Send documentation comments to nexus5kdocs@cisco.com

Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes,

for Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c)

Release Date: March 3, 2011
Part Number: OL-24564-01 U0
Current Release: NX-OS Release 5.0(3)N1(1c)

Deferred Release: NX-OS Release 5.0(3)N1(1b)

Deferred Release: NX-OS Release 5.0(3)N1(1a)

Deferred Release: NX-OS Release 5.0(3)N1(1)

This document describes the features, caveats, and limitations for Cisco Cisco Nexus 5000 Series switches and the Cisco Nexus 2000 Series Fabric Extenders. Use this document in combination with documents listed in the "Related Documentation" section on page 31.

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 Cisco Nexus 5000 Series and Cisco Nexus 2000 Series release notes: http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/release/notes/Nexus_5000_Release_Notes.html

Note Table 1 shows the online change history for this document.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table 1 Online History Change

Revision	Date	Description
A0	March 3, 2011	Created NX-OS Release 5.0(3)N1(1) release notes.
B0	March 7, 2011	Created NX-OS Release 5.0(3)N1(1a) release notes. Added: CSCtn70380 and CSCtn76613. Updated: Supported Upgrade and Downgrade Paths, page 16. Updated: Changed Software Features, page 14.
C0	March 9, 2011	Added: CSCtn79039, CSCtn82286, and CSCtn87115. Published release notes for Cisco NX-OS Release 5.0(3)N1(1a).
D0	March 17, 2011	Updated Upgrade and Downgrade Guidelines to include information about upgrading or downgrading to Cisco NX-OS Release 4.1(3). Updated Limitations with Cisco Nexus 2148 Fabric Extender information.
E0	March 28, 2011	Updated Limitations section with IGMP snooping Limitation.
F0	April 1, 2011	Corrected Unified Port Module reference to N55-M16UP.
G0	April 5, 2011	Updated Fabric Extender Scaling.
H0	April 7, 2011	Created NX-OS Release 5.0(3)N1(1b) release notes. Added CSCtn87115, CSCto23248, CSCto43675, and CSCto50140.
I0	April 12, 2011	Added CSCto63412.
J0	April 13, 2011	Updated CSCto23248.
K0	April 18, 2011	Moved CSCtn79039 to Resolved list.
L0	May 2, 2011	Created NX-OS Release 5.0(3)N1(1c) release notes. Added Resolved Caveats—Cisco NX-OS Release 5.0(3)N1(1c), page 29.
M0	May 31, 2011	Added Unified Port Configurations on Cisco Nexus 5500 Platform Switches, page 14.
N0	June 20, 2011	Added CSCto34674 and CSCtq04991 to Resolved list. Updated SPAN Limitations on Fabric Extender Ports.
P0	July 1, 2011	Added Note about RJ45 ports to Layer 3 Routing Modules.
Q0	August 12, 2011	Added Converged Network Adapters to Hardware Supported section. Updated Limitations on the Cisco Nexus 5010 and Cisco Nexus 5020.
R0	September 22, 2011	Added Reversed Airflow and DC Power Options, page 9.
S0	October 26, 2011	Added CSCtq13290 to Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c) Open Caveats.
T0	June 8, 2012	Removed incorrect grace period information.
U0	July 31, 2012	Updated Supported Upgrade and Downgrade Paths.

Contents

This document includes the following sections:

Introduction

The Cisco NX-OS software is a data center-class operating system built with modularity, resiliency, and serviceability at its foundation. Based on the industry-proven Cisco MDS 9000 SAN-OS software, Cisco NX-OS helps ensure continuous availability and sets the standard for mission-critical data center environments. The highly modular design of Cisco NX-OS makes zero-effect operations a reality and enables exceptional operational flexibility.

Several new hardware and software features are introduced for the Cisco Nexus 5000 Series switch and the Cisco Nexus 2000 Series Fabric Extender (FEX) to improve the performance, scalability, and management of the product line. Cisco NX-OS Release 5.0 also supports all hardware and software supported in Cisco NX-OS Software Release 4.2.

Cisco Nexus 5000 Series Switches

The Cisco Nexus 5000 Series switches include a family of line-rate, low-latency, lossless 10-Gigabit Ethernet, Cisco Data Center Ethernet, Fibre Channel over Ethernet (FCoE), and now native Fibre Channel switches for data center applications. The Cisco Nexus 5000 Series includes the Cisco Nexus 5500 Platform and the Cisco Nexus 5000 Platform.

Cisco NX-OS Software Release 5.0(3)N1(1b) introduces two new Cisco Nexus 5500 Platform switches that extend the versatility of the data-center class Cisco Nexus 5000 Series switches and provide higher density, lower latency, multilayer services.

The Cisco Nexus 5500 Platform includes the following switches:

- Cisco Nexus 5596UP switch
- Cisco Nexus 5548UP switch
- Cisco Nexus 5548P switch

For information about the new Cisco Nexus 5596UP switch and Cisco Nexus 5548UP switch, see the "New Hardware Features" section on page 6.

The Cisco Nexus 5000 Platform includes the following:

- Cisco Nexus 5020 switch

- Cisco Nexus 5010 switch.

For information about the Cisco Nexus 5000 Series, see the *Cisco Nexus 5000 Series and Cisco Nexus 5500 Platform Hardware Installation Guide*.

Cisco Nexus 2000 Series Fabric Extenders

The Cisco Nexus 2000 Series FEX is a highly scalable and flexible server networking solution that works with the Cisco Nexus 5000 Series switches to provide high-density and low-cost connectivity for server aggregation. Scaling across 1-Gigabit Ethernet, 10-Gigabit Ethernet, unified fabric, rack, and blade server environments, the FEX is designed to simplify data center architecture and operations.

The FEX integrates with its parent Cisco Nexus 5000 Series switch which allows zero-touch provisioning and automatic configuration. The FEX provides a single point of management that supports a large numbers of servers and hosts that can be configured with the same feature set as the parent Cisco Nexus 5000 Series switch, including security and quality of service (QoS) configuration parameters. Spanning Tree Protocol (STP) is not required between the Fabric Extender and its parent switch, because the Fabric Extender and its parent switch allow you to enable a large multi-path, loop-free, active-active topology.

Software is not included with the Fabric Extender. Cisco NX-OS software is automatically downloaded and upgraded from its parent switch. For information about configuring the Cisco Nexus 2000 FEX, see the “Configuring the Fabric Extender” chapter in the *Cisco Nexus 5000 Series Layer 2 Switching Configuration Guide*.

System Requirements

This section includes the following topics:

Hardware Supported

The Cisco NX-OS software supports the Cisco Nexus 5000 Series. You can find detailed information about supported hardware in the *Cisco Nexus 5000 Series Hardware Installation Guide*.

Table 2 shows the hardware supported by Cisco NX-OS Release 5.0(x) software.

Table 2 Hardware Supported by Cisco NX-OS Release 5.0(x) Software

		Cisco NX-OS Release Support		
Hardware	**Part Number**	**5.0(3)N1(1b) 5.0(3)N1(1c)**	**5.0(2)N2(1)**	**5.0(2)N1(1)**
Cisco Nexus 5000 Series				
Cisco Nexus 5596UP switch	N5K-C5596UP-FA	X	—	—
Cisco Nexus 5548UP switch	N5K-C5548UP-FA	X	—	—
Cisco Nexus 5548P switch	N5K-C5548P-FA	X	X	X
Cisco Nexus 5020P switch	N5K-C5020P-BF	X	X	X
Cisco Nexus 5010P switch	N5K-C5010P-BF	X	X	X

Table 2 Hardware Supported by Cisco NX-OS Release 5.0(x) Software (continued)

		Cisco NX-OS Release Support		
Hardware	**Part Number**	**5.0(3)N1(1b) 5.0(3)N1(1c)**	**5.0(2)N2(1)**	**5.0(2)N1(1)**
Cisco Nexus 2000 Series				
Cisco Nexus 2332PP FEX	N2K-C2232PP-10GE	X	X	X
Cisco Nexus 2248TP FEX	N2K-C2248TP-1GE	X	X	X
Cisco Nexus 2224TP FEX	N2K-C2224TP-1GE	X	X	X
Cisco Nexus 2148T FEX	N2K-C2148T-1GE	X	X	X
Expansion Modules				
16-port Universal GEM	N55K-M16UP	X	—	—
N5596 Layer 3 GEM	N55K-M160L3	X	—	—
N5548 Layer 3 daughter card	N55-D160L3	X	—	—
16-port SFP+ Ethernet	N55-M16P	X	X	X
8-port SFP+ Ethernet Ports 8-port SFP+ Fibre Channel Ports	N55-M8P8FP	X	X	X
Transceivers				
SFP+ Optical				
10-Gigabit Ethernet—short range	SFP-10G-SR(=)	X	X	X
10-Gigabit Ethernet—long range	SFP-10G-LR(=)	X	X	X
SFP+ Copper				
10GBASE-CU SFP+ Cable (1 meters)	SFP-H10GB-CU1M(=)	X	X	X
10GBASE-CU SFP+ Cable (3 meters)	SFP-H10GB-CU3M(=)	X	X	X
10GBASE-CU SFP+ Cable (5 meters)	SFP-H10GB-CU5M(=)	X	X	X
10GBASE-CU SFP+ Cable (7 meters)	SFP-H10GB-ACU7M(=)	X	X	X
10GBASE-CU SFP+ Cable (10 meters)	SFP-H10GB-ACU10M(=)	X	X	X
Fibre Channel				
4-,2-, 1-Gbps Fibre Channel—short wavelength	DS-SFP-FC4G-SW(=)	X	X	X
4-,2-, 1-Gbps Fibre Channel—long wavelength	DS-SFP-FC4G-LW(=)	X	X	X
Converged Network Adapters				
Generation-1 (Pre-FIP) CNAs[1]	—	X	X	X

1. Generation-1 (Pre-FIP) CNAs are supported on the Nexus 5000 Platform switches; however, they are not supported on the Nexus 5500 Series.

