Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes, Releases 4.1(3)N1(1), 4.1(3)N1(1a), 4.1(3)N2(1) and 4.1(3)N2(1a)

Current Release: 4.1(3)N2(1a) -December 15, 2009
Part Number: OL-16601-01 Q0

This document describes the features, caveats, and limitations for Cisco Nexus 5000 Series switches and the Cisco Necus 2000 Series Fabric Extenders. Use this document in combination with documents listed in the "Related Documentation" section on page 35.

Note Release notes are sometimes updated with new information about restrictions and caveats. See the following website for the most recent version of the Cisco Nexus 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.

Table 1 Online History Change

Revision	Date	Description
A0	June 03, 2008	Created release notes.
B0	June 16, 2008	Added information for Release 4.0(0)N1(1a).
C0	June 30, 2008	Added information for Cisco Fabric Manager Release 3.4(1a).
D0	July 22, 2008	Added information for Release 4.0(0)N1(1a).
E0	August 13, 2008	Added information for Release 4.0(0)N1(2).
F0	September 29, 2008	Added information for Release 4.0(0)N1(2a).
G0	December 03, 2008	Added information for Release 4.0(1a)N1(1).

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

Table 1 Online History Change (continued)

Revision	Date	Description
H0	February 26, 2009	Added information for Release 4.0(1a)N2(1).
I0	July 26, 2009	Added information for Release 4.1(3)N1(1).
J0	September 21, 2009	Added information for Release 4.1(3)N1(1a).
K0	November 13, 2009	Added information for Release 4.1(3)N2(1).
L0	December 15, 2009	Added information for Release 4.1(3)N2(1a).
M0	July 22, 2010	Updated information for Power Sequencer and CSCdy21017.
N0	March 17, 2011	Updated Limitations section with Cisco Nexus 2148 Fabric Extender information.
P0	March 28, 2011	Updated Limitations section with IGMP Snooping Limitation.
Q0	August 17, 2011	Added Enabling NPIV feature information.

Contents

This document includes the following sections:

- Introduction, page 2
- New and Changed Features, page 5
- Upgrade/Downgrade, page 6
- Installing Expansion Modules, page 9
- Limitations, page 10
- Caveats, page 13
- Related Documentation, page 35
- Obtaining Documentation and Submitting a Service Request, page 35

Introduction

This section includes the following topics:

- Cisco Nexus 5000 Series Switches, page 2
- Cisco Nexus 2000 Series Fabric Extenders, page 4

Cisco Nexus 5000 Series Switches

The Cisco Nexus 5000 Series switches comprise a family of line-rate, low-latency, lossless 10-Gigabit Ethernet, Cisco Data Center Ethernet, and Fibre Channel over Ethernet (FCoE) switches for data center applications. The Cisco Nexus 5000 Series includes the Cisco Nexus 5020 switch and the Cisco Nexus 5010 switch.

The Cisco Nexus 5000 Series switch hardware is described in the following topics:

- Cisco Nexus 5020 Switch, page 3

- Cisco Nexus 5010 Switch, page 3

Cisco Nexus 5020 Switch

The Cisco Nexus 5020 is a 56-port switch. It is a two rack unit (2 RU), 10-Gigabit Ethernet, Cisco Data Center Ethernet, FCoE, and Fibre Channel switch that provides 1.04 terabits per second (Tbps) throughput with very low latency.

It has the following features:

- Forty fixed 10-Gigabit Ethernet, Cisco Data Center Ethernet, and FCoE Small Form Factor Pluggable Plus (SFP+) ports. Sixteen of the forty fixed ports support both Gigabit Ethernet and 10-Gigabit Ethernet. The default is 10-Gigabit Ethernet.
- Two expansion module slots that can be configured to support up to 12 additional 10-Gigabit Ethernet, Cisco Data Center Ethernet, and FCoE SFP+ ports, up to 16 Fibre Channel switch ports, or a combination of both.
- Serial console port and an out-of-band 10/100/1000-Mbps Ethernet management port.
- 1+1 redundant, hot-pluggable power supplies.
- 4+1 redundant, hot-pluggable fan modules to provide highly reliable front-to-back cooling.

For additional information about the Cisco Nexus 5020 switch, see the *Cisco Nexus 5000 Series Hardware Installation Guide*.

Cisco Nexus 5010 Switch

The Cisco Nexus 5010 is a 28-port switch. It is a 1 RU, 10-Gigabit Ethernet, Cisco Data Center Ethernet, FCoE, and Fibre Channel switch that provides more than 500-Gbps throughput with very low latency. It has the following features:

- Twenty fixed 10-Gigabit Ethernet, Cisco Data Center Ethernet, and FCoE SFP+ ports. Eight of the twenty fixed ports support Gigabit Ethernet and 10-Gigabit Ethernet speed.
- One expansion module slot that can be configured to support up to 6 additional 10-Gigabit Ethernet, Cisco Data Center Ethernet, and FCoE SFP+ ports, up to 8 Fibre Channel switch ports, or a combination of 4 additional 10-Gigabit Ethernet, Cisco Data Center Ethernet, and FCoE SFP+ ports with 4 additional Fibre Channel switch ports.
- Serial console port and an out-of-band 10/100/1000-Mbps Ethernet management port.
- 1+1 redundant, hot-pluggable power supplies.
- 1+1 redundant, hot-pluggable fan modules to provide highly reliable front-to-back cooling.

For additional information about the Cisco Nexus 5010 switch, see the *Cisco Nexus 5000 Series Hardware Installation Guide*.

Note The Cisco Nexus 5020 switch and the N5K-M1404 and N5K-M1600 gatos expansion modules (GEMs) use a release 4.0(0)N1(1) or later image. The Cisco 5010 switch and the N5K-M1008 GEM use a release 4.0(1a)N1(1) or later image. The N5K-M1060 8GFC GEM uses release 4.1(3)N2(1).

Cisco Nexus 2000 Series Fabric Extenders

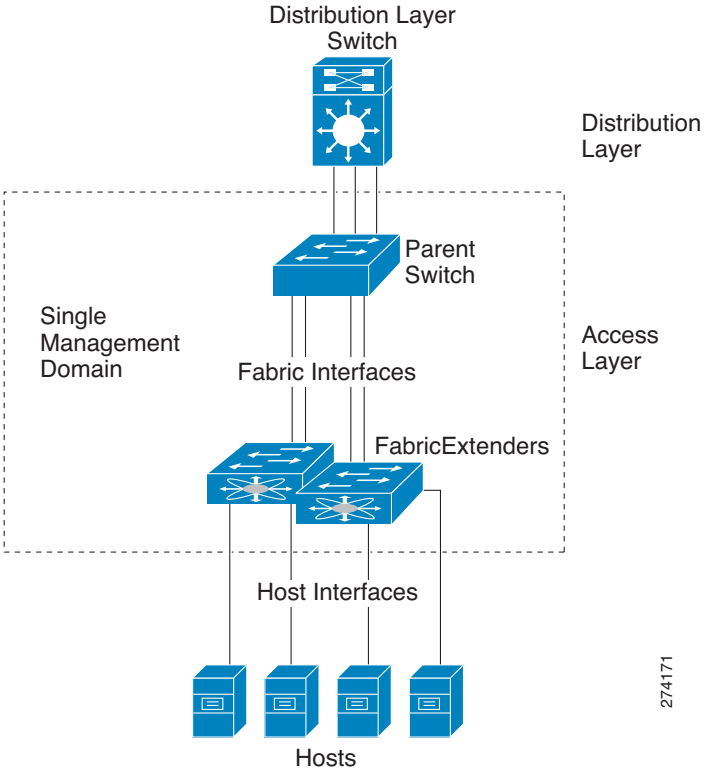
The Cisco Nexus 2000 Series Fabric Extender was first released in Release 4.0(1a)N2(1). It is a highly scalable and flexible server networking solution that works with the Cisco Nexus 5000 Series switches to provide high-density and low-cost connectivity for server aggregation.

Scaling across a multitude of 1-Gigabit Ethernet, 10-Gigabit Ethernet, unified fabric, rack, and blade server environments, the Fabric Extender is designed to simplify data center architecture and operations.

The Fabric Extender integrates with its parent switch, allowing zero-touch provisioning as well as automatic configuration. This integration allows large numbers of servers and hosts to be supported using the same feature set as the parent Nexus 5000 Series switch, including security and quality of service (QoS) configuration parameters, with a single point of management as shown in Figure 1-1. Spanning Tree Protocol (STP) is not required between the Fabric Extender and its parent switch, because the Fabric Extender an its parent switch allow you to enable a large multi-path, loop-free, active-active topology.

Since the Fabric Extender is designed to connect to servers directly, by default, all Fabric Extender host ports are edge ports. In addition, BPDU guard and BPDU filters are also enabled on Fabric Extender host ports by default.

Figure 1-1 Single Management Domain



This section describes the 2148T Fabric Extender. It includes the following topic:

- Cisco Nexus 2148T Fabric Extender, page 5

Cisco Nexus 2148T Fabric Extender

The first product in the Cisco Nexus 2000 Series is the Nexus 2148T Fabric Extender, a 1 RU chassis designed for rack mounting. The chassis supports redundant hot-swappable fans and power supplies.

The Cisco Nexus 2148T Fabric Extender forwards all traffic to a parent Cisco Nexus 5000 Series switch over 10-Gigabit Ethernet fabric uplinks, allowing all traffic to be inspected by policies established on the Cisco Nexus 5000 Series switch. No software is included with the Nexus 2148T. Software is downloaded and upgraded from its parent Cisco Nexus 5000 Series switch.

