Cisco Nexus 3500 Series NX-OS Release Notes, Release 6.0(2)A8(2)

This document describes the features, bugs, and limitations for Cisco Nexus 3500 Series switches. Use this document in **combination with documents listed in the "Obtaining Documentation and Submitting a Service Request" section.**

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 3500 Series release notes:
http://www.cisco.com/c/en/us/support/switches/nexus-3000-series-switches/products-release-notes-list.html.

Table 1 shows the online change history for this document.

Table 1. Online History Change

Date	Description
August 09, 2016	Created NX-OS Release 6.0(2)A8(2) release notes
November 24, 2016	Added a limitation about SSH/SCP sessions.

Contents

Introduction

Several new hardware and software features are introduced for the Cisco Nexus 3548 switch to improve the performance, scalability, and management of the product line. Cisco NX-OS Release 6.0 also supports all hardware and software supported in 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 topics:

- Cisco Nexus 3500 Series Switches

- Cisco Nexus 3548 Switch

- Cisco Nexus 3524 Switch

Cisco Nexus 3500 Series Switches

The Cisco Nexus 3500 platform is an extension of the Cisco Nexus 3000 Series of 100M, 1, 10, and 40 Gigabit Ethernet switches built from a switch-on-a-chip (SoC) architecture. Switches in the Cisco Nexus 3500 series include Algorithm Boost (or Algo Boost) technology that is built into the switch application-specific integrated circuit (ASIC). Algo Boost allows the Cisco Nexus 3548 switch to achieve Layer 2 and Layer 3 switching latencies of less than 200 nanoseconds (ns). In addition, Algo Boost contains several innovations for latency, forwarding features, and performance visibility, including two configurable modes for low latency:

- Normal mode: This mode is suitable for environments needing low latency and high scalability.

- Warp mode: This mode consolidates forwarding operations within the switching ASIC, lowering latency by up to an additional 20 percent compared to normal operation.

Active buffer monitoring accelerates the collection of buffer utilization data in hardware, allowing significantly faster sampling intervals. Even on the lowest-latency switches, data packets can incur a millisecond or more of latency during periods of congestion. Previous buffer utilization monitoring techniques were based entirely on software polling algorithms with polling with higher polling intervals that can miss important congestion events.

Cisco Nexus 3548 Switch

The Cisco Nexus 3548 switch is the first member of the Cisco Nexus 3500 platform. As a compact one-rack-unit (1RU) form-factor 10 Gigabit Ethernet switch, the Cisco Nexus 3548 switch provides line-rate Layer 2 and Layer 3 switching at extremely low latency. The switch runs Cisco NX-OS software that has comprehensive features and functions that are widely deployed globally. The Cisco Nexus 3548 contains no physical layer (PHY) chips, which allows low latency and low power consumption. The switch supports both forward and reversed airflow and both AC and DC power inputs.

Cisco Nexus 3524 Switch

The Cisco Nexus 3524 switch is a Cisco Nexus 3548 switch, but with only 24 ports active and can be upgraded to use all 48 ports. As a compact one-rack-unit (1RU) form-factor 10 Gigabit Ethernet switch, the Cisco Nexus 3548 switch is the lowest entry point for main-stream top-of-rack (TOR) data center deployments which offers line-rate Layer 2 and Layer 3 switching with a comprehensive feature set, including Algo Boost technology, and ultra-low latency.

For information about the Cisco Nexus 3500 Series, see the *Cisco Nexus 3500 Series Hardware Installation Guide*.

System Requirements

This section includes the following topics:

- [Memory Requirements](#)

- [Hardware Supported](#)

Memory Requirements

The Cisco NX-OS Release 6.0(2)A8(2) software requires 203 MB of flash memory.

Hardware Supported

Cisco NX-OS Release 6.0(2)A8(2) supports the Cisco Nexus 3500 Series switches. You can find detailed information about supported hardware in the Cisco Nexus 3500 Series Hardware Installation Guide.

