



Cisco Nexus 3000 Series NX-OS Release Notes, Release 7.0(3)I5(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."

Table 1 shows the online change history for this document.

Table 1 Online History Change

Date	Description
October 31, 2016	Created NX-OS Release 7.0(3)I5(1) release notes.
March 09, 2017	Added CSCvc95305 in 'Known Behaviors for this Release' Section.
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.....	2
System Requirements.....	3
New and Changed Information	6
Caveats	8
Upgrade and Downgrade Guidelines	13
Upgrade Matrix	14
Limitations	15

MIB Support.....	17
Related Documentation	18
Documentation Feedback	18
Obtaining Documentation and Submitting a Service Request	18

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.

System Requirements

- 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)I5(1) software requires 135 MB of flash memory.

Hardware Supported

Cisco NX-OS Release 7.0(3)I5(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
Cisco Nexus 3132Q-X switch	N3K-C3132Q-40GX
Cisco Nexus C3172TQ-XL switch	N3K-C3172TQ-XL
Cisco Nexus C3172PQ-XL switch	N3K-C3172PQ-XL
Cisco Nexus C3132Q-XL switch	N3K-C3132Q-XL
Cisco Nexus 3172TQ switch	N3K-C3172TQ-10GT
Cisco Nexus 3172PQ switch	N3K-C3172PQ-10GE
Cisco Nexus 3132Q-V switch	N3k-C3132Q-V
Cisco Nexus 3132Q switch	N3K-C3132Q-40GE
Cisco Nexus 31108TC-V	N3K-C31108TC-V
Cisco Nexus 31108PC-V switch	N3K-C31108PC-V
Cisco Nexus 3064-X switch	N3K-C3064PQ-10GX
Cisco Nexus 3064-X reversed airflow (port-side intake) AC power supply	N3K-C3064-X-BA-L3
Cisco Nexus 3064-X forward airflow (port-side intake) DC power supply	N3K-C3064-X-BD-L3
Cisco Nexus 3064-X forward airflow (port-side exhaust) DC power supply	N3K-C3064-X-FD-L3
Cisco Nexus 3064-X forward airflow (port-side exhaust) AC power supply	N3K-C3064-X-FA-L3
Cisco Nexus 3064-TQ switch	N3K-C3064TQ-10GT

Hardware	Part Number
Cisco Nexus 3064-T 500W reverse airflow (port-side intake) AC power supply	NXA-PAC-500W-B
Cisco Nexus 3064-T 500W forward airflow (port-side exhaust) AC power supply	NXA-PAC-500W
Cisco Nexus 3064-E switch	N3K-C3064PQ-10GE
Cisco Nexus 3064 switch	N3K-C3064PQ
Cisco Nexus 3064 fan module with reverse airflow (port-side intake); also used in the Cisco Nexus 3016	N3K-C3064-FAN-B
Cisco Nexus 3064 fan module with forward airflow (port-side exhaust); also used in the Cisco Nexus 3016	N3K-C3064-FAN
Cisco Nexus 3048 switch	N3K-C3048TP-1GE
Cisco Nexus 3048 fan module with reverse airflow (port-side intake)	N3K-C3048-FAN-B
Cisco Nexus 3048 fan module with forward airflow (port-side exhaust)	N3K-C3048-FAN
Cisco Nexus 3016 switch	N3K-C3016Q-40GE
Cisco Nexus 3000 power supply with reverse airflow (port-side intake)	N2200-PAC-400W-B
Cisco Nexus 3000 power supply with forward airflow (port-side exhaust)	N2200-PAC-400W
Cisco Nexus 2000 power supply with forward airflow (port-side exhaust)	N2200-PDC-400W
Cisco Nexus 2000 DC power supply with reverse airflow (port-side intake)	N3K-PDC-350W-B

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.

New and Changed Information

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)I5(1):

- New Supported Hardware
- New Software Features

New Supported Hardware

Cisco NX-OS Release 7.0(3)I5(1) does not support any new hardware.

New Software Features

Cisco NX-OS Release 7.0(3)I5(1) includes the following new software features:

- Archiving: Support added for configuration archive and archive log.

