Supported Cisco Software Releases

Table 2 summarizes information about the Cisco Nexus platforms and software release versions that Cisco OpenFlow Plug-in supports.

Table 2. Cisco Plug-in for OpenFlow Compatibility Matrix

Switches	Cisco Plug-in for OpenFlow
Cisco Nexus 9300 Series switches and Cisco Nexus 31128PQ switches NX-OS 7.0(3)I2(1)	ofa-2.1.0-r1-nxos-SPA-k9.ova

Supported Device Hardware

Table 3 lists the Cisco Nexus 9000 Series hardware that Cisco NX-OS Release 7.0(3)I2(1) supports. For additional information about the supported hardware, see the Hardware Installation Guide for your Cisco Nexus 9000 Series device.

Table 3. Cisco Nexus 9000 Series Hardware

Product ID	Hardware	Quantity

Product ID	Hardware	Quantity
N9K-C9516	Cisco Nexus 9516 16-slot chassis	1
N9K-C9516-FM	Cisco Nexus 9500 Series fabric module	3-6 depending on the line card
N9K-C9516-FAN	Cisco Nexus 9516 fan trays	3
N9K-C9508	Cisco Nexus 9508 8-slot chassis	1
N9K-C9508-FM	Cisco Nexus 9508 Series fabric module	3-6 depending on the line card
N9K-C9508-FAN	Cisco Nexus 9508 fan trays	3
N9K-X9564PX	Cisco Nexus 9500 Series 48-port, 1-/10-Gbps SFP+ plus 4-port QSFP I/O module	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 16 in the Cisco Nexus 9516
N9K-X9564TX	Cisco Nexus 9500 Series 48-port, 1-/10-Gbps BASE-T plus 4-port QSFP I/O module	■ Up to 8 in the Cisco Nexus 9508 ■ Up to 4 in the Cisco Nexus 9504 ■ Up to 16 in the Cisco Nexus 9516

Product ID	Hardware	Quantity
N9K-X9536PQ	Cisco Nexus 9500 36-port, 40 Gigabit Ethernet QSFP aggregation module	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 16 in the Cisco Nexus 9516
N9K-X9636PQ	Cisco Nexus 9500 Series 36-port 40-Gigabit QSFP I/O module Note: Not supported on the Cisco Nexus 9516 switch (N9K-C9516).	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508
N9K-X9464PX	Cisco Nexus 9500 Series 48-port 10-Gigabit SFP+ plus 4-port QSFP I/O module	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 16 in the Cisco Nexus 9516
N9K-X9464TX	Cisco Nexus 9500 Series 48-port 10-GBASE-T plus 4-port QSFP I/O module	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 16 in the Cisco Nexus 9516

Product ID	Hardware	Quantity
N9K-X9432PQ	Cisco Nexus 9500 Series 32-port 40-Gigabit QSFP I/O module Note: The Cisco Nexus X9432PQ I/O module supports static breakout.	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 16 in the Cisco Nexus 9516
N9K-X9408PC-CFP2	Cisco Nexus 9500 Series 8-port 100-Gigabit CFP2 I/O module for the Cisco Nexus 9504, 9508, and 9516 modular switches	■ Up to 4 in the Cisco Nexus ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 16 in the Cisco Nexus 9516
N9K-SC-A	Cisco Nexus 9500 Series System Controller Module	2
N9K-SUP-A	Cisco Nexus 9500 Series supervisor module	2
N9K-SUP-B	Cisco Nexus 9500 Series supervisor B module	2
N9K-PAC-3000W-B	Cisco Nexus 9500 Series 3000 W AC power supply	■ Up to 4 in the Cisco Nexus 9504 ■ Up to 8 in the Cisco Nexus 9508 ■ Up to 10 in the Cisco Nexus 9516
N9K-C9504	Cisco Nexus 9504 4-slot chassis	1
N9K-C9504-FM	Cisco Nexus 9504 fabric module	3 to 6 depending on line card
N9K-C9504-FAN	Cisco Nexus 9504 fan trays	3

Product ID	Hardware	Quantity
N9K-C9396PX	Cisco Nexus 9300 48-port, 1/10-Gigabit Ethernet SFP+ and 12-port, 40-Gigabit Ethernet QSPF switch	1
N9K-C9396TX	Cisco Nexus 9300 48-port, 1/10-Gigabit Ethernet BASE-T and 12-port, 40-Gigabit Ethernet QSFP switch	1
N9K-C9372PX	Cisco Nexus 9300 48-port, 1/10-Gigabit Ethernet SFP+ and 6-port, 40-Gigabit Ethernet QSFP switch	1
N9K-C9372PX-E	An enhanced version of the N9K-C9372PX.	
N9K-C9372TX	Cisco Nexus 9300 48-port, 1/10-Gigabit Ethernet BASE-T and 6-port, 40-Gigabit Ethernet QSFP switch	1
N9K-C9332PQ	Cisco Nexus 9300 32-port, 40-Gigabit Ethernet QSFP switch with support for 4x10G breakout mode ■ Ports 1 to 26 (except 13 and 14) support 4x10G breakout mode. ■ Ports 27 to 32 (ALE uplink ports) support using QSA for 10G SFP/SFP+ transceivers in QSFP+ ports	1
N9K-C93128TX	Cisco Nexus 9300 switch with 96 1-/10-Gigabit BASE-T ports and eight 40-Gigabit Ethernet QSPF ports (The 1-/10-Gigabit BASE-T ports also support a speed of 100 Megabits.)	1
N9K-C93120TX	Cisco Nexus 93120TX switch with 96 1-/10-Gigabit BASE-T ports and 6 QSFP uplink ports	
N9K-PAC-650W	Cisco Nexus 9300 650 W AC power supply, hot air out (red) Note: For use with the Cisco Nexus 9396 switch (N9K-C9396PX).	2 or less
N9K-PAC-650W-B	Cisco Nexus 9300 650 W AC power supply, cold air in (blue) Note: For use with the Cisco Nexus 9396 switch (N9K-C9396PX).	2 or less
N9K-PAC-1200W	Cisco Nexus 9300 1200 W AC power supply, hot air out (red) Note: For use with the Cisco Nexus 93128 switch (N9K-C93128TX).	2 or less
N9K-PAC-1200W-B	Cisco Nexus 9300 1200 W AC power supply, cold air in (blue) Note: For use with the Cisco Nexus 93128 switch (N9K-C93128TX).	2 or less
N9K-C9300-FAN1	Cisco Nexus 9300 fan 1, hot air out (red) Note: For use with the Cisco Nexus 9396 switch (N9K-C9396PX).	3

