Cisco Nexus 3000 Series NX-OS Release Notes, Release 7.0(3)I2(1)

This document describes the features, bugs, and limitations for Cisco Nexus 3000 Series and Cisco Nexus 3100 Series switches. Use this document in combination with documents listed in the *Obtaining Documentation and Submitting a Service Request* section.

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 "n3000."

Note: Release notes are sometimes updated with new information about restrictions and bugs. See the following website for the most recent version of the Cisco Nexus 3000 Series release notes: http://www.cisco.com/c/en/us/support/switches/nexus-3000-series-switches/products-release-notes-list.html.

Important Information about This Release

For Cisco Nexus 3000 vPC topologies, a non-disruptive upgrade from Cisco NX-OS Release 6.0(2)U6(3a) to 7.0(3)I2(1) is not supported as the upgrade will cause a traffic disruption. However, for Cisco Nexus 3000 vPC topologies, a non-disruptive upgrade from Cisco NX-OS Release 6.0(3)U6(3) to Release 7.0(3)I2(1) is not supported as the upgrade will cause a traffic disruption. When you upgrade a Cisco Nexus 3000 Switch from Cisco NX-OS Release 6.0(3)U6(3) to another Device Under Test (DUT) running Cisco NX-OS Release 7.0(3)I4(x) or later, and if the upgrading DUT is in a vPC configuration, it is likely that one vPC peer is running 7.0(3)I4(x) and while the other is running the 6.0(3)U6(3) version. If both the vPC peers have the command "spanning-tree port type edge default" configured globally, then the mismatch of TLVs between the asymmetric versions, a type-1 inconsistency error gets triggered and the Multichassis EtherChannel Trunk (MCT) link fails. It is highly recommended that customers with vPC topologies to wait for the next maintenance release of 7.0(3)I4(x), to avoid traffic disruption during upgrade.

Beginning with Cisco NX-OS Release 7.0(3)I2(1), kickstart and system images are no longer used to install the Cisco NX-OS software image on Cisco Nexus 3000 and 3100 Series switches. Instead, a single binary image is used. Note that this filename has changed to start with "nxos" instead of "n3000" (for example, nxos.7.0.3.I2.1.bin). To install the software, you would use the install all nxos bootflash:nxos.7.0.3.I2.1.bin command.

Use the following documents (along with this Nexus 3000 Series Release Note) for a list of changes in this release:

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

Date	Description
October 13,2015	Added the following statement: 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 "n3000."
December 2, 2015	Added new information about downgrading to a 6.x release.
January 7, 2016	Removed a bug Id (CSCuq92481) from Limitations.
February 10, 2016	Removed CSCut82376 from *Open Bugs in this Release*.
November 22, 2017	Added a note to specify the requirements while upgrading from Cisco NX-OS Release 6.0(2)U6(2) (CSCvb78728).
March 9, 2018	Added a limitation for IGMP snooping.
November 17, 2018	Replaced instances of Cisco NX-OS Release 6.0(2)U6(2) and 6.0(2)U6(3) with Cisco NX-OS Release 6.0(2)U6(2a) and 6.0(2)U6(3a).

Contents

Introduction

Several new hardware and software features are introduced for the Cisco Nexus 3000 Series and Cisco Nexus 3100 Series devices to improve the performance, scalability, and management of the product line. Cisco NX-OS Release 7.x

also supports all hardware and software supported in Cisco NX-OS Release 6.x, Cisco NX-OS Release 5.1, and Cisco NX-OS Release 5.0.