New and Changed Information

- Interfaces: Added support for per-member link BFD; Added support for Layer 3 over vPC; Added support for Q-in-Q to Q-in-VNI and dot1Q to Q-in-VNI.
- Port Security: Configures Layer 2 physical interfaces and Layer 2 port-channel interfaces to allow inbound traffic from only a restricted set of MAC addresses. Port security is not supported on vPCs, and we do not recommend enabling port security in vPC deployments.
- x509v3 authentication for SSH: Configures SSH authentication using X.509v3 certificates (RFC 6187) and a smartcard to enable two-factor authentication for Cisco device access.
- Enhanced ISSU (Container-based in-service software upgrade): Enables you to upgrade the device software while the switch continues to forward traffic, which reduces the downtime typically caused by software upgrades (just like a regular ISSU, also known as a non-disruptive upgrade). However, with enhanced ISSU, the software runs inside a separate Linux container (LXC) for the supervisor and line cards, and a third container is created as part of the ISSU procedure and is brought up as a standby supervisor. Enhanced ISSU is supported only for the Cisco Nexus 31108PC-V, 31108TC-V, and 3132Q-V switches.

Note: After you upgrade to Cisco NX-OS Release 7.0(3)I5(1) from an earlier release, you can enable enhanced ISSU for use with future upgrades.

- IPv6 ACLs: Added support for IPv6 ACLs for tap aggregation. Starting with Release 7.0(3)I5(1), support for IPv6 ACLs is added on the Cisco Nexus 3000 Series switches. The redirect action is supported in IPv6 ACLs. All the match options that are currently supported for IPv6 PACL are now supported with the redirect action.
- GIR Enhancements: Starting with Release 7.0(3)I5(1), multiple maintenance mode GIR enhancements have been added to Cisco Nexus 3000 Series switches.
- IGMP snooping over VXLAN: Starting with Release 7.0(3)I5(1), you can configure IGMP snooping over VXLAN. The configuration of IGMP snooping is same in VXLAN as the configuration of IGMP snooping in regular VLAN domain. All the configuration CLIs remain the same.
- Scale up to 2034 VNIs: Starting with Release 7.0(3)I5(1), you can configure up to 2034 Layer 2 VNIs with 32 static ingress replication peers on the Cisco Nexus 3132Q-V, 31108TC-V, and the 31108PC-V platforms. Also, the range of values for the VXLAN virtual network identifier (VNID) range is changed to <1-16777214>.
- MPLS Label Stack Imposition: Added support for MPLS label stack imposition where an outgoing label stack having one or more labels can be statically provisioned using this feature.
- Egress Peer Engineering using BGP: Cisco Nexus 3000 Series switches are often deployed in massive scale data centers (MSDCs). In such environments, there is a requirement to support BGP Egress Peer Engineering (EPE) with Segment Routing (SR). The SR-based EPE solution allows a centralized (SDN) controller to program any egress peer policy at ingress border routers or at hosts within the domain. With the introduction of RFC 7752 and draft-ietf-idr-bgppls-segment-routing-epe in Cisco NX-OS Release 7.0(3)I5(1), you can configure Egress Engineering. The feature is valid only for external BGP neighbors and is not configured by default.
- Non-disruptive ISSU: Starting with Release 7.0(3)I5(1), support for non-disruptive ISSU is added for segment routing.

Caveats

- VXLAN OAMs: Starting with Release 7.0(3)I5(1), the VXLAN operations, administration, and maintenance (OAM) protocol is supported on Cisco Nexus 3000 Series platforms. This enables to monitor and troubleshoot Ethernet networks to enhance management in VXLAN-based overlay networks.
- DNS IPv6 Gaps (SCP, FTP, SFTP, HTTP): Starting with Release 7.0(3)I5(1), DNS commands on Cisco Nexus 3000 Series platforms support IPv6.
- Ingress Policing: Starting with Release 7.0(3)I5(1), ingress and egress policing is supported on Cisco Nexus 3000 Series platforms.

