



# Cisco Nexus 3548 Series NX-OS Release Notes, Release 6.0(2)A1(1)

**Release Date:** May 22, 2013  
**Part Number:** OL-29566-01  
**Current Release:** Cisco NX-OS Release 6.0(2)A1(1)

This document describes the features, caveats, and limitations for Cisco Nexus 3548 switches. Use this document in combination with documents listed in the “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](http://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)” section on page 11.



## Note

Release notes are sometimes updated with new information about restrictions and caveats. See the following website for the most recent version of the Cisco Nexus 3548 release notes:  
[http://www.cisco.com/en/US/products/ps11541/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps11541/prod_release_notes_list.html)



## Note

[Table 1](#) shows the online change history for this document.

**Table 1** *Online History Change*

Part Number	Revision	Date	Description
OL-29566-01	C0	February 27, 2014	Added a limitation pertaining to the <b>ip igmp join-group</b> command.
OL-29566-01	B0	October 22, 2013	Added upgrade and downgrade guidelines to the NX-OS Release 6.0(2)A1(1) release notes.
OL-29566-01	A0	May 22, 2013	Created NX-OS Release 6.0(2)A1(1) release notes.



# Contents

This document includes the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 3](#)
- [New and Changed Features, page 5](#)
- [Upgrade and Downgrade Guidelines, page 7](#)
- [Limitations, page 7](#)
- [Caveats, page 8](#)
- [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: \[www.cisco.com/go/trademarks\]\(http://www.cisco.com/go/trademarks\). 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. \(1110R\), page 11](#)

## 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.

## Cisco Nexus 3500 Series Switches

The Cisco Nexus 3500 platform is an extension of the Cisco Nexus 3000 Series of 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.

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, page 3](#)
- [Hardware Supported, page 3](#)

## Memory Requirements

The Cisco NX-OS Release 6.0(2)A1(1) software requires 135 MB of flash memory.

## Hardware Supported

Cisco NX-OS Release 6.0(2)A1(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)A1(1) software.

**Table 2**      **Hardware Supported by Cisco NX-OS Release 6.0(2)A1(1) Software**

Hardware	Part Number	Supported Software Release
<b>Cisco Nexus 3500 Series</b>		
Cisco Nexus 3548 switch	N3K-C3548P-10G	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
<b>Transceivers</b>		
<b>10-Gigabit</b>		
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
<b>1-Gigabit Ethernet</b>		
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

**Table 2**      **Hardware Supported by Cisco NX-OS Release 6.0(2)A1(1) Software (continued)**

Hardware	Part Number	Supported Software Release
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

## New and Changed Features

This section describes the new features introduced in Cisco NX-OS Release 6.0(2)A1(1). This section includes the following topics:

- [New Supported Hardware, page 5](#)
- [New Software Features, page 5](#)

### New Supported Hardware

Starting with Cisco NX-OS Release 6.0(2)A1(1), the following transceivers are supported:

- DWDM-SFP10G: 10GBASE-DWDM long-range transceiver module 80 km with single mode duplex fiber
- GLC-T: 1000BASE-T SFP

### New Software Features

Cisco Nexus 3548 switches are supported by Cisco NX-OS Release 6.0(2)A1(1). Cisco NX-OS interoperates with any networking operating system, including Cisco IOS software, that conforms to the networking standards listed in the product data sheet.

Cisco NX-OS Release 6.0(2)A1(1) is a major new release that includes the following new software features:

#### 40-Gigabit Interface Support

Starting with this release for the Cisco Nexus 3548 switch, you can enable 40 Gbps speed on up to 12 interfaces. This enhancement allows you to enable 40-Gbps speed on the first port of a group of four adjacent ports.

#### BGP Add-Path

To promote path diversity and reduce multi-exit discriminator (MED) oscillations, you can configure BGP Additional Paths so that multiple paths in the same peering session can advertise the same prefix without the new paths replacing any previous paths.

## Configurable CoPP

Control Plane Policing (CoPP) protects the control plane and separates it from the data plane, which ensures network stability, reachability, and packet delivery. This feature allows a policy map, much like a QoS policy, to be applied to the control plane. The policy map is applied to all traffic destined to any of the IP addresses of the router or Layer 3 switch. The Cisco NX-OS device provides CoPP to prevent Denial of Service (DoS) or similar attacks from affecting performance.

## Select Layer 3 as the Default Port Mode

Default Layer 3 mode allows you to select the default port mode as Layer 3 when the switch is reloaded without a start-up configuration. This feature ensures that no incorrect forwarding occurs before you confirm the port mode.