Product ID	Hardware	Quantity
N9K-C9300-FAN1-B	Cisco Nexus 9300 fan 1, cold air in (blue) Note: For use with the Cisco Nexus 9396 switch (N9K-C9396PX).	3
N9K-C9300-FAN2	Cisco Nexus 9300 fan 2, port side intake (red) Note: For use with the Cisco Nexus 93128 switch (N9K-C93128TX).	3
N9K-C9300-FAN2-B	Cisco Nexus 9300 fan 2, port side exhaust (blue) Note: For use with the Cisco Nexus 93128 switch (N9K-C93128TX).	3
NXA-FAN-30CFM-F	Cisco Nexus 9300 fan, port-side exhaust Note: For use with the Cisco Nexus 93128 switch (N9K-C93128TX).	4
NXA-FAN-30CFM-B	Cisco Nexus 9300 fan, port-side intake Note: For use with the Cisco Nexus 9332PQ, 9372PX, and 9372TX switches (N9K-C9332PQ, N9K-C9372PX, and N9K-9372TX).	4
N9K-M12PQ	Cisco Nexus GEM 9300 uplink module, 12-port, 40-Gigabit Ethernet QSPF Note: The front-panel ports on these GEM modules do not support auto negotiation with copper cables. Manually configure the speed on the peer switch	1 (required)
N9K-M6PQ	Cisco Nexus GEM 6-port 40-Gigabit Ethernet uplink module for the Cisco Nexus 9396PX, 9396TX, and 93128TX switches Note: The front-panel ports on these GEM modules do not support auto negotiation with copper cables. Manually configure the speed on the peer switch.	1
N9K-M6PQ-E	An enhanced version of the N9K-M6PQ.	
N9K-M4PC-CFP2	Cisco Nexus 9300 uplink module for the 93128TX (2 active ports), 9396PX (4 active ports), and 9396TX (4 active ports) Top-of-rack switches	1

Table 4 lists the Cisco Nexus 3164Q switch hardware that Cisco NX-OS Release 7.0(3)I2(1) supports.

Table 4. Cisco Nexus 3164Q Switch Hardware

Product ID	Hardware	Quantity
N3K-C3164Q-40GE	Cisco Nexus 3164Q switch	1

N9K-C9300-FAN3	Cisco Nexus 3164Q fan module	3
N9K-PAC-1200W	Cisco Nexus 3164Q 1200W AC power supply	2

For additional information about the supported hardware, see the *Cisco Nexus 3000 Series Hardware Installation Guide*.

Table 5 lists the Cisco Nexus 31128PQ switch hardware that Cisco NX-OS Release 7.0(3)I2(1) supports.

Table 5. Cisco Nexus 31128PQ Switch Hardware

Product ID	Hardware	Quantity
N3K-C31128PQ-10GE	Nexus 31128PQ, 96 SFP+ ports, 8 QSFP+ ports, 2RU switch	1

Supported Optics

See the *Cisco 10-Gigabit Ethernet Transceiver Modules Compatibility Matrix* for a list of supported optical components.

Supported FEX Modules

Cisco NX-OS Release 7.0(3)I2(1) supports the following FEXes on Cisco Nexus 9332PQ (support for 2300 only), 9372PX, 9372PX-E, 9396PX and 9500 Series Switches:

- Cisco Nexus 2224TP
- Cisco Nexus 2232PP
- Cisco Nexus 2232TM and 2232TM-E
- Cisco Nexus 2248PQ
- Cisco Nexus 2248TP and 2248TP-E
- Cisco Nexus 2348UPQ
- Cisco Nexus B22Dell
- Cisco Nexus B22HP
- Cisco Nexus NB22FTS
- Cisco Nexus NB22IBM
- Cisco Nexus 2348TQ

Note: Please note the following:

- The 9408 line card is not supported with the 2300 FEX.

- Cisco Nexus 9300 Series switches do not support FEX on uplink modules (ALE).
- For FEX HIF port channels, Cisco recommends that you enable STP port type edge using the spanning tree port type edge [trunk] command.
- Cisco 2248PQ supports 4xQSFP (16x10GE SPF+) as network interfaces. To connect from the 2248PQ to the Nexus 9300 or 9500, use the supported QSPF+ to SFP+ breakout cables.

  Note: For Cisco Nexus 9500 switches, 4x10G breakout for FEX connectivity is not supported. Native 10G or 40G should be used.

New and Changed Information

This section lists the following topics:

- New Hardware Features in Cisco NX-OS Release 7.0(3)I2(1)
- New Software Features in Cisco NX-OS Release 7.0(3)I2(1)

New Hardware Features in Cisco NX-OS Release 7.0(3)I2(1)

Cisco NX-OS Release 7.0(3)I2(1) supports the following new hardware features:

- Cisco Nexus 31128PQ switch
- Cisco Nexus 9372PX-E switch (enhanced version of the Cisco Nexus 9372PX switch)
- M6PQ-E uplink module (enhanced version of the M6PQ uplink module used for the Cisco Nexus 93120TX, 9396PX, and 9396TX switches)

New Software Features in Cisco NX-OS Release 7.0(3)I2(1)

Cisco NX-OS Release 7.0(3)I2(1) includes the following new software features for the Cisco Nexus 9000 Series switches, the Cisco Nexus 31128PQ switch, and the Cisco Nexus 3164Q switch:

FEX Features

- N2K-C2348UPQ, NB22IBM, N2K-C2348TQ-10GE, and NB22FTS – Added support for these FEX modules. For more information, see the *Cisco Nexus 2000 Series NX-OS Fabric Extender Configuration Guide for Cisco Nexus 9000 Series Switches*.