Table 2 shows the hardware supported by Cisco NX-OS Release 6.0(2)A8(2) software.

Table 2. Hardware Supported by Cisco NX-OS Release 6.0(2)A8(2) Software.

Hardware	Part Number	Supported Software Release
Cisco Nexus 3500 Series		
Cisco Nexus 3548 switch	N3K-C3548P-10G	5.0(3)A1(1) and later releases
Cisco Nexus 3548x switch, 48 SFP+	N3K-C3548P-10GX	6.0(2)A6(1) and later releases
Cisco Nexus 3524 switch	N3K-C3524P-10G	6.0(2)A6(1) and later releases
Cisco Nexus 3524 switch, 24 SFP+	N3K-C3524P-10GX	5.0(3)A1(1) and later releases
Cisco Nexus 2000 or Nexus 3000 individual fan, forward airflow (port side exhaust	NXA-FAN-30CFM-F	5.0(3)A1(1) and later releases

Hardware	Part Number	Supported Software Release
Cisco Nexus 2000 or Nexus 3000 individual fan, reversed airflow (port side intake)	NXA-FAN-30CFM-B	5.0(3)A1(1) and later releases
Cisco Nexus 2000 or Nexus 3000 400W AC power supply, forward airflow (port side exhaust)	N2200-PAC-400W	5.0(3)A1(1) and later releases
Cisco Nexus 2000 or Nexus 3000 400W AC power supply, reversed airflow (port side intake)	N2200-PAC-400W-B	5.0(3)A1(1) and later releases
Cisco Nexus 2000 or Nexus 3000 400W DC power supply, forward airflow (port side exhaust)	N2200-PDC-400W	5.0(3)A1(1) and later releases
Cisco Nexus 2000 or Nexus 3000 350W DC power supply, reversed airflow (port side intake)	N3K-PDC-350W-B	5.0(3)A1(1) and later releases
Transceivers		
10-Gigabit		
10GBASE-ZR SFP+ module (single-mode fiber [SMF])	SFP-10G-ZR	6.0(2)A3(1) and later releases
10GBASE-CU SFP+ cable 1.5 m (Twinax cable)	SFP-H10GB-CU1-5M	6.0(2)A3(1) and later releases
10GBASE-CU SFP+ cable 2 m (Twinax cable)	SFP-H10GB-CU2M	6.0(2)A3(1) and later releases
10GBASE-CU SFP+ cable 2.5 m (Twinax cable)	SFP-H10GB-CU2-5M	6.0(2)A3(1) and later releases
Active optical cable 1 m	SFP-10G-AOC1M	6.0(2)A3(1) and later releases
Active optical cable 3 m	SFP-10G-AOC3M	6.0(2)A3(1) and later releases
Active optical cable 5 m	SFP-10G-AOC5M	6.0(2)A3(1) and later releases
Active optical cable 7 m	SFP-10G-AOC7M	6.0(2)A3(1) and later releases
10GBASE-DWDM long-range transceiver module 80 km with single mode duplex fiber	DWDM-SFP10G-C	6.0(2)A3(1) and later releases
10GBASE-DWDM long-range transceiver module 80 km with single mode duplex fiber	DWDM-SFP10G	6.0(2)A1(1) and later releases

