



Cisco Nexus 3500 Series NX-OS Release Notes, Release 6.0(2)A7(1)

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
October 26, 2015	Created NX-OS Release 6.0(2)A7(1) release notes
March 22, 2016	Removed the following statement from <i>Limitations</i> : IP DHCP snooping is not supported.

Contents

Introduction	2
System Requirements	3
New and Changed Information	6
Upgrade Path to Cisco NX-OS Release 6.x	7
Limitations	7
Best Practices	8
Open and Resolved Bugs	8
MIB Support	9
Related Documentation	9
Documentation Feedback	10
Obtaining Documentation and Submitting a Service Request	10

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)A7(1) software requires 203 MB of flash memory.

Hardware Supported

Cisco NX-OS Release 6.0(2)A7(1) 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)A7(1) software.

Table 2. Hardware Supported by Cisco NX-OS Release 6.0(2)A7(1) 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

System Requirements

Hardware	Part Number	Supported Software Release
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
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

System Requirements

Hardware	Part Number	Supported Software Release
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
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-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

Hardware	Part Number	Supported Software Release
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
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)A7(1).

- New Supported Hardware
- New Software Features

New Supported Hardware

Cisco NX-OS Release 6.0(2)A7(1) does not include new hardware.

New Software Features

Cisco NX-OS Release 6.0(2)A7(1) includes the following new software features:

- Debounce timer support for 40G bundle interface – Ability to support debounce timers on a 40G bundle interface.
- IGMP Host Proxy – Proxies PIM joins or prunes received by sending IGMP joins or Leaves on the proxy interface.
- IP Event Dampening – Reduces high CPU usage caused by excessive interface flap updates.

- Latency Monitoring – Provides a real-time view of the latency incurred by packets travelling through the switch on a per-port basis.
- MBGP – The multiprotocol BGP feature adds capabilities to BGP that enable the multicast routing policy throughout the Internet and to connect multicast topologies within and between BGP autonomous systems.
- NXAPI – On Cisco Nexus devices, command-line interfaces (CLIs) are run only on the device. NX-API improves the accessibility of these CLIs by making them available outside of the switch by using HTTP/HTTPS. You can use this extension with the existing Cisco Nexus CLI system on the Cisco Nexus 3500 Series devices. NX-API supports show commands, configurations, and Linux Bash. NX-API supports JSON-RPC.
- Policy Based Routing – Provides a flexible means of routing packets based on configured policies.
- Puppet Support – IT automation software for defining and enforcing the state of the infrastructure.
- PVLAN – Enables the partitioning of L2 broadcast domains into sub domains.
- Unicast RPF – A security feature that the network admins can use to limit the malicious traffic on an enterprise network.
- VRF Aware NAT – Enables a switch to understand an address space in a VRF and to translate the packet. This allows the NAT feature to translate traffic in an overlapping address space that is used between two VRFs.

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.

Limitations

The following are the known limitations for Cisco NX-OS Release 6.0(2)A7(1):

- 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 [CSCuq93225](#)):
 - 1 Disable (shut) the 40G port
 - 2 Change the speed from 40G to 10G

Best Practices

- 3 Perform an OIR on the cable or optics
- 4 Change the speed from 10G to 40G
- 5 Re-enable (no shut) the port

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.

Open and Resolved Bugs

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 in this Release](#)
- [Open Bugs for this Release](#)

Resolved Bugs in this Release

Table 3 lists descriptions of resolved bugs in Cisco NX-OS Release 6.0(2)A7(1). 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)A7(1) – Resolved Bugs

Record Number	Resolved Bug Headline
CSCui21504	The Cisco Nexus 3500 shows an extreme periodic time adjustment when acting as slave. This is periodic and is not a continuous process. It is hard to see unless always monitoring the ptp correction.
CSCup41806	<p>On the Cisco Nexus 3500 platform, the ALGO_BOOST_SERVICES_PKG license (N3548-ALGK9) offers the following 3 features:</p> <ul style="list-style-type: none"> ■ Warp Mode ■ Warp SPAN ■ Static NAT <p>But when the warp mode of forwarding is configured, the license status remains "not in use", and the configuration of warp mode of forwarding does not trigger the license usage.</p>

MIB Support

Record Number	Resolved Bug Headline
CSCuq39947	A Cisco Nexus 3548 needs ip local-proxy-arp enabled to respond to ARP requests for Inside Global addresses, which falls under the connected subnet, while performing static NAT.
CSCus48206	The Cisco Nexus 3548 experiences Q-in-Q traffic loss.
CSCuv95538	A Cisco Nexus 3500 running 6.0(2)A6(3) experiences a memory leak due to an AFM service hap reset.
CSCuw02037	<p>A vulnerability in the Address Resolution Protocol (ARP) feature of the Cisco Nexus Operating System (NX-OS) could allow an unauthenticated, adjacent attacker to cause a partial denial of service (DoS) condition due to the ARP process unexpectedly restarting.</p> <p>The vulnerability is due to improper input validation of the fields in the ARP packet header. An attacker could exploit this vulnerability by sending a crafted ARP packet from an adjacent network to the affected device. An exploit could allow the attacker to cause a partial DoS condition because the ARP process could unexpectedly restart when processing the crafted ARP packet.</p>
CSCuw02851	When RACL is configured on a sub-interface, the traffic is blocked or allowed on another sub-interface.
CSCuw10287	The filter option for local span is not working. The filter gets applied on a different monitor session.
CSCuw33914	<p>The CPU spikes to +50% when running the following commands:</p> <ul style="list-style-type: none"> ■ show version ■ show startup-config ■ show accounting log
CSCuw44058	The UTC offset value is not reused by the boundary clock when the utc_offset_valid flag is FALSE from the grand master.
CSCuw58833	show platform afm event-history log is not included in show tech aclmgr.

Open Bugs for this Release

There are no open bugs in Cisco NX-OS Release 6.0(2)A7(1).

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.

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)

© 2015 Cisco Systems, Inc. All rights reserved.