Cisco NX-OS offers the following benefits:

- Cisco NX-OS runs on all Cisco data center switch platforms: Cisco Nexus 7000, Nexus 5000, Nexus 4000, Nexus 3000, Nexus 2000, and Nexus 1000V Series switches.
- Cisco NX-OS software interoperates with Cisco products that run any variant of Cisco IOS software and also with any networking operating system that conforms to common networking standards.
- Cisco NX-OS modular processes are triggered on demand, each in a separate protected memory space. Processes are started and system resources are allocated only when a feature is enabled. The modular processes are governed by a real-time preemptive scheduler that helps ensure timely processing of critical functions.
- Cisco NX-OS provides a programmatic XML interface that is based on the NETCONF industry standard. The Cisco NX-OS XML interface provides a consistent API for devices. Cisco NX-OS also provides support for Simple Network Management Protocol (SNMP) Versions 1, 2, and 3 MIBs.
- Cisco NX-OS enables administrators to limit access to switch operations by assigning roles to users. Administrators can customize access and restrict it to the users who require it.

This section includes the following:

Cisco Nexus 3000 Series Switches

The Cisco Nexus 3000 Series switches are high-performance, high-density, ultra-low-latency Ethernet switches that provide line-rate Layer 2 and Layer 3 switching. The Cisco Nexus 3000 Series includes the following switches:

- The Cisco Nexus 3064 switch is a 1 RU switch that supports 48 1- or 10-Gigabit downlink ports, four Quad Small Form-Factor Pluggable (QSFP+) ports that can be used as a 40 Gigabit Ethernet port or 4 x10-Gigabit Ethernet ports, one 10/100/1000 management port, and one console port.
- The Cisco Nexus 3048 switch is a 1 rack unit (RU) switch that supports 48 10/100/1000 Ethernet server-facing (downlink) ports, four 10-Gigabit network-facing (uplink) ports, one 100/1000 management port, and one console port.
- The Cisco Nexus 3016 is a 1 RU, 16-port QSFP+ switch. Each QSFP+ port can be used as a 40-Gigabit Ethernet port or 4 x10-Gigabit Ethernet ports.

Each switch includes one or two power supply units and one fan tray module, and each switch can be ordered with either forward (port-side exhaust) airflow or reverse (port-side intake) airflow for cooling. All platforms support both AC and DC power supplies. All combinations of power (AC/DC) and airflow (forward/reverse) are available. The Cisco Nexus 3000 Series switches run the Cisco NX-OS software.

For information about the Cisco Nexus 3000 Series, see the Cisco Nexus 3000 Series Hardware Installation Guide.

Cisco Nexus 3100 Series Switches

The Cisco Nexus 3100 Series switches are high-performance, high-density, ultra-low-latency Ethernet switches that provide line-rate Layer 2 and Layer 3 switching. In Cisco NX-OS Release 6.0(2)U2(2), the Cisco Nexus 3100 Series includes the Cisco Nexus 3132 and Nexus 3172 switches.

The Cisco Nexus 3172PQ switch is a 10-Gbps Enhanced Small Form-Factor Pluggable (SFP+)–based ToR switch with 48 SFP+ ports and 6 Enhanced Quad SFP+ (QSFP+) ports.

The Cisco Nexus 3172TQ switch is a 10GBASE-T switch with 48 10GBASE-T ports and 6 Quad SFP+ (QSFP+) ports.

Each SFP+ port can operate in 100-Mbps, 1-Gbps, or 10-Gbps mode, and each QSFP+ port can operate in native 40-Gbps or 4 x 10-Gbps mode. This switch is a true physical-layer-free (phy-less) switch that is optimized for low latency and low power consumption.

The Cisco Nexus 3132Q switch is a 1RU, 40-Gbps QSFP-based switch that supports 32 fixed 40-Gbps QSFP+ ports. It also has 4 SFP+ ports that can be internally multiplexed with the first QSFP port. Each QSFP+ port can operate in the default 40-Gbps mode or 4 x 10-Gbps mode, up to a maximum of 104 10-Gbps ports.

Each switch includes dual redundant power supply units, four redundant fans, one 10/100/1000 management port, and one console port. Each switch can be ordered with either forward (port-side exhaust) airflow or reverse (port-side intake) airflow for cooling. It supports both AC and DC power supplies. All combinations of power (AC/DC) and airflow (forward/reverse) are available. The Cisco Nexus 3100 Series switches run the Cisco NX-OS software.

