Cisco Nexus 5500 Series Release Notes, Release 7.x

Release Date: January 29, 2014
Part Number: OL-30872-01 A0
Current Release: NX-OS Release 7.0(0)N1(1)

This document describes the features, caveats, and limitations for the Cisco Nexus 5500 devices and the Cisco Nexus 2000 Series Fabric Extenders. Use this document in combination with documents listed in the "Related Documentation" section on page 22.

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 5500 and Cisco Nexus 2000 Series release notes:
http://www.cisco.com/en/US/docs/switches/datacenter/nexus5500/sw/release/notes/Nexus_5500_Release_Notes.html

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

Table 1 Online History Change

Part Number	Revision	Date	Description
OL-30872-01	A0	January 29, 2014	Created NX-OS Release 7.0(0)N1(1) release notes.

Contents

This document includes the following sections:

Cisco Systems, Inc.
www.cisco.com

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 5500 Series device and the Cisco Nexus 2000 Series Fabric Extender (FEX) to improve the performance, scalability, and management of the product line.

Cisco Nexus Devices

The Cisco Nexus devices include a family of line-rate, low-latency, lossless 10-Gigabit Ethernet, Cisco Data Center Ethernet, Fibre Channel over Ethernet (FCoE), and native Fibre Channel devices for data center applications.

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

Cisco Nexus 2000 Series Fabric Extenders

The Cisco Nexus 2000 Series Fabric Extender (FEX) is a highly scalable and flexible server networking solution that works with the Cisco Nexus 5500 Series devices 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 device, which allows zero-touch provisioning and automatic configuration. The FEX provides a single point of management that supports a large number of servers and hosts that can be configured with the same feature set as the parent Cisco Nexus 5500 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 5500 Series NX-OS Layer 2 Switching Configuration Guide, Release 7.x.*

System Requirements

This section includes the following topics:

Hardware Supported

The Cisco NX-OS software supports the Cisco Nexus devices. Starting with Cisco NX-OS Release 7.0(0)N1(1), the Cisco Nexus 5010 and 5020 switches are not supported. You can find detailed information about supported hardware in the *Cisco Nexus 5500 Series Hardware Installation Guide*.

Table 2 shows the hardware supported by Cisco NX-OS Release 7.x software.

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software

Cisco NX-OS Release Support		
Hardware	**Part Number**	**7.0(0)N1(1)**
Cisco Nexus 5500 Series		
Cisco Nexus 5596T switch[1]	N5K-C5596T-FA	X
Cisco Nexus 5596UP switch	N5K-C5596UP-FA	X
Cisco Nexus 5548UP switch	N5K-C5548UP-FA	X
Cisco Nexus 5548P switch	N5K-C5548P-FA	X
Cisco Nexus 2000 Series		
Cisco Nexus B22DELL FEX[2]	N2K-B22DELL-P	X
Cisco Nexus B22IBM FEX[3] [4]	N2K-B22IBM-P	X
Cisco Nexus 2248PQ FEX[5]	N2K-C2248PQ-10GE	X
Cisco Nexus 2232TM-E FEX[6]	N2K-C2232TM-E-10GE	X
Cisco Nexus B22F FEX	N2K-B22FTS-P	X
Cisco Nexus B22HP FEX[7]	N2K-B22HP-P	X
Cisco Nexus 2232TM FEX	N2K-C2232TM-10GE	X

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support		
Hardware	**Part Number**	**7.0(0)N1(1)**
Cisco Nexus 2232PP FEX	N2K-C2232PP-10GE	X
Cisco Nexus 2248TP-E FEX	N2K-C2248TP-E-1GE	X
Cisco Nexus 2248TP FEX	N2K-C2248TP-1GE	X
Cisco Nexus 2224TP FEX	N2K-C2224TP-1GE	X
Cisco Nexus 2148T FEX	N2K-C2148T-1GE	—[8]
Expansion Modules		
4-port QSFP+ 10GBE GEM	N55-M4Q	X
12-port 10GBASE-T GEM[9]	N55-M12T	X
16-port Universal GEM	N55-M16UP(=)	X
N5596 Layer 3 GEM	N55-M160L3(=)	X
N5548 Layer 3 daughter card	N55-D160L3(=)	X
Layer 3 GEM	N55-M160L3-V2	X
Version 2 Layer 3 daughter card	N55-D160L3-V2	X
16-port SFP+ Ethernet	N55-M16P(=)	X
8 10-Gigabit Ethernet and 8 10-Gigabit FCoE ports	N55-M8P8FP(=)	X
Transceivers		
Fabric Extender Transceivers		
10-Gigabit Ethernet SFP (for Cisco Nexus 2000 Series to Cisco Nexus 6000 Series connectivity)	FET-10G(=)	X
SFP+ Optical		
Cisco 40GBASE-LR4 QSFP+ Module for SMF	QSFP-40GE-LR4	6.0(2)N1(2)
4x10-Gigabit QSFP module	QSFP-4SFP10G-CU1M	X