Interfaces Features

- BFD startup timer – Delays the startup time for BFD sessions in order to give the routes that are being used by local and remote routers time to settle down in the hardware. Using this feature can prevent BFD flaps in higher scale scenarios.
- GRE tunnel enhancement - Enables GRE v6 payload (IPv6) over v4 tunnel support and enables GRE v4 payload (IPv4) over v6 tunnel support.
- IP-in-IP tunnel mask - Enables the source address and destination address for an IP tunnel to be specified by IP address and mask (length).

- MAC-embedded IPv6 (MEv6) address − Embeds the MAC address in the IPv6 address so that the device can extract the MAC address directly from the MEv6 address instead of going through neighbor discovery (ND).
- Q-in-Q VLAN tunnel - Enables configuration of IEEE 802.1 Q-in-Q VLAN tunnels.
- Regex based interface ranges - The regex command option is an extension that is available for all interface commands.
- Source interface support - The source-interface command option provides support for management applications to configure an IPv4 and/or IPv6 inband or outband source IP address for the copy command and other processes (such as tacacs, ntp, ping/ping6, icmp-error and traceroute).
- Static and dynamic network address translation (NAT) - Enables private IP internetworks that use nonregistered IP addresses to connect on Cisco Nexus Series 9300 Series switches.
- SVI autostate disable - Enables switch virtual interfaces (SVIs) to stay up even if no interface is up in the corresponding VLAN.
- Switch autostate exclude - Excludes specific ports and port channels while defining the status of the SVI.
- Switchport isolated − The switchport isolated feature allows disabling STP on an interface. Using this feature allows a 96000 maximum of virtual ports (4K VLAN * 24 ports). Configuring the switchport isolated feature places all 4K VLANS in forwarding state for that port (Removing a VLAN does not bring down the logical port.).

For more information, see the *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*.

IP SLA Features

- IP service level agreements (IP SLAs) - Enables active traffic monitoring for measuring network performance.

Label Switching Features

- Static MPLS - Enables you to statically configure the binding between an MPLS label and an IPv4 or IPv6 prefix as well as the action (label swap or pop) assigned to the binding. For more information, see the *Cisco Nexus 9000 Series NX-OS Label Switching Configuration Guide.*

Layer 2 Switching Features

- PVLAN FEX support - Enables PVLAN support for all FEXes. For more information, see the *Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*.

Multicast Features

- PIM bidirectional shared trees (Bidir) - Uses the same tree for traffic from sources toward the rendezvous point (RP) and from the RP to receivers.
- PIM source-specific multicast (SSM) - Allows receivers to connect to sources outside of the PIM domain.

For more information, see the *Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide*.

Programmability Features

- Chef - Chef is an open-source software package developed by Chef Software, Inc. It is a systems and cloud infrastructure automation framework that deploys servers and applications to any physical, virtual, or cloud location, no matter the size of the infrastructure.
- Guest Shell 2.0 - Guest Shell is a decoupled execution space running within a Linux Container (LXC).

- iPXE - iPXE is an open source network boot firmware based gPXE/Etherboot. gPXE is an open-source PXE client firmware and bootloader derived from Etherboot. Standard PXE clients use TFTP to transfer data, gPXE extends it to support additional protocols.
- Kernel stack - Kernel Stack (kstack) uses well known Linux APIs to manage the routes and front panel ports.
- NX-API REST – See the *Cisco Nexus 9000 Series NX-API REST SDK User Guide and API Reference*.
- OpenFlow 1.3 – Cisco plug-in for OpenFlow, Release 1.3 provides better control over networks making them more open, programmable, and application-aware and supports the following specifications defined by the Open Networking Foundation (ONF) standards organization:
  - OpenFlow Switch Specification Version 1.0.1 (Wire Protocol 0x01) (referred to as OpenFlow 1.0)
  - OpenFlow Switch Specification Version 1.3.0 (Wire Protocol 0x04) (referred to as OpenFlow 1.3)

Note: OpenFlow is supported on the Cisco Nexus 9300, the Nexus 3000, and the Nexus 3100 Series switches, but not the Cisco Nexus 3164Q.

- Puppet - The Puppet software package, developed by Puppet Labs, is an open source automation toolset for managing servers and other resources by enforcing device states, such as configuration settings.
- Python – See the *Cisco Nexus 9000 Series Python SDK User Guide and API Reference*.
- Third-Party applications - These are pre-built third-party applications verified by Cisco. Custom applications are also possible. See the following link for examples of third-party applications that have been tested: https://devhub.cisco.com/artifactory/enxos-release-yum/7.0-3-I2-1/x86_64/
  - collectd is a daemon which collects system performance statistics periodically and provides mechanisms to store the values in a variety of ways.
  - Ganglia is a scalable distributed monitoring system for high-performance computing systems such as clusters and Grids. It is based on a hierarchical design targeted at federations of clusters. It leverages widely used technologies such as XML for data representation, XDR for compact, portable data transport, and RRDtool for data storage and visualization.
  - LLDP is an industry standard protocol designed to supplant proprietary Link-Layer protocols such as EDP or CDP. The goal of LLDP is to provide an inter-vendor compatible mechanism to deliver Link-Layer notifications to adjacent network devices.
  - tcollector is a client-side process that gathers data from local collectors and pushes the data to OpenTSDB. You run it on all your hosts, and it does the work of sending each host's data to the TSD.

For more information about programmability features, see the *Cisco Nexus 9000 Series NX-OS Programmability Guide*, Release 7.x.

QoS Features

- FEX QoS - Enables FEX system QoS (IPv4) to differentiate high priority traffic. For more information, see the *Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide*.