For information about the Cisco Nexus 3100 Series, see the Cisco Nexus 3000 Series Hardware Installation Guide.

System Requirements

This section includes the following topics:

- Memory Requirements
- Hardware Supported
- Twinax Cable Support on Cisco Nexus 3000 Switches
- Cisco QSFP 40-Gbps Bidirectional Short-Reach Transceiver

Memory Requirements

The Cisco NX-OS Release 7.0(3)I2(1) software requires 135 MB of flash memory.

Hardware Supported

Cisco NX-OS Release 7.0(3)I2(1) supports the Cisco Nexus 3000 Series switches. You can find detailed information about supported hardware in the Cisco Nexus 3000 Series Hardware Installation Guide. See Table 2 for the hardware supported by the Cisco NX-OS Release 7.x software.

Table 2. Hardware Supported by Cisco NX-OS Related 7.x Software.

Hardware	Part Number	Release 7.0(3)I2(1)

Hardware	Part Number	Release 7.0(3)I2(1)
Cisco Nexus 3132Q-X switch	N3K-C3132Q-40GX	X
Cisco Nexus 3172TQ switch	N3K-C3172TQ-10GT	X
Cisco Nexus 3172PQ switch	N3K-C3172PQ-10GE	X
Cisco Nexus 3132Q switch	N3K-C3132Q-40GE	X
Cisco Nexus 3016 switch	N3K-C3016Q-40GE	X
Cisco Nexus 3048 switch	N3K-C3048TP-1GE	X
Cisco Nexus 3064-TQ switch	N3K-C3064TQ-10GT	X
Cisco Nexus 3064-X switch	N3K-C3064PQ-10GX	X
Cisco Nexus 3064-E switch	N3K-C3064PQ-10GE	X
Cisco Nexus 3064 switch	N3K-C3064PQ	X
Cisco Nexus 3048 fan module with forward airflow (port-side exhaust)	N3K-C3048-FAN	X
Cisco Nexus 3048 fan module with reverse airflow (port-side intake)	N3K-C3048-FAN-B	X
Cisco Nexus 3064-T 500W forward airflow (port-side exhaust) AC power supply	NXA-PAC-500W	X
Cisco Nexus 3064-T 500W reverse airflow (port-side intake) AC power supply	NXA-PAC-500W-B	X
Cisco Nexus 3064-X forward airflow (port-side exhaust) AC power supply	N3K-C3064-X-FA-L3	X
Cisco Nexus 3064-X reversed airflow (port-side intake) AC power supply	N3K-C3064-X-BA-L3	X
Cisco Nexus 3064-X forward airflow (port-side exhaust) DC power supply	N3K-C3064-X-FD-L3	X
Cisco Nexus 3064-X forward airflow (port-side intake) DC power supply	N3K-C3064-X-BD-L3	X

Hardware	Part Number	Release 7.0(3)I2(1)
Cisco Nexus 3064 fan module with forward airflow (port-side exhaust); also used in the Cisco Nexus 3016	N3K-C3064-FAN	X
Cisco Nexus 3064 fan module with reverse airflow (port-side intake); also used in the Cisco Nexus 3016	N3K-C3064-FAN-B	X
Cisco Nexus 3000 power supply with forward airflow (port-side exhaust)	N2200-PAC-400W	X
Cisco Nexus 3000 power supply with reverse airflow (port-side intake)	N2200-PAC-400W-B	X
Cisco Nexus 2000 power supply with forward airflow (port-side exhaust)	N2200-PDC-400W	X
Cisco Nexus 2000 DC power supply with reverse airflow (port-side intake)	N3K-PDC-350W-B	X

Twinax Cable Support on Cisco Nexus 3000 Switches

Starting with Cisco Release NX-OS 5.0(3)U1(1), the following algorithm is used to detect copper SFP+ twinax, QSFP+ twinax, and QSFP+ splitter cables on Cisco Nexus 3000 Series switches.