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support		
Hardware	**Part Number**	**7.0(0)N1(1)**
4x10-Gigabit QSFP module	QSFP-4SFP10G-CU3M	X
4x10-Gigabit QSFP module	QSFP-4SFP10G-CU5M	X
4x10-Gigabit QSFP module	QSFP-4SFP10G-ACu7M	X
4x10-Gigabit QSFP module	QSFP-4SFP10G-ACu10M	X
Cisco 40GBASE-CR4 QSFP+ to 4 10GBASE-CU SFP+ direct-attach breakout 7-meter cable, active	QSFP-4X10G-AC7M	6.0(2)N1(2) and later
Cisco 40GBASE-CR4 QSFP+ to 4 10GBASE-CU SFP+ direct-attach breakout 10-meter cable, active	QSFP-4X10G-AC10M	6.0(2)N1(2) and later
Gigabit Ethernet SFP, LH transceiver[10]	GLC-LH-SMD	X
Gigabit Ethernet SFP, EX transceiver[11]	GLC-EX-SMD	X
1000BASE-ZX SFP transceiver module for SMF	GLC-ZX-SM(=)	X
10-Gigabit Ethernet—short range SFP+ module	SFP-10G-SR(=)	X
10-Gigabit Ethernet—long range SFP+ module	SFP-10G-LR(=)	X
10-Gigabit Ethernet—extended range SFP+ module	SFP-10G-ER(=)	X
1000BASE-T standard	GLC-T(=)	X
Gigabit Ethernet SFP, LC connector SX transceiver (MMF)	GLC-SX-MM	X

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support		
Hardware	**Part Number**	**7.0(0)N1(1)**
Gigabit Ethernet SFP, LC connector SX transceiver (MMF), extended temperature range and DOM	GLC-SX-MMD	X
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF)	GLC-LH-SM	X
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF), extended temperature range and DOM	GLC-LH-SMD	X
SFP+ Copper		
10GBASE-CU SFP+ Cable (1 meter)	SFP-H10GB-CU1M(=)	X
10GBASE-CU SFP+ Cable (3 meters)	SFP-H10GB-CU3M(=)	X
10GBASE-CU SFP+ Cable (5 meters)	SFP-H10GB-CU5M(=)	X
10GBASE-CU SFP+ Cable (7 meters)	SFP-H10GB-ACU7M(=)	X
10GBASE-CU SFP+ Cable (10 meters)	SFP-H10GB-ACU10M(=)	X
10GBASE CU SFP+ cable[12]	SFP-H10GB-CU1.5M	X
10GBASE CU SFP+ cable[13]	SFP-H10GB-CU2M	X
10GBASE CU SFP+ cable[14]	SFP-H10GB-CU2.5M	X
Fibre Channel		
8-Gbps Fibre Channel—short wavelength	DS-SFP-FC8G-SW(=)	X
8-Gbps Fibre Channel—long wavelength	DS-SFP-FC8G-LW(=)	X
4-Gbps Fibre Channel—short wavelength	4DS-SFP-FC4G-SW(=)	X

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support		
Hardware	**Part Number**	**7.0(0)N1(1)**
4-Gbps Fibre Channel—long wavelength	4DS-SFP-FC4G-LW(=)	X
4-Gbps CWDM SFP		
1470 nm CWDM 1/2/4-Gbps Fibre Channel, Gray	DS-CWDM4G1470(=)	X
1490 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Violet	DS-CWDM4G1490(=)	X
1510 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Blue	DS-CWDM4G1510(=)	X
1530 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Green	DS-CWDM4G1530(=)	X
1550 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Yellow	DS-CWDM4G1550(=)	X
1570 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Orange	DS-CWDM4G1570(=)	X
1590 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Red	DS-CWDM4G1590(=)	X
1610 nm CWDM 1/2/4-Gbps Fibre Channel SFP, Brown	DS-CWDM4G1610(=)	X
Extended Temperature Range		
1000BASE-T SFP, extended temperature range	SFP-GE-T(=)	X
Gigabit Ethernet SFP, LC connector SX transceiver (MMF), extended temperature range and digital optical monitoring (DOM)	SFP-GE-S(=)	X

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support		
Hardware	**Part Number**	**7.0(0)N1(1)**
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF), extended temperature range and DOM	SFP-GE-L(=)	X
Converged Network Adapters		X
Generation-1 (Pre-FIP) CNAs[15]		X