Hardware	Part Number	Supported Software Release
10GBASE-SR SFP+ module (multimode fiber [MMF])	SFP-10G-SR	5.0(3)A1(1) and later releases
10GBASE-LR SFP+ module (single-mode fiber [SMF])	SFP-10G-LR	5.0(3)A1(1) and later releases
Cisco 10GBASE-ER SFP+ Module for SMF	SFP-10G-ER	5.0(3)A1(1) and later releases
10GBASE-SR SFP+ module (multimode fiber [MMF])	SFP-10G-SR-S	6.0(2)A8(2) and later releases
10GBASE-LR SFP+ module (single-mode fiber [SMF])	SFP-10G-LR-S	6.0(2)A8(2) and later releases
Cisco 10GBASE-ER SFP+ Module for SMF	SFP-10G-ER-S	6.0(2)A8(2) and later releases
10GBASE-ZR SFP+ module (single-mode fiber [SMF])	SFP-10G-ZR-S	6.0(2)A8(2) and later releases
10GBASE-CU SFP+ cable 1 m (Twinax cable)	SFP-H10GB-CU1M	5.0(3)A1(1) and later releases
10GBASE-CU SFP+ cable 3 m (Twinax cable)	SFP-H10GB-CU3M	5.0(3)A1(1) and later releases
10GBASE-CU SFP+ cable 5 m (Twinax cable)	SFP-H10GB-CU5M	5.0(3)A1(1) and later releases
Active Twinax cable assembly, 7 m	SFP-H10GB-ACU7M	5.0(3)A1(1) and later releases
Active Twinax cable assembly, 10 m	SFP-H10GB-ACU10M	5.0(3)A1(1) and later releases
1-Gigabit Ethernet		
1000BASE-T SFP	GLC-TE	6.0(2)A3(1) and later releases
Gigabit Ethernet SFP, LC connector EX transceiver (MMF)	GLC-EX-SMD	6.0(2)A3(1) and later releases
Gigabit Ethernet SFP, LC connector ZX transceiver (MMF)	GLC-ZX-SMD	6.0(2)A3(1) and later releases
1000BASE-T SFP	GLC-T	6.0(2)A1(1) and later releases
Gigabit Ethernet SFP, LC connector SX transceiver (MMF)	GLC-SX-MM	5.0(3)A1(1) and later releases
Gigabit Ethernet SFP, LC connector SX transceiver (MMF)	GLC-SX-MMD	5.0(3)A1(1) and later releases

Hardware	Part Number	Supported Software Release
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF)	GLC-LH-SM	5.0(3)A1(1) and later releases
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF)	GLC-LH-SMD	5.0(3)A1(1) and later releases
100-Megabit Ethernet		
1000BASE-T SFP transceiver module with extended operating temperature range	SFP-GE-T	6.0(2)A3(1) and later releases
100BASE-FX SFP module for Gigabit Ethernet ports GLC-GE-100FX	GLC-GE-100FX	6.0(2)A3(1) and later releases

New and Changed Information

This section lists the new and changed features in Release 6.0(2)A8(2).

- New Supported Hardware
- New Software Features

New Supported Hardware

Cisco NX-OS Release 6.0(2)A8(2) does not include any new hardware.

New Software Features

Cisco NX-OS Release 6.0(2)A8(2) includes the following new software features:

- Layer 3 over VPC support

- Supports VPC in warp mode

- LPM TCAM carving for increased multicast scale in both normal mode and warp mode

- DHCP snooping Option 82 with configurable string

- MAC address table loop-detect port down feature

- Generate marker packet for OpenFlow NDB requirement to timestamp ttag packets

- Enable DOM monitoring for low and high threshold warnings

- Splunk tool integration for Active buffer monitoring and Latency monitoring features

- Storm control on a port level

Caveats

The open and resolved 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.

This section includes the following topics:

- Resolved Bugs for this Release

- Open Bugs for this Release

Resolved Bugs for this Release

Table 3 lists descriptions of resolved bugs in Cisco NX-OS Release 6.0(2)A8(2). You can use the record ID to search Cisco Bug Search Tool for details about the bug.