Security Features

- DHCP client - Enables the configuration of an IPv4 or IPv6 address on a routed port, the management port, or a switch virtual interface (SVI). This feature is supported on the Cisco Nexus 9300 Series switches, the Cisco

Nexus 3164Q switch, and the Cisco Nexus 31128PQ switch. It is not supported on Cisco Nexus 9500 Series switches.

- HTTP method match enhancement – Enables the HTTP method to match packets with the variable-length TCP options header.
- Secure login enhancements:
  - Ability to block login attempts and enforce a quiet period
  - Ability to restrict the maximum login sessions per user
  - Ability to restrict the password length
  - Ability to prompt the user to enter a password after entering the username
  - Ability to hide the shared secret used for RADIUS or TACACS+ authentication or accounting
  - SHA256 hashing support for encrypted passwords

For more information, see the *Cisco Nexus 9000 Series NX-OS Security Configuration Guide*.

Software Upgrade and Downgrade Features

- Fast reload - Enables you to reboot the switch faster than with the reload command and to upgrade the software on the switch. This feature is being added to Cisco NX-OS 7.x software for the Cisco Nexus 3164Q switch. Fast reload is not supported on the Cisco Nexus 9000 Series switches.
- SHA256 algorithm - Displays the SHA256 checksum for the Cisco NX-OS image file, which can be used to verify the operating system integrity and ensure that the downloaded image is safe to install and use.

For more information, see the *Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide*.

System Management Features

- Configuration synchronization (config-sync) - Allows you to configure a switch profile and have the configuration be automatically synchronized to the peer switch. Note that only Cisco Nexus 9300 Series switches and the Cisco Nexus 3164Q switch support switch profiles.
- ERSPAN enhancements:
  - Adds the allow-pfc option to the source interface type rx command to allow the spanning of priority flow control (PFC) frames in the Rx direction.
  - Adds egress interface information to the output of the show monitor session command.
  - Adds the ability to span forward packet drops in the ingress pipeline.
  - Adds support for user-defined field (UDF)-based ERSPAN to help analyze and isolate packet drops in the network.
  - Adds the set-erspan-gre-proto and set-erspan-dscp actions to the ERSPAN ACL.
- Graceful insertion and removal (GIR) - Gracefully ejects a switch and isolates it from the network in order to perform debugging or upgrade operations and then returns the switch to its fully operational (normal) mode.
- MPLS stripping - Strips single-labeled packets off MPLS label headers so that standard network monitoring tools can be used to monitor the MPLS traffic.

- Sampled flow (sFlow) - Allows you to monitor real-time traffic in data networks that contain switches and routers.
- SPAN enhancements - Adds support for user-defined field (UDF)-based SPAN to help analyze and isolate packet drops in the network.

For more information, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*.

Troubleshooting Features

- HTTPS support - The copy command now supports the HTTPS file system for copying files.
- PCAP SNMP parser – Analyzes SNMP packets captured in .pcap format. For more information For more information, see the *Cisco Nexus 9000 Series NX-OS Troubleshooting Guide*.
- **watch** [**differences**] [**interval** *seconds*] *command* command - Allows you to refresh and monitor Cisco NX-OS CLI command output or Unix command output (through the **run bash** *command* command).

Unicast Routing Features

- BGP RFC 5549 – Enables you to configure an IPv4 address family for a neighbor with an IPv6 address.
- Nonhierarchical routing mode - Programs longest prefix match (LPM) routes in the line cards to improve convergence performance but does not program routes in the fabric modules. This feature is already supported on Cisco Nexus 9500 Series switches and is now being added for the Cisco Nexus 3164Q switch.
- VRF route leaking enhancement - Adds support for VRF route leaking from a non-default VRF to the default VRF.

For more information, see the *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*.

Virtual Machine Tracker Features

- Auto configuration- Enables VM tracker auto configuration support on Cisco Nexus Series 9300 Series switches. For more information, see the *Cisco Nexus 9000 Series NX-OS Virtual Machine Tracker Configuration Guide*.

VXLAN Feature

- Inner VLAN and outer VLAN mapping on a trunk port - Enables VLAN translation from an inner VLAN and an outer VLAN to a local (translated) VLAN on a port. This feature is supported on any Cisco Nexus 9000 Series switch that supports VXLAN and is also supported on the Cisco Nexus 3164Q switch.
- Port VLAN mapping on a trunk port - Enables VLAN translation between the ingress (incoming) VLAN and a local (translated) VLAN on a port. This is with switching and routing support on Cisco Nexus Series 9300 and 9500 switches.
- Q-in-VNI tunnel - Provides a way to segregate traffic by mapping to a specified port.
- VXLAN BGP eVPN control plane ingress replication - Enables VXLAN BGP eVPN control plane ingress replication support on Cisco Nexus 9500 Series switches.
- VXLAN flood and learn multicast and ingress replication - Enables VXLAN flood and learn multicast and ingress replication support for Cisco Nexus Series 9500 Series switches.
- VXLAN support for HIF - Enables VXLAN support for FEX host interface ports.

For more information, see the *Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide*.

Upgrade Instructions

To perform a software upgrade, follow the installation instructions in the *Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide*.

Note: When upgrading to 7.0(3)I2(1), Guest Shell automatically upgrades from 1.0 to 2.0. In the process, the contents of the guest shell 1.0 root filesystem will be lost. To keep from losing important content, copy any needed files to /bootflash or an off-box location before upgrading to 7.0(3)I2(1).

Downgrade Instructions

Disable the Guest Shell if you need to downgrade from Cisco NX-OS Release 7.0(3)I2(1) to an earlier release.

Note:

- Downgrading with PVLANs configured is only supported with 6.1(2)I3(4x) releases.
- For a boot-variable change and reload to a 7.0(3)I1(1x) release, the PVLAN process is not brought up, and the PVLAN ports are kept down. For a boot-variable change to the 6.1(2)I3(3) release and earlier, an ASCII replay will be tried, but feature PVLANs and other PVLAN configurations will fail.

Software Maintenance Upgrades

For information about software maintenance upgrades, see the “Performing Software Maintenance Upgrades” section in the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide.