The Nexus 2148T has 48 1-Gigabit Ethernet host interfaces for its downlink connection to servers or hosts and 4 10-Gigabit Ethernet fabric interfaces with SFP+ interface adapters for its uplink connection to the parent switch.

New and Changed Features

This section briefly describes the new features introduced in the Cisco NX-OS 4.1(3)N2(1a), 4.1(3)N2(1), 4.1(3)N1(1a) and 4.1(3)N1(1) releases. This section includes the following topics:

- Enabling NPIV, page 5
- Cisco NX-OS Release 4.1(3)N2(1a), page 5
- Cisco NX-OS Release 4.1(3)N2(1), page 5
- Cisco NX-OS Release 4.1(3)N1(1a), page 6
- Cisco NX-OS Release 4.1(3)N1(1), page 6

Enabling NPIV

Beginning with Cisco NX-OS Release 4.1(3)N1(1), use the **feature npiv** command to enable NPIV. In previous releases, use the **npiv enable** command.

Cisco NX-OS Release 4.1(3)N2(1a)

Cisco NX-OS Release 4.1(3)N2(1a) has no new features.

Cisco NX-OS Release 4.1(3)N2(1)

Cisco NX-OS Release 4.1(3)N2(1) includes the following new or changed features:

- Support for N5K-M1060 8GFC GEM
- Support for 8GFC optics
- Modification of non-Cisco certified CX1 cable detection message
- Support for CiscoWorks, FM/DM, DCNM Network Mgmt objectives
- 64-bit counters for SNMP
- ACLs on Mgmt0 interface
- Support for VRF Logging option

- Multicast performance enhancement on PortChannels
- AAA command authorization with TACACS
- vPC enhancement to bring up vPCs when one of the vPC peer switches is down

Cisco NX-OS Release 4.1(3)N1(1a)

Cisco NX-OS Release 4.1(3)N1(1a) has no new features.

Cisco NX-OS Release 4.1(3)N1(1)

Cisco NX-OS Release 4.1(3)N1(1) includes the following new or changed features:

- 750 Watt power supply
- NX-OS 4.1.3 parity features
- Virtual Port Channels (VPC)
- Cisco Nexus 2000 Active-Active over VPC
- EtherChannel Enhancements
  - 16-Port Etherchannel
  - 16 Etherchannels
  - Etherchannel load balancing commands
- Cisco Nexus 2000 connectivity over expansion modules
- ACL for Cisco Nexus 2000 ports over FEX-fabric port-channel
- PVLAN isolated and promiscuous trunk
- Support for 512 VLANs (512 minus number of VSANs configured)
- Native 802.1q VLAN tag
- ACL based QoS classification and Marking
- FCoE: Support for T11 based FIP
- CEE DCBX
- FCoE co-existence with VPC
- Support for SMI-S
- DCNM support

For more information about the features listed, see the Cisco Nexus 5000 Series and the Cisco Nexus 2000 Series documentation listed in the"Related Documentation" section on page 35.

Upgrade/Downgrade

This section describes issues you may encounter when you upgrade to or downgrade from the Cisco NXOS 4.1(3) N1(1) or later releases on the Cisco Nexus 5000 Series switch.

This section includes the following topics:

- Cisco NX-OS Release 4.1(3)N2(1a), page 7

- Cisco NX-OS Release 4.1(3)N2(1), page 7
- Cisco NX-OS Release 4.1(3)N1(1a), page 7
- Upgrading Power Sequencer, page 8
- Cisco NX-OS Release 4.1(3)N1(1), page 8

Cisco NX-OS Release 4.1(3)N2(1a)

When you downgrade from the Cisco NX-OS Releases 4.1(3)N2(1) or 4.1(3)N2(1a) to the Cisco NX-OS Release 4.1(3)N1(1) or 4.1(3)N1(1a), the **feature fc-port-security** command does not get converted to **feature port-security**. As a result, the FC port security configuration gets lost and remains disabled. As a workaround, after the downgrade to Cisco NX-OS Releases 4.1(3)N1(1) or 4.1(3)N1(1a), re-enable the FC port security feature by executing the **command feature port-security**. See CSCtd70554 for details.

When you upgrade to or downgrade from Cisco NX-OS Release 4.1(3)N2(1) and earlier releases to Cisco NX-OS Release 5.0(3)N1(1c) and above, a short delay might occur before the startup configuration is applied.

Cisco NX-OS Release 4.1(3)N2(1)

This section includes the following topics:

- Upgrading from Cisco NX-OS Release 4.1(3)N1(1), page 7
- Downgrading from Cisco NX-OS Releases 4.1(3)N2(1), page 7

Upgrading from Cisco NX-OS Release 4.1(3)N1(1)

Power cycle after an upgrade.

Downgrading from Cisco NX-OS Releases 4.1(3)N2(1)

When you downgrade from the Cisco NX-OS Release 4.1(3)N2(1) to the Cisco NX-OS Release 4.1(3)N1(1) or 4.1(3)N1(1a), the **feature fc-port-security** command does not get converted to **feature port-security**. As a result, the FC port security configuration gets lost and remains disabled. As a workaround, after the downgrade to Cisco NX-OS Releases 4.1(3)N1(1) or 4.1(3)N1(1a), re-enable the FC port security feature by executing the **command feature port-security**. See CSCtd70554 for details.

Cisco NX-OS Release 4.1(3)N1(1a)

Under certain conditions, a voltage spike exceeding the system voltage guard band and glitch filter settings may result in a power cycle of the system mezzanine board. This results in the failure of ports on the mezzanine board. For details, see CSCsy21017. To solve the issue, you need to upgrade to the Cisco NX-OS 4.2(1)N1(1) release to get the fix for CSCdy21017, and makes sure that power sequencer has been upgraded to V1.2 version (show version). For details, see Upgrading Power Sequencer, page 8.

Upgrading Power Sequencer

Under certain conditions, a voltage spike exceeding the system voltage guard band and glitch filter settings may result in a power cycle of the system mezzanine board. This results in the failure of ports on the mezzanine board.

To solve the issue, you need to upgrade to the Cisco NX-OS 4.2(1)N1(1) release and makes sure that power sequencer has been upgraded to V1.2 version (show version). For details, see CSCsy21017. If the switch is upgraded to the Cisco NX-OS 4.2(1)N1(1) release, but is not power-cycled as the procedure instructs, the switch will have instructions for power sequencer upgrade, but the power sequencer will not actually be upgraded. The show version will indicate a v1.2 power sequencer, but that only indicates the power sequencer upgrade instructions have been programmed. Therefore, if the switch admin cannot confirm the power off/on of the switch, it is advisable to perform a power off/on to ensure the power sequencer is actually upgraded.

The steps to upgrade the power-sequencer with the Cisco NX-OS release 4.2.(1))N1(1) are as follows, assuming the switch is on a version that can upgrade directly to release 4.2.(1))N1(1):

Step 1 Download the Cisco NX-OS Release 4.2.(1))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 release4.2.(1))N1(1). When prompted to confirm the upgrade, review the upgrade table and select y to proceed.

Step 3 After completing the installation, the system reloads and displays a Cisco NX-OS Release 4.2.(1))N1(1) image.

Step 4 Repeat step 2 to re-install the Cisco NX-OS Release 4.2.(1))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 5 After **install all** has completed installation, power-cycle the system. If you skip this step, the power-sequencer will not be updated till the next power-cycle.

Step 6 After the system comes up, confirm that the power-sequencer has been upgraded by running **show version**. The **show version** only confirms if the power-sequencer has the updated instructions. The updated instructions do not take effect if the system was not power-cycled.

Cisco NX-OS Release 4.1(3)N1(1)

This section includes the following topics:

- Upgrading from Cisco NX-OS 4.0(1a)N1-Based Releases to 4.1(3)N1-Based Releases, page 8
- Downgrading from Cisco NX-OS 4.1(3)N-Based Releases, page 9
- QoS Upgrade and Downgrade, page 9

Upgrading from Cisco NX-OS 4.0(1a)N1-Based Releases to 4.1(3)N1-Based Releases

When you upgrade your Cisco Nexus 5000 Series switch from Cisco NX-OS 4.0(1a)N1-Based Releases to 4.1(3)N1-Based Releases, the following occurs:

- QoS configuration will be automatically converted to the new syntax

- If an ACL has more than 549 ACEs then the ACL fails to get applied. This is due to a new limit on the number of ACEs in an ACL
- The Interface **fcoe mode on** command is deprecated.

Alternatively, you can contact Cisco Customer Support for help with upgrading and converting your configuration to the new format.

Downgrading from Cisco NX-OS 4.1(3)N-Based Releases

- Downgrade is only supported for the following releases:
  - Cisco NX-OS 4.0(1a)N1(1) release
  - Cisco NX-OS 4.0(1a)N1(1a) release
  - Cisco NX-OS 4.0(1a)N2(1) release
  - Cisco NX-OS 4.0(1a)N2(1a) release
- **Install all** will warn of all configurations that need be undone before proceeding.

Note Not all QoS configurations will be converted properly on downgrade. It is recommended that the QoS configuration be verified and re-applied after a downgrade.

QoS Upgrade and Downgrade

During an upgrade from 4.0(1a)N1-Based Releases to 4.1(3)N1-Based Releases, the class-maps, policy-maps, and service-policies with a particular name will be split up into multiple instances, each with a different type and associated match conditions/actions.