If the attached interconnect (transceiver) is a copper SFP+ twinax or QSFP+ twinax cable:

- Verify the transceiver SPROM to match the Cisco magic code.
- If the check succeeds, bring up the interface. Otherwise, print the following warning message appears stating that a non-Cisco transceiver is attached and that you should try to bring up the port.

  2009 Oct 9 01:46:42 switch %ETHPORT-3-IF_NON-CISCO_TRANSCEIVER: Non-Cisco transceiver on interface Ethernet1/18 is detected.

  If the attached transceiver is a QSFP+ splitter cable, then no special check is performed. The Cisco NX-OS software tries to bring up the port.

  The following disclaimer applies to non-Cisco manufactured and non-Cisco certified QSFP copper splitter cables:

  If a customer has a valid support contract for Cisco Nexus switches, Cisco TAC will support twinax cables that are a part of the compatibility matrix for the respective switches. However, if the twinax cables are not purchased through Cisco, a customer cannot return these cables through an RMA to Cisco for replacement.

If a twinax cable that is not part of the compatibility matrix is connected into a system, Cisco TAC will still debug the problem, provided the customer has a valid support contract on the switches. However TAC may ask the customer to replace the cables with Cisco qualified cables if there is a situation that points to the cables possibly being faulty or direct the customer to the cable provider for support. Cisco TAC cannot issue an RMA against uncertified cables for replacement.

Cisco QSFP 40-Gbps Bidirectional Short-Reach Transceiver

The Cisco QSFP 40-Gbps Bidirectional (BiDi) transceiver is a short-reach pluggable optical transceiver with a duplex LC connector for 40-GbE short-reach data communications and interconnect applications by using multimode fiber (MMF). The Cisco QSFP 40-Gbps BiDi transceiver offers a solution that uses existing duplex MMF infrastructure for 40-GbE connectivity. With the Cisco QSFP 40-Gbps BiDi transceiver, customers can upgrade their network from 10-GbE to 40-GbE without incurring any fiber infrastructure upgrade cost. The Cisco QSFP 40-Gbps BiDi transceiver can enable 40-GbE connectivity in a range of up to 100 meters over OM3 fiber, which meets most data center reach requirements. It complies with the Multiple Source Agreement (MSA) QSFP specification and enables customers to use it on all Cisco QSFP 40-Gbps platforms and achieve high density in a 40-GbE network. It can be used in data centers, high-performance computing (HPC) networks, enterprise and distribution layers, and service provider transport applications.

New and Changed Information

This section lists the new and changed information in Release 7.0(3)I2(1):

- New Supported Hardware
- New Software Features

New Supported Hardware

Cisco NX-OS Release 7.0(3)I2(1) does not include new hardware.

New Software Features

All Cisco Nexus 3000 Series switches are supported by Cisco NX-OS Release 7.0(3)I2(1). Cisco NX-OS interoperates with any networking operating system, including Cisco IOS software, that conforms to the networking standards listed in the product data sheet.

Note: See the *New and Changed information* section of the 7.x Cisco Nexus 3000 configuration guides for a list of default and behavior changes on the Nexus 3000 Series switches from the 6.x release to the 7.x release.

- N3K and N9K modes - The Cisco Nexus 3100 Series switches now support two modes: the N3K mode and the N9K mode. The N3K mode is the default mode. It uses the same CLI commands as previous Cisco Nexus 3000 Series and Cisco Nexus 3100 Series NX-OS releases (Release 6.0(2)U6(2) and earlier). The N9K mode enables the Cisco Nexus 3100 Series switches to use the same CLI commands as the Cisco Nexus 9000 Series switches. The N9K mode on 3100 switches is configured using the `system switch-mode n9k` command. Refer to the Cisco Nexus 9000 Series configuration guides for the N9K CLI commands. Refer to the *Cisco Nexus 3000 Series NX-OS Fundamentals Configuration Guide* for instructions on using the `system switch-mode n9k` command.