Note: If you perform a software maintenance upgrade (SMU) and later upgrade your device to a new Cisco NX-OS software release, the new image will overwrite both the previous Cisco NX-OS release and the SMU package file.

Limitations

This section lists limitations related to Cisco NX-OS Release 7.0(3)I2(1).

- Generation 1 100G line cards (N9K-X9408PC-CFP2) and generic expansion modules (N9K-M4PC-CFP2) only support 40G flows.
- N9K-X9408PC-CFP2 line cards do not support port channeling.
- In-Service Software Upgrades (ISSU) are not supported on Cisco Nexus 9000 Series switches.
- CoPP (Control Plane Policing) cannot be disabled. If you attempt to disable it in Cisco NX-OS Release 7.0(3)I3(1), an error message appears. In previous releases, attempting to disable CoPP causes packets to be rate limited at 50 packets per seconds.
- The Skip CoPP policy option has been removed from the Cisco NX-OS initial setup utility because using it can impact the control plane of the network.
- The hardware profile front portmode command is not supported on the Cisco Nexus 9000.
- PV (Port VLAN) configuration through an interface range is not supported.
- Layer 3 routed traffic for missing Layer 2 adjacency information is not flooded back onto VLAN members of ingress units when the source MAC address of routed traffic is a non-VDC (Virtual Device Context) MAC

address. This limitation is for hardware flood traffic and can occur when the SVI (Switched Virtual Interface) has a user-configured MAC address.

- neighbor-down fib-accelerate command is supported in a BGP (Border Gateway Protocol)-only environment.
- Uplink modules should not be removed from a Cisco Nexus 9300 Series switch that is running Cisco NX-OS Release 7.0(3)I2(1). The ports on uplink modules should be used only for uplinks.
- PortLoopback and BootupPortLoopback tests are not supported.
- PFC (Priority Flow Control) and LLFC (Link-Level Flow Control) are supported for all Cisco Nexus 9300 and 9500 Series hardware except for the 100G 9408PC line card and the 100G M4PC generic expansion module (GEM).
- FEXes configured with 100/full-duplex speed, without explicitly configuring the neighboring device with 100/full-duplex speed, will not pass data packet traffic properly. This occurs with or without the link appearing to be “up.”
  - no speed–Auto negotiates and advertises all speeds (only full duplex).
  - speed 100–Does not auto negotiate; pause cannot be advertised. The peer must be set to not auto negotiate (only 100 Mbps full duplex is supported).
  - speed 1000–Auto negotiates and advertises pause (advertises only for 1000 Mbps full duplex).
- Eight QoS groups are supported only on modular platforms with the Cisco Nexus 9300 N9K-M4PC-CFP2 uplink module, and the following Cisco Nexus 9500 Series line cards:
  - N9K-X9636PQ
  - N9K-X9464PX
  - N9K-X9464TX
  - N9K-X9432PQ
- Cisco NX-OS Release 7.0(3)I2(1) supports flooding for Microsoft Network Load Balancing (NLB) unicast mode on Cisco Nexus 9500 Series switches but not on Cisco Nexus 9300 Series switches. NLB is not supported in max-host system routing mode. NLB multicast mode is not supported on Cisco Nexus 9500 or 9300 Series switches.

Note: To work around the situation of Unicast NLB limitation, we can statically hard code the ARP and MAC address pointing to the correct interface. Please refer to bug ID CSCuq03168 in detail in the “Open Caveats–Cisco NX-OS Release 7.0(3)I2(1)” section.

- TCAM resources are not shared when:
  - Routed ACL (Access Control List) is applied to multiple SVIs in the egress direction
  - Applying VACL (VLAN ACL) to multiple VLANs
- Cisco Nexus 9000 Series switch hardware does not support range checks (layer 4 operators) in egress TCAM. Because of this, ACL/QoS policies with layer 4 operations-based classification need to be expanded to multiple entries in the egress TCAM. Egress TCAM space planning should take this limitation into account.
- Applying the same QoS policy and ACL on multiple interfaces requires applying the qos-policy with the no-stats option to share the label.

- Multiple port VLAN mappings configured on an interface during a rollback operation causes the rollback feature to fail.
- The following switches support QSFP+ with the QSA (QSFP to SFP/SFP+ Adapter) (40G to 10G QSA):
  - N9K-C93120TX
  - N9K-C93128TX
  - N9K-C9332PQ
  - N9K-C9372PX
  - N9K-C9372PX-E
  - N9K-C9372TX
  - N9K-C9396PX
  - N9K-C9396TX

Note: The Nexus 9300 support for the QSFP+ breakout has the following limitations:

- Only 10G can be supported using QSA on 40G uplink ports on N9300 switches in NX-OS.
- 1G with QSA is not supported.
- For the Cisco Nexus 9332PQ switch, all ports except 13-14 and 27-32 can support breakout
- All ports in the QSA speed group must operate at the same speed (see the configuration guide)

- The following switches support the breakout cable (40G ports to 4x10G ports):
  - N9K-C9332PQ
  - N9K-X9436PQ
  - N9K-X9536PQ
- Weighted ECMP (Equal-Cost Multi-Path) Nexus 3000 feature is not supported on the Cisco Nexus 9000 Series switch.
- Limitations for ALE (Application Link Engine) uplink ports are listed at the following URL:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/ale_ports/b_Limitations_for_ALE_Uplink_Ports_on_Cisco_Nexus_9000_Series_Switches.html

Guidelines and Limitations for Private VLANs

This section provides guidelines and limitations for configuring private VLANs.