During a downgrade from 4.1(3)N1-Based Release, to 4.0(1a)N1-Based Release , the following will occur:

- Checks will occur during the **install all** before reboot, alerting you to delete any new CLI in this release.
- The class-maps, policy-maps, and service-policies of different types but sharing the same name are combined into a single instance.
  - For policy-maps, if the resulting entity cannot be attached onto an interface in 4.0(1a)N1-Based Releases, the attachment for the whole policy-map will fail

If a **type qos** policy is configured at an interface and a downgrade is performed to a 4.0(1a)N-based release, the installer does not generate a warning about the incompatibility of this configuration. As a result, the entire qos configuration will be lost after the downgrade. If the **type qos** policy is unconfigured prior to the downgrade, the configuration loss can be avoided

Installing Expansion Modules

When you install an expansion module on a Cisco Nexus 5000 Series switch , check the status of the module installation in the system logs, as follows:

```
e7-dut-1# show module
Mod Ports  Module-Type                      Model                  Status
--- -----  -------------------------------- ---------------------- ------------
1    40     40x10GE/Supervisor               N5K-C5020P-BF-XL-SU    active *
```

```
2    6      6x1/2/4/8G FC Module            N5K-M1060             ok
3    6      6x1/2/4/8G FC Module            N5K-M1060             ok

Mod  Sw              Hw      World-Wide-Name(s) (WWN)
---  --------------  ------  --------------------------------------------------
1    4.1(3)N2(1)     1.2     --
2    4.1(3)N2(1)     0.0     20:41:00:0d:ec:b4:6a:80 to 20:46:00:0d:ec:b4:6a:80
3    4.1(3)N2(1)     0.0     20:81:00:0d:ec:b4:6a:80 to 20:86:00:0d:ec:b4:6a:80

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    000d.ecb4.6a88 to 000d.ecb4.6aaf         JAF1314AQHR
2    000d.ecb4.6ab0 to 000d.ecb4.6ab7         JAF1325BBGE
3    000d.ecb4.6ab8 to 000d.ecb4.6abf         JAF1325BBJG
```

If the module is not seated properly, an error message is displayed as follows:

```
2009 Aug  3 23:45:16 Edge-2 %PFMA-2-MOD_INSERTION_FAILED: Module 2 insertion fai led.
Module might not be seated properly. Please try removing the module and the n
re-insert after five seconds or more.
```

For details see, the Expansion Modules section of the Cisco Nexus 5000 Series Hardware Installation Guide.

Limitations

This section describes the limitations in Nexus 5000 Series switches and the Cisco Nexus 2000 Series Fabric Extenders for the Cisco NX-OS releases 4.1(3)N1(1a), 4.1(3)N1(1) , 4.1(3)N2(1) and 4.1(3)N2(1a).

- After you downgrade from release 4.1(3)N1, the QoS configuration is not restored if the class-map name is dfferent for type qos, network-qos,or queuing policy-maps. Make sure the class-names between different policy types are the same before you begin downgrade. (For details see CSCsz93815)
- After a downgrade, the interface policy may silently get added to the system level without a warning message. This may change the entire qos queuing policy. As a workaround, remove the system policy BW/SPQ parameters, configure the queuing policy and add the parameters again to the interfaces. (For details see CSCta00231)
- DCBX fails to converge between a Nexus 5000 switch running 4.1(3)N1(1) and another Nexus 5000 switch running a 4.0(1a)N based release. As a result, priority-flow-control does not work on this link. There is no workaround. (For details see CSCta74119)
- When you downgrade from release 4.1(3)N1(1) to 4.0(1a)N-based releases using Fabric Manager or when you upgrade from a 4.0(1a)N-based release to 4.1(3)N1(1) using Fabric Manager error messages such as the following are generated:

  ```
  2009 Jul 19 15:32:55 N5K-C snmpd: SNMP Operation (GET) timed out. reqId
  (1448314586) errno (62) on iso.3.6.1.4.1.9.9.360.1.1.4.2.0
  2009 Jul 19 15:32:56 N5K-C snmpd: SNMP Operation (GET) failed. Reason:13 reqId
  (1448314586) errno (0) error index (1)
  ```

  There is no workaround. This is a display issue only. (For details see CSCta85268)

- The channel-group configuration is not applied to the Cisco Nexus 2000 downlink interface after downgrading to the Cisco NX-OS Release 4.1(3)N1(1) software. This happens if the **speed 1000** command is present under the context of the port-channel. As a workaround, reconfigure the **channel-group** command after the system comes up and reapply the config 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 that the frame ingressed into the switch with. There is no workaround.
- In large scale configurations some Cisco Nexus 2000 Series Fabric Extenders may take up to 3 minutes to appear online after a **reload** command is issued. 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, all host facing ports are connected and each host facing interface has large configuration (supporting 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 only used on inter-switch links but the FEX ports are only meant to connect to servers. Since 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 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.
- 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** will be applied on a spanned frame.
- Spanned Fibre Channel over Ethernet (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 Fibre Channel over Ethernet (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.

- VACLs of more than one type on a single VLAN are unsupported. 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 gets 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 overcome this situation, use IP ACLs to apply access control to IP traffic instead of using a MAC ACL that matches the Ethertype to Ipv4 or Ipv6.
- 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. This could cause ingress buffers to be exhausted leading to frames being discarded. Use the **shut** command to disable the slow-draining port.
- The multicast storm control functionality in the Cisco Nexus 5000 Series hardware 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.
- 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.

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

- Ports on a Fabric Extender (FEX) can be configured as a tx-source in one sesssion 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, and Interface Ethernet100/1/1 on a FEX 100 is already configuredas a tx-source on SPAN sesssion-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 aan 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, will be SPAN-ed. 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 mutlicast 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. This 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 can not be configured as a SPAN destination. Only a switch port can be configured and used as a SPAN destination.

Caveats

This section includes the following topics:

- Open Caveats, page 13
- Resolved Caveats—Cisco NX-OS Release 4.1(3)N2(1a), page 23
- Resolved Caveats—Cisco NX-OS Release 4.1(3)N2(1), page 24
- Resolved Caveats—Cisco NX-OS Release 4.1(3)N1(1a), page 25
- Resolved Caveats—Cisco NX-OS Release 4.1(3)N1(1), page 26
- Resolved Caveats—Cisco NX-OS Release 4.0(1a)N2(1), page 29
- Resolved Caveats—Cisco NX-OS Release 4.0(1a)N1(1), page 30
- Resolved Caveats—Cisco NX-OS Release 4.0(0)N1(2a), page 32
- Resolved Caveats—Cisco NX-OS Release 4.0(0)N1(2), page 33
- Resolved Caveats—Cisco NX-OS Release 4.0(0)N1(1a), page 34
- Resolved Caveats—Cisco NX-OS Release 4.0(0)N1(1), page 35

Open Caveats

This section lists the open caveats for this release.

- CSCtd58753

  Symptom: After adding & removing channel-group config on an mrouter port, multicast traffic flood to the port continues indefinitely, even after the PIM router or IGMP querier on the port has been removed (and the port is not an mrouter port anymore).

  Workaround: Perform **shut**, **no shut** on the ffected interface.

- CSCtd70554

  Symptom: When you downgrade from the Cisco NX-OS Releases 4.1(3)N2(1) or 4.1(3)N2(1a) to the Cisco NX-OS Release 4.1(3)N1(1) or 4.1(3)N1(1a), the **feature fc-port-security** command does not get converted to **feature port-security**. As a result, the FC port security configuration gets lost and remains disabled.

  Workaround: After the downgrade to Cisco NX-OS Releases 4.1(3)N1(1) or 4.1(3)N1(1a), re-enable the FC port security feature by executing the **command feature port-security**.

- CSCtd15304

  Symptom:When you perform a Cisco Nexus 5000 series switch software install using the Fabric Manager, the Success Reset status message is shown just before the switch reboots.

  Workaround: To determine the status of the software install, do the following:

  – Close the wizard and go to the main FM screen

  – Click on the Rediscover...button in the toolbar and wait for the rediscovery to complete. Once the rediscovery is complete, you may encounter either of the scenarios :

  • If the topology shows the switch with a cross, the switch is rebooting/down. Wait for some time and repeat the second step again.

  If the topology shows the switch as discovered/managed, select the corresponding fabric tree node from the Logical Domains tree. In the right hand side panel, under the Switches tab information about the switches along with their current versions is displayed. Use this to confirm the status of the software install.

- CSCta77490

  Symptom: When the type of a pvlan is toggled from being a regular vlan to a pvlan and back to regular vlan in very small interval of time, the type change fails.

  Workaround: Issue the type change commands with a 5 seconds gap in between.

- CSCtb34546

  Symptom: When a PACL with **deny ip any any** is applied on mgmt0, CFS discovery gets stuck.

  ```
  ip access-list ip1
     10 deny ip any any
  ```
  Applying such a ACL on the mgmt0

  ```
  int mgmt 0
    ip access-group ip1 in
  ```
  would cause this issue.

  Workaround: Remove the **deny ip any any** rulefrom the PACL applied on mgmt0 interface.

- CSCtb61197

  Symptom: When a port-channel provisioning fails because the system has reached the limit of number of port-channels supported, output of **show san-portchannel** will still display the port-channel as present but **down**. The port-channel will be seen as **down** even if the member interface is operationally up because it could not be provisioned correctly due to resource limitation.

  Workaround: None.

- CSCtc44231

  Symptom: LACP port-channel doesn't come up. A vlan is deleted from the switch which is also configured as native vlan for the lacp port-channel.