For information about Cisco Nexus 5000 Series support for Fabric Manager, see the “Compatibility with Cisco Nexus 5000 Series Switches” section in the *Release Notes for Cisco Fabric Manager.*

New and Changed Features

This section describes the new features introduced in Cisco NX-OS Release 5.0(3)N1(1b). This section includes the following topics:

Cisco Nexus Unified Port Technology

Beginning in Cisco NX-OS Release 5.0(3)N1(1b), Cisco introduces unified port technology. Cisco Nexus unified ports allow you to configure a physical port on a Cisco Nexus 5500 Platform switch as a 1/10-Gigabit Ethernet, Fibre Channel over Ethernet (FCoE), or 1-, 2-, 4-, 8-Gigabit native Fibre Channel port.

Currently, most networks have two types of switches for different types of networks. For example, LAN switches carry Ethernet traffic up to Catalyst switches and SAN switches carry FC traffic from servers to MDS switches. With unified port technology, you can deploy a unified platform, unified device, and unified wire approach. Unified ports allow you to move from an existing segregated platform approach where you choose LAN and SAN port options to transition to a single, unified fabric that is transparent and consistent with existing practices and management software. A unified fabric includes the following:

- Unified platform—Uses the same hardware platform and the same software code level and certifies it once for your LAN and SAN environments.
- Unified device—Runs LAN and SAN services on the same platform switch. The unified device allows you to connect your Ethernet and Fibre Channel cables to the same device.
- Unified wire—Converges LAN and SAN networks on a single converged network adapter (CNA) and connects them to your server.

A unified fabric allows you to manage Ethernet and FCoE features independently with existing Cisco tools.

The new Cisco Nexus 5548UP switch and the Cisco Nexus 5596UP switch provides built-in unified port technology. In addition, a new unified port expansion module and two Layer 3 modules increase the benefits of a deployed unified fabric.

New Hardware Features

The Cisco Nexus 5500 Platform switches, FEXs, and unified port extender modules available in this release provide the following benefits:

- Scalability—Increased FEX, MAC address table, VLAN, and multicast scalability with up to 24 attached FEXs, an increased limit of 16,000 to 32,000 MAC addresses, a 4000 VLAN limit, and 4000 multicast groups.
- Performance—Highest density 10G switch with wire-speed performance, low latency and full 96 ports of 10G line rate.
- Versatility—Both universal port switches support Layer 3 routing and they are Cisco Layer 2 FabricPath-ready.

- Flexibility—Unified ports that allow you to customize configuration modes for each port.

This section describes the following new hardware:

Cisco Nexus 5596UP Switch

The Cisco Nexus 5596UP switch is an Ethernet, Fibre Channel, and FCoE unified fabric switch with the following features:

- 2 RU 10-Gigabit Ethernet, Fibre Channel, and FCoE switch that offers up to 1920 Gbps of throughput.
- 48 fixed ports (all are unified-port capable).
- Up to 96 unified-ports (48 fixed unified ports and three installed unified-port expansion modules).
- Three expansion slots that are used to increase the number of 10-Gigabit Ethernet and FCoE ports or to connect to Fibre Channel SANs with 1-, 2-, 4-, 8-Gbps Fibre Channel switch ports.
- 32,000 MAC addresses of which 24,000 are available for unicast.
- Low-latency cut-through design that provides predictable, consistent traffic latency regardless of packet size, traffic pattern, or enabled features on 10-Gigabit Ethernet interfaces.
- Line-rate traffic throughput on all ports.
- Extension through the Cisco Nexus 2000 Series.

The Cisco Nexus 5596UP supports the following expansion modules:

- Unified port module that provides up to 16 1- or 10-Gigabit Ethernet and FCoE ports using SFP+ transceivers or up to 16 1-, 2-, 4-, 8-Gbps native Fibre Channel port connectivity using SFP+ and SFP transceivers. In unified port modules, the use of 1- and 10-Gigabit Ethernet or 1-, 2-, 4-, 8-Gbps Fibre Channel ports is mutually exclusive but configurable for any of the 16 physical ports per module.
- Layer 3 module that provides up to 160 Gbps of Layer 3 forwarding capability (240 mpps) that can be shared by all the I/O ports in the switch.
- Ethernet module that provides 16 1- or 10-Gigabit Ethernet and FCoE ports using SFP+ transceivers.
- FCoE and Ethernet module that provides 8 1- or 10-Gigabit Ethernet and FCoE ports using SFP+ transceivers, and 8 1-, 2-, 4-, 8-Gbps native Fibre Channel ports using SFP+ and SFP transceivers.

Cisco Nexus 5548UP Switch

The Cisco Nexus 5548UP switch is an Ethernet, Fibre Channel, and FCoE unified fabric switch that offers the following features:

- 1 RU 1- or 10-Gigabit Ethernet, Fibre Channel, and FCoE switch that offers up to 960-Gbps throughput.

- Up to 48 unified-ports (32 fixed unified ports and 16 ports with an installed unified-port expansion module).
- 32 fixed SFP+ ports and up to 1 expansion module.
- Hardware that is capable of 1- or 10-Gigabit Ethernet.
- 32,000 MAC address table entries.
- Low-latency cut-through design that provides predictable, consistent traffic latency regardless of packet size, traffic pattern, or enabled features on 10-Gigabit Ethernet interfaces.
- Line-rate traffic throughput on all ports.
- Extension through the Cisco Nexus 2000 Series.

Cisco Nexus 5548UP supports the following expansion modules:

- Unified port module that provides up to 16 1- or 10-Gigabit Ethernet and FCoE ports using SFP+ transceivers or up to 16 1-, 2-, 4-, 8-Gbps native Fibre Channel ports using SFP and SFP transceivers. In unified port modules, the use of 1- or 10-Gigabit Ethernet or 1-, 2-, 4-, 8-Gbps Fibre Channel ports is mutually exclusive but configurable for any of the 16 physical ports per module.
- FCoE and Ethernet module that provides 8 1- or 10-Gigabit Ethernet and FCoE using SFP transceivers and 8 1-, 2-, 4-, 8-Gbps native Fibre Channel ports using SFP+ and SFP transceivers.
- Ethernet module that provides 16 1- or 10-Gigabit Ethernet and FCoE expansion module using SFP+ transceivers.

Expansion Modules

Beginning with Cisco NX-OS Release 5.0(3)N1(1b), one new unified port expansion module and two new Layer 3 routing modules are available:

- Unified Port Module, page 8
- Layer 3 Routing Modules, page 8

Unified Port Module

The new unified port module (N55-M16UP) has the following features:

- Supports the Cisco Nexus 5548P, Nexus 5548UP, and Nexus 5596UP switches.
- 16 1-, 2-, 4-, 8-Gigabit native Fibre Channel ports.
- 1- or 10-Gigabit Ethernet ports with FCoE FEX connectivity.
- SFP+ and SFP transceiver support.
- Flexibility to configure any port in Ethernet, Fibre Channel, or FCoE mode.
- No additional licensing is required; an installed and active FCoE license is used.
- Unified ports are colored orange to easily identify them.

Layer 3 Routing Modules

Two new Layer 3 routing modules are introduced in this release:

- Cisco Nexus 5548P and Nexus 5548UP switch daughter card (N55-D160L3).
- Cisco Nexus 5596UP expansion module (N55-M160L3).

The Cisco Nexus 5548P and Nexus 5548UP daughter card (N55-D160L3) has the following features:

- Provides Layer 3 routing capabilities on all 48 10-Gigabit Ethernet ports.
- Enables SVIs on all switch and FEX ports.
- Provides 160 Gbps Layer 3 processing.