- Configuring Private VLANs
- Secondary and Primary VLAN Configuration

- Private VLAN Port Configuration
- Limitations with Other Features

Configuring Private VLANs

Private VLANs have the following configuration guidelines and limitations:

- Private VLANs must be enabled before the device can apply the private VLAN functionality.
- VLAN interface feature must be enabled before the device can apply this functionality.
- VLAN network interfaces for all VLANs that you plan to configure as secondary VLANs should be shut down before being configured.
- When a static MAC is created on a regular VLAN, and then that VLAN is converted to a secondary VLAN, the Cisco NX-OS maintains the MAC that was configured on the secondary VLAN as the static MAC.
- Private VLANs support port modes as follows:
  - Community host
  - Isolated host
  - Isolated host trunk
  - Promiscuous
  - Promiscuous trunk
- When configuring PVLAN promiscuous trunks or PVLAN isolated trunks, it is recommended to allow non-private VLANs in the list specified by the switchport private-vlan trunk allowed id command.
- Private VLANs are mapped or associated depending on the PVLAN trunk mode.
- Private VLANs support the following:
  - Layer 2 forwarding
  - PACLs (Port Access Control Lists)
  - PVLAN across switches through a regular trunk port
  - RACLs (Router Access Control Lists)
- Private VLANs support SVIs as follows:
  - SVI allowed only on primary VLANs
  - Primary and secondary IPs on the SVI
  - HSRP on the primary SVI
- Private VLANs STP as follows:
  - MST (Multiple Spanning Tree)
  - RSTP (Rapid Spanning Tree Protocol)

- Private VLANs port mode is not supported on the following:
  - 40G interfaces of the Cisco Nexus C9396PX or Cisco Nexus C93128TX
  - Cisco Nexus 3164Q
- Private VLANs do not provide port mode support for the following:
  - Port channels
  - vPC (Virtual Port Channel) interfaces
- Private VLANs do not provide support on breakout.
- Private VLANs do not provide support for the following:
  - DHCP (Dynamic Host Channel Protocol) snooping
  - IP multicast or IGMP snooping
  - PVLAN QoS
  - SPAN (Switch Port Analyzer) when the source is a PVLAN VLAN
  - Tunnels
  - VACLs
  - VTP (VLAN Trunk Protocol)
  - VXLANs
- You cannot configure a shared interface to be part of a private VLAN. For more details, see the *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*.
- Although Cisco NX-OS CLI allows the configuration of multiple isolated VLAN configurations per PVLAN group, such a configuration is not supported. A PVLAN group can have at most one isolated VLAN.

Secondary and Primary VLAN Configuration

Follow these guidelines when configuring secondary or primary VLANs in private VLANs:

- You cannot configure the default VLAN (VLAN1) or any of the internally allocated VLANs as primary or secondary VLANs.
- You must use VLAN configuration (config-vlan) mode to configure private VLANs.
- A primary VLAN can have multiple isolated and community VLANs associated with it. An isolated or community VLAN can be associated with only one primary VLAN.
- Although private VLANs provide host isolation at Layer 2, hosts can communicate with each other at Layer 3.
- A PVLAN group can have at most one isolated VLAN. Multiple isolated VLAN configurations per primary VLAN configurations are not supported.
- When a secondary VLAN is associated with the primary VLAN, the STP parameters of the primary VLAN, such as bridge priorities, are propagated to the secondary VLAN. However, STP parameters do not necessarily propagate to other devices. You should manually check the STP configuration to ensure that the spanning tree

topologies for the primary, isolated, and community VLANs match exactly so that the VLANs can properly share the same forwarding database.

- For normal trunk ports, note the following:
  - There is a separate instance of STP for each VLAN in the private VLAN.
  - STP parameters for the primary and all secondary VLANs must match.
  - The primary and all associated secondary VLANs should be in the same MST instance.
- For nontrunking ports, note that STP is aware only of the primary VLAN for any private VLAN host port; STP runs only on theprimary VLAN for all private VLAN ports.

Note: We recommend that you enable BPDU Guard on all ports that you configure as a host port; do not enable this feature on promiscuous ports.

- For private VLAN promiscuous trunk ports, note that you can configure a maximum of 16 private VLAN primary and secondary VLAN pairs on each promiscuous trunk port.
- For private VLAN isolated trunk ports, note the following:
  - You can configure a maximum of 16 private VLAN primary and secondary VLAN pairs on each isolated trunk port.
  - The native VLAN must be either a normal VLAN or a private VLAN secondary VLAN. You cannot configure a private VLAN primary port as the native VLAN for a private VLAN isolated trunk port.
- To downgrade a system that has private VLAN ports configured, you must unconfigure these ports.
- Before you configure a VLAN as a secondary VLAN, you must shut down the VLAN network interface for the secondary VLAN.

Private VLAN Port Configuration

Follow these guidelines when configuring private VLAN ports:

- Use only the private VLAN configuration commands to assign ports to primary, isolated, or community VLANs.
- The Layer 2 access ports that are assigned to the VLANs that you configure as primary, isolated, or community VLANs are inactive while the VLAN is part of the private VLAN configuration. Layer 2 trunk interfaces, which may carry private VLANs, are active and remain part of the STP database.
- If you delete a VLAN used in the private VLAN configuration, the private VLAN ports (promiscuous ports or host ports, not trunk ports) that are associated with the VLAN become inactive.

Limitations with Other Features

Consider these configuration limitations with other features when configuring private VLANs:

Note: In some cases, the configuration is accepted with no error messages, but the commands have no effect.

- User has to ensure consistent pvlan type, states and configuration across vpc peers. There is no pvlan consistency check for vpc currently. Inconsistent pvlan configs across vpc peers may end up in incorrect forwarding and impacts.

- A private VLAN port can be configured as a SPAN source port.
- Private VLAN host or promiscuous ports cannot be a SPAN destination port.
- A destination SPAN port cannot be an isolated port. (However, a source SPAN port can be an isolated port.)
- After you configure the association between the primary and secondary VLANs, the dynamic MAC addresses that learned the secondary VLANs are aged out.
- After you configure the association between the primary and secondary VLANs, if you delete the association, all static MAC addresses that were created on the primary VLANs remain on the primary VLAN only.
- In private VLANs, STP controls only the primary VLAN.

Note: See the *Cisco Nexus 9000 Series NX-OS Security Configuration Guide* for information on configuring static MAC addresses.