  Workaround: Create the vlan or remove the native vlan config from the lacp port-channel.

- CSCtc77180

  Symptom: Ports are error disabled with error **Ethernet interface not present** if f**eature fcoe** is enabled immediately after the switch prompt comes up on bootup.

  Workaround: Enable **feature fcoe** after confirming that the interfaces are displayed in the output of **show interface brief**.

- CSCtb58641

  Symptom: If a mac-address moves from an isolated host port to a promiscous trunk port, in certain conditions, the mac-address is never cleared from the system.

  Workaround: None

- CSCtc36345

  Symptom: CDP is not supported over downlink interfaces of a dual-homed Nexus2K fabric extender. But **show cdp neighbor** sometimes displays information about neighbors on one of the vPC peer switches.

  Workaround: Disable CDP on the N2K host interfaces.

- CSCtc09510

  Symptom: On bootup of the switch, some of fex host interfaces go into BPDU errdisable state even when BPDU filter is enabled on that interface. This happens when BPDUs are received and processed on an interface, on bootup, before the BPDU filter configuration is applied.

  Workaround: Bring the interface(s) administratively down and re-enable them.

  ```
  switch# configure terminal
  switch(config)# interface ethernet 109/1/1
  switch(config-if)# shut
  switch(config-if)# no shut
  ```

- CSCtc36397

  Symptom: Changing the role-priority and flapping the peer-link does not change the roles of the vPC peers. This happens when one of the switch has its role as Operational primary due to an earlier reload of the primary switch.

  Workaround: None

- CSCtb84512

  Symptom: In mixed span mode where ethernet port-channel, vfc and FC ports are span sources and ethernet interface is a span destination, vfc flap causes the traffic coming in on ethernet port-channel to be not spanned.

  Workaround: Remove and add span source command for the ethernet port-channel.

- CSCtb94310

  Symptom: With a san port-channel as the source and ethernet interface as the destination, removing the channel-group config from the san port-channel member causes monitor session to go to error state.

  Workaround: Unconfigure and reconfigure the monitor session.

- CSCtb53820

  Symptom: After **save** and **reload** with a monitor session configuration where source is a vsan and destination is an fc port, the monitor session goes to error state.

  Workaround: Unconfigure and reconfigure the monitor session.

- CSCtb95741

  Symptom: vPC configured on a port-channel with FEX host interface as a member does not come up. The **show vpc inconsistency** shows STP parameters as mismatched.

  This happens when you configure port-channel on FEX host interface, configure spanning tree parameters (for example **port-type edg**e) on the port-channel and configure vpc on the the port-channel.

  Workaround: First, remove the vpc config on the port-channel and remove spanning tree parameters on the port-channel. Next, configure vpc on the port-channel and add spanning tree parameters, if needed.

- CSCtd02411

  Symptom: The vfc interface **description** command is not restored after upgrade.

  Workaround: Reconfigure the vfc interface **description** command after upgrade.

- CSCtc04213

  Symptom: Vlan related configurations do not get applied on a range of interfaces. This issue may occur when you try to configure a vlan configuration on a range of interfaces in a way that the number of interfaces being configured at a time is greater than 192. As a result, even though the vlan configuration command returns with no errors on the console, the vlans do not get aplied to the interfaces. You can confirm this by running the cli, **show system internal ethpm info interface** *one of affected*

  Workaround: Select a smaller range of interfaces to apply the vlan configuration to.

- CSCsz82199

  Symptom: You cannot enable std.pause on a port-channel interface connected between two Cisco Nexus 5000 Series switches. Enable std.pause between two Cisco Nexus 5000 Series switches and configure std.pause in the hardware.

  Workaround: None

- CSCsv39939

  Symptom: Incorrect values are displayed for interface capabilities for ports for Cisco Nexus 2000 Series Fabric extenders connected to a Cisco Nexus 5000 Series switch. In particular, the number of input and output queues for the ports are displayed as zero instead of two.

  Workaround: This is a display issue and does not impact functionality.

- CSCsz81365

  Symptom: SPAN session should stop reflecting packets as soon as mapping is removed.

  Workaround: None.

- CSCta04383

  Symptom: When you install a new image from one of two vPC switches, the vPC switch gets upgraded. Also, each of the connected Fabric Extenders update their firmware with the new version, but continue to run the current version and stay connected to the other vPC switch. When you reload the upgraded switch, but revert back to the older version of software on the switch, both the vPC

switches and all the Fabric Extenders run the older version of software. However, the Fabric Extenders have the more recent version of software in the firmware. When the Fabric Extenders reload there is loss of connectivity with the hosts.

Workaround: Re-install the older version of software from either of the two switches while the Fabric Extenders are connected to that switch.

- CSCsx35870

  Symptom: The CLI times out when a large number of VLANs are created and deleted followed by PVLAN creation and deletion. The system indicates that the Ethernet Port Manager (ethpm) has timed out to communicate with the SPAN manager or PVLAN manager. As a result, some of the PVLAN interfacse will be error disabled.

  Workaround: Perform **shut** and **no shut** on the error disabled interfaces.

- CSCsx59489

  Symptom: Call home notifications for events generated when both a switch and a Fabric Extender are rebooting may contain a timestamp of January 1 1970 as shown in the following example:

  ```
  System Notification from sample-system - environment:minor - 1970-01-01 00:00:00
  GMT+0000
  ```

  The most likely scenario where this would occur is after a power failure or after issuing the **reload all** command. The event is generated before the Fabric Extender connects with the switch and before the local time is updated for the Fabric Extender.

  Workaround: None.

- CSCsx60187

  Symptom: Configure duplicate IP address for multiple SVI interfaces.

  Workaround: Do not configure two or more SVIs with the same IP address.

- CSCsx80279

  Symptom: When traffic is sent at line rate as a single burst, all addresses are not learned when egress interfaces are FEX facing ports. This problem does not occur if sustained traffic is sent for more than 0.4 seconds.

  Workaround: Resending the unlearned MAC addresses would render them relearned.

- CSCsy99816

  Symptom: When a Cisco Nexus 2000 Fabric Extender is already online and a fabric interface that is not part of a port channel is configured with a serial number that does not match that of the FEX, the fabric interface will be brought down, and **show interface fex** does not display the reason for being down.

  Workaround: None. This is a display issue.

- CSCsy02439

  Symptom: Under some circumstances, the FC MAC driver displays the following error message:

  ```
  %KERN-3-SYSTEM_MSG: FCP_ERRFCP_PORT: gat_fcp_isr_ip_fcmac_sync_intr@424, jiffies =
  0x1c422:Unknown intr src_id 41 - kernel
  ```

  The error message is when an unused interrupt in the MAC fires. The error message does not indicate any functional problem.

  Workaround: None

- CSCsx68778

  Symptom: You cannot configure commands under the interface range

  Workaround: Configure command sunder HIF ports of one FEX at a time.

- CSCsx60187

  Symptom: Duplicate IP addresses are configured for multiple SVI interfaces.

  Workaround: Do not configure two more SVIs with the same IP address.

- CSCsx35870

  Symptom: The CLI times out when large number of VLANs are created and deleted followed by PVLAN creation and deletion. The system will syslog indicating that Ethernet Port Manager (ethpm) timing out to communicate with SPAN manager or PVLAN manager. As a result, some of the PVLAN interfaces will be error disabled. FEX ports are configured as a member of PVLAN and some of them are member of regular VLAN.

  Workaround: Perform **shut** and **no shut** on the error disabled interfaces.

- CSCsx40562

  Symptom: ACL drop traffic with 802.1p cos values greater than 3 may not get spanned if all four user qos classes are not configured in **system qos service-policy** configuration.e

  Workaround: Configure all four user qos classes (except **class-default** and **class-fcoe**) under **system qos service-policy** to span all ACL drop traffic.

- CSCsw21301

  Symptom: Cisco NX-OS does not provide offline configuration support. The creation of a FEX interface depends on the FEX coming online after a fabric interface configuration. When you restore configuration from a file, there periodwhen FEX interfaces are not yet created but interface configuration is applied and fails.

  Workaround: If system configuration is to be restored from a configuration file (copied locally or through tftp), you can separate the FEX interface part of the configuration (if any) into a different file. Copy the main file first, then wait for FEX to come online, and then copy the separate FEX interface configuration file. Alternately, you can copy twice.

- CSCsv93263

  Symptom: Cisco NX-OS does not provide offline configuration support. The creation of a FEX interface depends on the FEX coming online after a fabric interface configuration. When you restore configuration from a file, there periodwhen FEX interfaces are not yet created but interface configuration is applied and fails.

  Workaround: If system configuration is to be restored from a configuration file (copied locally or through tftp), you can separate the FEX interface part of the configuration (if any) into a different file. Copy the main file first, then wait for FEX to come online, and then copy the separate FEX interface configuration file. Alternately, you can copy twice.

- CSCsv81694

  Symptom: The auto learn static MAC entry is removed if the port on which the same MAC address is dynamically learned is flapped. The static MAC address is removed from the software as well as the hardware.

  Workaround: Re-add the static MAC entry through the CLI.

- CSCsv56881

  Symptom: Each Switched Virtual Interface (SVI) for inband management must be configured with a different IP address. IPv6 has an error check feature. When an administrator enters a duplicate IPv6 address across two SVIs, the software fails the command due to the duplicate address. A similar error check should exist for IPv4 address configuration on SVIs.

  Workaround: Do not configure duplicated IPv4 or IPv6 addresses.