Note The Cisco Nexus 5548P and Nexus 5548UP switch daughter card has two RJ45 ports. These ports are not enabled and cannot be used.

The Cisco Nexus 5596UP (N55-M160L3) expansion module has the following features:

- Provides Layer3 routing capabilities on all 96 ports.
- Enables SVIs on all switch and FEX ports.
- Provides 160-Gbps Layer 3 processing expandable to 480-Gbps processing. (This module functions as a 48-port module capable of up to 160 Gbps of Layer 3 forwarding capability (240 mpps) that can be shared by all the I/O ports on the switch.)

Note Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c) supports one active expansion module at a time.

1-Gigabit Transceiver Support

Beginning with Cisco NX-OS Release 5.0(3)N1(1b), the following 1-Gigabit optical transceivers are supported on all SFP+ ports on the Cisco Nexus 5500 platform, unified port expansion module, and Layer 2 routing modules:

- GLC-T, GLC-SX-MM, GLC-LH-SM
- SFP-GE-T, SFP-GE-S, SFP-GE-L

Reversed Airflow and DC Power Options

The Cisco Nexus 2200 Series Fabric Extenders offer a choice of standard airflow (port-side exhaust) and reversed airflow (port-side intake), as well as a choice for AC and DC power options.

Table 3 shows the part numbers and descriptions of the available Cisco Nexus 2000 Series FEX airflow and power options. You can order standard airflow with dual AC power supplies, reversed airflow with dual AC power supplies, or standard airflow with dual DC power supplies package. The default option is the standard airflow with dual AC power supply.

Note Power supplies embed a fan and need to match the installed fan settings (standard or reversed).

Table 3 Cisco Nexus 2000 Series FEX Reversed Airflow and Power Options

Part Number	Description
N2K-C2248-FAN-B(=)[1]	Cisco Nexus 2200 Series FEX Gigabit Ethernet Fan, Reversed Airflow (port-side intake)
N2K-C2232-FAN-B(=)	Cisco Nexus 2200 Series FEX 10-Gigabit Ethernet Fan, Reversed Airflow (port-side intake)

Table 3 Cisco Nexus 2000 Series FEX Reversed Airflow and Power Options

Part Number	Description
N2200-PAC-400W-B(=)[1]	Cisco Nexus 2200 Series FEX AC Power Supply, Reversed Airflow (port-side intake)
N2200-PDC-400W(=)	Cisco Nexus 2200 Series FEX 400W DC Power Supply, Standard Airflow (port-side exhaust)

1. Available spare.

NEBS Compliance for the Cisco Nexus 2248TP and Cisco Nexus 2232PP Fabric Extenders

The Cisco Nexus 2248TP and Cisco Nexus 2232PP Fabric Extenders (starting with hardware version 3) meet the NEBS level 3 standard standards. To determine the hardware version, use the **show inventory** command. For important information about NEBS Compliance and ETSI environmental requirements for the Cisco Nexus 2248TP and Cisco Nexus 2232PP Fabric Extenders, see the *Regulatory Compliance and Safety Information for the Cisco Nexus 5000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders*.

Fabric Extender Scaling

Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c) supports the following on Cisco Nexus 5500 Platform switches (Nexus 5548, Nexus 5548UP, and Nexus 5596UP switches):

- 24 Fabric Extenders in Layer 2 mode.
- 16 Fabric Extenders in Layer 3 mode.

Note On Cisco Nexus 5000 Series switches (Nexus 5020 and Nexus 5010 switches), the scalability remains unchanged: Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c) support 12 Fabric Extenders in Layer 2 mode.

For more information please refer to the *Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 5.0(3)1(1a)*.

New Software Features

Cisco NX-OS Release 5.0(3)N1(1b) includes the following new or changed software features:

- Layer 3 Routing Features, page 10
- Licensing, page 12
- Network Time Protocol (NTP), page 13
- Rate Limited SPAN, page 14

Layer 3 Routing Features

The following new Layer 3 routing features are available in this release:

- Layer 3 Unicast Routing, page 11
- Layer 3 Multicast Routing, page 11

Layer 3 Unicast Routing

Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c) supports IP version 4 (IPv4) and the following routing protocols:

- Static routing
- Routing Information Protocol Version 2 (RIPv2)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPF) Protocol Versions 2 (IPv4)
- Border Gateway Protocol (BGP)
- First-Hop Redundancy Protocols (FHRP) (HSRP/VRRP)
- Up to 8000 IPv4 host routing table entries (/32 entries)
- Up to 8000 IPv4 longest prefix match routing table entries

All protocols support Ethernet interfaces, virtual interfaces (VLAN interfaces), subinterfaces, and port channels.

For more information, see the *Cisco Nexus 5000 Series NX-OS Unicast Routing Configuration Guide, Release 5.0(3)N1(1)*.

Layer 3 Multicast Routing

The following multicast routing protocols are supported in this release:

- Protocol Independent Multicast Source Specific Multicast IPv4 (PIM-SM)
- Internet Group Management Protocol (IGMP) Versions 2 and 3 router role
- Multicast Source Discovery Protocol (MSDP)
- Up to 2000 IGMP Groups

The implementations of these protocols are fully compliant with the latest standards and include 4-byte autonomous system numbers (ASNs) and incremental Shortest Path First (SPF). All unicast protocols support Non-Stop Forwarding Graceful Restart (NSF-GR). All protocols support all interface types, including Ethernet interfaces, switched virtual interfaces (VLAN interfaces) and subinterfaces, port channels, tunnel interfaces, and loopback interfaces.

Note Sending multicast traffic over a vPC peer-link to each receiver VLAN that does not have orphan ports is not supported if the Cisco Nexus 5500 Platform switch has attached dual-homed FEX.

For more information, see the *Cisco Nexus 5000 Series NX-OS Multicast Routing Configuration Guide, Release 5.0(3)N1(1)*.

Layer 3 Interfaces

The following interfaces are supported in this release:

- Layer 3 routing interfaces and subinterfaces on Cisco Nexus 5500 Series ports and SVI routing for all other interfaces
- Routed 1- or 10-Gigabit Ethernet interfaces
- Port channel interfaces
- 16-way equal-cost multipathing (ECMP) interfaces

Segmentation

Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c) supports virtual route forwarding (VRF), VRF-lite (IP VPN), VRF-aware unicast, and VRF-aware multicast.

Quality of Service

Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c) supports the following QoS features:

- CoS trust
- Port-based CoS assignment
- Modular QoS CLI (MQC) compliance
- ACL-based QoS classification (Layers 2, 3, and 4)
- MQC CoS marking and DSCP marking
- Per-port virtual output queuing
- CoS-based egress queuing
- Egress strict-priority queuing
- Egress port-based scheduling: Weighted Round-Robin (WRR)

Redundancy

Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c) supports Hot-standby Routing Protocol (HSRP) and Virtual Routing Redundancy Protocol (VRRP).

Security

Unicast Reverse Path Forwarding (uRFP) checks with port-based ACLs (PACLs).

Licensing

The Cisco NX-OS licensing feature allows you to access premium features on the device after you install the appropriate license for that feature. Any feature not included in a license package is bundled with the Cisco NX-OS software and is provided to you at no extra charge.

You must purchase and install a license for each device.

Licensing Grace Period

You can enable most features without installing a license. The Cisco NX-OS software provides a grace period for most features during which time you can try out a feature before purchasing its license.

The Layer 3 features do not have a grace period and require an installed Layer 3 Base license to use the routing features.

Beginning with Cisco NX-OS Release 5.0(3)N1(1b), two new Layer 3 licenses are available:

- Layer 3 Base License, page 13
- Layer 3 LAN-Enterprise License, page 13

Layer 3 Base License

The Layer 3 base license (N55-BAS1K9) is included with the Cisco Nexus 5500 Platform switch. The license provides the following support:

Connected, Static, RIPv2, OSPF (256 Dynamically Learnt Routes), EIGRP-Stub, HSRP, VRRP, IGMPv2/3, PIMv2, RACLs, uRPF, VRF-Lite.

Layer 3 LAN-Enterprise License

The Layer 3 LAN Enterprise license (N55-LAN1K9) includes the following:

- All base license features
- Full EIGRP
- Unrestricted OSPF routes
- BGP

Note The base license package bundled with the Cisco NX-OS system images allows you to use the default VRF and the management VRF for the mgmt0 port. The two default VRFs are automatically created. The VRF-lite feature allows you to create additional VRFs. The additional VRFs require the Layer 3 LAN-Enterprise license.

For detailed information about the features that require licensing and Cisco NX-OS license installation, see the *Cisco NX-OS Licensing Guide*.

For information about troubleshooting licensing issues, see the Cisco Nexus 5000 Series NX-OS Troubleshooting Guide.

Network Time Protocol (NTP)

Network Time Protocol (NTP) configuration is currently not provided in the Cisco Nexus 5000 Series NX-OS System Management Configuration Guide.