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)I5(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)I5(1) –Resolved Bugs

Record Number	Description
CSCuc19423	POAP executes successfully although the script file is empty.
CSCur38613	Link down on certain ports of Cisco Nexus 3132 switch is observed when the connected third-party switch is reloaded.
CSCuj82460	Duplicate unicast and multicast packets are observed while doing shut or unshut to the L3 port-channel.
CSCuz17880	With a bfd echo-interface loopback configuration and when BFD IPv6 Session end-point address is Link-local, the OSPFv3 BFD IPv6 sessions do not work in Echo mode.
CSCva27273	On the Cisco Nexus 3000 series switches, when uplink 40G ports are used as 10G ports with the CVR-QSFP-SFP10G module, these interfaces undergo a link flap.
CSCva76772	Transceiver type not retrieved on an SNMP get.

Caveats

Record Number	Description
CSCva80886	Cisco Nexus 3100 switches running 7.0(3)I4(2) image are seen to allow the per VLAN MAC aging configuration.
CSCva91740	On the Cisco Nexus 3000 switches, under the vPC environment, ingress ACL not relevant to communication is dropping packets.
CSCva93139	Cisco Nexus 3000 switches such as 3172 or 3064 running 7.0(3)I3(1) or earlier image seems to have fan idle speed around 30% to 40%. Immediately after an upgrade to 7.0(3)I3(1) image or later, the fan idle speed is increased to 70% or more.
CSCvb17376	On one of the t2psanity testbeds (tb_952), neutron_usd core was seen with box in idle state.
CSCvb18010	Cisco Nexus 31xx switches show incorrect maximum L2 table capacity.
CSCvb26651	While adding and removing flows, at some point the software flows does not match the TCAM entries.
CSCuw10613	Cisco Nexus 3xxx switches may reload due to neutron_usd process. Neutron is the component that is using USB for internal communication. A defect in the USB library might be the cause for this issue.
CSCvb83940	For the N3K-C3172PQ-XL platform, port LED on Ethernet 1/36 and Ethernet 1/54 stays AMBER while inserting SFP and after link up.

Open Bugs for this Release

Table 4 lists descriptions of open bugs in Cisco NX-OS Release 7.0(3)I5(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)I5(1) –Open Bugs

Record Number	Description
CSCvb63195	SSL/https remote file access support required in python (bash shell) for release 7.0(3)I4(2).
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.
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.

Known Behaviors for this Release

Table 5 lists descriptions of known behaviors in Cisco NX-OS Release 7.0(3)I5(1). 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)I5(1) –Known Behaviors

Record Number	Description
CSCvb11259	On the Cisco Nexus 3000 DME enabled platform, the GLC-T 1G interface allows configuring 10G speed since the speed command is handled through DME and there is absolutely no functional issue.
CSCuz54126	From Cisco Nexus 3000 release 7.0(3)I4(2) onwards, there is a minor issue on differences between startup and running SNMP configurations after ASCII replay is done.
CSCvb15949	Rollback checkpoint fails when the checkpoint configuration has a peer-gateway configuration under VPC domain.
CSCvb69499	For the MPLS label imposition, the show mpls switching command does not show correct out-label if the next-hop is SR-RNH.
CSCvb65594	For the MPLS label imposition, ECMP is not programmed if next-hops are a mix of RNH and CNH.
CSCvb25811	For the MPLS label imposition, contention between prefixes learned via label imposition and SR BGP.
CSCva80216	Default-Mgmt VRF route Leak: Strict compatibility check is missing.