1. The Cisco Nexus 5596T and the 12-port 10-GBase-T GEM are supported starting with Cisco NX-OS Release 5.2(1)N1(1b).
2. The Cisco Nexus B22DELL P FEX is supported starting with Cisco NX-OS Release 5.2(1)N1(3).
3. The Cisco Nexus B22IBM FEX is supported with Cisco NX-OS Release 6.0(2)N2(1b)
4. The Cisco Nexus B22IBM FEX is not supported with Cisco NX-OS Release 6.0(2)N2(2) and Cisco NX-OS Release 7.0(0)N1(1).
5. The Cisco Nexus 2248PQ FEX does not support Gen1 cables.
6. The Cisco Nexus 2232TM-E FEX is supported starting with Cisco NX-OS Release 5.2(1)N1(1a).
7. The Cisco Nexus B22HP FEX is supported starting with Cisco NX-OS Release 5.0(3)N2(2).
8. Starting with Cisco NX-OS Release 6.0(2)N1(1), 2148T FEX is not supported on Cisco Nexus 5500 series devices.
9. The 12 port 10-GBASE-T GEM is only supported on the Cisco Nexus 5596T starting with Cisco NX-OS Release 5.2(1)N1(1b).
10. Added support for Gibabit Ethernet SFP LX transceiver starting with Cisco NX-OS Release 6.0(2)N1(2).
11. Added support for Gibabit Ethernet SFP EX transceiver starting with Cisco NX-OS Release 6.0(2)N1(2).
12. Added support for 10GBASE CU SFP+ cable starting with Cisco NX-OS Release 6.0(2)N1(2).
13. Added support for 10GBASE CU SFP+ cable starting with Cisco NX-OS Release 6.0(2)N1(2).
14. Added support for 10GBASE CU SFP+ cable starting with Cisco NX-OS Release 6.0(2)N1(2).
15. Generation-1 (Pre-FIP) CNAs are supported on the Nexus 5000 Platform switches; however, they are not supported on the Nexus 5500 Series.

Online Insertion and Removal Support

Table 3 shows the hardware and Cisco NX-OS Release 7.x software that supports online insertion and removal (OIR).

Table 3 Online Insertion and Removable Support by Cisco NX-OS Release 7.x Software

Hardware	Part Number	Cisco NX-OS Release Support 7.0(0)N1(1)
Cisco Nexus 5500 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
Expansion Modules		
16-port Universal GEM	N55-M16UP(=)	X
Layer 3 GEM[1]	N55-M160L3-V2[1]	—
Version 2 Layer 3 daughter card[1]	N55-D160L3-V2[1]	—
16-port SFP+ Ethernet	N55-M16P(=)	X
8-port SFP+ Ethernet ports and 8-port SFP+ Fibre Channel ports	N55-M8P8FPL(=)	X
N5596 Layer 3 GEM[1]	N55-M160L3(=)[1]	—
N5548 Layer 3 daughter card[1]	N55-D160L3(=)[1]	—

1. Does not support online insertion and removal. You must power down the Cisco Nexus 5500 Series switch before removing or inserting a Layer 3 GEM or Version 2 Layer 3 daughter card expansion module.

New and Changed Features

This section describes the new features introduced in Cisco NX-OS Release 7.x. This section includes the following topics:

New Software Features in Cisco NX-OS Release 7.0(0)N1(1)

Cisco NX-OS Release 7.0(0)N1(1) is a major release that includes bug fixes and the following software features and enhancements:

Anycast HSRP

Anycast HSRP is a FabricPath-based feature in which the traditional HSRP can be extended to an n-Gateway solution with all the gateways actively forwarding traffic. This feature supports active load balancing of traffic among all the gateways configured apart for redundancy. A maximum of 4 Gateways is supported.

Early Warning for Forwarding Information Base Exhaustion

When the Forwarding Information Base (FIB) table is 90% full, the following messages is displayed:

FIB_TCAM_RESOURCE_EXHAUSTION:FIB TCAM exhausted

Explicit Congestion Notification with Weighted Random Early Detection

Explicit Congestion Notification (ECN) with Weighted Random Early Detection (WRED) solves the delay and packet loss problems for applications that are sensitive to these issues.

FabricPath Operations, Administration, and Management

Support for Fabric Path Operations, Administration and Management has been added in this software release.

Fibre Channel and Fibre Channel Over Ethernet Slow Drain

Fiber Channel (FC) and Fibre Channel over Ethernet (FCoE) slow drain addressed the issue of slow drain devices that cause congestion in the network.