To allow consistency with previous releases, the user is able to select the default port mode in the first setup script, for example, as shown in the following command:

```
configure default interface layer (L3/L2) [L2]: 13
```

## Dynamic NAT

Dynamic Network Address Translation (NAT) translates a group of real IP addresses into mapped IP addresses that are routable on a destination network. A dynamic NAT configuration automatically creates a firewall between your internal network and outside networks or the Internet. Dynamic NAT allows only connections that originate inside the stub domain—a device on an external network cannot connect to devices in your network, unless your device has initiated the contact. The dynamic NAT feature supports Port Address Translation (PAT) and access control lists (ACLs).

## ERSPAN

Encapsulated Remote Switched Port Analyzer (ERSPAN) features are introduced in Cisco Nexus 3000 Series Release 6.02(U)1(1). The Cisco NX-OS system supports the Encapsulated Remote Switching Port Analyzer (ERSPAN) feature on both source and destination ports. ERSPAN transports mirrored traffic over an IP network.

## Link Level Flow Control

Release 6.02(U)1(1) introduces link-level flow control, which is a congestion management technique that pauses data transmission on the link, based on pause requests from the receiver, until the congestion in the system is resolved. Link level flow control is independently configurable in either direction on the same link.

## Wildcard Mask in permit ip Command

In previous releases, a wildcard mask was incorrectly applied as a net mask in the following command context:

```
permit ip src-ip wildcard mask dst-ip wildcard mask
```

Starting with this release, these masks will be treated correctly as wildcard masks.

## PIM-Bidir

Bidirectional Protocol Independent Multicast (PIM-Bidir) is a variant of the PIM protocol that allows bidirectional distribution trees. In PIM-Bidir, traffic flows along the distribution tree in either direction. PIM-Bidir eliminates the need to keep source-specific state information and allows trees to scale to any number of sources.

## POAP

PowerOn Auto Provisioning (POAP) automates the process of upgrading software images and installing configuration files on Cisco Nexus switches that are being deployed in the network for the first time.

## POAP Use of First MAC Address

In Power-On Auto-Provisioning, you can now use the MAC address to identify the new switch in the Client Option field during the DHCP Discovery phase. The MAC address also appears on the shipping label for the new switch.

## Precision Time Protocol

This release introduces certain Precision Time Protocol (PTP) capabilities and commands. PTP is a time synchronization protocol for nodes that are distributed across a network. Its hardware timestamp provides greater accuracy than other time synchronization protocols such as the Network Time Protocol (NTP).

## VRF Route Leaking

With an Enterprise license and Border Gateway Protocol- (BGP)-enabled, Virtual Routing and Forwarding (VRF) route leaking is allowed in a VRF-lite scenario, based on certain configuration guidelines and limitations. With VRF route leaking, you can import IP prefixes from the global routing table (the default VRF) into any other VRF by using an import policy. The VRF import policy uses a route map to specify the prefixes to be imported into a VRF. IP prefixes that are imported into a VRF through this import policy cannot be reimported into another VPN VRF. The maximum number of prefixes that can be imported from the default VRF is controlled by a limit that you configure.

# Upgrade and Downgrade Guidelines

## 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

Cisco NX-OS Release 6.0(2)A1(1) has the following limitation:

In Cisco NX-OS releases older than Cisco NX-OS Release 6.0(2)A1(1), you can use the **ip igmp join-group** command to bind a Nexus 3548 switch to a multicast group. The switch generates an Internet Group Management Protocol (IGMP)-join for the specified group, and any multicast packets destined to the group are sent to the CPU. If there are receivers connected to the Nexus 3548 switch, which request for the group, then a copy of the packet is also sent to the receiver.

In Cisco NX-OS Release 6.0(2)A1(1) and higher releases, you cannot use the **ip igmp join-group** command to program any Outgoing Interface Lists (OILs) in the hardware. Even if there are receivers that request for the stream, no packets are sent to them. To bind a Nexus 3548 switch to a multicast group, use the **ip igmp static-oif** command instead of the **ip igmp join-group** command.

You can use the **ip igmp join-group** command only if the **ip routing multicast enforce-rpf** command, which is hidden, is enabled. This command can only be enabled if LISP is not in use, and LISP is not available on Nexus 3548 switches.

## Caveats

Open and resolved caveat record numbers are provided with links to the Bug Toolkit where you can find details about each caveat.