Caveats

Record Number	Description
CSCvb45282	When IGMP report is received from only one NVE peer on an NVE interface, access to network traffic is replicated to all NVE peers even when those peers are not sending any IGMP join requests.
CSCvb45258	When IGMP snooping is enabled, the NVE interface is added by default as a static mrouter port. This causes traffic to be received on all the remote VTEPs.
CSCvb35966	MPLS label imposition statistics are not displayed correctly.
CSCvb08421	Due to an IGMP enhancement, the display for show ip igmp snooping command is changed.
CSCva08222	When the ethanalyzer is used to monitor the packets for more than 30 minutes, a syslog is generated to indicate the system temporary directory (\tmp) usage is full.
CSCuw38487	python/yum crashes when /tmp is full.
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.
CSCuw63806	A BGP session flap is seen after a reboot/fast-reload on QI/Nep platforms.
CSCuw75771	In a vPC scenario where one peer is upgraded to 7.0(3)I2 and another peer is still running 6.0(2)U6: If on one peer, a vPC peer link is configured to be part of an SVI interface but the other end is not configured to be part of the SVI, a type 2 inconsistency is reported in peer running 7.0(3)I2. The same is not reported in the peer running 6.0(2)U6 as this consistency check is specific to 7.0(3)I2 release only. This has no functional impact and would be seen only in the mentioned transient scenario.
CSCuw86732	HSRP standby device tunnels the packet to vPC peer.
CSCuw92666	After invoking the clear fabric database host command, the profile remains applied on the secondary vPC switch.
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.
CSCux08559	The show routing hash does not show the exact path for Routes over tunnel.
CSCux10586	OFA: of_agent memory leak during install scale flows.
CSCux10898	OFA: openflow configure gone after reload.
CSCux15298	Alibaba: loopack interface not down after nve shut.
CSCux20954	VRF static route should move to the bottom in show running.

Caveats

Record Number	Description
CSCux22283	Bootup time of the box is high.
CSCux23914	For L3 interfaces, for RFC 5549 traffic (advertising v4 routes over v6 interface/neighbors), even if the egress interface is not v4-aware, the traffic will still be forwarded and not dropped.
CSCux24415	PTP Corrections values are higher than expected.
CSCux28141	Counter is not showing CRC error packets in egress direction.
CSCux33633	VPC: Auto-pulled hosts are out of sync among peers.
CSCux35347	ISSU is blocked for upgrade.
CSCux37273	L3 orphan ports on a vPC setup may get duplicate traffic, which is avoidable with some changes in config.
CSCux38031	After configuring Dynamic Arp Inspection, the switch drops the invalid ARP request packets with target protocol address 0.0.0.0 as expected. But statistics for these drop packets are not shown in the show ip arp inspection statistics vlan CLI. These are reflected in the show ip arp statistics CLI.
CSCux38601	Block non-disruptive ISSU if SDK firmware changed.
CSCux39947	TFTP image download fails as ARP to gateway fails in loader prompt.
CSCux46895	Service impacting upgrade/downgrade as it is a ToR switch.
CSCux56810	Management IP address is not reachable from the kickstart boot prompt (also known as recovery prompt).
CSCux58869	N3K-C3132Q-40G-SUP: interface port LED's are flapped during an ISSU.
CSCux64729	Tx span is unsupported while configuring vlan interface as source.
CSCux70434	Automatic ARP resolution does not happen for IR peers in VPC setup in specific scenarios.
CSCux76023	N3K_IMR4: XCVR Wavesplitter type is shown as "unknown" type.
CSCux79934	When configuring large access-list on a switch port (> 1533 entries with the default TCAM carving of 1536 entries for the region), the error message:" ERROR: Sufficient free entries are not available in TCAM bank" is seen.
CSCux80557	Feature bash-shell will get enabled on executing show tech install. Error will be seen on executing show tech install with network operator role.
CSCux86255	show run bgp all does not reliably nvgen allowas-in [occurrences].
CSCux87794	copy r s is getting stuck at 97% on QI2CR-XL 16GB switch.
CSCuy02203	When the setup script is executed after the system is up and interfaces are configured with non-default configs, the default interface layer and default switchport interface state set in the setup script will not affect those interfaces with non-default configuration.
CSCuy06098	Hide Shrinkimage option from ISSU command if it is not supported.