Intermediate System to Intermediate System Protocol

Intermediate System to Intermediate System (IS-IS) is an Interior Gateway Protocol (IGP) based on Standardization (ISO)/International Engineering Consortium (IEC) 10589. Cisco Nexus devices support Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). IS-IS is a dynamic link-state routing protocol that can detect changes in the network topology and calculate loop-free routes to other nodes in the network. Each router maintains a link-state database that describes the state of the network and sends packets on every configured link to discover neighbors. IS-IS floods the link-state information across the network to each neighbor. The router also sends advertisements and updates on the link-state database through all the existing neighbors.

Layer 2 Bidirectional Forwarding Detection

The Bidirectional Forwarding Detection (BFD) provides fast forwarding-path failure detection times for media types, encapsulations, topologies, and routing protocols. You can use BFD to detect forwarding path failures at a uniform rate, rather than at variable rates for different protocol hello mechanisms. BFD makes network profiling and planning easier and reconvergence time consistent and predictable.

Multi-Destination Tree

A Multi-Destination Tree (MDT), also referred to as a forwarding tag or ftag, is a spanning-tree used for forwarding packets within a topology. A topology has two MDTs/ ftags: topology 0 has ftag 1 and 2, topology 1 has ftag 3 and 4.

One Platform Kit (OnePK)

Support has been added for One Platform Kit (onePK) Turbo API. OnePK is a cross-platform API and software development kit that enables you to develop applications that interact directly with Cisco networking devices. onePK provides you access to networking services by using a set of controlled APIs that share the same programming model and style. For more information, see the following URL:

http://www.cisco.com/en/US/partner/prod/iosswrel/onepk.html

OpenFlow v1.0

The OpenFlow feature is a specification from the Open Networking Foundation (ONF) that defines a flow-based forwarding infrastructure (L2-L4 Ethernet switch model) and a standardized application programmatic interface (protocol definition) to learn capabilities, add and remove flow control entries and request statistics. OpenFlow allows a controller to direct the forwarding functions of a switch through a secure channel.

Overload Bit

Intermediate System to Intermediate System (IS-IS) uses the overload bit to tell other routers not to use the local router to forward traffic but to continue routing traffic destined for that local router.

Port Channel Max Links

The Port Channel Max Links feature defines the maximum number of bundled ports allowed in an LACP port channel.

Protocol Independent Multicast

Protocol Independent Multicast (PIM), which is used between multicast-capable routers, advertises group membership across a routing domain by constructing multicast distribution trees. PIM builds shared distribution trees on which packets from multiple sources are forwarded, as well as source distribution trees on which packets from a single source are forwarded.

Switch Port Analyzer with Access Control List Filtering

The Switch Port Analyzer (SPAN) with Access Control List (ACL) filtering feature allows you to filter SPAN traffic so that you can reduce bandwidth congestion. To configure SPAN with ACL filtering, you use ACL's for the session to filter out traffic that you do not want to span. An ACL is a list of permissions associated to any entity in the system; in the context of a monitoring session, an ACL is a list of rules which results in spanning only the traffic that matches the ACL criteria, saving bandwidth for more meaningful data. The filter can apply to all sources in the session.

TCAM Carving

You can create and administer up to 16 templates to resize the regions in ternary content-addressable memory (TCAM).

New HardwareFeatures in Cisco NX-OS Release 7.0(0)N1(1)

Cisco NX-OS Release 7.0(0)N1(1) supports the following new optics:

- QSFP-10G-AOC (1/2/3/5/7/10m)
- PSF1PXA3.5MBU
- PSF1PXA4MBU
- QSFP- AOC (1/2/3/5/7/10m)
- QSFP 4X10 AOC (1/2/3/5/7/10m)

Upgrading or Downgrading to a New Release

This section describes the upgrade and downgrade paths that are supported for Cisco NX-OS Release 7.0(0)N1(1) on the Cisco Nexus device.

The section includes the following topics:

Upgrade and Downgrade Guidelines

The following guidelines apply to Cisco NX-OS Release 7.0(0)N1(1) for Cisco Nexus devices:

- If host interface (HIF) port channels or EvPCs are configured in the system, and if the system was already upgraded to NX-OS Release 5.1(3)N1(1) or Release 5.1(3)N1(1a) from any release earlier than Release 5.1(3)N1(1), ensure that the system was reloaded at least once before you upgrade to Release 5.1(3)N2(1a) or Release 5.1(3)N2(1). If the switch was not previously reloaded, reload it and upgrade to Release 5.1(3)N2(1a) or Release 5.1(3)N2(1).
- When a Layer 3 license is installed, the Cisco Nexus 5500 Platform does not support an ISSU. Hot swapping a Layer 3 module, for example, the Layer 3 GEM (N55-M160L3-V2) or Version 2 Layer 3 daughter card (N55-D160L3-V2), is not supported. You must power down the Cisco Nexus device before removing or inserting a Layer 3 expansion module.

