Cisco Nexus 9000 Series NX-OS Release Notes, Release 7.0(3)I1(2)

First Published: May 18, 2015

This document describes the features, caveats, and limitations for Cisco NX-OS Release 7.0(3)I1(2) software for use on the Cisco Nexus 9000 Series switches and the Cisco Nexus 3164Q switch. Use this document in combination with documents listed in *Related Documentation*.

Table 1 shows the online change history for this document.

Table 1. Online History Change

Date	Description
May 18, 2015	Created the release notes for Release 7.0(3)I1(2)
May 19, 2015	■ Removed DHCP relay with VxLAN limitations ■ Changed priority flow control limitation
June 17, 2015	Added CSCuu87126 to Open Caveats
June 19, 2015	Replaced the table in the *Supported Optics* section with a link to the compatibility matrix
June 30, 2015	Added *Guidelines and Limitations for Private VLANs*
July 8, 2015	Edited the *Downgrade Instructions* section
July 15, 2015	Added the port numbers that support breakout mode on the N9K-C9332PQ switch
July 22, 2015	Updated the *Limitations* section with QSA and breakout mode limitations
January 11, 2016	Added a link to the ALE limitations in the *Limitations* section.
March 4, 2016	■ Updated Limitations. ■ Updated *Supported FEX Modules*.
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

Date	Description
April 8, 2016	Added the following statement to *Limitations*: The N9K-X9408PC-CFP2 line card does not support port-channeling.
May 25, 2016	■ 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.

Contents

Introduction 4
System Requirements 4
New and Changed Information 10
Installation Notes 12
Upgrade Instructions 12
Downgrade Instructions 12
Software Maintenance Upgrades 13
Limitations 13
Guidelines and Limitations for Private VLANs 15
Unsupported Features 18
Caveats 20
Related Documentation 24
Obtaining Documentation and Submitting a Service Request 26

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 Device Hardware
- Supported Optics
- Supported FEX Modules

Supported Device Hardware

Table 2 lists the Cisco Nexus 9000 Series hardware that Cisco NX-OS Release 7.0(3)I1(2) supports. For additional information about the supported hardware, see the Hardware Installation Guide for your Cisco Nexus 9000 Series device.

Table 2. Cisco Nexus 9000 Series Hardware.

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

Product ID	Hardware	Quantity
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
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

Product ID	Hardware	Quantity
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
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

Product ID	Hardware	Quantity
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
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-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	

Product ID	Hardware	Quantity
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
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, hot air out (red) Note: For use with the Cisco Nexus 93128 switch (N9K-C93128TX).	3
N9K-C9300-FAN2-B	Cisco Nexus 9300 fan 2, cold air in (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 9332PQ, 9372PX, and 9372TX switches (N9K-C9332PQ, N9K-C9372PX, and N9K-9372TX).	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)

Product ID	Hardware	Quantity
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-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 3 lists the Cisco Nexus 3164Q switch hardware that Cisco NX-OS Release 7.0(3)I1(2) supports.

Table 3. 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*.

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)I1(2) supports the following FEXes on Cisco Nexus 9372PX, 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 B22Dell
- Cisco Nexus B22HP

Note:

- The 9408 line card is not supported with the 2300 FEX.
- On the Nexus 9500 series, X9464PX and X9564 PX line cards are supported for FEX connectivity using the SPF+ ports.
- For FEX HIF port channels, Cisco recommends that you enable STP port type edge using the spanning tree port type edge [trunk] command.
- 2248PQ supports 4xQSFP (16x10GE SPF+) as network interfaces. To connect from 2248PQ to Nexus 9300 or Nexus 9500, use the supported QSPF+ to SFP+ breakout cables. 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)I1(2)
- New Software Features in Cisco NX-OS Release 7.0(3)I1(2)

New Hardware Features in Cisco NX-OS Release 7.0(3)I1(2)

Cisco NX-OS Release 7.0(3)I1(2) supports the following new hardware features:

- 8-port 100-Gigabit CFP2 I/O module (N9K-X9408PC-CFP2), which is supported by the Cisco Nexus 9504, 9508, and 9516 modular switches
- The Cisco Nexus 9300 uplink module (N9K-M4PC-CFP2), which is supported by the Cisco Nexus 93128TX (2 active ports), 9396PX (4 active ports), and 9396TX (4 active ports) Top-of-Rack switches. For Cisco Nexus 93128TX (2 active ports), the two active ports will be 3,4 .
- The Cisco Nexus 93120TX switch (N9K-C93120TX), which is a 2-RU, fixed-port switch designed for Top-of-Rack (TOR), Middle-of-Rack (MoR), and End-of-Rack (EoR) deployment in data centers. This switch has 96 1-/10-Gigabit BASE-T ports and 6 QSFP uplink ports.