  Note: The Cisco Nexus 3000 Series switches do not support N9K mode.

Device File Features

- HTTPS support – The copy command now supports the HTTPS file system for copying files.

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.
- Grev6 – Enables v4 payload over Grev6.
- IP-in-IP tunnel – Added IP-In-IP tunnel source and destination subnet mask CLI enhancement.
- Interface breakout when changing the portmode from QSFP to SFP+ – Support was added for configuring interface breakout when changing the portmode from QSFP to SFP+.

For more information, see the *Cisco Nexus 3000 Series NX-OS interfaces Configuration Guide.*

IP SLA Features

- IP SLAs – The Cisco NX-OS IP SLAs use active traffic monitoring--the generation of traffic in a continuous, reliable, and predictable manner--for measuring network performance. For more information, see the *Cisco Nexus 3000 Series NX-OS IP SLAs Configuration Guide*.

Licensing

- New default and upgrade licenses N3172T-32T-LIC and N3172T-16T-UPG are available for Cisco Nexus 3172TQ platforms. For more information, see the *Cisco NX-OS Licensing Guide*.

Multicast Feature

- Configuring Multicast Table Size – Support for configuring multicast and unicast entries in the multicast table.

  For more information, see the *Cisco Nexus 3000 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.
- 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).

- 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.
- RPM– Software packaging has been migrated to an RPM-based model.
- 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/open-nxos/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 supported applications, see the *Cisco Nexus 3000 Series NX-OS Programmability Guide, Release 7.x.*

Security Feature

- HTTP method match enhancement - Enables the HTTP method to match packets with the variable length TCP options header. For more information, see *the Cisco Nexus 3000 Series NX-OS Security Configuration Guide.*

System Management Features

- 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.
  - Added set-erspan-gre-proto and set-erspan-dscp options for SPAN ACLs.
  - 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.
- PCAP SNMP parser – Analyzes SNMP packets captured in .pcap format.
- 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 3000 Series NX-OS System Management Configuration Guide.*

Troubleshooting Features

- Process Restartability –Process restartability has been added for additional processes in Cisco NX-OS Release 7.0(3)I2(1).

For more information, see the *Cisco Nexus 3000 Series NX-OS Fundamentals Configuration Guide.*

Unicast Features

- BGP weighted ECMP - You can configure BGP over weighed ECMP to deliver balanced traffic in the direct proportion to the application deployment distribution.
- Dynamic ECMP group resizing - Added support for configuring dynamic ECMP group resizing.

For more information, see the *Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide.*

Upgrade and Downgrade Guidelines

- The only supported method of upgrading is install all from Release 6.0(2)U6(1) due to the need to upgrade the BIOS. Without the Release 7.0(3)I2(1) BIOS, the 7.0(3)I2(1) image will not load.
- The no-save option is now required to downgrade from Release 7.x to Release 6.x. The bios-force is a hidden option that is only available on Cisco Nexus 3000 Series switches that are running 7.x releases.
- Cisco Nexus 3000 Series switches that use software versions older than Cisco NX-OS Release 5.0(3)U5(1) need to be updated to Cisco NX-OS Release 5.0(3)U5(1) before they are upgraded to Cisco NX-OS Release 6.0(2).
- Cisco NX-OS Release 5.0(3)U3(1) does not support a software upgrade from Cisco NX-OS Release 5.0(3)U2(2c). If you want to upgrade through this path, see CSCty75328 for details about how to work around this issue.

  Note: It is recommended that you upgrade to Cisco NX-OS Release 7.0(3)I2(1) by using Cisco NX-OS install procedures.