Table 3 Cisco NX-OS Release 6.0(2)A8(2) – Resolved Bugs

Record Number	Resolved Bug Headline
CSCuw38075	The default drop open flow not capturing all traffic. Because the pre-programmed drop flow with a priority of zero do not match any traffic, in typical open flow environments, the mac learning ability is turned off and the traffic floods to all ports.
CSCux19309	PTP timestamp do not change in the PTP packets that are sent out of a PTP Master port and the MeanPath delay is not calculated on the impacted device.
CSCux48252	Higher priority flow not matching with EtherType 0x0.
CSCux50309	Virtual PortChannel auto-recovery timer change. The minimum value for vPC auto-recovery timer on Nexus3500 is 240 Secs. Suggested a change to 60 Secs.
CSCux59824	Issues with enabling Warp mode on N3548 that is running A7.1 code.
CSCux83523	Multicast service-reflect feature may remove the output interface for the S1,G1 groups, which will result in receivers not receiving traffic on S2,G2.
CSCux84200	Marker packets are sent to wrong destination IP after changes to ERSPAN destination IP.
CSCux87710	A vulnerability in Network Time Protocol (NTP) package of Cisco NX-OS Software and Cisco Multilayer Director Switch (MDS) could allow an unauthenticated, remote attacker to cause a Denial of Service (DoS) condition on an affected device.
CSCux92568	Nexus 3548X locator LED turned on by default.
CSCuy00153	Because vPC is not a supported feature in WARP mode, it must be blocked as it causes traffic disruption.
CSCuy06002	A Nexus 3548 running 6.0(2)A1(1c) and newer version may crash in Precision Time Protocol (PTP).
CSCuy15403	The UTC_offset field in the ERSPAN marker packets may be incorrectly set to 0x23.
CSCuy16991	N3K-C3548P-10GX with 6.0(2)A7(1) may experience "Monitor hap reset" because of a HA policy Reset.
CSCuy25800	A vulnerability in Cisco NX-OS Software running on Cisco Nexus 3000 Series Switches and Cisco Nexus 3500 Platform Switches could allow an unauthenticated, remote attacker to log in to the device with the privileges of the root user with bash shell access.
CSCuy28520	IGMP may encounter a hap reset in the course of updating the policy applied to it's IGMP enabled interfaces.
CSCuy56095	The N3548X link goes down when SR optics is replaced by SR-S after reload.
CSCuy57375	10Gbase-SR SFPs are not coming up on Nexus 3548-X.
CSCuy63407	N3500 RACL not hit when configured with DHCP relay on same interface.

Record Number	Resolved Bug Headline
CSCuy69477	Between two Nexus 3500 devices, multicast traffic that switches from a source to the link between the 2 nexus 3500 may result in a very low amount of CRC erred frames being received by the receiving nexus 3500.
CSCuy76055	After an upgrade from A1(1d) to A6(5), some of NAT rules cannot be deleted.
CSCuy81094	Incorrect ifHCInOctets values on 3548.
CSCuy84877	Marker and ERSPAN packets not in synchronizing at 1 nanosecond granularity.
CSCuy90166	An ingress DHCP broadcast packet will be forwarded across the Peer Link and reflected back down the same vPC leg it was received on, leading to MAC flaps on downstream switches.
CSCuy92412	N3500 crashes when configuring Regex.
CSCuy96311	Device punts all the traffic to the CPU potentially crashing the it with a log that indicates FIB Adjacency table is full even when there is enough space for hardware adjacency table to create new entries.
CSCuz00868	N3500 Service Reflect - The multicast service reflection feature is supported only on Cisco Nexus 3548-X platforms from Release 6.0(2)A6(1).
CSCuz07246	An orphan port stale adjacency for peer MAC is black holing traffic.
CSCuz09640	Captured traffic is no longer received on the ERSPAN destination device after an interface flaps on the ERSPAN source Nexus 3500 switch.
CSCuz19834	NX-OS is missing subnet check when considering new IGMP snooping querier. Query received on a VLAN from a different VLAN with querier address belonging to a different subnet.
CSCuz20812	N3500 as DR creates duplicates of IGMP GQs.
CSCuz30590	N3500 must reject RACL on Layer 2 ports configuration.
CSCuz50034	The scheduler process slowly increases memory that holds under the libaaa.so component.
CSCuz53130	Discrepancy in the order of access-group applied on the interface on running-configuration and start-up configuration.
CSCuz72942	MTC_USD service crashes on N3500.
CSCuz35039	N3500 multicast loses packets because of periodic delayed null-register.
CSCva54837	Forwarding Manager (FWM) crashes repeatedly on vPC primary after upgrading secondary switch.
CSCva64570	Command "service unsupported-transceiver" stops working after upgrading from 6.0(2)A6(5) to 6.0(2)A6(8).
CSCva55859	Some of the Layer 3 interfaces converted to Layer 2 interfaces after upgrading from 6.0(2)A6(5a) to 6.0(2)A6(8)
CSCva24927	N3500 switches running A8(1) does not count jumbo frames in tx direction while the same frames are counted as jumbo frames in rx direction.
CSCva20344	Nexus 3500 Buffer block / lockup - no TX multicast or broadcast.