This section includes the following topics:

- [Resolved Caveats in Cisco NX-OS Release 6.0\(2\)A\(1\), page 8](#)
- [Open Caveats in Cisco NX-OS Release 6.0\(2\)A1\(1\), page 9](#)

## Resolved Caveats in Cisco NX-OS Release 6.0(2)A(1)

[Table 3](#) lists descriptions of resolved caveats in Cisco NX-OS Release 6.0(2)A(1). The record ID links to the Cisco Bug Toolkit where you can find details about the caveat.

**Table 3** *Cisco NX-OS Release 6.0(2)A(1)—Resolved Caveats*

Record Number	Resolved Caveat Headline
<a href="#">CSCua66832</a>	<a href="#">CSCua66832</a> has been superseded by <a href="#">CSCua49361</a> (resolved). The Open Shortest Path First (OSPF) protocol link state advertisement (LSA) is not advertised and the route is not in the forwarding information base (FIB) or the routing information base (RIB).
<a href="#">CSCuc24329</a>	A port goes to an error disabled state on the port configured by the <b>switchport monitor</b> command when you try to change to Layer 3 using the <b>no switchport</b> command.
<a href="#">CSCuc38422</a>	While deleting NAT entries, the top entry in the TCAM gets reset first.
<a href="#">CSCuc52002</a>	SFP, port LED, and status errors occur.
<a href="#">CSCuc86075</a>	When changing NAT inside or outside on SVIs, the switch displays a “service not responding” message.
<a href="#">CSCuc99396</a>	Duplicate of <a href="#">CSCuc07245</a> . Logging source-interface loopback 0" required a space between loopback and 0. Resolution allows you to configure a source-interface so that any valid IP can be accepted as the source.



**Table 3** *Cisco NX-OS Release 6.0(2)A1(1)—Resolved Caveats (continued)*

Record Number	Resolved Caveat Headline
<a href="#">CSCud68615</a>	Warp SPAN is not removed when downgrading from Cisco NX-OS Release 5.0(3)A1(2) to Release 5.0(3)A1(1).
<a href="#">CSCud82687</a>	Session 18 is converted to a WARP session after upgrading to Cisco NX-OS Release 5.0(3)A1(2).

## Open Caveats in Cisco NX-OS Release 6.0(2)A1(1)

[Table 1-4](#) lists open caveats in Cisco NX-OS Release 6.0(2)A1(1). The record ID links to the Cisco Bug Toolkit, where you can find details about the caveat.

**Table 1-4 Cisco NX-OS Release 5.0(3)A1(2a)—Open Caveats**

Record Number	Open Caveat Headline
<a href="#">CSCua42953</a>	During a class-default MTU check, the system checks against itself.
<a href="#">CSCub43220</a>	Monitor session is up even though the span destination is down.
<a href="#">CSCub46233</a>	A Multiple Spanning Tree Protocol (MSTP) instance does not get deleted, even though its VLANs are shut down.
<a href="#">CSCub64511</a>	Layer IPv6 traffic does not set or rewrite CoS correctly.
<a href="#">CSCub89134</a>	2-tuple is not displayed in the incompatibility check.
<a href="#">CSCuc02277</a>	Need to add support for the <b>hardware profile multicast prefer-source-tree</b> command.
<a href="#">CSCuc12318</a>	IGMP snooping v3 report suppression cannot be enabled.
<a href="#">CSCuc86978</a>	Find SFP detection failure, LED error after SFP OIR in quick succession.
<a href="#">CSCue80692</a>	EDEN:clear counters on CLI is clearing the interface mib counters.
<a href="#">CSCue90910</a>	Bidir: (S,G) shown up in conversion ASM- >Bidir with IGMP S,G joins.
<a href="#">CSCuf21894</a>	Removing the feature vPC doesn't change the prune list on a peer.
<a href="#">CSCug18837</a>	With 20 ERSPAN destination sessions, the fifth local session that is added lacks a hardware resource.
<a href="#">CSCug22867</a>	Learning not disabled for mac move between vpc po and orphan port.
<a href="#">CSCug77292</a>	POAP-Syntax error while parsing 'ip igmp snooping mrouter interface po2.
<a href="#">CSCug85517</a>	The 40-Gbps port-channel speed goes to 'auto' instead of "no speed."

## 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 3548 switch. The MIB Support List is available at the following FTP sites:

<ftp://ftp.cisco.com/%2Fpub/mibs/supportlists/nexus3548/Nexus3548MIBSupportList.html>

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: <http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

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](http://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)

© 2013 Cisco Systems, Inc. All rights reserved.