- In Cisco NX-OS Release 5.0(3)U3(1), support for IPv6 has been added in Control Plane Policing (CoPP). To enable redirection of IPv6 control packets to the CPU, you must configure IPv6 CoPP on the system. Entering the write erase command on a device that runs Release 5.0(3)U3(1) automatically applies CoPP on the device and ensures that all IPv4 and IPv6-related CoPP configuration is set up correctly.
- If you upgrade from a Cisco NX-OS release that does not support the CoPP feature to a release that does support the CoPP feature, you must run the setup utility after the upgrade to enable CoPP on the device.
- If you upgrade from Cisco NX-OS Release 5.0(3)U2(2), which supports the CoPP feature, to Cisco NX-OS Release 5.0(3)U3(1), which adds CoPP classes for IPv6 support, you must run the setup script to enable the IPv6 CoPP feature on the device.
- In Cisco NX-OS Release 6.0(2)U2(2), the default interface name in LLDP MIB is in short form. To make it long form, you must set lldp portid-subtype to 1. In Cisco NX-OS Release 6.0(2)U2(3), this behavior was reversed. The default interface name in LLDP MIB is now in long form. To make it short form, you must set lldp portid-subtype to 0.

- If you have set lldp port-subtype to 1 and you are upgrading to Cisco NX-OS Release 6.0(2)U2(4), ensure that you set lldp port-subtype to 0.

Upgrade Matrix

This section provides information on upgrading Cisco Nexus 3000 and 3100 Series switches to Cisco NX-OS Release 7.0(3)I2(1).

> Note: Beginning with this release, kickstart and system images are no longer used to install the Cisco NX-OS software image on Cisco Nexus 3000 and 3100 Series switches. Instead, a single binary image is used (for example, nxos.7.0.3.I2.1.bin). To install the software, you would use the install all nxos bootflash:nxos.7.0.3.I2.1.bin command.

From	To	Limitations	Recommended Procedure
6.0(2)U6(3a)[1]	7.0(3)I2(1)	None	Install all and fast reload are the only upgrade methods supported because of a BIOS upgrade requirement. Warning: Make sure that you store the pre-Release, 6.0(2)U6(3a)'s configuration file. For more information, see the Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.x.
6.0(2)U6(2a)[2]	7.0(3)I2(1)	First, upgrade to Cisco NX-OS Release 6.0(2)U6(3a) or a later release. Note: A Cisco Nexus 3048 switch requires an additional step when you upgrade from a software version older than Cisco NX-OS 6.0(2)U6(2a), otherwise the switch can fail to boot. You must first upgrade the switch to Cisco NX-OS Release 6.0(2)U6(2a), then to Cisco NX-OS Release 6.0(2)U6(3a), and finally to Cisco NX-OS Release 7.0(3)I2(1).	Install all and fast reload are the only upgrade methods supported because of a BIOS upgrade requirement. For more information, see the Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.x.

[1] Cisco NX-OS Release 6.0(2)U6(3) is no longer available for a software download through www.cisco.com. This software release has been replaced by Cisco NX-OS Release 6.0(2)U6(3a).
[2] Cisco NX-OS Release 6.0(2)U6(2) is no longer available for a software download through www.cisco.com. This software release has been replaced by Cisco NX-OS Release 6.0(2)U6(2a).

Limitations

The following are the known limitations for Cisco NX-OS Release 7.0(3)I2(1).

- While installing the NXAPI https certificate that is present in the device, the following error message can appear if the user does not have the permission to install this certificate (See CSCup72219):

  Certificate file read error.Please re-check permissions.

- After configuring the NXAPI feature, the default http port (port 80) is still in the listening state even after we run the no nxapi http command. This results in the sandbox becoming accessible. Although the sandbox becomes accessible, HTTP requests from the sandbox to the device do not go through. Thus, the functionality is not affected. (See CSCup77051).

- Chunking is enabled while displaying XML output for any CLI, and html tags (& lt; and & gt;) are displayed instead of < and > both on the sandbox and while running the Python script (See CSCup84801).