Record Number	Description
CSCuy09656	LED Status shown as incorrectly on QS.
CSCuy11513	User is able to change the configuration on the vPC peer when the peer is going through ISSU in conditions where the user already in the config mode.
CSCuy85644	VXLAN access and network ports have been added to the broadcast (BCAST) and multicast (MCAST) domains; this causes packets to flood on all VXLAN ports attached to the MCAST and BCAST domains, including the source port. However, packets are dropped on the egress of the source port. As a result, unknown unicast and broadcast traffic is incremented in the Out-Discard counter without affecting the Xmit-Err counter.
CSCvc95305	If you attempt to copy an image with compact option through SCP with the image name similar to the one already present in the DUT (compacted one), the copying will fail in spite of enabling the deletion of the image using allow delete boot-image command.

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(3)** due to the need to upgrade the BIOS. Without the Release 7.0(3)I5(1) BIOS, the 7.0(3)I5(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)I5(1) by using Cisco NX-OS install procedures.

- 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.

Upgrade Matrix

- 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.
- While performing a non-disruptive ISSU, VRRP and VRRPV3 will display the following messages:
 - If VRRPV3 is enabled:


```
2015 Dec 29 20:41:44 MDP-N9K-6 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: ISSU ERROR: Service "vrrpv3" has sent the following message: Feature vrrpv3 is configured. User can change vrrpv3 timers to 120 seconds or fine tune these timers based on upgrade time on all Vrrp Peers to avoid Vrrp State transitions. - sysmgr
```
 - If VRRP is enabled:


```
2015 Dec 29 20:45:10 MDP-N9K-6 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: ISSU ERROR: Service "vrrp-eng" has sent the following message: Feature vrrp is configured. User can change vrrp timers to 120 seconds or fine tune these timers based on upgrade time on all Vrrp Peers to avoid Vrrp State transitions. - sysmgr
```
- Packet loss may occur on Cisco Nexus 31108PC-V, 31108TC-V and 3132Q-V switches when they are in the default cut-through switching-mode and the default oversubscribed port mode. These packet losses are seen in hardware counters on the egress port as TERR and/or TFCS. One of the following workarounds can be implemented to address this issue without NX-OS upgrade. To view more details, see [CSCvf87120](#).
 1. Change the port mode from oversubscribed to line-rate and then reload the switch:
 - on Nexus 31108PC-V and 31108TC-V switches, change from 48x10g+6x100g to 48x10g+4x100g+2x40g.
 - on Nexus 3132Q-V switches change from 32x40g or 26x40g to 24x40g.
 2. Change the switching-mode from cut-through to store-and-forward and then reload the switch.

Upgrade Matrix

This section provides information on upgrading Cisco Nexus 3000 and 3100 Series switches to Cisco NX-OS Release 7.0(3)I5(1).

Note: Beginning **with the 7.0(3)I2(1) 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.I4.1.bin). To install the software, you would use the install all nxos bootflash:nxos.7.0.3.I4.1.bin command.

From	To	Limitations	Recommended Procedure
7.0(3)I2(1) or later	7.0(3)I5(1)	None	install all is the recommended upgrade method supported.

Limitations

6.0(2)U6(3a) ¹	7.0(3)I5(1)	None	<p>install all is the only upgrade method supported because of a BIOS upgrade requirement.</p> <p>Warning: Make sure that you store the pre-Release, 6.0(2)U6(3)'s configuration file.</p> <p>For more information, see the <i>Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.x</i>.</p>
6.0(2)U6(2a) ² or earlier	7.0(3)I5(1)	<p>First, upgrade to Cisco NX-OS Release 6.0(2)U6(3a) or a later release.</p> <p>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)I5(1).</p>	<p>install all is the only upgrade method supported because of a BIOS upgrade requirement.</p> <p>For more information, see the <i>Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.x</i>.</p>

Limitations

The following are the known limitations for Cisco NX-OS Release 7.0(3)I5(1).

- The fast reload feature is not supported.
- Subinterfaces cannot be used as network ports.
- 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.

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

- 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.

MIB Support

- Users who upgrade to 7.0(3)I5(1) need to run the set up script if they want to enable the MPLS static or the VRRpv3 feature.
- The following Cisco 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
 - Port VLAN (PV) switching and routing support for VXLAN
 - 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

There is 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2016 Cisco Systems, Inc. All rights reserved.