For more information on NTP commands, see the *Cisco Nexus 5000 Series NX-OS System Management Command Reference*.

Rate Limited SPAN

The Rate Limited SPAN feature allows you to rate-limit the SPAN traffic to 1Gbps across the entire monitor session to avoid impacting the monitored production traffic. Use the **switchport monitor rate-limit 1G** command to set the rate limit. This feature is not necessary and not supported on the Nexus 5500 Platform.

For more information about these features, see the Cisco Nexus 5000 Series and the Cisco Nexus 2000 Series documentation listed in the"Related Documentation" section on page 31.

Changed Software Features

The following software features have changed in this release:

- Beginning with Cisco NX-OS Release 5.0(3)N1(1b), HTTP Server is not supported.
- Device Manager is no longer packaged with Cisco Nexus 5000 NX-OS releases. You can download Fabric Manager/DCNM-SAN software (which contains Device Manager) directly from Cisco.com. For additional information, see the Release Notes for Cisco Fabric Manager.

Unified Port Configurations on Cisco Nexus 5500 Platform Switches

Unified ports allow you to configure ports as Ethernet, native Fibre Channel or FCoE ports. By default, the ports are Ethernet ports but you can change the port mode to Fibre Channel on the following unified ports:

- Any port on the Cisco Nexus 5548UP switch or the Cisco Nexus 5596UP switch.
- The ports on the Cisco N55-M16UP expansion module that is installed in a Cisco Nexus 5548P switch.

This example shows how to configure a unified port on a Cisco Nexus 5548UP switch or Cisco Nexus 5596UP switch:

```
switch# config t
switch(config)# slot 1
switch(config-slot)# port 32 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
```

This example shows how to configure a unified port on a Cisco N55-M16UP expansion module:

```
switch# config t
switch(config)# slot 2
switch(config-slot)# port 32 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
```

Port Order

You must configure Ethernet ports and FC ports in a specified order:

- FC ports must be configured from the last port of the module.
- Ethernet ports must be configured from the first port of the module.

If the order is not followed, the following errors are displayed:

```
ERROR: Ethernet range starts from first port of the module
ERROR: FC range should end on last port of the module
```

On a Cisco Nexus 5548UP switch, the 32 ports of the main slot (slot1) are unified ports. The Ethernet ports start from port 1/1 to port 1/32. The FC ports start from port 1/32 backwards to port 1/1.

This example shows how to configure 20 ports as Ethernet ports and 12 as FC ports:

```
switch# config t
switch(config)# slot 1
switch(config-slot)# port 21-32 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
```

Upgrading or Downgrading to a New Release

This section describes the upgrade and downgrade paths that are supported for Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c) on the Cisco Nexus 5000 Series switch.

This section includes the following topics:

Upgrade and Downgrade Guidelines

The following guidelines apply to Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c) for the Cisco Nexus 5000 Series switches:

- Do not change any configuration settings or network settings during the upgrade. Any changes in the network settings may cause a disruptive upgrade.
- Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c) are ISSU-compatible with NX-OS Release 4.2(1)N1(1) and later releases.
- Downgrading from NX-OS Release 5.0(2) to NX-OS Release 4.2(1) is disruptive.
- Upgrading from NX-OS Release 4.2(1) to NX-OS Release 5.0(2) is a nondisruptive upgrade (ISSU).
- Upgrading from a Cisco NX-OS Release 4.2(1)-based release to NX-OS Release 5.0(2)N1(1) is nondisruptive.
- Downgrading from Cisco NX-OS Release 5.0(2)N1(1) to a previous release is disruptive.
- When a Layer 3 license is installed, the Cisco Nexus 5500 Platform does not support an ISSU. Hot swapping a Layer 3 module is not supported.

Supported Upgrade and Downgrade Paths

Table 4 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c):

Table 4 Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c) Supported Upgrades and Downgrades

Current Cisco NX-OS Release	Upgrade to Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c)	Downgrade from Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c)
5.0(2)N2(1)	Nondisruptive upgrade (ISSU)	Disruptive downgrade
5.0(2)N1(1)	Nondisruptive upgrade (ISSU)	Disruptive downgrade
4.2(1)N2(1a) 4.2(1)N2(1) 4.2(1)N1(1)	Nondisruptive upgrade (ISSU)	Disruptive downgrade

Upgrading the Power Sequencer on the Cisco Nexus 5010 and Cisco Nexus 5020 Switches

Under certain conditions, a voltage spike that exceeds the system voltage guard band and glitch filter settings may result in a power cycle of the system mezzanine board which results in the failure of ports on the mezzanine board. To solve the issue, you need to upgrade to Cisco NX-OS Release 5.0(2)N1(1) and make sure that the power sequencer has been upgraded to v1.2 using the **show version** command. Follow the power sequencer upgrade procedure to upgrade the power sequencer to v1.2 and to work around CSCsy21017 and CSCth33969.

If you upgrade the switch to Cisco NX-OS Release 5.0(2)N1(1), but do not power cycle the switch following this procedure, even though the switch has instructions for the power sequencer upgrade, the power sequencer is not upgraded. The **show version** command output displays a v1.2 power sequencer, but that only indicates that the power sequencer upgrade instructions have been programmed. If you cannot confirm a power cycle, We recommend that you perform a power off/on to ensure the power sequencer is upgraded.

To upgrade the power sequencer with Cisco NX-OS Release 5.0(2)N1(1), follow these steps:

Note A power sequencer upgrade is not necessary if you already upgraded to an earlier version that includes the Power Sequencer v1.2, for example Cisco NX-OS Release 4.2(1).

Step 1 Download the Cisco NX-OS Release 5.0(2)N1(1) kickstart and system image to the system.

Step 2 Enter the **install all kickstart** *kickstart_url* **system** *system_url* command to start and upgrade to the Cisco NX-OS Release 5.0(2)N1(1). When prompted to confirm the upgrade, review the upgrade table and choose **y** to proceed.

After completing the installation, the system reloads and displays a Cisco NX-OS Release 5.0(2)N1(1) image.

Step 3 Repeat Step 2 to reinstall the Cisco NX-OS Release 5.0(2)N1(1) image. During this process, the upgrade table should display the upgrade action for the power sequencer and then upgrade the power sequencer.

Step 4 After the installation is complete, power cycle the switch. The power sequencer is not updated until a power cycle is completed.

Step 5 After the system comes up, confirm that the power sequencer has been upgraded by entering the **show version** command.The **show version** command only confirms if the power sequencer has the updated instructions. The upgrade does not take effect until the switch is power cycled.

Limitations

This section describes the limitations for Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c).

- When upgrading from Cisco NX-OS Release 4.2(1)N1(1) and earlier releases, to any release, the policy description is lost. This problem does not occur when upgrading from Cisco NX-OS Release 4.2(1)N1(1) and later releases. After an upgrade, We recommend that you reconfigure the policy description. For details, see CSCth14225.
- Starting with Cisco NX-OS Release 4.2(1)N2(1), LACP fast timers are supported. If you downgrade to an earlier release that does not support this feature, entering the **install all** command displays the following warning:

```
"Configuration not supported - Lacp fast rate is enabled",
  "Use \"lacp rate normal\" on those interfaces"
```

  Before downgrading to an earlier release, change the LACP rate to normal. If you ignore the warning and force the installation, then it is possible that the leftover LACP rate fast configuration would still be active with previous releases of software but the behavior would be unpredictable and link flap might occur. We recommend that you change the LACP rate setting to normal. For details, see CSCth93787.
- When an FC SPAN destination port is changed from SD to F mode and back to SD mode on a NPV switch, the port goes into an error-disabled state. Perform a shut/no-shut after the mode change recovers the port. This issue occurs only in NPV mode. For details, see CSCtf87701.
- If you configure a Cisco Nexus 2248TP port to 100 Mbps instead of autonegotiation, autonegotiation does not occur, which is expected behavior. Both sides of the link should be configured to both hardwired speed or both autonegotiate.

  no speed—Autonegotiates and advertises all speeds (only full duplex)

  speed 1000—Autonegotiates only for a 802.3x pause

  speed 100—Does not autonegotiate; pause cannot be advertised. The peer must be set to not autonegotiate and fix at 100 Mbps (similar to the N2248TP)

  For details, see CSCte81998.
- Given the implementation of a single CPU ISSU, the STP root on the PVST region with switches on an MST region is not supported. The PVST simulation on the boundary ports go into a PVST SIM inconsistent blocked state that breaks the STP active path. To work around this issue, move all STP roots on the MST region. However, the work around causes a nondisruptive ISSU to fail because Non-Edge Designated Forwarding Ports are required for an ISSU. For additional information, see CSCtf51577. For information topologies that a nondisruptive upgrade is supported, see to the *Cisco Nexus 5000 Series NX-OS Upgrade and Downgrade Guide*.
- IGMP queries sent in CSCtf94558 are group-specific queries that are sent with the destination IP/MAC address as the group's address.