New Software Features in Cisco NX-OS Release 7.0(3)I1(2)

Cisco NX-OS Release 7.0(3)I1(2) includes the new software features described in these sections for the Cisco Nexus 9000 Series switches and the Cisco Nexus 3164Q switch:

- 64-Bit ALPM routing mode support on the Cisco Nexus 3164Q switch
- BFD support on BFD support on Cisco ALE port sub interfaces

- Portchannel subinterface support
- Private VLAN support - Enables association of primary and secondary VLANs to form a private VLAN.
- IP-in-IP tunnel support - Enables encapsulation and decapsulation of packets to create a tunnel.
- Negotiate auto command support - Enables configuration of speed, duplex, and automatic flow control for an - Ethernet interface.
- Subinterface support on port-channel interfaces - Support for one or more subinterfaces on a port-channel interface.
- Delayed LACP support - The delayed LACP feature enables the delay of port-channel members to come up until LACP PDUs are received.
- 100G device support - Added support for 100G devices.
- Enabling egress QoS - Added support for egress QoS TCAM carving.
- VXLAN EVPN ingress replication on 9300 - Enables ingress-replication for BUM traffic to remote VTEPs.
- Port VLAN mapping on a trunk port for VxLAN VLANs - Enables VLAN translation between the ingress VLAN and a local VLAN that is mapped to a vn-segment on a port.
- Static MAC for VXLAN VTEP support - Enables the configuration of static MAC addresses behind a peer VTEP.
- vPC Consistency Check for vPC VTEPs - Enables two switches configured as a vPC pair to exchange and verify their configuration compatibility.
- Support for Cisco Discovery Protocol (CDP) on FEX HIFs - Added support for Cisco Discovery Protocol (CDP).
- FEX (straight-through) on 9500, host vPC FEX on 9500 - Enables support for two line cards (N9K-X9564PX and N9K-X9464PX) on the 9500.
- Label sharing support for QoS policies under VLANs - Enables label sharing when the same QoS policy is applied on multiple VLANs.
- Cisco NX-OS to ACI Conversion - Added the ability to boot the ACI image from Cisco NX-OS mode (instead of from the loader> prompt) while converting a Cisco Nexus 9000 Series switch from Cisco NX-OS to ACI boot mode. For additional information, see the *Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide*.

Note: The Cisco Nexus 3164Q switch operates only in Cisco NX-OS mode and cannot be converted to ACI boot mode.

- Cut-through switching support–By default, all HiGig™ links operate at 42G to compensate for the HiGig™ header over fabric and to support the full line rate of 40G from the front-panel ports. However, the speed mismatch could result in packets being forwarded in store-and-forward mode. To make sure that the traffic is cut through, you can use the switching-mode fabric-speed 40g command to change the HiGig™ links on the 42G ports to operate at 40G and use the show switching-mode fabric-speed command to verify the configuration. This feature is supported only for the Cisco Nexus 3164Q switch and the Cisco Nexus 9500 Series switches with the 9636PQ line card. It is not supported for the Cisco Nexus 9300 Series switches. Operating at 40G improves latency but prevents the fabric from supporting the full line rate.
- Intelligent Traffic Director (ITD) – ITD is an intelligent, scalable load-balancing engine that addresses the performance gap between a multi-terabit switch and gigabit servers and appliances. With this feature on the

switch, you can deploy servers and appliances from any vendor without a network or topology upgrade. This feature is supported on the following:

- Cisco Nexus 9372PX, 9372TX, 9396PX, 9396TX, 93120TX, and 93128TX switches
- Cisco Nexus 9500 Series switches with Cisco Nexus X9464PX, X9464TX, X9564PX, and X9564TX line cards

It is not supported on 40G ports, on Cisco Nexus 9300 Series switch uplink ports, or on the Cisco Nexus 3164Q switch. For additional information, see the *Cisco Nexus 9000 Series NX-OS Intelligent Traffic Director Configuration Guide*.

- Traceroute - Added source interface support. For additional information, see the *Cisco Nexus 9000 Series NX-OS Troubleshooting Guide*.

Security features

- DHCP snooping − Added support for multiple IP addresses with the same MAC address and VLAN in static binding entries.
- Switchport blocking − Prevents the flooding of unknown multicast or unicast egress packets on a specified interface. For additional information, see the *Cisco Nexus 9000 Series NX-OS Security Configuration Guide*.
- DHCP − Added DHCP relay source interface support for IPv4

System Management features

- Precision Time Protocol (PTP) − Added support for all Cisco Nexus 9000 Series and 3164Q hardware except for the 100G 9408PC line card and the 100G M4PC generic expansion module (GEM).
- TAP aggregation − Added support for 100G ports.