  This is expected behavior. Each chunk should be in XML format for you to parse it and extract everything inside the <body> tag. This is done so that it can be later concatenated with similar output from all the chunks of the CLI XML output. After all the chunks are concatenated to get the complete XML output for the CLI, this complete XML output can be parsed for any parameter.

  The following workaround is recommended to address this issue:

  - Concatenate the <body> outputs from each chunk
  - Replace all the html tags (& lt; and & gt;) with < and >
  - Parse for any XML tag needed

- If you use the write erase command, you cannot view the output for the show startup *feature* command. To view the startup configuration, you must then use the show startup-config command. This limitation will remain until you run the copy running-config startup-config command. After that, the show startup-config feature command will display the feature-only configuration output as expected (See CSCuq15638).

- A Python traceback is seen while running the show xml command by using the Python shell. The exception type is httplib.IncompleteRead. This happens when you use Python scripts to leverage the NXAPI for retrieving switch data through XML or JSON. You should handle the exceptions in your Python scripts (See CSCuq19257).

- While upgrading to a new release, when you create a checkpoint without running the setup script, the checkpoint file does not contain the copp-s-mpls class. After you run the write erase command and reload the switch, the copp-s-mpls class is created when the default configuration is applied. When a rollback is done to this checkpoint file, it detects a change in the CoPP policy and tries to delete all class-maps. Because you cannot delete static class-maps, this operation fails and, in turn, the rollback also fails.

  This can also happen if you create a checkpoint, then create a new user-defined class and insert the new class before any other existing class (See CSCup56505).

  The following workarounds are recommended to address this issue:

  - Run setup after upgrading to a new release.
  - Always insert the new classes at the end before a rollback.

- When both the ip icmp-errors source and ip source *intf* icmp error commands are configured, then the command that is configured last takes effect.

Thereafter, if the last configured command is removed, the switch does not get configured with the command that was configured first.

- Users who upgrade to 7.0(3)I2(1) need to run the set up script if they want to enable the MPLS static or the VRRpv3 feature.
- The following Nexus 9000 features are not supported on the Cisco Nexus 3100 Series switches in N3K or N9K mode.
  - FEX
  - Network address translation (NAT)
  - Multicast PIM Bidir
  - Support for up to 4000 VLANs
  - Q-in-VNI support for VXLAN
  - Q-in-Q support for VXLAN
  - Port VLAN (PV) switching and routing support for VXLAN
  - VXLAN BGP eVPN control plane
  - Auto-Config
  - Port profiles
  - 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
  - SHA256 algorithm to verify operating system integrity
  - Non-hierarchical routing mode
  - NX-API REST
- Link Level Flow Control (LLFC) is not supported on Cisco Nexus 3000 series and Cisco Nexus 3100 series switches.
- You can disable IGMP snooping either globally or for a specific VLAN.
- You cannot disable IGMP snooping on a PIM enabled SVIs. The warning message displayed is: IGMP snooping cannot be disabled on a PIM enabled SVIs. There are one or more VLANs with PIM enabled.

Caveats

The open bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Note: You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. if you do not have one, you can register for an account.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

- Resolved Bugs
- Open Bugs for this Release
- Known Behaviors for this Release

Resolved Bugs

Table 3 lists descriptions of resolved bugs in Cisco NX-OS Release 7.0(3)I2(1). You can use the record ID to search the Cisco Bug Search Tool for details about the bug.