GS queries are sent for IP address: 224.1.14.1 to 224.1.14.100 [0100.5E01.0E01 to 0100.5E01.0E64]

These are not link-local addresses. By default, they are not flooded by the hardware into the VLAN. They are sent only to the ports that have joined this group.

This is expected behavior during an ISSU.

In another scenario, the IGMP global queries [dest IP 224.0.0.1] get flooded correctly in the VLAN.

Group-specific queries are not forwarded to ports other than the one that joined the group during ISSU. The reason to forward group-specific queries toward hosts is to avoid having them leave the group. However, if a group has not joined the group, then this is not an issue. If there is an interface that has joined the group, then the queries are expected to make it to the host. While the behavior is different when ISSU is not occurring, it is sufficient and works as expected and there is no impact to traffic. For details, see CSCtf94558.

- The meaning of an MTU configuration has changed in Cisco NX-OS Release 4.2(1)N1(1) and earlier releases. In releases earlier than Cisco NX-OS Release 4.2(1)N1(1), the configured MTU included the Ethernet payload and Ethernet headers. In Cisco NX-OS Release 4.2(1)N1(1), the configured MTU includes only the Ethernet payload and not the Ethernet headers. When upgrading or downgrading between Cisco NX-OS Release 4.2(1)N1(1) and earlier releases, Cisco NX-OS automatically converts the configuration to address this semantic change by adding or subtracting 38 to the MTU to address the Ethernet header size.

  In a vPC configuration, the MTU per class needs to be consistent on both switches in the vPC domain for the vPC peer link to come up. When upgrading/downgrading a working vPC setup between pre-4.2(1)N1(1) and 4.2(1)N1(1) releases, the MTU is adjusted to make sure that the MCT peer-link always comes up.

  However if you add a peer-link between two switches in a vPC domain that are identically configured (MTU in particular) with one switch running Cisco NX-OS Release 4.2(1)N1(1) and another switch running an earlier release, then the vPC peer link does not come up because the MTU is inconsistent between the two switches.

  This is not an issue when upgrading or downgrading peer switches in a vPC domain; this is only an issue when adding a peer link between two switches running Cisco NX-OS Release 4.2(1)N1(1) and earlier releases that were not previously in the same vPC domain.

  To resolve this issue, upgrade or downgrade one switch to match the version on the other switch and reconfigure the MTU to be consistent on both sides. For details, see CSCtg27538.

- The channel-group configuration is not applied to the Cisco Nexus 2000 Series downlink interface after downgrading to the Cisco NX-OS Release 4.1(3)N1(1) software. This issue occurs if the **speed 1000** command is present under the context of the port channel. To work around this issue, reconfigure the **channel-group** command after the system comes up and reapply the configuration from the saved configuration in the bootflash. For details, see CSCtc06276.
- When a private VLAN port is configured as a TX (egress) SPAN source, the traffic seen at the SPAN destination port is marked with the VLAN of the ingressed frame. There is no work around.
- In large-scale configurations, some Cisco Nexus 2000 Series Fabric Extenders may take up to 3 minutes to appear online after entering the **reload** command. A configuration can be termed large scale when the maximum permissible Cisco Nexus 2000 Series Fabric Extenders are connected to a Cisco Nexus 5000 Series switch, and all host-facing ports are connected and each host-facing interface has a large configuration (that supports the maximum permissible ACEs per interface).

- The Cisco Nexus 2000 Fabric Extender does not support PVLANs over VLAN trunks used to connect to another switch. The PVLAN trunks are used only on inter-switch links but the FEX ports are only meant to connect to servers. Because it is not a valid configuration to have an isolated secondary VLAN as part of a Fabric Extender port configured as a VLAN trunk, all frames on isolated secondary VLANs are pruned from going out to a FEX.
- Egress scheduling is not supported across the drop/no-drop class. Each Fabric Extender host port does not support simultaneous drop and no drop traffic. Each Fabric Extender host port can support drop or no drop traffic.
- The Cisco Nexus 2148 Fabric Extender does not support frames with the dot1p vlan 0 tag.
- VACLs of more than one type on a single VLAN are unsupported. Cisco NX-OS software supports only a single type of VACL (either MAC, IPv4, or IPv6) applied on a VLAN. When a VACL is applied to a VLAN, it replaces the existing VACL if the new VACL is a different type. For instance, if a MAC VACL is configured on a VLAN and then an IPv6 VACL is configured on the same VLAN, the IPv6 VACL is applied and the MAC VACL is removed.
- A MAC ACL is applied only on non-IP packets. Even if there is a **match eth type = ipv4** statement in the MAC ACL, it does not match an IP packet. To avoid this situation, use IP ACLs to apply access control to the IP traffic instead of using a MAC ACL that matches the EtherType to IPv4 or IPv6.
- Multiple **boot kickstart** statements in the configuration are not supported.
- If you remove an expansion module with Fibre Channel ports, and the cable is still attached, the following FCP_ERRFCP_PORT errors are displayed:

```
2008 May 14 15:55:43 switch %KERN-3-SYSTEM_MSG: FCP_ERRFCP_PORT:
gat_fcp_isr_ip_fcmac_sync_intr@424, jiffies = 0x7add9a:Unknown intr src_id 42 - kernel
2008 May 14 15:55:43 switch %KERN-3-SYSTEM_MSG: FCP_ERRFCP_PORT:
gat_fcp_isr_ip_fcmac_sync_intr@424, jiffies = 0x7add9a:Unknown intr src_id 41 - kernel
```

  These messages are informational only, and result in no loss of functionality.

Configuration Synchronization Limitation

When you remove a switch profile using the **no switch-profile** *name* **[all-config | local-config]** command, the configuration in the switch profile is immediately removed from the running configuration. This disrupts the configurations that were present in the switch profile. For example, port channel and vPC configurations are disrupted. For current information about this issue, refer to CSCtl87240 and CSCtl87260.

Limitations on the Cisco Nexus 5010 and Cisco Nexus 5020

The limitations on the Cisco Nexus 5010 switch and the Cisco Nexus 5020 switch are as follows:

- If the SPAN source interface sends more than 6Gbps traffic or if traffic bursts too much, a Nexus 5020 switch or Nexus 5010 switch drops traffic on the source interface. You can use the switchport monitor rate-limit 1G command on the SPAN destination to reduce the dropping of actual traffic on the source interface; however, SPAN traffic is restricted to 1Gb.
- Traffic going out the Ethernet SPAN destination is always tagged. The SPAN destination can be in the access or trunk mode and frames on the SPAN source port can be tagged or untagged. Frames are always tagged internally as they travel through the system. Information about whether the frame was originally tagged or untagged, as it appeared in the SPAN source, is not preserved in the SPAN destination. The spanned traffic exiting the SPAN destination port always has the VLAN tag on it.

The correct VLAN tag is applied on the frame as it goes out the SPAN destination. The only exception is if frames ingress on a SPAN source port on an invalid VLAN. In this case, **vlan 0** is applied on a spanned frame.

- Spanned FCoE frames do not preserve original SMAC and DMAC fields. The Ethernet header gets modified as the frame is spanned to the destination. The modified header fields are displayed when monitored on the SPAN destination.
- The CoS value in spanned FCoE frames on the Ethernet SPAN destination port does not match with the CoS value in the SPAN FCoE source frame. The CoS value on the captured SPAN FCoE frame should be ignored.
- The class-fcoe cannot be removed even if Fibre Channel is not enabled on a switch.
- If a port drains traffic at a rate less than 100 Kbps, it is errdisabled in 10 seconds to avoid buffer exhaustion. However, if the drain rate is larger than 100 Kbps, the port may not be consistently errdisabled within 10 seconds which exhaust ingress buffers and discard frames. Use the **shut** command to disable the slow-draining port.
- The multicast storm control functionality in the Cisco Nexus 5000 Series does not distinguish between IP, non-IP, registered, or unregistered multicast traffic. All multicast traffic is subject to a single-multicast storm control policer when configured.

IGMP Snooping Limitation

On the Cisco Nexus 5010 switch and the Cisco Nexus 5020 switch with a Cisco Nexus 2000 Series Fabric Extender (FEX) installed, unregistered IP multicast packets on one VLAN are forwarded to other VLANs where IGMP snooping is disabled. We recommend that you do not disable IGMP snooping on the Cisco Nexus 5010 switch and the Cisco Nexus 5020 switch. A static IGMP join can be configured for devices intended to receive IP multicast traffic but not to send IGMP join requests. This limitation applies to the Cisco Nexus 5010 switch and the Cisco Nexus 5020 switch only.