- CSCsv02866

  Symptom: The command s**how interface ethernet transceiver details** may show invalid calibration for DOM-supported 1 G SFP.

  Workaround: None.

- CSCsv00989

  Symptom: The **show interface ethernet transceiver details** command may show all zero values for a DOM-capable 1 G SFP.

  Workaround: None.

- CSCsu77946

  Symptom: Within a configuration session, when you enable statistics on the PACL add more than 252 ACES to the ACL, and apply it to an interface, an error message is generated as the statistics counter is exhausted. Even if you try to remove the statistics keyword, it does not get removed. The result is that the ACL cannot be applied to the interface. This problem occurs only with a configuration session, and only after a configuration failure.

  Workaround: Reduce the size of the ACL (fewer than 252 ACES) and re-apply the ACL to an interface. The statistics keyword will still remain and consume hardware resources.

- CSCsv19979

  Symptom: Any FC port set to SD mode does not come up until the speed is configured manually. The port goes into the error disabled state and the only way to bring it online as SD is to manually set the speed 2 G or 4 G.

  Workaround: Configure the speed manually to 2 G or 4 G.

- CSCsr20499

  Symptom: When you restore a configuration to running-config from a configuration file, ACL manager may leak memory. The size of the leak is related to the size of ACL configurations and the number of times the restoration occurs. The switch may reboot if the ACL configuration is very large and the restoration occurs too many times.

  Workaround: None.

- CSCsq64251

  Symptom: TACACS+ fails if the user name input at login initiates a directed request authentication. The syntax to authenticate a directed request to a switch is **username@**(*IP address or name of TACACS+ server*).

  Workaround: Use RADIUS for directed request authentication.

- CSCsq76688

  Symptom: The neighboring device for the Cisco Discovery Protocol (CDP) is not removed after shutting down the port for CDP hold time interval.

  Workaround: None.

- CSCsl62545

  Symptom: The fan LED on the Device Manager displays in amber color even though the fan is operating properly.

  Workaround: None.

- CSCsr28868

  Symptom: When the Fibre Channel over Ethernet (FCoE) feature is disabled, any untagged Ethernet packet with 00 00 in the Ethertype/length field is treated as an invalid packet and is forwarded out with a bad Ethernet CRC.

  Workaround: None.

- CSCsr35452

  Symptom: When the **ntp peer** command is configured on the MDS fabric and is distributed using CFS, the Nexus 5000 Series switch appends an incorrect VRF name **AC** to the command instead of **VRF management**.

  Workaround: Use the **ntp server** command to synchronize time across the fabric.

- CSCsr36661

  Symptom: When IGMP group membership is statically configured with private VLAN (PVLAN) host ports, the hardware gets programmed correctly. However, the membership information is not programmed for PVLAN host ports after the switch is reloaded.

  Workaround: Delete and add the private VLAN association once again

- CSCsr68690

  Symptom: When an egress SPAN is configured on a port transmitting jumbo or large frames, the spanned frames are truncated to 2384 bytes.

  Workaround: None.

- CSCsl21529

  Symptom: An incorrect MTU value is displayed in the **show interface** command output. The Cisco Nexus 5000 Series switch only supports class-based MTU. Per-interface level MTU configuration is not supported. The switch supports jumbo frames by default. However, the **show interface** command output currently displays an incorrect MTU value of 1500 bytes.

  Workaround: None.

- CSCsm03765

  Symptom: The Set operation on the CISCO-IP-IF-MIB is not supported. You cannot set the mgmt0 IP address using SNMP.

  Workaround: Use the CLI to set the mgmt0 IP address.

- CSCsm16222

  Symptom: CFS does not support roles configuration distribution. Enter the **show cfs application** command to see the registered applications.

  Workaround: Any features not registered with CFS need to be configured locally on the switch.

- CSCsl73766

  Symptom: CFS does not support RADIUS configuration distribution. Enter the **show cfs application** command to see the registered applications.

  Workaround: Any features not registered with CFS need to be configured locally on the switch.

- CSCso25966

  Symptom: When an LACP port channel is configured between Catalyst 6500 and Cisco Nexus 5000 Series switches, and the configurations on both sides of the port channel do not match, the Catalyst 6500 LACP ports may change to the errordisable state.

  Workaround: Fix the configuration to make it consistent on both peer switches of the port channel, and perform a **shut** and **no shut** operation on the Catalyst 6500 port channel interface.

- CSCso27446

  Symptom: When a **shutdown** command is issued to the mgmt0 interface on a Cisco Nexus 5000 Series switch, the link never goes down and the remote end does not indicate that the link is down.

  Workaround: None.

- CSCso46345

  Symptom: The current version of NX-OS software running on the Cisco Nexus 5000 Series switches does not support Brocade i10K interop mode 4. The i10k v9.2.0.8 is supported by MDS in SAN-OS 3.2(2c), and 3.2(3) with interop mode 1 and 4.

  Workaround: None.

- CSCso74872

  Symptom: When two SNMP walks are started simultaneously, one of them may fail with the following error:

  ```
  OID not increasing
  ```

  This problem does not occur with a single SNMP walk.

  Workaround: This is not a permanent failure. Restart the walk and the problem will not occur as long as there is no other SNMP walk in progress.

- CSCso84269

  Symptom: Occasionally, when reload is executed after bootup, and there has been no configuration change, the switch will display the following warning:

  ```
  'WARNING: There is unsaved configuration!!!'
  ```

  Workaround: Enter the **copy running startup** command. The problem will disappear.

- CSCsq10026

  Symptom: When the small form-factor pluggable (SFP) is not in the Ethernet port, the **show interface** command output displays a bandwidth of 1 Gbps. When the SFP is plugged in, the bandwidth is displayed correctly (10 Gbps).

  Workaround: None.

- CSCsq17571

  Symptom: When an SNMP user creates or deletes virtual interface group (VIG), virtual Ethernet (VEth) or virtual FC (VFC) interfaces, the accounting log displayed by the **show accounting log** command does not get updated.

  Workaround: Use the CLI for the configuration, which will update the accounting log.

- CSCsq35527

  Symptom: When IGMP snooping is enabled on a switch, and the switch is the STP root and an STP topology change occurs, the IP multicast traffic may take a long time to converge. During this time, the IP multicast traffic may get affected.

Workaround: Configure a shorter query interval on the IGMP router to reduce the time it takes for ip-multicast traffic to converge in this topology.

- CSCsq35728

  Symptom: When a SAN port channel is created, the following syslog message is displayed:

  ```
  2008 May 20 06:09:13 switch %PORT_CHANNEL-3-MSG_SEND_FAILURE: failed to send
  MAP_PARAM_FROM_CHANNEL to sap 45: Broken pipe"
  ```

  There is no functionality loss and this message can be ignored.

  Workaround: None.

- CSCso01268

  Symptom: The following error message is displayed when a module is hot-swapped out:

  ```
  2005 Jan  1 00:08:23 switch %KERN-4-SYSTEM_MSG: SI-VDC map entry <0, 0x0> does not
  exist! - kernel"
  ```

  There is no functionality loss and the message can be ignored.

  Workaround: None.

- CSCsq57558

  Symptom: Enhanced Inter Switch Link (EISL) encapsulation is not supported on a Fibre Channel SPAN destination port. When EISL encapsulation is configured on the SPAN destination (SD) port, a VFT header is added to the packets going out of the SD port. The VFT header has VSAN information that helps distinguish traffic for various VSANs. This applies to any Fibre Channel SPAN source. By default, EISL encap is not added and packets are sent out without a VFT header, and independent of the type of SPAN source port. For a Cisco Nexus 5000 Series switch, the **switchport encap** EISL command does not have any effect.

  Workaround: Use the Ethernet SPAN destination port to SPAN Fibre Channel traffic. FCoE packets going out of the Ethernet SPAN destination port will contain VSAN information in the Ethernet VLAN tag.

- CSCsq90423

  Symptom: EISL encapsulation is not supported on Fibre Channel SPAN destination port in NPV mode. When EISL encapsulation is configured on the SPAN destination (SD) port, a VFT header is added to the packets going out of the SD port. The VFT header has VSAN information, which helps distinguish traffic for various VSANs. This applies to any Fibre Channel SPAN source. By default, EISL encapsulation is not added and packets are sent out without a VFT header, and independent of the type of SPAN source port. For a Cisco Nexus 5000 Series switch, the **switchport encap** EISL command does not have any effect.

  Workaround: Use the Ethernet SPAN destination port to SPAN Fibre Channel traffic. FCoE packet going out of the Ethernet SPAN destination port will contain VSAN information in the Ethernet VLAN tag.

- CSCsv93922

  Symptom: If the modulo(%) operator is used in a Cisco Nexus 2000 Series Fabric Extender description the **show fex <fex-id>** command brings up the following error message

  ```
  ERROR: bad format: non escaped % not followed by 's'.
  ```

  Workaround: Remove the modulo(%) operator from the Cisco Nexus 2000 Series Fabric Extender description

- CSCsv95478

  Symptom:The Cisco Nexus 2000 Series Fabric Extender pinning redistribute command does not wait for user prompt with a yes or no operation.

  Workaround: None.

- CSCsv15775

  Symptom: When priority tagged frames are received on Cisco Nexus 2000 Series Fabric Extender ports, they are dropped and not forward on the nativeor default VLAN of the port. The MAC addresses are not learned.

  Workaround: None.