Unsupported Features

This section lists features that are not supported in the current release.

- VXLAN
- DHCP
- FEX
- Cisco Nexus 9408 Line Card and 9300 Series Leaf Switches
- Other Unsupported Features

VXLAN

This section lists VXLAN features that are not supported.

- Switched Port Analyzer (SPAN) Tx for VXLAN traffic is not supported for the access-to-network direction.
- QoS classification is not supported for VXLAN traffic in the network-to-access direction.
- The QoS buffer-boost feature is not applicable for VXLAN traffic.
- ACL and QoS for VXLAN traffic in the network-to-access direction is not supported.
- Native VLANs for VXLAN are not supported. All traffic on VXLAN Layer 2 trunks needs to be tagged.
- Consistency checkers are not supported for VXLAN tables.
- We do not support VXLAN routing and VXLAN Bud Nodes features on the 3164Q platform.
- DHCP snooping and DAI features are not supported on VXLAN VLANs.
- IGMP snooping is not supported on VXLAN VLANs.
- Static MAC pointing to remote VTEP is not supported with BGP EVPN.

VXLAN ACL Limitations

The following ACL related features are not supported:

- Ingress RACL that is applied on an uplink Layer 3 interface that matches on the inner or outer payload in the network-to-access direction (decapsulated path)
- Egress RACL that is applied on an uplink Layer 3 interface that matches on the inner or outer payload in the access-to-network direction (encapsulated path)
- Egress VACL for decapsulated VXLAN traffic

We recommend that you use a PACL or VACL on the access side to filter out traffic entering the overlay network.

DHCP

DHCP subnet broadcast is not supported.

FEX

- VTEP connected to FEX host interface ports is not supported.
- FEX is supported only on the Cisco Nexus 9332PQ, 9372PX, 9372PX-E and 9396PX and 9500 switches. It is not supported on the other Cisco Nexus 9300 Series.
- Cisco Nexus 9300 Series switches do not support FEX on uplink modules (ALE).
- FEX vPC is not supported between any model of FEX and the Nexus9300 (TOR) and 9500 Switches (EOR) as the parent switches
- ASCII replay with FEX needs be done twice for HIF configurations to be applied. The second time should be done after the FEXs have come up.
- IPSG is not supported on FEX ports.

Cisco Nexus 9408 Line Card and 9300 Series Leaf Switches

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

- Breakout ports
- Port-channel (No LACP)
- vPC
- MCT (Multichassis EtherChannel Trunk)
- FEX
- PTP (Precision Time Protocol)
- PFC/LLFC
- 802.3x

- PVLAN
- Storm Control
- VXLAN access port.
- SPAN destination/ERSPAN destination IP
- Shaping support on 100g port is limited

Other Unsupported Features

The following lists other features not supported in the current release:

- Due to a Poodle vulnerability, SSLv3 is no longer supported.
- The Cisco Nexus 9300 Series switches do not support the 64-bit ALPM routing mode.
- IPSG is not supported on the following:
  - The last 6 40G physical ports on the 9372PX, 9372TX, and 9332PQ switches
  - All 40G physical ports on the 9396PX, 9396TX, and 93128TX switches

Caveats

This section includes the Open Caveats and Resolved Caveats sections.

- Open Caveats–Cisco NX-OS Release 7.0(3)I2(1)
- Resolved Caveats–Cisco NX-OS Release 7.0(3)I2(1)

Open Caveats–Cisco NX-OS Release 7.0(3)I2(1)

Table 6 lists the open caveats in Cisco NX-OS Release 7.0(3)I2(1). Click the bug ID to access the Bug Search tool and see additional information about the bug.

Table 6 Open Caveats in Cisco NX-OS Release 7.0(3)I2(1)

Bug ID	Description
CSCuj51631	A DHCP relay to a subnet broadcast address does not work. Workaround: Configure “ip directed-broadcast.”
CSCul18670	The show license usage command shows the incorrect license if a valid license is installed over an honor license.

Bug ID	Description
CSCun26726	HSRP packet decoding fails with an assertion error.
CSCun34856	All VLANs are suspended if one has a QoS policy, but the TCAM is not configured.
CSCuo86036	Spurious error messages appear when an peer-link port-channel member is shut.
CSCup03921	The N9K accepts untagged packets with a dot1Q tag configuration. If the other end is not configured with a dot1Q configuration, and is sending untagged packets, the untagged packets will be accepted on the N9K.
CSCup32728	An ACL or source VLAN on a SPAN session affects traffic on other sessions.
CSCup35239	The Ethanalyzer does not see packets that egress on a virtual interface on an ALE-asic port.
CSCup55774	No drop counters are displayed when a FEX HIF is congested.
CSCuq03168	Microsoft NLB traffic being routed into the destination VLAN is experiencing packet loss.
CSCuq68788	Traffic is not spanned if SPAN ACL and policy-based routing are enabled.
CSCur22618	The show queuing interface command returns empty output when executed for FEX HIF interfaces.
CSCur30555	The show policy-map type queuing command does not show statistics for FEX HIF interfaces.
CSCur37816	When QoS Lite TCAM is configured, policer violated statistics shown as part of the show policy-map interface command are reported as 0 instead of NA (Not-Applicable).