SPAN Limitations on Fabric Extender Ports

The SPAN limitations on Fabric Extender ports are as follows:

- On a Cisco Nexus 5000 Series switch, if the SPAN source is a FEX port then the frames will always be tagged when leaving the SPAN destination.
- On a Cisco Nexus 5010 switch or a Nexus 5020 switch, if the SPAN source is an access port on a switch port or FEX port, the spanned frames at the SPAN destination will be tagged.
- On a Cisco Nexus 5010 switch or a Nexus 5020 switch, if the span source is an access port on a switch port or FEX port, the spanned frames at the SPAN destination will be tagged.
- On a Cisco Nexus 5500 Platform switch, if the SPAN source is on an access port on the switch port, then the frames will not be tagged when leaving the SPAN destination.
- Ports on a FEX can be configured as a tx-source in one session only.

  If two ports on the same FEX are enabled to be tx-source, the ports need to be in the same session. If you configure a FEX port as a tx-source and another port belonging to the same FEX is already configured as a tx-source on a different SPAN session, then a error is displayed on the CLI.

  In the following example, Interface Ethernet100/1/1 on a FEX 100 is already configured as a tx-source on SPAN session-1:

```
swor28(config-monitor)# show running-config monitor
```

```
version 4.0(1a)N2(1)
monitor session 1
    source interface Ethernet100/1/1 tx
    destination interface Ethernet1/37
    no shut
```

If you add an interface Ethernet100/1/2 as a tx-source to a different SPAN session (session-2) the the following error is displayed:

```
swor28(config)# monitor session 2
swor28(config-monitor)# source interface ethernet 100/1/2 tx
ERROR: Eth100/1/2: Ports on a fex can be tx source in one session only
swor28(config-monitor)#
```

- When a FEX port is configured as a tx-source, the multicast traffic on all VLANs for which the tx-source port is a member, is spanned. The FEX port sends out only multicast packets that are not filtered by IGMP snooping. For example, if FEX ports 100/1/1-12 are configured on VLAN 11 and the switch port 1/5 sends multicast traffic on VLAN 11 in a multicast group, and hosts connected to FEX ports 100/1/3-12 are interested in receiving that multicast traffic (through IGMP), then that multicast traffic goes out on FEX ports 100/1/3-12, but not on 100/1/1-2.

  If you configure SPAN Tx on port 100/1/1, although the multicast traffic does not egress out of port 100/1/1, the SPAN destination does receive that multicast traffic, which is due to a design limitation.
- When a FEX port is configured as both SPAN rx-source and tx-source, the broadcast, non-IGMP Layer-2 multicast, and unknown unicast frames originating from that port may be seen twice on the SPAN destination, once on the ingress and once on the egress path. On the egress path, the frames are filtered by the FEX to prevent them from going out on the same port on which they were received. For example, if FEX port 100/1/1 is configured on VLAN 11 and is also configured as SPAN rx-source and tx-source and a broadcast frame is received on that port, the SPAN destination recognizes two copies of the frame, even though the frame is not sent back on port 100/1/1.
- A FEX port cannot be configured as a SPAN destination. Only a switch port can be configured and used as a SPAN destination.

Checkpoint and Configuration Rollback Limitation

When FCoE is enabled, the checkpoint and configuration rollback functionality is disabled.

Layer 3 Limitations

Asymmetric Configuration

In a vPC topology, two Cisco Nexus 5000 switches configured as vPC peer switches need to be configured symmetrically for Layer 3 configurations such as SVIs, Peer Gateway, routing protocol and policies, and RACLs.

Note vPC consistency check does not include Layer 3 parameters.

SVI

When a Layer 3 module goes offline, all SVIs are shutdown.

Upgrading and Downgrading

When a Layer 3 license is installed, the Cisco Nexus 5500 Platform does not support an ISSU. Layer 3 module hot swaps are not supported.

Cisco Nexus 5548P Daughter Card (N55-D160L3)

Before installing a Layer 3 daughter card (N55-D160L3) into a Cisco Nexus 5548P switch, you must upgrade to Cisco NX-OS Release 5.0(3)N1(1b) or NX-OS Release 5.0(3)N1(1c) and then install the card into the chassis.

Caveats

Beginning in Cisco NX-OS Release 5.0(3)N1(1b), the open and resolved caveat record numbers are provided with links to the But Toolkit where you can find details about each caveat.

This section includes the following topics:

Open Caveats

Table 6 lists descriptions of open caveats in Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c). The record ID links to the Cisco Bug Toolkit where you can find details about the caveat.

The caveats are listed in the following categories:

Table 5 Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c) Open Caveats

Record Number	Open Caveat Headline
New Open Caveats	
CSCtj30588	A port was removed from a port channel even when the wrong channel ID is specified.
CSCtj31760	On a Nexus 5596UP switch, the port LED does not blink with the beacon configured after a reboot.
CSCtj94130	The Layer 3 traffic over an MCT link has dropped.
CSCtk31209	When downgrading the image from Release 5.0(2)N2(1) to Release 5.0(2)N1(1), the secondary PVLANs became nonoperational.
CSCtk84182	The **show incompatibilities** command does not display an incompatible configuration.
CSCtl09648	The interface from the static IGMP group cannot be removed if it is part of a range.
CSCtl45495	After the license has been reinstalled, the Layer 3 DC remains offline until the switch is rebooted.
CSCtl46093	OSPF does not come up with a Layer 3 interface MTU of 9000 because the supervisor MTU is 2000.
CSCtl51447	All Layer 3 features remain enabled after you remove the Layer 3 license.
CSCtl51493	Information about IPv6 is not in the HSRP summary.
CSCtl51832	MAC addresses do not age out after you configure IPSG.
CSCtl53720	The service does not respond when you delete the Layer 3 port channel and SVI interfaces.
CSCtl56923	The speed 1000 command cannot be deleted from the WS HIF port.
CSCtl66943	DHCP validation errors have occurred in the PVLAN setup.
CSCtl87598	The QoS Type-2 inconsistency is not displayed in the show vpc command.
CSCtl87649	A commit failed when copying a configuration to the running configuration twice as per the recommended procedure.
CSCtl88086	On a host interface port in a straight-through topology, the channel-grp command displays an error due to "Slot in vpc A-A mode"
CSCtl94228	No IP load-sharing not reset to default mode
CSCtl94853	Syntax err for mrouter as PO i/f after loading saved cfg to running cfg
CSCtl95221	On the Cisco Nexus 5010 switch, an error message is displayed after you issue the **wrr cos queue** command.
CSCtl95401	The FIB does not synchronize with the RIB after the FIB hit the hardware limit and the entries aged out.
CSCtl99388	A syntax error occurred after parsing the router-id and applying the saved configuration.
CSCtl99537	When downgrading the image from Release 5.0(3)N1(1b) to Release 4.2(1)N2(1), the RMON traps became disabled.
CSCtn19019	Sometimes, the configuration does not synchronize when the switch is rebooted.
CSCtn19504	The HIF port is stuck in the vpc-peer-link-down state during a switchover test.

Table 5 Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c) Open Caveats

Record Number	Open Caveat Headline
CSCtn27125	Traffic leaking on SVI ACL during switch bootup
CSCtn31018	On a host interface port in a straight-through topology, the **channel-grp** command displays an error message indicating “Slot in vpc A-A mode".
CSCtn40301	The syslog is consistently using more than 95% CPU after a switch upgrade.
CSCtn40667	A FEX does not recover after a failed hitless upgrade during an ISSU.
CSCtn47093	The 32 entries that point to ECMP are not supported.
CSCtn50937	The (s,g) mroutes do not expire if the source stopped and (*,g) is still joined.
CSCtn51223	Clis hap reset on powering on module 2 on O2-48
CSCtn52446	A problem occurs when adding routes in VRF.
CSCtn57847	An NPV switch has dropped FCoE after an ISSU and an OIR GEM.
CSCtn58324	Packets are not forwarded when an IPSG-enabled access port is made into a trunk.
CSCtn64093	The **no ip igmp snooping mrouter vpc-peer-link** command is not supported with FEX in a dual-homed topology.
CSCtn70380	Switch vPC member ports on the secondary switch go into a suspended-by-vpc state when configuring or removing configurations using config-sync mode.
CSCtn76099	A gratuitous ARP broadcast storm occurs when multiple vPCs are configured between Cisco Nexus 7000 Series devices and Cisco Nexus 5000 Series switches.
CSCtn76613	Upgrading from Cisco NX-OS Release 4.1(3) to NX-OS Release 5.0(3) is not successful.
CSCtn82286	After an upgrade from NX-OS Release 5.0(2)N1(1) to NX-OS Release 5.0(3)N1(1b), the port channel type shows as Edge.
CSCtn87115	A Nexus 5000 Series switch running NX-OS Release 5.0(3)N1(1b) with an N5K-M1060 FC expansion module installed and FCOE is enabled, might fail when issuing the **show queuing interface** or **show queuing interface fcx/y** commands.
CSCto23248	DHCP relay drops DHCP reply frames.
CSCto50140	A vPC crash occurs when configuring a value of 9216 in a range of interfaces. This is followed by a reboot on both Nexus 5000 Series peer switches.
CSCto63412	In a Cisco Nexus 5548 switch with a Layer 3 module running Cisco NX-OS Release 5.0(3)N1(1b), due to address aliasing, groups in the range of [225-239].0.0.x cannot be used.
Platform, Infrastructure	
CSCso01268	VDC-related syslog message appears when a module is hot-swapped.
CSCsv95478	On a FEX, the **fex pinn redist** command does not wait for a user prompt with a y/n.
CSCti11823	When upgrading from NX-OS Release 4.2(1)N1(1) to NX-OS Release 4.2(1)N2(1), the 1-Gb HIF LED blinks amber after an ISSU.
CSCti14663	On the Cisco Nexus 5548, the diagnostics and **show environment temperature** command are not synchronized.
CSCtj22747	On a failing type_check, GEMs do not recover from that state
CSCtq13290	VPC PO goes to FWD after ISSU with MST multiple regions configured