- CSCsu48008

  Symptom: When a Virtual Fibre Channel (VFC) interface is down, the **fcIfOperStatusCause** MIB object does not report the correct reason.

  Workaround: Get the OperStatus from the CLI using the **show interface vfc x** command.

- CSCsu01188

  Symptom: No traps are sent when SFPs for Gigabit Ethernet and 10-Gigabit Ethernet are removed or inserted.

  Workaround: None.

- CSCta13997

  Symptom: When vpc peer-link is down on Cisco Nexus 5000 Series switches, ports fail to come up on a Cisco Nexus 2000 Fabric Extender that is dual homed to the Nexus 5000 Series switches with vPC.

  Workaround: Restore the peer-link before making new connections to the Cisco Nexus 2000 Fabric Extender.

- CSCth93531

  Symptom: The show port-channel load-balance command shows the correct output only when the source interface is specified.

  Workaround: None.

Resolved Caveats—Cisco NX-OS Release 4.1(3)N2(1a)

This section lists the resolved caveats for this release.

- CSCtd41571

  Symptom:

  When an Ethernet port connected to an FIP snooping bridge is flapped on the Cisco Nexus 5000 series switch, the host connected to the FIP snooping bridge may not be able to rediscover the targets.

  Workaround: To clear the issue, perform **shut**, **no-shut** of the VFC interfaces for the CNAs being serviced over the FIP snooping bridge.

- CSCtd35046

  Symptom:The Cisco Nexus 5000 series switch does not support Class-2 FC. However a Class-2 FLOGI from an AIX server is not being rejected. As a result, the AIX host does not proceed to performing a Class-3 FLOGI. This prevents the AIX host from logging into the SAN fabric.

Workaround: None

- CSCtd00699

  Symptom:

  An industry-wide vulnerability exists in the Transport Layer Security (TLS) protocol that could impact any Cisco product that uses any version of TLS and SSL. The vulnerability exists in how the protocol handles session renegotiation and exposes users to a potential man-in-the-middle attack.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20091109-tls.shtml.

- CSCtd64019

  Symptom:'The **show tech-support** command causes the lacp process to crash and reboot the switch. This is suspected to happen when an ethernet expansion module is hotswapped with an FC expansion module but the insertion of the FC expansion module does not go through due to a seating error.

  Workaround:Reseating the FC module properly until it is online will avoid the crash.

- CSCtd74877

  Symptom:Creating indications subscription from third party tool CimNavigator fails.No special conditions needed to see issue.

  Workaround:None.

- CCSCtd07295

  Symptom: When routers that run PIM are connected to Cisco Nexus 5000 switches on non vPC ports the routers will fail to establish PIM adjacency. This is caused due to the Cisco Nexus 5000 switch discarding PIM hello messages on the vPC peer-link. This occurs when IGMP snooping is enabled on a Cisco Nexus 5000 switch.

  Workaround: Change the topology to connect the routers on vPC ports.

Resolved Caveats—Cisco NX-OS Release 4.1(3)N2(1)

This section lists the resolved caveats for this release.

- CSCsv93278

  Symptom:The **logging server vrf** command works only with the management vrf. There is no functional impact if the syslog is to be sent over management vrf.

  Workaround: None.

- CSCta78541

  Symptom:

  VSH crashes and generate a core when you do the following:

  ```
  attach fex 102
  show system error-id list
  ```

  The Cisco Nexus 2000 Fabric Extender does not reload and the core does not impact the functionality of the Fabric Extender.

  Workaround: None

- CSCtc07689

  Symptom: Upgrade the primary and secondary switches with the FEX A-A set up simultaneously to the Cisco NX-OS Release 4.1(3)N1(1) or Cisco NX-OS Release 4.1(3)N1(1a) image. When both the switches come up, the Cisco Nexus 2000 downlink interface configs are lost.

```
d14-switch-2(config)# show running-config interface eth100/1/1-2
version 4.1(3)N2(1)
interface Ethernet100/1/1
interface Ethernet100/1/2
```

  Workaround: To avoid this issue, follow the instructions in the *Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide* to upgrade the switches one after the other. If this issue was encountered after an upgrade or a downgrade, reconfigure the Cisco Nexus 2000 downlink interfaces after **show fex** shows the Fabric Extender as **Online**.

- CSCtc06403

  Symptom: The **cli show sprom module 3** causes the Cisco Nexus 5010 switch to crash. The crash is a result of a crash of pfma services.

  Workaround: The Cisco Nexus 5010 switch has only one slot for a pluggable module. Do not use the **show sprom module 3** on the Cisco Nexus 5010 switch.

Resolved Caveats—Cisco NX-OS Release 4.1(3)N1(1a)

This section lists the resolved caveats for this release.

- CSCsy21017

  Symptom: The Cisco Nexus 5020 switch may experience problems with most or all ports on the mezannine card and may display the following error messages:

```
 2009 Feb 22 06:35:00 switch %NOHMS-2-NOHMS_DIAG_ERROR: Module 1: Runtime diag
detected major event: Fabric port failure Ethernet2/4
2009 Feb 22 06:35:00 switch %NOHMS-2-NOHMS_DIAG_ERROR: Module 1: Runtime diag
detected major event: Fabric port failure Ethernet2/5
16) TestFabricPort :
Eth    1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20
    Port ------------------------------------------------------------
           F  F  .  .  F  F  .  .  F  F  .  .  F  F  .  .  F  F  .  .
Eth   21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40
    Port ------------------------------------------------------------
           F  F  .  .  F  F  .  .  F  F  .  .  F  F  .  .  F  F  .  .
19) TestFrontPort :
Eth    1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20
    Port ------------------------------------------------------------
           F  F  .  .  F  F  .  .  F  .  .  .  F  F  .  .  F  F  .  .
Eth   21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40
    Port ------------------------------------------------------------
           F  F  .  .  F  F  .  .  F  F  .  .  F  F  .  .  F  .  .  .
```

  Workaround: None.

- CSCtb90384

  Symptom: When you upgrade from the Cisco NX-OS Release 4.1(3)N1(1), the installer may fail to upgrade the BIOS and displays the following error message:

```
Module 1: Refreshing compact flash and upgrading bios/loader/bootrom/power-seq.
Warning: please do not remove or power off the module at this time.
Note: On success of power-seq upgrade, please power-cycle the system.
[#                   ]   0% -- FAIL. Return code 0x4071000F (BIOS source image
corrupt).
```

```
CAUTION: The BIOS/loader/bootrom of above module may be in corrupted state. Please try
programming it again and DO NOT reboot without programming it successfully, otherwise
you have to manually take out the flash from the card and program it in a BIOS
programming station.
```

Upgrade of the rest of the system continues successfully. This issue can be seen on both the Cisco Nexus 5020 and the Cisco Nexus 5010 switches.

Workaround: Once the system comes back up after the upgrade, re-install the upgraded image (follow the upgrade instructions from the user guide) associated with that release.

- CSCta07153

  Symptom: IGMP snooping cannot detect mrouter ports based on PIM Hellos. PIM Hellos are sent from a Catalyst 600 on a trunk port. IGMP snooping does not create an mrouter port for the received PIM Hellos. The **show ip igmp snooping mrouter** and **show ip igmp snooping statistics** indicate that IGMP snooping did not receive any PIM hellos.

  Workaround: Statically make the port a router port using the **vlan** mode command:

  ```
  switch(config-vlan)# ip igmp snooping mrouter interface ethernet x/y
  ```

- CSCtb71126

  Symptom: The IBM director does not detect the Cisco Nexus 5010 or the Cisco 5020 switch. The IBM director queries ipAdEntIfindex field of the IpAddrTable MIB to acquire management context for the switch. Since this query returns an invalid value, the IBM director is unable to proceed with the discover process.

  Workaround: None.

- CSCtb91500

  Symptom: The Cisco Nexus 5000 switch corrupts packets having ethertype 8880, 8881, 8882 and 8890. When a packet of ethertype 8880, 8881, 8882 or 8890 approaches a Cisco Nexus 5000 switch, the packet is modified at the egress in a way that the frames CRC is incorrect.

  Workaround: None.

- CSCtb05020

  Symptom: The vPC peer-link does not come up. The system runs out of resources needed to bring up the vPC peer-link and the following syslog is displayed:

  ```
  FWM_OIFL_MCAST_IDX_LIMIT_REACHED
  ```

  Workaround: None

- CSCtb94329

  Symptom: Running the **show vlan** or the **show vlan id vlan number** cli causes the vlan-mgr to crash and the switch to reset. This may occur if the interfaces are down (due to admin-shut or link failure) in a way that there are several discontinuities within a range of interfaces.

  Workaround: None.

Resolved Caveats—Cisco NX-OS Release 4.1(3)N1(1)

This section lists the resolved caveats for this release.

- CSCsx39376

  Symptom: If user is created w/ AES privacy password and login without the privacy password, user won't be able to delete any normal user. System will just times out

Workaround: If user is created w/ A

- CSCsw39639

  Symptom: When a rule that refers to a specific interface name (e.g. Ethernet 1/1) is entered in the role definition CLI, the command could hang. Ctrl-C can be issued to get back the CLI prompt.

  Workaround: Do not configure rules that refer to specific interfaces in the role definition CLI.

- CSCsv13371

  Symptom: Interface reset and clearing counters do not get updated.

  Workaround: None

- CSCsv65911

  Symptom: The RMON alarm configuration is not shown when issuing show running-config. This is only a show issue, the configuration gets saved correctly with copy running-config startup-config and is restored correctly after a reload.

  Workaround: None.