Table 3 Cisco NX-OS Release 7.0(3)I2(1) —Resolved Bugs

Record Number	Open Bug Headline
CSCty07258	Cisco devices running NX-OS include hidden commands that could allow an authenticated, local attacker to view arbitrary files on the underlying operating system. This could result in the disclosure of critical system information.
CSCul00132	■ IPV6 NA with hop-limit 254 is on same subnet ■ Source MAC is different from the IPv6 source L3 interface.
CSCum46478	On Cisco Nexus 3000 Series switches, the local password md5 hashes are displayed in show tech for both show run and show startup.
CSCun07999	Switch reloads when OSPFv2/v3 crashes.
CSCup66750	Cisco Nexus 7000 Series switches running with versions 6.1.5 and 6.2.8 stop advertising the routes to neighboring peers as soon as default address-family ipv4/6 unicast is issued under the neighbor statement.
CSCus40634	The Cisco Nexus 3100 Series switch consistency checker does not complete.
CSCut88214	The Cisco Nexus 3100 Series switch is not able to suppress the software forwarded copies of IP redirected packets. This results in duplicate packets being forwarded to the intended host. This has been observed only on the Cisco Nexus 3100 Series platform but not on the Cisco Nexus 3500 Series.
CSCuu70539	Cisco Nexus 5000 Series switch BGP process crash causes a hap reset.
CSCuv29295	POAP is not initiating reload when CLIs in the config file require a reload.

Open Bugs for this Release

Table 4 lists descriptions of open bugs in Cisco NX-OS Release 7.0(3)I2(1). You can use the record ID to search the Cisco Bug Search Tool for details about the bug.

Table 4 Cisco NX-OS Release 7.0(3)I2(1)—Open Bugs

Record Number	Open Bug Headline
CSCuu69356	For Cisco Nexus 3000 Series switch vPC topologies, a non-disruptive upgrade from Cisco NX-OS Release 6.0(2)U6(3) to 7.0(3)I2(1) is not supported as the upgrade will cause traffic disruption. An upcoming maintenance release will support non-disruptive upgrades for vPC topologies. It is highly recommended that customers with vPC topologies wait for the next maintenance release of 7.0(3)I2(x) to avoid traffic disruption during the upgrade.
CSCuq01107	Static MAC addresses pointing to a vPC PO are flushed and traffic flooding is seen when the vPC PO is made shut.
CSCur14762	After running no shut on the vPC peer-link, some packet duplication occurs for all the sourced multicast groups.
CSCur76020	VRRPv3 tracking support to be added.
CSCur96529	Error message failed to allocate shared memory for per-protocol nexthop (nh) type.
CSCus32402	Multihop Recursive routes may not be properly installed with MPLS static.
CSCuu69356	Upon upgrading a Cisco Nexus 3000/3100 Series switch from Release 6.0(2)U6(2) to 7.0(3)I2(1), if utilizing a vPC as part of the configuration, the vPC domain will incur downtime of up to 5 minutes if both parent nodes in the vPC configuration are upgraded simultaneously.

Known Behaviors for this Release

This section lists known behaviors for this release.

Large core files are split into 3 or more files. For example:

- 1405964207_0x101_fwm_log.3679.tar.gzaa
- 1405964207_0x101_fwm_log.3679.tar.gzab
- 1405964207_0x101_fwm_log.3679.tar.gzac

To decode the multiple core files, first club the files to a single file:

```
$ cat 1405964207_0x101_fwm_log.3679.tar.gz* > 1405964207_0x101_fwm_log.3679.tar.gz
```

MIB Support

The Cisco Management Information Base (MIB) list includes Cisco proprietary MIBs and many other Internet Engineering Task Force (IETF) standard MIBs. These standard MIBs are defined in Requests for Comments (RFCs). To find specific

MIB information, you must examine the Cisco proprietary MIB structure and related IETF-standard MIBs supported by the Cisco Nexus 3000 Series switch. The MIB Support List is available at the following FTP sites:

ftp://ftp.cisco.com/pub/mibs/supportlists/nexus3000/Nexus3000MIBSupportList.html

Related Documentation

Documentation for the Cisco Nexus 3000 Series Switch is available at the following URL:

http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html

New Documentation

- *Cisco Nexus 3000 Series NX-OS IP SLAs Configuration Guide*
- *Cisco Nexus 3000 Series NX-OS Label Switching Configuration Guide*
- *Cisco Nexus 3000 Series NX-OS Verified Scalability Guide*
- *Cisco NX-OS Release 7.0(3)I2(1) Overview*
- *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 nexus3k-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, 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

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.