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

Installation Notes

Only one software image (called nx-os) is required to load the Cisco NX-OS operating system. This image runs on all Cisco Nexus 9000 Series switches and the Cisco Nexus 3164Q switch. For installation instructions, see the *Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade 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*.

Downgrade Instructions

Disable the Guest Shell if you need to downgrade from Cisco NX-OS Release 7.0(3)I1(2) 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)I1(2).

- 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.
- 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.
- The 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)I1(2). 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

Note: In a non-BGP eVPN environment, the SVI for L2/L3 boundary is expected to be on a non-VTEP routing block (a router attached to a VTEP).

- Cisco NX-OS Release 7.0(3)|1(2) does not support the Cisco NX-OS to ACI conversion feature with the ability to boot the ACI image from Cisco NX-OS mode instead of from the loader> prompt (feature added in the Cisco Release 6.1(2)|3(3)).
- Cisco NX-OS Release 7.0(3)I1(2) 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)I1(2)" 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-C9396PX
  - N9K-C9396TX
  - N9K-C93128TX
  - N9K-C9372PX,
  - N9K-C9372TX
  - N9K-C9332PQ

Note: The Nexus 9300 support for the QSFP+ with QSA adapter 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
- Limitations for ALE 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:
  - Promiscuous
  - Promiscuous trunk
  - Isolated host
  - Isolated host trunk
  - Community host

- When configuring PVLAN promiscuous 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:
  - PACLs (Port Access Control Lists)
  - RACLs (Router Access Control Lists)
  - Layer 2 forwarding
  - PVLAN across switches through a regular trunk port
- Private VLANs support SVIs as follows:
  - SVI allowed only on primary VLANs
  - Primary and secondary IP's on the SVI
  - HSRP on the primary SVI
- Private VLANs support PVLAN and STP as follows:
  - RSTPs
  - MSTs
- Private VLANs do not provide support for Cisco Fabric Extenders (FEXs).
- 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
  - vPCs (Virtual Port Channels) interfaces
- Private VLANs do not provide support on breakout.
- Private VLANs do not provide support for the following:
  - IP multicast or IGMP snooping
  - DHCP (Dynamic Host Channel Protocol) snooping
  - PVLAN QoS
  - VACLs
  - VTP (VLAN Trunk Protocol)
  - Tunnels

  - VXLANs
  - SPAN (Switch Port Analyzer) when the source is a PVLAN VLAN

- Shared interfaces cannot be configured to be part of a private VLAN. For more details, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide.
- Configuring multiple isolated VLAN configurations per PVLAN group is allowed by the Cisco NX-OS CLI. However, 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:

- Default VLANs (VLAN1), or any of the internally allocated VLANs, cannot be configured as primary or secondary VLANs.
- VLAN configuration (config-vlan) mode must be used to configure private VLANs.
- Primary VLANs can have multiple isolated and community VLANs associated with it. An isolated or community VLAN can be associated with only one primary VLAN.
- Private VLANs provide host isolation at Layer 2. However, hosts can communicate with each other at Layer 3.
- PVLAN groups can have one isolated VLAN at most. 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.
  - Primary and all associated secondary VLANs should be in the same MST instance.
- For non-trunking ports, STP is aware only of the primary VLAN for any private VLAN host port; STP runs only on the primary VLAN for all private VLAN ports.

Note: Cisco recommends that you enable BPDU Guard on all ports that you configure as a host port and not enable this feature on promiscuous ports.

- Private VLAN promiscuous trunk ports allow you to 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.

- Downgrading a system that has private VLAN ports configured requires unconfiguring the ports.
- Before configuring 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.

- Ensure consistent PVLAN type, states and configuration across vPC peers. There is currently no PVLAN consistency check for vPC. Inconsistent PVLAN configs across vPV peers may end up in incorrect forwarding and impacts.
- Private VLAN ports can be configured as SPAN source ports.
- Private VLAN host or promiscuous ports cannot be SPAN destination ports.
- Destination SPAN ports cannot be isolated ports. However, a source SPAN port can be an isolated port.
- After configuring the association between the primary and secondary VLANs:
  - Dynamic MAC addresses that learned the secondary VLANs are aged out.
  - Static MAC addresses for the secondary VLANs cannot be created.
- After configuring 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
- Other Unsupported Features

VXLAN

This section lists VXLAN features that are not supported.

- TX SPAN (Switched Port Analyzer) 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.
- QoS buffer-boost 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.
- BGP eVPN neighbors are not supported over VPC interfaces.
- VXLAN routing and VXLAN Bud Nodes features on the 3164Q platform are not supported.
- 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.
- Rollback is not supported on VXLAN VLANs that are configured with the Port VLAN mapping feature.