- CSCsw64952

  Symptom: If the Cisco Nexus 5000 Series switch has more than 3K STP instances and an STP hello time of 1 second is used in the Bridge assurance configuration, the STP may not converge.

  Workaround: Use aa STP hello time of 2 second in the Bridge Assurance mode.

- CSCsx67695

  Symptom: When a gatos expansion module (GEM) port has an interface policy configuration that is consistent with the system policy, then when the GEM is removed from the switch, the system policy is changed to a new one. When the GEM is inserted into the switch, there can be an inconsistency between the GEM port interface policy and the new system policy (the new system policy may not have a system class that was in the old system policy). No error is reported for this inconsistency.

  Workaround: Remove the GEM port interface policy, fix the interface policy, then reapply to the GEM port.

- CSCsx39481

  Title: After **vlan intf delete**, its ipv6 address cannot be added to a diff.

  Symptom: After deleting an up vlan interface which contains an ipv6 address, you cannot add the same ipv6 address to another vlan interface. This is only seen with ipv6 addresses.IPV4 addresses do not have this problem.

  Workaround: Bring back the deleted VLAN interface, delete the IPv6 address and then delete the VLAN interface again. Followed by the addition of the same IPv6 address on a different VLAN interface.

- CSCsx54086

  Symptom: If source-vlan is configured for a monitor session and a downgrade is done from 4.0(1a)N2(1), the source-vlan configuration will be lost. The impact is the src-vlan traffic may not get spanned as desired after downgrade.

  Workaround: After downgrade, reconfigure the source-vlan configuration for a monitor session

- CSCsx54270

  Symptom: When upgrading to 4.0(1a)N2(1), if all cos values map to no-drop classes in the **system qos service-policy** configuration, the service-policy application will fail. The impact is the traffic may not conform to the expected behavior after upgrade.

Workaround: After upgrade, reconfigure the policymap to include atleast one cos in a non no-drop class and reapply policymap to **system qos service-policy** configuration.

- CSCsv52871

  Symptom: When multiple FEX host ports congest FEX uplinks with no-drop class of traffic, pause asserted on the FEX host ports is uneven. As a result, traffic from some FEX host ports observe a better throughput than others.

  Workaround: None

- CSCsx24526

  Symptom: When a FEX host port is congested, an uncongested port in the same block of 8 ports will experience some traffic loss. The loss varies based on how many sources are trying to congest the congested port.

  Workaround: None

- CSCsv24214

  Symptom: When downgrading a Cisco Nexus 5000 Series switch from running a 4.0(1a)N1 image to a 4.0(0)N1(1) or 4.0(0)N1(1a) image, the startup configuration is not restored. This is caused by the defect CSCsq74395, which was resolved in 4.0(0)N1(2) and 4.0(0)N1(2a).

  Workaround: After a downgrade, manually copy the startup configuration to the running configuration and reboot the system.

- CSCsv10783

  Symptom: The s**how startup-config** command does not show the correct mode for a channel group. It shows the current mode for the channel group. The correct mode is stored. On a subsequent reload, the correct mode is configured on the channel group. The **show startup-config** always shows the current mode instead of the mode that was saved to startup. On a subsequent reload, the correct mode is configured. This is only a show command issue.

  Workaround: None.

- CSCsu93313

  Symptom: Within a configuration session, 125 unique VACLs are created with a total of 1023 TCAM entries. The verify command fails with the following message:

  ```
  d2-switch-2(config)# configure session 30
  Config Session started, Session ID is 1
  d2-switch-2(config-s)# verify
  Failed to start Verification: Message Timed Out
  d2-switch-2(config-s)# commit
  Failed to complete Verification: no free label
  ```

  This problem occurs with large VACL configurations. Once the Cisco Nexus 5000 Series switch is in this state, subsequent VACL configurations fail.

  Workaround: Reload to recover the configuration.

- CSCsv00402

  Symptom: When you downgrade from the Cisco NX-OS 4.0(1a)N1 release to a previous software release, any static IGMP entries that have been configured over an Ether channel are lost after the downgrade.

  Workaround: After you downgrade to the previous release and reload the switch, reconfigure any static IGMP groups configured over an etherchannel. Alternately, you can also do a **copy startup running** to reload the startup configuration. After that do a **copy running startup** to make sure the static IGMP entries are re added properly to the startup configuration.

- CSCsr64291

  Symptom: When a port is congested due to traffic from multiple inputs, the traffic mapped to a user-defined QoS class can get discarded at a very slow rate (fewer frames per second) in spite of being configured with strict priority scheduling.

  Workaround: None.

- CSCsw79515

  Symptom: If a Cisco Nexus 2000 Series Fabric Extender is power cycled multiple times in quick succession, some links between the Cisco Nexus 5000 Series switches and the Cisco Nexus 2000 Series Fabric Extenders may go into an error disabled state.

  Workaround: Fabric ports recover after few seconds. No user intervention is required.

- CSCsw66216

  Symptom: When member fex-fabric ports are added or removed from a channel-group, frames could be lost for few seconds until the Cisco Nexus 5000 Series switch and the Cisco Nexus 2000 Series Fabric Extender complete updating port-channel forwarding configurations. This impacts existing traffic that is being redistributed to new port-channel member ports due to the configuration change.

  Workaround: None.

Resolved Caveats—Cisco NX-OS Release 4.0(1a)N2(1)

This section lists the resolved caveats for this release.

- CSCsv70815

  Symptom: The default VRF is the system default for a VRF setting. Ideally, applications using VRF (such as TACACS+) assume a default VRF value if a VRF configuration is not specified by the administrator. However, TACACS+ is not set up properly unless the default VRF is configured.

  Workaround:

  The Cisco Nexus 5000 Series switch supports two possible VRFs, the default and the management. Configure the desired VRF when using TACACS+ service. You can configure the desired VRF using either of these configurations:

```
aaa group server tacacs+ t1
    server 10.193.149.54
    use-vrf management

aaa group server tacacs+ t2
server 20.1.1.2
use-vrf default
```

- CSCsv55655

  Symptom: When the Cisco Nexus 5000 Ethernet port is configured in the 1 G mode of operation using the **speed 1000** command, it does not advertise and auto-negotiate the flow-control configuration. As a result, the link peer does not learn about the capabilities of the Cisco Nexus 5000 Series switches and does not enable flow-control on its end.

  Workaround: Disable auto-negotiation on the link peer and enable flow control for flow control to work over the link.

- CSCsv52513

  Symptom: The VLAN interface 1 is internally created by the SVI daemon by default, so this VLAN interface cannot be deleted from the CLI.

  Workaround: None.

- CSCsu50589

  Symptom: If an invalid IP address is configured within a RADIUS configuration (such as a RADIUS server), any manipulation of the RADIUS configuration causes timeouts to the console such as **show running-configuration** or **copy running to startup**.

  Workaround: Configure a valid IP address for a RADIUS configuration.

- CSCsu66201

  Symptom: If the name server IP address is unreachable, the TACACS daemon gets stuck trying to resolve the server names. While it is stuck, TACACS commands, including common commands such as **show running-config** and **copy running-config startup-config,** are not processed.

  Workaround: Fix the network connectivity to the name server IP address.

- CSCso65934

  Symptom: Virtual interfaces are created by specifying the interface name in configuration mode. If the interface does not exist, the system creates the interface, and then enters interface configuration mode. If the user role prohibits access to that interface, this CLI is rejected and the user does not enter interface configuration mode, although the interface is created. Similarly, if a user does not have access to a virtual interface, the interface can still be deleted with the **no interface** command.

  Workaround: None.

- CSCso82992

  Symptom: Delete and insert role scopes for a role may fail and display the following error:

  ```
  entry already exists
  ```

  The problem occurs when you execute the following steps:

  - Delete all role scopes for a role.
  - Insert new role scopes for the same role.

  Workaround: Repeat the above steps once again.

Resolved Caveats—Cisco NX-OS Release 4.0(1a)N1(1)

This section lists the resolved caveats for this release.

- CSCso91286

  Symptom: When TACACS+ authentication is used to authenticate AAA users using ACS, the Cisco Cisco Nexus 5000 Series switch ignores the user to role binding information specified in theACS. Users are logged in with their default roles. The default role for a new user is network-operator and for a user who is an administrator is network-admin.

  Workaround: The user-to-role binding needs to be configured locally on the Cisco Nexus 5000 Series switch for the role binding to take effect.

- CSCsu32247

  Symptom: The Cisco Nexus 5000 Series switch executes the power on self test (POST) at bootup to validate hardware integrity of the ASICs. When a Fibre Channel port is connected to an HBA, the HBA driver could assert a LOS that causes a false failure to be reported by POST for one of the ASICs. As a result, all the ports serviced by the ASIC on the GEM are marked for hwFailure.

  Workaround: Bypass POST at bootup by performing the following steps:

  ```
  switch(config)# diagnostic bootup level bypass
  switch(config)# copy running-config startup-config
  switch(config)# reload
  ```

- CSCsv05115

  Symptom: The Cisco Nexus 5000 Series switch crashes if CFS callhome is enabled on a it after a CFS callhome commit is performed on an attached MDS.

  Workaround: None.

- CSCsv30392

  Symptom: The Cisco Nexus 5020 switch has a Pktmgr memory leak in version 4.0(0)N1(2). This causes STP to stop functioning after awhile causing a Layer 2 Loop. After breaking the redundant connections, the switch is unable to be managed, due to a No buffer space available message.