Supported Upgrade and Downgrade Paths

Table 4 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 7.0(0)N1(1). For more information, see the *Cisco Nexus 5500 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.0*.

Table 4 Cisco NX-OS Release 7.0(0)N1(1)Supported Upgrade and Downgrade Paths

Current Cisco NX-OS Release	Upgrade to NX-OS Release 7.0(0)N1(1)	Downgrade from NX-OS Release 7.0(0)N1(1)
6.0(2)N2(1b) 6.0(2)N2(2) 6.0(2)N2(1) 6.0(2)N1(2a) 6.0(2)N1(2) 6.0(2)N1(1a) 6.0(2)N1(1)	Nondisruptive upgrade (ISSU)	Disruptive downgrade
5.2(1)N1(5) 5.2(1)N1(4) 5.2(1)N1(3) 5.2(1)N1(2a) 5.2(1)N1(2) 5.2(1)N1(1b) 5.2(1)N1(1a) 5.2(1)N1(1)	Nondisruptive upgrade (ISSU)	Disruptive downgrade

Limitations

This section describes the limitations for Cisco NX-OS Release 7.0(0)N1(1).

- Ingress inter-VLAN-routed Layer3 multicast packets are treated as “unknown multicast” by the storm-control feature. This is due to the Layer 3 forwarding design in the Cisco Nexus 5500 Series switch. For details, see CSCuh34068.

- When performing an ISSU from Cisco NX-OS Release 5.1(3)N1(1) or Cisco NX-OS Release 5.1(3)N2(1) to Cisco NX-OS Release 5.2(1)N1(1), a Forwarding Manager (FWM) core can occur, which causes the system to reset. This situation occurs when network interface virtualization (NIV) is enabled. To work around this issue, use the **force** option in the **install** command to perform a disruptive upgrade. For details, see CSCty92117.
- The SAN admin user role (san-admin) is a new predefined user role in Cisco NX-OS Release 5.2(1)N1(1). If you have an existing user role with the name san-admin in Cisco NX-OS Release 5.1(3)N1(1) or Cisco NX-OS Release 5.1(3)N2(1), the new system-defined role is removed when you upgrade. To resolve this issue, downgrade to the previous release, rename the user role, and perform the upgrade. For details, see CSCua21425.
- Bridge and STP traps are displayed in the downgrade incompatibility list when you downgrade from Cisco NX-OS Release 5.2(1)N1(1) to Cisco NX-OS Release 5.0(3)N1(1c). To resolve this issue, reset the STP/Bridge trap configuration to the default settings by entering the **no snmp-server enable traps bridge**, the **no snmp-server enable traps stpx** command, and then the **copy running-config startup-config** command. For details, see CSCua75907.
- The Server Virtualization Switch (SVS) connection is not deleted during a rollback when NIV is enabled. To resolve this issue, delete the current SVS connection and reapply the original SVS connection. For details, see CSCts17033.
- If SPAN traffic is rate-limited by entering the switchport monitor rate-limit 1G command, then a maximum transmission unit (MTU) truncation size cannot be used to truncate SPAN packets. For details, see CSCua05799.
- When an FC SPAN destination port is changed from SD to F mode and back to SD mode on an 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, then autonegotiation does not occur, which is the 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 an 802.3x pause.

  speed 100—Does not autonegotiate; pause cannot be advertised. The peer must be set to not autonegotiate and to 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 goes into a PVST SIM inconsistent blocked state that breaks the STP active path. To work around this issue, move all STP roots to the MST region. However, the workaround causes a nondisruptive ISSU to fail because nonedge designated forwarding ports are not allowed for an ISSU. For additional information, see CSCtf51577. For information about topologies that support a nondisruptive upgrade, see the *Cisco Nexus 5500 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 port has not joined the group, then this is not an issue. If there is an interface that has joined the group, 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 the traffic. For details, see CSCtf94558.