Record Number	Resolved Bug Headline
CSCuz94305	Single Source Multicast routed traffic gets dropped on Nexus 3500 switch.
CSCva15538	Layer 3 flow punted to CPU because of Layer 3 MTU failure.
CSCuz13351	OSPF process is not starting after reload ascii and copy r s reload commands issues on a VXLAN setup.

Open Bugs for this Release

Table 4 list descriptions of open bugs in Cisco NX-OS Release 6.0(2)A8(2). You can use the record ID to search Cisco Bug Search Tool for details about the bug.

Table 4 Cisco NX-OS Release 6.0(2)A8(2) – Open Bugs

Record Number	Open Bug Headline
CSCva82122	System does not throw any incompatibility errors when you downgrade from release 6.0(2)A8(2) to any of the earlier releases that has both vPC and warp mode configured.
CSCva81933	Trace route packets destined for self-ip received on MCT peer links are dropped.

Upgrade Path to Cisco NX-OS Release 6.x

If a custom CoPP policy is applied after upgrading to Cisco NX-OS Release 6.0(2)A1(1) or later, and if the Nexus 3548 switch is downgraded to Cisco NX-OS Release 5.0, where changes to the CoPP policy are not permitted, the custom CoPP policy is retained and cannot be modified.

Note: copy r s and reload is not a supported method for an upgrade.

Limitations

The following are the known limitations for Cisco NX-OS Release 6.0(2)A8(2):

- PBR and NAT cannot be supported on the same interface.

- set ip default next hop cannot be applied in PBR.

- IGMP packets, which are filtered by report policies on the local switch on which IGMP filtering is enabled, will still get forwarded to the peer switch (See CSCup50141).

- Counters for the warp SPAN destination port do not work. To check these counters, connect another switch to the destination ports (See CSCuq66372).

- In a vPC setup, because of a hardware limitation, non-RPF traffic for (S,G) that comes in on the RPF interface for (*,G) hits the (*,G) entry instead of being treated as (S,G) non-RPF traffic and dropped. (S,G) non-RPF traffic is

then incorrectly forwarded by (*,G) entry, thus causing traffic duplication. To avoid duplication of Layer 3 multicast traffic by sending the (S,G) RP-bit prune, run the ip pim pre-build-spt command (See CSCun34760).

■ While performing Online Insertion Removal (OIR) on the cable or optics of a 40G bundle, you must perform the following sequence of steps for the OIR to be successful (See CSCug93225):

1 Disable (shut) the 40G port

2 Change the speed from 40G to 10G

3 Perform an OIR on the cable or optics

4 Change the speed from 10G to 40G

5 Re-enable (no shut) the port

■ SSH/SCP sessions with Cisco Nexus 3500 series switches running 6.0(2)A8(x) release may fail with a "no matching cipher found" message. This failure is due to the weaker CBC ciphers getting deprecated for security reasons (See CSCun41202).

Best Practices

The syntax of the poap_script.py file should be validated using the python validation tool before using the file for POAP. Otherwise, if the poap_script.py file is edited with a syntax error, the POAP process will exit without giving an error.

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

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.