Table 5 Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c) Open Caveats

Record Number	Open Caveat Headline
Configuration Synchronization	
CSCti19892	Pressing Ctrl + Z does not interrupt a switch-profile deletion.
CSCti40833	Long failure detection times occur for the verify and commit (commands or actions?) in certain cases.
CSCti45602	The order of a committed configuration on one peer might fail during a merge.
CSCti63620	An import has failed verification for channel-group member interfaces.
CSCti68764	Some spanning-tree commands are not supported in the switch profile.
CSCtj10460	A failure has occurred while deleting a switch profile.
CSCtj26673	A configuration synchronization import has failed for an implicitly generated QoS configuration.
CSCtl87240	A switch profile has been removed to display a warning message prior to execution.
CSCtl87260	A switch profile has been removed so as not to impact the running configuration.
Layer 2 Switching	
CSCso25966	The Catalyst 6500 Series LACP ports go to the err disable state when a peer Cisco Nexus 5000 Series switch PC has a configuration mismatch.
CSCso27446	The management port does not bring down/up a link when you enter the **shut**/**no shut** commands.
CSCso84269	An unsaved configuration warning appears even when there was no configuration change after a reload.
CSCsq35527	When doing IGMP snooping, the ip-mcast might take longer to converge on an STP top change.
CSCsr36661	Static IGMP groups with PVLAN host ports are not restored after a reload.
CSCsv56881	Inconsistent behavior occurs when duplicate IPv4/IPv6 addresses are configured.
CSCsv81694	A flap occurs when the dynamically learned port removes the auto-learn static mac entry.
CSCsv93922	If the modulos operator “(%)” is used in a FEX description, the show command will not display information correctly.
CSCsx35870	If the modulos operator “(%)” is used in a FEX description, the show command will not display information correctly.
CSCta77490	When you quickly toggle the primary VLAN type, a failure of the type change occurs.
CSCtb58641	Entering the **clear mac-address** command did not delete a MAC address.
CSCtc04213	The VLAN configuration doesn’t get applied on a range of interfaces.
CSCtc36397	A vPC role switchover does not occur when the vPC role is a primary operational role.
CSCtc44231	When a VLAN is deleted from the switch, the LACP port channels that have that VLAN set as a native VLAN fail to come-up.
CSCtd31131	This caveat was superseded by CSCtb70565.

Table 5 Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c) Open Caveats

Record Number	Open Caveat Headline
CSCtf79253	Multiple alternate ports results in a root port failover and transient loops in a vPC topology.
CSCtg33706	Debug LACP is not available on FEX ports.
CSCth69160	An SVI over a secondary PVLAN is not working.
CSCti19511	An IGMP mrouter port is not removed immediately if you shut an individual port on a peer switch.
CSCti22121	When configuring LACP fast rate, unidirectional CFS peering occurred after an MCT flap.
CSCti86007	When a peer-link comes up and vPC ports are in the process of coming up, if a peer switch reboots, there is a small window where vPC ports don't come up due to the peer-link down status.
CSCtj27113	When configuring the LACP fast rate, an MCT member port went to the UDLD empty echo state.
CSCtj29477	Switch VPC ports go to UDLD Empty Echo on MCT Flap.
CSCtj44387	An snmpwalk on BRIDGE-MIB during a vpc peer-link shutdown causes high CPU utilization.
CSCtj85867	Entering the **show run** command is not displaying the switchport trunk VLAN list when a port profile is inherited.
CSCtk08499	The vlan_mgr consumes the CPU for several minutes when walking the VTP MIB.
SAN Switching	
CSCso46345	The i10K interop 4 mode is not supported.
CSCsq35728	When creating a SAN port channel, a MAP_PARAM_FROM_CHANNEL syslog message is displayed.
CSCsr28868	When you disable FCoE, the untagged Ethernet packet type 0000 shows CRC errors.
CSCsv19979	The speed should be configured manually for Fibre Channel ports in SD mode.
CSCsx80279	Addresses are not learned when egress interfaces are only FEX-facing ports.
CSCsy02439	An FC port error message displays occasionally.
CSCsy99816	The wrong FEX serial number does not show as an Identity-Mismatch in the output of the **show interface fex** command.
CSCtb61197	There are inconsistent SAN-port member states in the output of the **show interface** and **show san-port** commands.
CSCth98138	The command output for the **show fc-port-security** command for some virtual Fibre Channel interfaces is wrong.
CSCti51365	During an ISSU, if SAN port channels are down, the down status is not displayed correctly.
CSCti99872	A virtual Fibre Channel goes into the errdisabled state when you remove and recreate a VSAN after an ISSU.
CSCtj19861	Shutting down nontrunking SAN port channel members takes more than 30 seconds.

Table 5 Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c) Open Caveats

Record Number	Open Caveat Headline
FCoE	
CSCtc77180	When you enable FCoE, ports are error-disabled.
CSCti87913	When you upgrade from NX-OS Release 4.2(1)N to NX-OS Release 5.0(2)N1(1), FLOGI fails after an ISSU.
Installation/Upgrade/Downgrade	
CSCtd15304	A successful reset occurred during the upgrade of Release 4.1(3)N1(1) to Release 4.1(3)N2(1) using Fabric Manager.
CSCtd70554	The fc-port-security configuration did not get converted when downgrading from NX-OS Release 4.1(3)N2(1) to NX-OS Release 4.1(3)N1(1).
CSCtf98638	During an ISSU, the following message appears: %SYSMGR-5-SUBPROC_KILLED "System Manager (core-client)"
Pre-Provisioning	
CSCti84186	The output of the **show run all** command shows an inconsistent configuration for the pre-provisioned interface.
Security	
CSCsl21529	The command-line interface has been enhanced to display the per-class maximum transmission unit (MTU).
CSCsq64251	A directed request does not work with TACACS+.
CSCsr20499	During a configuration restore to the running configuration from a configuration file using the **copy <file> running-config** command, the aclmgr may leak memory.
CSCsu77946	You cannot unconfigure statistics from an ACL in a configuration session.
CSCsv39939	Incorrect values are displayed for the interface capabilities for ports on a Cisco Nexus 2000 Series Fabric Extender connected to a Cisco Nexus 5000 Series switch.
CSCsz82199	When priority-flow-control is disabled between two Cisco Nexus 5000 Series switches, std.pause (interface flowcontrol) configuration does not take affect.
CSCtc62994	When combining RBAC roles (multiple roles assigned to the same user account), interface policies in those roles aren't working on a per-role basis.
CSCti15226	On Cisco Nexus 5500 platform switches, no error is identified when you configure an ACL-based qos policy for class-fcoe.
CSCti34155	The output for the **show run ipqos all** command does not show the default queuing class map.
CSCti61513	The **match ip rtp** command is not supported in the match-all class.
Configuration Rollback	
CSCti77835	A rollback fails to revert to the earlier VLAN configuration.
CSCti87532	A rollback fails when changes are made in the buffer-size for class-fcoe.