- 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 workaround.
- In large-scale configurations, some Cisco Nexus 2000 Series Fabric Extenders might 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 device, all host-facing ports are connected, and each host-facing interface has a large configuration (that supports the maximum permissible ACEs per interface).
- 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 dot1q 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 appear:

```
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.

- If you configure Multiple Spanning Tree (MST) on a Cisco Nexus device, we recommend that you avoid partitioning the network into a large number of regions.
- A downgrade from Cisco NX-OS Release 5.1(3)N1(1) to any 5.0(3)N1(x) image can cause the Cisco Nexus device to fail. For details, see CSCty92945.
- If you upgrade a vPC peer switch from Cisco NX-OS Release 5.0(3)N2(1) to Cisco NX-OS Release 5.1(3)N2(1) or Cisco NX-OS Release 5.2(1)N1(1), and feature-set FabricPath is enabled on the upgraded switch, the vPC Peer-Link enters STP Bridge Assurance Inconsistency, which affects all VLANs except VLAN 1 and affects traffic forwarding for vPC ports.

  To avoid this issue, upgrade the peer switch that is running Cisco NX-OS Release 5.0(3)N2(1) to Cisco NX-OS Release 5.1(3)N2(1) or later release and then enable feature-set FabricPath on the switch or switches. If you accidentally enable feature-set FabricPath in Cisco NX-OS Release 5.1(3)N2(1) when the peer vPC switch is running Cisco NX-OS Release 5.0(3)N2(1), disable the feature-set FabricPath and the vPC will resume the STP forwarding state for all VLANs.

- By design, vEth interfaces do not share the underlying behavior of a vPC port. As a result, a VLAN does not get suspended when the peer switch suspends it. For example, when you shut a VLAN on a primary switch, the VLAN continues to be up on the secondary switch when the vEth interface is on a FEX. When the VLAN on the primary switch goes down, the VLAN on the vEth interface on the primary is suspended, but the vEth on the secondary switch is up because it is an active VLAN on the secondary switch.
- Rol-based Access Control List (RBACL) policy enforcement is performed on VLANs on which Cisco Trusted Security (CTS) enforcement is not configured. This situation occurs when there is at least one VLAN in the switch where CTS is enforced. On a VLAN where CTS is not enforced, RBACL policy lookup occurs for ingress packets and the packet is denied or permitted according to the policies in the system. To work around this issue, make sure that all VLANs on which SGT tagged packets ingress enforce CTS.
- The packet length in the IP GRE header of a packet exiting from the switch is not equal to the MTU value configured in the ERSPAN source session. This is true for SPAN or ERSPAN. This situation can occur whenever the MTU value that is configured in an ERSPAN or SPAN session is smaller than the SPAN packet, such as when the packet is truncated. The IP GRE packet is truncated to a value that differs by –2 to 10 bytes from the expected MTU.
- When you configure a Layer 3 interface as an ERSPAN source, and configure the ERSPAN termination on a Catalyst 5500 switch or a Cisco Nexus 7000 Series switch, you cannot terminate the Layer 3 interface ERSPAN source on the Cisco Nexus 7000 Series switch or the Catalyst 5500 switch. To work around this issue, configure VLAN 1 to 512 on the Cisco Nexus 7000 Series switch or the Catalyst 6000 switch.
- Unknown unicast packets in FabricPath ports are counted as multicast packets in interface counters. This issue occurs when unknown unicast packets are sent and received with a reserved multicast address (that floods to a VLAN) in the outer FabricPath header, and the Cisco Nexus device increments the interface counter based on the outer FabricPath header. As a result, multicast counters are incremented. In the case of a Cisco Nexus 7000 Series switch, unicast counters are incremented as they are based on an inner Ethernet header. There is no workaround for this issue.
- If you configure a speed of 1 G on a base or GEM port and then check for compatibility with a Cisco NX-OS Release 5.0(2) image, no incompatibility is shown. However, because 1 G was not supported in the Cisco NX-OS Release 5.0(2), an incompatibility should be shown. To work around this issue, manually remove the 1 G configuration from the ports before downgrading to Cisco NX-OS Release 5.0(2) or an earlier release.
- In an emulated switch setup, inband keepalive does not work. The following steps are recommended for peer keepalive over switch virtual interface (SVI) when a switch is in FabricPath mode:
  - Use a dedicated front panel port as a vPC+ keepalive. The port should be in CE mode.
  - Use a dedicated VLAN to carry the keepalive interface. The VLAN should be a CE VLAN.
  - Add the **management** keyword to the corresponding SVI so that the failure of a Layer 3 module will not bring down the SVI interface.
  - Enter the **dual-active exclude interface-vlan** *keepalive-vlan* command to prevent the SVI from going down on the secondary when a peer-link goes down.
- FabricPath requires 802.1Q tagging of the inner Ethernet header of the packet. Native VLAN packets that are sent by a Cisco Nexus 7000 Series switch are not tagged. As a result, a Cisco Nexus device drops packets due to packet parsing errors. To work around this issue, enter the **vlan dot1q tag native** command on the Cisco Nexus 7000 Series switch to force 802.1Q tagging of native VLAN packets.
- SPAN traffic is rate limited on Cisco Nexus 5500 Series devices to prevent impact to production traffic:

  - SPAN is rate limited to 5 Gbps per ASIC (every 8 ports share one ASIC).
  - SPAN is rate limited to 0.71 Gbps per monitor source port when the RX traffic on the port exceeds 5 Gbps.

  For details, see CSCti94902.

- Cisco Nexus 5548UP and Cisco Nexus 5598UP devices with a fibre-channel connection to HP Virtual Connect modules experience link destabilization and packet loss when the speed is set to 8 GB. To work around this issue, leave the speed set to 4 GB. For details, see CSCtx52991.
- A nondisruptive ISSU is not supported when ingress policing is configured.
- The maximum IP MTU that can be set on Layer 3 interfaces on which Layer 3 protocols are running is 9196, because of the internal header used inside the switch. The network-qos policy must be set to 9216.

Limitations on the Cisco Nexus Device

The limitations on the Cisco Nexus device 5500 Series devices are as follows:

- SPAN Limitations on Fabric Extender Ports, page 17
- Checkpoint and Configuration Rollback Limitation, page 18

SPAN Limitations on Fabric Extender Ports

The SPAN limitations on Fabric Extender ports are as follows:

- On a Cisco Nexus device, if the SPAN source is a FEX port, the frames will always be tagged when leaving the SPAN destination.
- On a Cisco Nexus 5500 Platform switch, if the SPAN source is on an access port on the switch port, 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, an 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 following error appears:

```
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), 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 might 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.
- Cisco NX-OS Release 5.1(3)N2(1) does not support SPAN on a VM FEX.

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 devices configured as vPC peer switches need to be configured symmetrically for Layer 3 configurations such as SVIs, the peer gateway, routing protocol and policies, and RACLs.

Note The vPC consistency check does not include Layer 3 parameters.

SVI

When a Layer 3 module goes offline, all non-management SVIs are shut down. An SVI can be configured as a management SVI by entering the **interface vlan** command and configuring *management*. This configuration allows traffic to the management SVIs to not go through the Layer 3 module which maintains connectivity in case of a Layer 3 module failure.

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 NX-OS Release 5.0(3)N1(1c) or a later release, and then install the card into the chassis.

Caveats

This section includes the open and resolved caveat record numbers for this release. Links are provided to the Bug Toolkit where you can find details about each caveat.

This section includes the following topics:

Open Caveats

Table 5 lists descriptions of open caveats in Cisco NX-OS Release 7.0(0)N1(1).

The record ID links to the Cisco Bug Toolkit where you can find details about the caveat.

Table 5 Cisco NX-OS Release 7.0x Open Caveats

Record Number	Open Caveat Headline
CSCts71048	On an NPV switch, VFCs do not come up after delete/add VLAN/VSAN.
CSCty33678	MACs not synced after ISSU on AA HIF trink with PSEC;non-default timers.
CSCuh30885	RBACL update and programming fails in certain scenarios.
CSCui94565	Service not responding under certain CTS scale scenarios.
CSCuh25992	A Cisco Nexus 5500 switch running BFD over a Layer 3 port-channel may be reset by a kernel crash if the port-channel has more than 10 members.
CSCuh17828	On a Cisco Nexus 5500 switch, when the command sequence **copy file start** is used, copying the saved configuration to the running configuration takes too long.
CSCuf82183	In some scenarios, policy statistics are not enabled when a service policy is applied to ports.
CSCuh34068	Ingress inter-VLAN-routed Layer 3 multicast packets are treated as “unknown multicast” by the storm-control feature.
CSCtx84752	The MVR receiver-port output for an AA FEX port displays ACTIVE after a switchover.
CSCtx99080	The FEX temperature does not reflect the correct value.
CSCug90859	On the Cisco Nexus 5500 switch, PBR does not work on a PVLAN SVI.
CSCty43038	After a rollback, the **show tech-support ethpm** command displays unconfigured VLANs, and FWM forwards unconfigured VLANs.
CSCtz78363	If you change the VLAN mode from FabricPath to Classical Ethernet and then back to FabricPath, some Hot Standby Router Protocol (HSRP) gateway-based traffic may be affected.

Table 5 Cisco NX-OS Release 7.0x Open Caveats (continued)