VXLAN Topology Restrictions

- FEX host interface ports are not supported for VLANs extended with VXLAN.

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

- FEX is supported only on the Cisco Nexus 9372PX and 9396PX and 9500 switches. It is not supported on the other Cisco Nexus 9300 Series.
- FEX vPC is not supported between Nexus9372PX/9396PX (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.

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)I1(2)
- Resolved Caveats–Cisco NX-OS Release 7.0(3)I1(2)

Open Caveats–Cisco NX-OS Release 7.0(3)I1(2)

Table 4 lists the open caveats in Cisco NX-OS Release 7.0(3)I1(2). Click the bug ID to access the Bug Search tool and see additional information about the bug.

Table 4 Open Caveats in Cisco NX-OS Release 7.0(3)I1(2)

Bug ID	Description
CSCuj51631	A DHCP relay to a subnet broadcast address does not work. Workaround: Configure “ip directed-broadcast.”

Bug ID	Description
CSCul18670	The show license usage command shows the incorrect license if a valid license is installed over an honor license.
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 Cisco Nexus 9000 Series switch 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 Cisco Nexus 9000 Series switch.
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.

Bug ID	Description
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).
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.
CSCus54038	The default interface does not remove all the switchport vlan mapping commands.
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.

Bug ID	Description
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.
CSCut04823	A rollback operation may fail after removing the port VLAN mapping and restoring to a previous checkpoint that has the port VLAN mapping.
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.”

Resolved Caveats—Cisco NX-OS Release 7.0(3)I1(2)

Table 5 lists the Resolved Caveats in Cisco NX-OS Release 7.0(3)I1(2). Click the bug ID to access the Bug Search tool and see additional information about the bug.

Table 5 Resolved Caveats in Cisco NX-OS Release 7.0(3)|1(2)

Bug ID	Description
CSCur63227	BGP prefixes can experience a temporary traffic drop during a supervisor switchover when BGP prefixes have the Nexthop learned over BGP (Recursive Nexthop) in the presence of a default route in the system.
CSCur68966	BFDv6 session keeps flapping "Reason: Control Detection Time Expired."
CSCus27641	Bud node is currently not supported when using SVI links.
CSCus41382	High CPU utilization for L2RIB on changing the source-interface with HIGH SCALE.
CSCus47689	On a VPC peer switch, when uplinks to IP core are down, Broadcast, Unknown unicast, or Multicast (BUM) packets ingressing on the switch cannot be forwarded to remote ingress replication VTEPs.
CSCus69937	When the overlay BGP has multiple BGP sessions with the same peer, there is a routing loop.

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

Configuration Guides

Cisco Nexus 2000 Series NX-OS Fabric Extender Software Configuration Guide for Cisco Nexus 9000 Series Switches

Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide

Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide

Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide

Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide

Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide

Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide

Cisco Nexus 9000 Series NX-OS Security Configuration Guide

Cisco Nexus 9000 Series NX-OS System Management Configuration Guide

Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide

Cisco Nexus 9000 Series NX-OS Verified Scalability Guide

Cisco Nexus 9000 Series NX-OS Virtual Machine Tracker Configuration Guide

Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide

Other Software Documents

Cisco Nexus 7000 Series and 9000 Series NX-OS MIB Quick Reference

Cisco Nexus 9000 Series NX-OS Programmability Guide

Cisco Nexus 9000 Series Software Upgrade and Downgrade Guide

Cisco Nexus 9000 Series NX-OS System Messages Reference

Cisco Nexus 9000 Series NX-OS Troubleshooting Guide

Cisco NX-OS Licensing Guide

Cisco NX-OS XML Interface User Guide

Hardware Documents

Cisco Nexus 9332PQ NX-OS-Mode Switch Hardware Installation Guide

Cisco Nexus 9372PX NX-OS-Mode Switch Hardware Installation Guide

Cisco Nexus 9372TX NX-OS-Mode Switch Hardware Installation Guide

Cisco Nexus 9396PX NX-OS-Mode Switch Hardware Installation Guide

Cisco Nexus 9396TX NX-OS-Mode Switch Hardware Installation Guide

Cisco Nexus 93128TX NX-OS-Mode Switch Hardware Installation Guide

Cisco Nexus 9504 NX-OS-Mode Switch Hardware Installation Guide

Cisco Nexus 9508 NX-OS-Mode Switch Hardware Installation Guide

Cisco Nexus 9516 NX-OS-Mode Switch Hardware Installation Guide

Release Notes

Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes

Cisco Nexus 9000 Series NX-OS Release Notes

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 Nexus 9000 Series NX-OS Release Notes, Release 7.0(3)I1(2)