  Condition: The Cisco Nexus 5020 switch is setup in a triangle topology with two 6500 switches. Code version 4.0(0)N1(2) is loaded on the the Cisco Nexus 5020 switch. The redundant link had to be shut down in order to stop the loop.

  Workaround: To fix the broken state, do not configure SVI.

- CSCso99821

  Symptom: If PVLANs are created and deleted continuously and without pausing, the Ethernet interface may not be configurable and you have to reboot.

  Workaround: Pause between the creation and deletion of PVLANs and do not perform multiple PVLAN operations at the same time. Alternately, you can create a PVLAN before any PVLAN interface is created and remove the switch port PVLAN from the interface before the PVLAN is deleted.

- CSCsr52118

  S**ymptom**: When you perform delete, add, shutdown or no shutdown operations on a VLAN, the port channel interface may lose VLAN membership in the forwarding plane. As a result, ports will not participate in any of the forwarding operations on that VLAN. This behavior applies to access port channels where the switch port access VLAN configuration matches the deleted and re-added VLAN. This behavior can occur for trunk port channels, if the deleted or re-added VLAN matches the native VLAN of the port channel.

  Workaround: Enter the **shutdown** command or the **no shutdown** command on the port channel.

- CSCsr39670

  Symptom: Although SNMP notification is enabled on the switch, traps for the power supply and fan modules are not received.

  Workaround: None.

- CSCsr47531

  Symptom: When a VSAN is configured as SPAN source, traffic from all the member ports is spanned to the SPAN destination port. When a switch is rebooted, the VSAN SPAN source remains in the down state.

Workaround: Delete and add the VSAN sources for the SPAN session.

Resolved Caveats—Cisco NX-OS Release 4.0(0)N1(2a)

- CSCsu08988

  Symptom: Telnet access is available only after reloading the Nexus 5020 switch with the **no telnet server enable** command running.

  Workaround: Execute the **no telnet server enable** command once again after reload even if the command is saved in the startup-config. Additionally, you can also apply filters to the SVI to allow only trusted hosts to communicate with the system.

- CSCsu32247

  Symptom: The Nexus 5000 Series switch executes the power-on self-test (POST) at bootup to validate hardware integrity of the ASICs. When a Fibre Channel port is connected to a host bus adapter (HBA), the HBA driver can trigger a signal loss that causes a false failure to be reported by POST for one of the ASICs. As a result, all the ports serviced by the ASIC on the GEM are marked for hardware failure.

  Workaround: Do not connect HBAs to the FC expansion modules.

- CSCsu40126

  Symptom: When the Cisco Nexus 5000 Series switch is configured to operate in the N-port virtualization (NPV) mode, the LOGOs received over the server port are not processed properly. This results in stale Fibre Channel IDs at the switch.

  Workaround: Perform **shut** and **no shut** command operations on all the server ports to clear the stale state on the NPV switch.

- CSCsm66194 and CSCsr66209

  Symptom: Logins may not be uniformly balanced across all available border ports when the Cisco Nexus 5000 Series switch operates in the NPV mode under conditions such as the following:

  - The switch is reloaded.
  - NPIV is disabled and re-enabled on the NPV core-switch.
  - The NPV core-switch is reloaded.
  - A new NP link is added.

  Workaround: Perform **shut** and **no shut** command operations on all the server ports to rebalance the logins.

- CSCsu25775

  Symptom: When the Cisco Nexus 5020 Series switch is connected to a 110 V power supply, the following problems occur:

  - The syslog displays warnings at bootup. Although the hardware supports the 110 V input, the operating system incorrectly logs the warning message.
  - The show environment power command incorrectly displays the available power as a negative value.

  Workaround: The problem is not significant and the system operates normally with 110 V power supply input. There is no workaround to avoid the syslog message.

Resolved Caveats—Cisco NX-OS Release 4.0(0)N1(2)

This section lists the resolved caveats for this release.

- CSCsq61505

  Symptom: Problems are encountered while upgrading to Cisco NX-OS Release 4.0(0)N1(2) from Cisco NX-OS Releases 4.0(0)N1(1) or 4.0(0)N1(1a).

  Workaround: None.

- CSCsq67305

  Symptom: When the switch is operating in theN-port virtualization (NPV) mode, traffic may be disrupted on active Fibre Channel links if you enter the **shutdown** or **no shutdown** command on any of the NP mode uplink interfaces. The disruption also occurs if you change the interface mode of a port from F to NP or from NP to F. Traffic is disrupted for all F mode ports in the same VSAN as the NP-mode port.

  Workaround: Change only the interface state or interface mode on NP mode Fibre Channel interfaces during a maintenance window.

- CSCso56749

  Symptom: The current software does not have the ability to tag supervisor sourced frames separately depending on control or data. The frame always goes out with CoS 0.

  Workaround: None.

- CSCso91286

  Binding information specified in the Access Control System (ACS) is ignored when the Terminal Access Controller Access Control Plus (TACACS+) authentication is used to authenticate the AAA user using ACS.

  Symptom: When TACACS+ authentication is used to authenticate the AAA user using ACS, the Cisco Nexus 5000 Series switch ignores the user-to-role binding information specified in the ACS. You are logged in with the default role of network-operator (for new users) and network-admin.

  Workaround: Configure the user-to-role binding locally on the Cisco Nexus 5000 Series switch for the role binding to take effect.

- CSCsq23027

  Symptom: Occasional Phy loopback failure is reported in power-on self-test (POST) routines. This is a sporadic issue with front port POST routines. Occasionally, when the system comes up, ports fail the loopback test.

  Workaround: Reload the switch to confirm that it is a hardware defect.

- CSCsq27576

  Symptom: FC-SP authentication is supported only with a switch over the E/TE port. Authentication with native Fibre Channel (FC) and Fibre Channel over Ethernet (FCoE) initiator or target is not supported.

  Workaround: None.

- CSCsq32710

  Symptom: SNMP users configured with a user-defined roles cannot retrieve any Fibre Channel interfaces.

  Workaround: Use one of the predefined roles on the switch such as network-admin or network-operator.

- CSCsq37899

  Symptom: Deleting class-fcoe or class-default from an output policy map will cause **show policy-map** and **show running-config terminal** commands to be inconsistent if the **priority** keyword was configured for either of the classes.

  Workaround: The default bandwidth percentage for **class-fcoe** and **class-default** is 50 percent. Before you remove these classes from an output policy, make sure that the remaining classes in the policy map do not exceed 50 percent. Alternatively, if you want to allocate minimum bandwidth to class-fcoe or class-default, configure the bandwidth for these classes to 0 percent.

- CSCsq39683

  Symptom: Fibre Channel links with traffic running on it might generate syslog errors such as the following:

  ```
  2008 May 21 15:08:55 switch %KERN-3-SYSTEM_MSG: FCP_ERRFCP_PORT:
  gat_fcp_isr_process_blk_intr@1441, jiffies = 0xb1cec:ISR threshold reached, reg_block
  = 0x8, num_regs = 6, idx = 0, src_bit = 11 - kernel
  ```

  There is no loss in functionality and these messages can be ignored.

  Workaround: None.

- CSCso83662

  Symptom: One global MAC address is used in all STP and PVRST frames originating on various ports. This can result in inconsistent MAC moves on peer switches connected with multiple links.

  Workaround: None.

Resolved Caveats—Cisco NX-OS Release 4.0(0)N1(1a)

This section lists the resolved caveats for this release.

- CSCsq53614

  Symptom: Ethernet port channels configured between two Cisco Nexus 5000Series switches cause a memory leak in the DCBX process. This leak eventually leads to the DCBX process crashing and a system reboot (in a few days). This issue occurs only with Ethernet port channels between Cisco Nexus 5000 Series switches. Port channels using the Catalyst 6500 Series switches do not have this problem.

  Workaround: Disable receive and transmit Link Layer Discovery Protocol (LLDP) on the port channel members by entering the following configuration under each Ethernet interface that is a member of the port channel:

  ```
  Interface Ethernet 1/1
      no lldp receive
      no lldp transmit
  ```

- CSCsq36609

  Symptom: For a virtual Ethernet or virtual Fibre Channel interface configured as a SPAN source, changing the interface administrative state results in a memory leak. Deleting and adding SPAN sessions also causes memory leaks. The memory leaks eventually cause a switch reboot.

  Workaround: Avoid using virtual Ethernet and virtual Fibre Channel interfaces as SPAN sources. Avoid deleting and adding SPAN sessions.

Resolved Caveats—Cisco NX-OS Release 4.0(0)N1(1)

This was the first release of Cisco NX-OS for Nexus 5000 Series switches. There are no resolved caveats for this release.

Related Documentation

The Nexus 5000 Series documentation 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 documents:

- *Cisco Nexus 5000 Series Switch CLI Software Configuration Guide , Cisco NX-OS Release 4.1*
- *Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Release 4.1*
- *Cisco Nexus 5000 Series Hardware Installation Guide, Cisco NX-OS Release 4.1*
- *Cisco MDS 9000 and Nexus 5000 Series Fabric Manager Software Configuration Guide, Cisco Fabric Manager Release 4.1*
- *Cisco Nexus 5000 Series and CiscoNexus 2000 Series MIB Quick Reference*

Cisco Nexus 2000 Series documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps10110/tsd_products_support_series_home.html

The following are related Cisco Nexus 2000 Series documents:

- *Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide, Cisco NX-OS Release 4.1*
- *Cisco Nexus 2000 Series Fabric Extender Hardware Installation Guide, Cisco NX-OS Release 4.1*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.