Record Number	Open Caveat Headline
CSCua27097	The **no feature private-vlan** command does not remove the entire configuration.
CSCuc12211	Channel-group configuration missing after reload on HIF port.
CSCuc25187	The **config-sync** process does not remove the VLAN QoS policy and offset configuration.
CSCuc43503	The IGMP vPC optimization knob does not work when feature-set virtualization is configured.
CSCud43962	CDPv6 shows the address of different interfaces, not the connected interfaces.
CSCud53059	DAI is blocking traffic for FEX HIF ports.
CSCue22038	After a module is powered off, a timeout occurs for the line card removal sequence. As a result, the slot becomes unusable and must be reloaded.
CSCue33173	IPSG blocks traffic for private VLAN isolated trunk ports, even when a valid DHCP snooping binding entry exists.
CSCuh44777	Support should be available to log enabled IP ACL as a class-map match.
CSCug72465	A test harness does not properly treat closing of the TCP flow.
CSCuf52331	The minimum suppression value needs to be handled properly in switch/HIF/NIF storm-control.
CSCuh04973	The **default-interface** command is not resetting the speed command on an HIF port-channel interface.
CSCuf16457	On a Cisco Nexus 5500 switch, applying policy maps fails with the error %RPM-2-PPF_SES_VERIFY.
CSCug98105	Cisco Nexus 5500-BGP v6 peering is not coming up if the same address in a different VRF uses MD5.
CSCuh36797	PIM process restart CLI is visible but not supported on the Cisco Nexus 5500.
CSCuh26111	N64P- Some mroutes are not removed from the last hop router following an admin shut of the SVI.
CSCuf47724	On a Cisco Nexus 5500 switch, SVI Counters show incorrect results.
CSCui56698	Slow drain: Need support for non-default CoS value for class-fcoe.
CSCul27686	Interfaces might go down after upgrade and cannot be recovered.
CSCul51416	FCoE slowdrain - pause events not detected for bind MAC configuration.
CSCuj12958	U6RIB structure errors seen during withdraw/add routes.
CSCuj12998	FCOE/EEM - 100% CPU for EEM actions with low timeout/high pause rate.
CSCuj13018	FCoE/EEM - Only 18 actions are taken when 19 actions are accepted.
CSCuj43607	NAT: With same static and dynamic NAT policy, packets punted to CPU.
CSCuj58467	Router MAC is not getting installed when changing the ASID.
CSCuj69824	Python script is not working when called using the **python** *script_name* command.
CSCuj78048	Interface VLAN shows up in the **show run** command after creating a configuration profile.
CSCuj83153	POAP: Addition of python-run and python-exec files to bootflash.
CSCuj86321	Pause events not seen if slow drain is enabled before VFC is up.

Table 5 Cisco NX-OS Release 7.0x Open Caveats (continued)

Record Number	Open Caveat Headline
CSCul23467	Port-monitor and FC slow drain configurable on NPV switch.
CSCul49154	Flow match statistics are displaying 0 for default frop flow.
CSCul81869	10Mb FEX:ISSU downgrade from 7.0(0)N1(1) to 6.0(2)N2(1) should be incompatible with Speed 10.
CSCul82850	While configuring no IPv6 access-list acl_pbrIpv6L3PO_N5K getting error.
CSCul99528	Openflow: default-miss cascade normal not working in pipeline 201.
CSCum08767	WCCP: Interfaces level CLI configurations removed after invalid ID to spm.
CSCum11052	MAC address out of sync between two switches.
CSCum64907	FCOE Slowdrain: Pause Events not triggered on sh/no shut PO mem.
CSCum68574	Do not advertise Anycast SID when overload asserted.
CSCum83908	Port-security is not learning all addresses upon changing the port mode.

Resolved Caveats in Cisco NX-OS Release 7.0(0)N1(1)

Table 6 Cisco NX-OS Release 7.0(0)N1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtu31087	BGP update generation blocked because of large number of idle/active peers.
CSCud48710	Layer 2 multicast traffic can be lost up to 1 to 2 minutes upon unshut of the fabric PO in an AA topology. This happens only under the following conditions: • AA topology. • The group is downgraded to V2 of a V3 receiver. • The FEX fabric port is shut on one side. • When the fabric port is unshut, Layer 2 multicast traffic loss may be seen until the next join comes in.
CSCud72942	When all the FEXs are reloaded at the same time, Layer 2 multicast traffic may not recover on one of the HIF ports.
CSCud73169	The policer stats are not enabled if police action is added after it is applied to the interface configuration.
CSCuh36961	A QoS policy with qos-group 1 cannot be applied on a non-FCoE class.
CSCui77868	Add support for 10M speed on FEX interfaces.
CSCum14020	dot1x: traffic flooding due to miss mac address in MAC table

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 5500 Series switch.

The MIB Support List is available at the following FTP site:

ftp://ftp.cisco.com/pub/mibs/supportlists/nexus5000/Nexus5000MIBSupportList.html

Related Documentation

Documentation for Cisco Nexus 5500 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 documentation set includes the following types of documents:

- Licensing Information Guide
- Release Notes
- Installation and Upgrade Guides
- Configuration Guides
- Configuration Examples and TechNotes
- Programming Guides
- Operations Guides
- Error and System Message Guides
- Field Notices
- Security Advisories, Responses and Notices
- Troubleshooting Guide
- Command References
- MIB Reference Guide

Documentation Feedback

To provide technical feedback on this document or to report an error or ommission, please send your comments to nexus5k-docfeedback@cisco.com. We appreciate your feedback.

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.