Cisco Nexus 3000 Series NX-OS Release Notes, Release 7.0(3)I2(5)

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."

Table 1 shows the online change history for this document.

Table 1. Online History Change

Date	Description
January 17, 2017	Created NX-OS Release 7.0(3)I2(5) release notes
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

Contents 1
Introduction 2
System Requirements 3
New and Changed Information 6
Caveats 6
Upgrade and Downgrade Guidelines 9
Upgrade Matrix 10
Limitations 11
MIB Support 13
Related Documentation 14

Documentation Feedback 14
Obtaining Documentation and Submitting a Service Request 14

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
- Cisco Nexus 3100 Series Switches

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(5) software requires 135 MB of flash memory.

Hardware Supported

Cisco NX-OS Release 7.0(3)I2(5) 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(5)
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 C3172PQ-XL switch	N3K-C3172PQ-XL	X
Cisco Nexus C3172TQ-XL switch	N3K-C3172TQ-XL	X
Cisco Nexus C3132Q-XL switch	N3K-C3132Q-XL	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

Hardware	Part Number	Release 7.0(3)I2(5)
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
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(5):

- New Supported Hardware
- New Software Features

New Supported Hardware

Cisco NX-OS Release 7.0(3)I2(5) does not include new hardware features.

New Software Features

Cisco NX-OS Release 7.0(3)I2(5) does not include new software features.

Caveats

The open and resolved bugs and the known behaviors 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 for this Release
- Open Bugs for this Release
- Known Behaviors for this Release

Resolved Bugs for this Release

Table 3 lists descriptions of resolved bugs in Cisco NX-OS Release 7.0(3)I2(5). 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(5) –Resolved Bugs

Record Number	Description
CSCvc19817	QoS policy does not send the traffic to the correct ACL. Traffic that is sent from Spirent, to a Cisco Nexus 3064 Switch with multiple ACLs configured, does not go the correct ACL. Instead, it hits the ACL that is precedent to the targeted ACL.
CSCvc43949	When a Cisco Nexus 3000 Switch is setup as DHCPv6 Relay Agent, DHCPv6 clients are not able to lease IP. Packets are not punted to CPU and consequently not seen in ethanalyzer. ERSPAN shows the packets were received on switchport. DHCP event logs and debug logs confirm that the packets are not punted.
CSCuw10613	Cisco Nexus 3000 Switch may crash due to neutron_usd process. Neutron is the component that is using USB for internal communication. Crash may happen because of a defect in the USB library.
CSCvb26651	OpenFlow software flows does not match hardware TCAM entries. While adding and removing flows, the software flows (show OpenFlow switch 1 flows) does not match the TCAM entries (show hardware access-list interface Ethernet x/y input entries detail module 1). As a result, you may experience traffic loss.
CSCvb64127	Some of the Nexus 3000 Series platforms (N3K-C3064PQ-10GX, N3K-C3132Q-40GX, N3K-C3172TQ-10GT, N3K-C3172PQ-10GE, N3K-C3048TP-1GE) fail to upgrade to 7.0(x) images with MD5Sum mismatch error.
CSCvb77073	NXAPI SSL certificate is not applied via POAP on Cisco Nexus 3000 switches.
CSCvc00843	Cisco Nexus 3048T Switch cannot bring up the uplink port after changing the speed to 10G.
CSCvc22632	The 10G SFP SFP-H10GB-CU5M, SFP-H10GB-CU2M, or SFP-10G-SR is incorrectly recognized to be 1000base-CX for SFP-H10GB-CU5M, SFP-H10GB-CU2M or unknown for SFP-10G-SR after switch reload or SFP reseat. Reseating the SFP resolves this issue.
CSCuy46002	You might get a Diagnostic Error log message when the front port mode is configured as "hardware profile front port mode SFP-plus" in Cisco Nexus 3132 platform switches that are in Cisco Nexus 9000 mode.
CSCuz76071	TACACS authentication fails on Cisco Nexus 3000 switches with an error message.
CSCva92767	Port speed fails to set in hardware if link type changed on Cisco Nexus 3048 switches.