Bug ID	Description
CSCur46879	When copying the tunnel configuration file to running, the tunnel may flap before stabilizing.
CSCur59482	Policer action is not supported when a QoS policy of type qos is applied with the no-stats keyword.
CSCur61647	Even though there are no QoS classification policies currently active on any of the FEX HIF interfaces, the show incompatibility command still reports FEX QoS incompatibility during downgrade from 3.2 to earlier versions of software.
CSCur87839	Traffic cannot be routed using policy-based routing if the next-hop reachability is across the vPC peer link and the local vPC leg is down.
CSCus06693	ERPSAN sessions with a destination on the port-channel sub-interface is not supported.
CSCus07061	When a remote end of a vPC port channel member is shut down, the local end takes ~10 seconds to shut down. This only occurs when the port channel is 'active' (i.e., has LACP enabled).
CSCus29812	When the interface is in the STP block state, and DHCP snoop is configured on the VLANs of this interface, the DHCP packets coming from the VLANs cannot be blocked by STP.
CSCus58475	Vntag-mgr times out after changing VLANS for a range of 20 vPC port-channels.
CSCus60275	Some receivers see duplicate traffic when the peer_link_exclude_flag is set to FALSE for some groups (for some VLANS) that have a source on a VPC VLAN.
CSCus63613	When a user reloads the active supervisor, the standby supervisor also reloads. During the reload process, the Service Policy Manager (SPM) cannot send data to the standby supervisor. A syslog is observed, notifying the active supervisor that the SPM has not successfully updated its data base to the standby supervisor. The active supervisor reloads the standby supervisor again, and the standby supervisor eventually reaches a good standby state.
CSCus64140	VXLAN:BGP-EVPN sessions fail to come up after removing and re-adding an “nv overlay evpn” configuration in scale scenarios.

Bug ID	Description
CSCut36556	The source VLAN configuration in a monitor session does not error out when the SPAN TCAM is not carved. SPAN on a source VLAN will not work unless the SPAN TCAM is configured.
CSCut56520	The wrong PV mapping configuration will not be detected across vPC links.
CSCut96161	With 2 hosts that have the same MAC and different IP addresses, a mac move that will happen 5 times. After that one of the hosts will be rendered "frozen" or unable to communicate. This will require a manual deletion of the other MAC and ARP to enable this host to communicate again.
CSCuu15598	When a QoS policy with a policer is applied on a FEX HIF port, the actual policing happens at the switch and not at the FEX. As a result, the internal VNTAG header of 6 bytes is also considered by the policer.
CSCuu31392	ERSPAN packets are dropped on the intermediate switches if more than one ERSPAN session resolves over 40 Gig uplinks on a ToR.
CSCuu33640	An ITD policy is shown in "no shut" state. However, no policy is actually applied to the ingress policy if an invalid ACL is used for "exclude."
CSCuu37225	Some show commands are having very slow reaction times and appear to hang with certain ITD configuration scenarios.
CSCuu87126	When 'access-list' is configured for ITD service, this error is received: "ACL cannot apply when more than one node is active."
CSCuv63473	MAC entries are not in sync between vPC peers. There are some MACs missing.
CSCuv90152	Packets are accepted on HIFPC members in suspended state.
CSCuv93600	When downgrading from Release 7.0(3)I2(1) to 7.0(3)I1(2), the clock timezone is not in effect.

Bug ID	Description
CSCuv96382	For single label mpls/stripped tap-agg packets, when the "mpls strip dest-mac xxxx.xxxx.xxxx" CLI is configured, dmac is not re-written on the modular (EOR) setup. The same will work on ToRs.
CSCuw02188	The Dynamic Twice NAT CLIs are not removable after upgrading the switch to 7.0(3)I2(1). Also, the Dynamic Twice NAT outside entry is not programmed in the hardware.

Resolved Caveats–Cisco NX-OS Release 7.0(3)I2(1)

Table 7 lists the Resolved Caveats in Cisco NX-OS Release 7.0(3)I2(1). Click the bug ID to access the Bug Search tool and see additional information about the bug.

Table 7 Resolved Caveats in Cisco NX-OS Release 7.0(3)I2(1)

Bug ID	Description
CSCus54038	The default interface does not remove all the switchport vlan mapping commands.
CSCut04823	A rollback operation may fail after removing the port VLAN mapping and restoring to a previous checkpoint that has the port VLAN mapping.
CSCut89402	Clear counter from nxos CLI does not clear the counters for the interface in Linux when run using ifconflig command
CSCuu25415	Auto configuration is failing for a VLAN that is used as a native VLAN under a port.
CSCuu35630	When GRE/IP-in-IP tunnels are initiated/terminated by 9500 switches, the TTL value is off by 1 because of the nature of hierarchical programming in 9500 switches (host routes programmed on LCs and prefix routes programmed on FMs)
CSCuu59308	VXLAN small packets padding issue on GEM port after decap.
CSCuu98041	The policy-map is not case-sensitive.
CSCuv06558	Post-MPLS stripped packet matching vs HTTP-method does not work.
CSCuv72640	Packets are not encapped properly (not using mask info) for IPIP Tunnel with mask feature.

Related Documentation

The entire Cisco Nexus 9000 Series NX-OS documentation set is available at the following URL:

http://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/tsd-products-support-series-home.html

The Cisco Nexus 3164Q Switch - Read Me First is available at the following URL:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3164/sw/6x/readme/b_Cisco_Nexus_3164Q_Switch_Read_Me_First.html

The Cisco Nexus 31128PQ Switch - Read Me First is available at the following URL:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus31128/sw/readme/b_Cisco_Nexus_31128PQ_Switch_Read_Me_First.html

New Documentation

- *Cisco Nexus 9000 Series NX-OS IP SLAs Configuration Guide, Release 7.x*
- *Cisco Nexus 9000 Series NX-OS Label Switching Configuration Guide, Release 7.x*
- *Cisco Nexus 9000 Series NX-OS Verified Scalability Guide, Release 7.0(3)I2(1)*
- *Cisco Nexus 3164Q NX-OS Verified Scalability Guide, Release 7.0(3)I2(1)*
- *Cisco Nexus 31128Q NX-OS Verified Scalability Guide, Release 7.0(3)I2(1)*
- *Cisco Nexus 31128Q Switch -- Read Me First*
- *Cisco Nexus 3000 Series NX-OS Label Switching Configuration Guide*
- *Cisco NX-OS Release 7.0(3)I2(1) Overview*

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.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Open a service request online at:

https://tools.cisco.com/ServiceRequestTool/create/launch.do

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks

mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Cisco Nexus 9000 Series NX-OS Release Notes, Release 7.0(3)I2(1)

© 2013 - 2015 Cisco Systems, Inc. All rights reserved.