Table 5 Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c) Open Caveats

Record Number	Open Caveat Headline
CSCti97003	A rollback fails and the output of the **show rollback log exec** command displays "Deletion of switch profile failed".
CSCtj16996	A rollback fails when the switch profile configuration involves a conditional feature.
System Management	
CSCsm03765	You cannot assign an IP address on the mgmt0 interface using Device Manager.
CSCso74872	When two SNMP walks are started simultaneously, one of them may fail with the following error - 'OID not increasing'.
CSCsq57558	The software does not support an EISL encapsulation on an SD port (VFT cannot be preserved).
CSCsq76688	A CDP neighbor is not removed immediately after the port is shut down.
CSCsq90423	In NPV mode, EISL encapsulation for an SD port is not supported.
CSCsr68690	When egress SPAN is configured on a port that is transmitting jumbo or large frames, the spanned frames are truncated to 2384 bytes.
CSCsx40562	When using a FEX, the ACL drop traffic is not reaching the SPAN destination in certain configuration cases.
CSCsx59489	When the switch and FEX bootup after entering the **reload all** command, the time of event for any environment call home event, such as temperature alarm, power supply or fan alarms, is set to 1970.
CSCsz81365	Even after private-vlan mapping is removed on a trunk port using the **no switchport private-vlan mapping trunk** command, traffic received over the VLAN continues to be SPANed.
CSCtb53820	The monitor session goes to the error state with VSAN as a source after a reload.
CSCtb84512	In a mixed SPAN mode where Ethernet port channels, vFCs, and FC ports are span sources and an Ethernet interface is a SPAN destination, a vFC flap causes the traffic coming in on the Ethernet port channel not to be spanned.
CSCtb94310	Removing or adding a SAN port member causes a monitor session to go into an error state.
CSCtf32340	An error occurs while changing the VSAN and Interface scope of an existing role name.
CSCti10941	The destination port is wrong in the **show interface brief** command output.
CSCtj53287	Traffic received over Fibre Channel ports cannot be monitored on SPAN.
CFS	
CSCsl73766	RADIUS configuration distribution via CFS is unsupported.
CSCsm16222	Roles configuration distribution via CFS is unsupported.
CSCsr35452	CFS-based distribution of the NTP peer configuration does not work.
CSCtb34546	Peer switches gets stuck in CFS discovery when you enter the **deny all ip pkts mgmt0** command.

Table 5 Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c) Open Caveats

Record Number	Open Caveat Headline
Fabric Extender	
CSCsv15775	The priority-tagged frames on FEX ports get dropped.
CSCsv93263	FEX port configurations are lost when a configuration restore is done after a write erase and reload.
CSCsx68778	Flowcontrol configuration on the FEX ports may fail when the **range** command is used with interfaces that are spread across FEXs.
CSCta04383	The FEX should automatically revert to an older image if a second switch boots with the same version.
Transceiver	
CSCsv00989	Transceiver details are read as zeros even on DOM-capable 1G SFPs.
CSCsv02866	The **show interface ethernet transceiver details** command may show "invalid calibration" for DOM supported 1G SFPs.

Resolved Caveats—Cisco NX-OS Release 5.0(3)N1(1c)

Table 6 lists the caveats that are resolved in Cisco NX-OS Release 5.0(3)N1(1c). The caveats may be open in previous Cisco NX-OS releases.

Table 6 Cisco NX-OS 5.0(3)N1(1c) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtj54918	On a Cisco Nexus 2000 Fabric Extender, the VLANs on a private VLAN host-port error after a vPC peer-link flap.
CSCtn01449	When a Cisco Nexus 5548 switch is connected to a N7K-M132XP-12L module on a Nexus 7000 Series device using twinax cables (any version), the connected port goes into an error disabled state due to excessive link flaps.
CSCtn24930	Messages are not sent to the syslog server (there no file or director).
CSCtn62877	During a software upgrade on a Cisco Nexus 5000 Series or Nexus 5500 Platform switch, the switch might reload with an fwm process crash.
CSCtn76099	A gratuitous ARP broadcast storm occurs when multiple vPCs are configured between Cisco Nexus 7000 Series devices and Cisco Nexus 5000 Series switches.
CSCtn89709	The BPDU loop guard is triggered when a vPC peer link is shut down.
CSCto34674	A vPC port-channel towards the STP root can go to an STP blocking state.
CSCto47633	On a Cisco Nexus 5000Series switch running Cisco NX-OS Release 5.0(3)N1(1a), the CPU spikes in the PID wwn.
CSCto68011	On Cisco Nexus 5000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders running in FC switching mode, an SNMP get request causes the fcdomain service to fail.
CSCto69352	On a Cisco Nexus 5596UP switch, the show tech-support command causes a service failure and the switch reboots.

Table 6 Cisco NX-OS 5.0(3)N1(1c) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCto75330	Unsupported FEXs are listed in the FEX-type configuration.
CSCto81320	A Cisco Nexus 2232 Fabric Extender fan module (N2K-C2232-FAN) is misidentified as N2K-C2232-FAN-B.
CSCtq00855	After a nondisruptive ISSU, the FCoE manager process may fail.
CSCtq03687	A Cisco Nexus 5000 Series or Nexus 5500 Platform switch running NX-OS Release 5.0(3)N1(1), NX-OS Release 5.0(3)N1(1a), or NX-OS Release 5.0(3)N1(1b) might crash when you enter the **show queuing interface** command on a FEX fabric interface which is administratively down.
CSCtq04991	In a vPC topology, both vpc peer switches are sending BPDUs towards the root.

Resolved Caveats—Cisco NX-OS Release 5.0(3)N1(1b)

Table 6 lists the caveats that are resolved in Cisco NX-OS Release 5.0(3)N1(1b). The caveats may be open in previous Cisco NX-OS releases.

Table 7 Cisco NX-OS 5.0(3)N1(1b) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCti22294	On a Nexus 5500 Platform switch, the GEM: multicast data is not received correctly after a reload or OIR.
CSCti82599	On a Nexus 5000 series switch, sometimes SPAN stops working after a flap of SPAN destination.
CSCti86620	On a Nexus 5500 Platform switch, port LEDs do not blink when a beacon is configured after a reboot.
CSCti92741	On a Nexus 5000 switch, the **show port-resources module** *x* command switch output may show some incorrect information for "Total bandwidth" and "Total shared bandwidth.
CSCtj05044	On a Nexus 5000 Series switch, IGMP groups are not relearned after a VLAN deletion or addition on a VLAN which is a SPAN source.
CSCtj13786	During a nondisruptive ISSU, multicast traffic is dropped for IGMP v3 groups.
CSCtj23007	The port profile database is not cleared after a GEM is removed or hot swapped.
CSCtj26863	On a Nexus 5000 Series switch, a newly created port channel counter shows large values.
CSCtj42415	When a FEX port that is member of more than 2000 VLANs is configured as a TX span source, an error occurs and a syslog message is displayed.
CSCtj90485	Approved transceiver cables show as non-supported cables and an error message is displayed.
CSCtk33187	A Nexus 5500 Platform switch may crash when an expansion module is removed from the switch and the expansion module has fabric ports that are used for control traffic.
CSCtn79039	Installation error is due to pc.log file size.

Table 7 Cisco NX-OS 5.0(3)N1(1b) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtn87115	A Nexus 5000 Series switch running NX-OS Release 5.0(3)N1(1b) with an N5K-M1060 FC expansion module installed and FCOE is enabled, might fail when issuing the **show queuing interface** or **show queuing interface fcx/y** commands.
CSCto43675	A Cisco Nexus 5548UP switch running Cisco NX-OS Release 5.0(3)N1(1a) or an earlier version may shutdown because of a temperature exceeding the major threshold.

Related Documentation

Documentation for Cisco Nexus 5000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders is available at the following URL:

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

The following are related Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Fabric Extender documents:

Release Notes

Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes

Cisco Nexus 5000 Series Switch Release Notes

Configuration Guides

Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 5.0(2)N1(1)

Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 4.2(1)N1(1) and Release 4.2(1)N2(1)

Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide

Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide

Cisco Nexus 5000 Series NX-OS Multicast Routing Configuration Guide

Cisco Nexus 5000 Series NX-OS Quality of Service Configuration Guide

Cisco Nexus 5000 Series NX-OS SAN Switching Configuration Guide

Cisco Nexus 5000 Series NX-OS Security Configuration Guide

Cisco Nexus 5000 Series NX-OS System Management Configuration Guide

Cisco Nexus 5000 Series NX-OS Unicast Routing Configuration Guide

Cisco Nexus 5000 Series Switch NX-OS Software Configuration Guide

Cisco Nexus 5000 Series Fabric Manager Configuration Guide, Release 3.4(1a)

Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.2

Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide

Send documentation comments to nexus5kdocs@cisco.com

Maintain and Operate Guides

Cisco Nexus 5000 Series NX-OS Operations Guide

Installation and Upgrade Guides

Cisco Nexus 5000 Series and Cisco Nexus 5500 Platform Hardware Installation Guide

Cisco Nexus 2000 Series Hardware Installation Guide

Cisco Nexus 5000 Series NX-OS Software Upgrade and Downgrade Guide, Release 4.2(1)N1(1)

Regulatory Compliance and Safety Information for the Cisco Nexus 5000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders

Licensing Guide

Cisco NX-OS Licensing Guide

Command References

Cisco Nexus 5000 Series Command Reference

Technical References

Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Fabric Extender MIBs Reference

Error and System Messages

Cisco NX-OS System Messages Reference

Troubleshooting Guide

Cisco Nexus 5000 Troubleshooting Guide

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/c/en/us/td/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 delivers content directly to your desktop using a reader application. The RSS feeds are a free service.