Record Number	Description
CSCva99353	DHCPv6 solicit messages are not relayed to DHCPv6 server. The custom CoPP policy rules added to the default CoPP policy map is increasing the number of CoPP TCAM entries being programmed. This causes DHCPv6 rules programmed lower in the TCAM regions send DHCP packets matching a default control plane TCAM entry before the DHCP rules. Because of this reason, the packets fail to reach DHCPv6 module.
CSCvb17376	Cisco Nexus 3064 Switches may crash due to neutron_usd process.
CSCuw50196	An older revision of DELTA PSU makes the redundant PS switch out with no output voltage. A power cycle or plug in/out of the power cable recovers the power supply. The recovery mechanism is implemented in the software.
CSCvc18340	Cisco Nexus 3100 Switch running 703I2.4 version of code does not program the RACL applied to SVI in the hardware correctly. The RACL is not used because of the incorrect label.

Resolved PSIRT CVEs–Cisco NX-OS Release 7.0(3)I2(5)

Error! Reference source not found. lists the Resolved PSIRT CVEs in Cisco NX-OS Release 7.0(3)I2(5). Click the bug ID to access the Cisco Bug Search Tool and see additional information about the bug.

Table 4 Resolved PSIRT CVEs in Cisco NX-OS Release 7.0(3)I2(5)

Record Number	Description
CSCuz92661	Cisco MDS 9000 Series Multilayer Switches, Cisco Nexus 3000 Series Switches, Cisco Nexus 5000 Series Switches, Cisco Nexus 6000 Series Switches, Cisco Nexus 7000 Series Switches, and Cisco Nexus 9000 Series Switches, include a version of ntpd that is affected by the vulnerabilities identified by the Common Vulnerability and Exposures (CVE) IDs: CVE-2016-4957, CVE-2016-4953, CVE-2016-4954, CVE-2016-4955, CVE-2016-4956 And disclosed in: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160603-ntpd This product is affected by one or more of the listed CVE ids.

Open Bugs for this Release

Table lists descriptions of open bugs in Cisco NX-OS Release 7.0(3)I2(5). You can use the record ID to search the Cisco Bug Search Tool for details about the bug.

Table 5 Cisco NX-OS Release 7.0(3)I2(5) –Open Bugs

Record Number	Description
CSCuw97656	When ALPM is enabled on vPC devices, inconsistency is detected between the hardware and software MAC table on both vPC nodes after learning more than 32K MAC addresses. In ALPM mode, the supported MAC table limit is 32K. MAC tables on both vPC devices go out of sync.
CSCux02214	The L2 consistency check fails to detect inconsistency between hardware and software L2 entries for an HSRP virtual MAC.

Record Number	Description
CSCuw10613	Nexus 3000 Switches crashes due to neutron_usd process. Neutron is the component that is using USB for internal communication. A defect in the USB library might may be the cause of this issue.

Known Behaviors for this Release

Table lists descriptions of known behaviors in Cisco NX-OS Release 7.0(3)I2(5). You can use the record ID to search the Cisco Bug Search Tool for details about the bug

Table 6 Cisco NX-OS Release 7.0(3)I2(5) –Known Behaviors

Record Number	Description
CSCuu87126	When the access-list is configured for ITD service, this error is received: "ACL can not apply when more than one node is active."
CSCuw56991	When a unicast ARP request packet for Virtual IP gets hashed to HSRP secondary, HSRP secondary should send the packet to active. However, in addition to this, the packet is also being flooded in the VLAN.
CSCuw75771	A vPC - Type-2 inconsistency is reported for VLANs.
CSCuw97319	**clear ip igmp snooping groups * vlan x** does not clear IGMP groups learned on a vPC peer.
CSCux01653	The **show interface transceiver** command output for 40 G copper passive cables changed in release 7.0(3)I2(2). Earlier releases included an additional "(passive)" field.
CSCux02214	The L2 consistency check fails to detect inconsistency between hardware and software L2 entries for an HSRP virtual MAC.

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
```

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(5) BIOS, the 7.0(3)I2(5) 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(5) 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(5).

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.I2.3.bin). To install the software, you would use the install all nxos bootflash:nxos.7.0.3.I2.3.bin command.

From	To	Limitations	Recommended Procedure

6.0(2)U6(3a)[1]	7.0(3)I2(2x) and later	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(3)'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] or earlier	7.0(3)I2(2x) and later	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(2), 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(5).	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.

Limitations

The following are the known limitations for Cisco NX-OS Release 7.0(3)I2(5).

- Cisco Nexus 3000-XL platforms do not support breakout using speed 10000 CLI command. Use the interface breakout module 1 port <num> map 10g-4x CLI command instead.
- 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

[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).

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(5) 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.

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

No new documentation for this release.

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.