Cisco Nexus 5000 Series Release Notes, Release 4.0(1a)N1(1a)

Current Release: 4.0(1a)N1(1a) -April 23, 2009
Part Number: OL-16601-01 G0

This document describes the features, caveats, and limitations for Nexus 5000 Series switches. Use this document in combination with documents listed in the "Related Documentation" section on page 26.

Note Release notes are sometimes updated with new information about restrictions and caveats. See the following website for the most recent version of the Nexus 5000 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

Part Number	Revision	Date	Description
OL-16601-01	A0	June 03, 2008	Created release notes.
OL-16601-01	B0	June 16, 2008	Added information for Release 4.0(0)N1(1a).
OL-16601-01	C0	June 30, 2008	Added information for Cisco Fabric Manager Release 3.4(1a).
OL-16601-01	D0	July 22, 2008	Added information for Release 4.0(0)N1(1a).
OL-16601-01	E0	August 13, 2008	Added information for Release 4.0(0)N1(2).
OL-16601-01	F0	September 29, 2008	Added information for Release 4.0(0)N1(2a).
OL-16601-01	G0	December 03, 2008	Added information for Release 4.0(1a)N1(1).
OL-16601-01	H0	April 23, 2009	Added information for Release 4.0(1a)N1(1a).

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

Contents

This document includes the following sections:

Introduction

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 switch hardware is described in the following topics:

Cisco Nexus 5020 Switch

The Cisco Nexus 5020 is a 56-port switch. It is a two rack unit (2RU), 10-Gigabit Ethernet, Cisco Data Center Ethernet, FCoE and Fibre Channel switch built to provide 1.04 terabit 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 GE and 10GE. The default is 10GE.
- 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 1RU, 10-Gigabit Ethernet, Cisco Data Center Ethernet, FCoE, and Fibre Channel switch providing 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 GE and 10GE 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 1/2/4-Gbps 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*.

New and Changed Features in Cisco NX-OS Release 4.0(1a)N1(1a)

The new or changed features for this release are described in the following topics:

The shutdown lan Command

The DCBX protocol provides a capability to signal LAN Logical Link Status (LLS) to a CNA that is connected to the Cisco Nexus 5000 switch over an Ethernet interface. This signaling can be used by the bonding driver in the host to perform a failover to the standby link to the LAN.

The **shutdown lan** command provides the LAN administrator with the capability to trigger an LLS-Down to the CNA. This operation can be performed without any impact to the SAN traffic on the Ethernet interface. When the **shutdown lan** command is configured on an Ethernet interface, all VLANs that are not enabled for FCoE are brought down on the interface. This in turn triggers the LLS-Down signal. If non-FCoE VLANs are brought down by other means (like **vlan shutdown**) they trigger LLS-Down signaling if the only VLANs active on an Ethernet interface are enabled for FCoE.

```
switch(config)# interface Ethernet 1/1
switch(config-if)# shutdown ?
  <CR>
  force  Enable/disable an interface
  lan    Shut all LAN VLANs on interface

switch(config-if)# [no] shutdown lan
```

The errdisable recovery cause pause-rate-limit Command

```
switch(config)# errdisable recovery cause ?
  pause-rate-limit  Enable timer to recover from pause rate limit error
                    disabled state
switch(config)# [no] errdisable recovery cause pause-rate-limit
```

When an Ethernet port experiences severe congestion due to a large amount of flow control (pause) frames received from the peer for an extended duration of time (10s), the port is placed in an error disabled state. The **errdisable recovery cause pause-rate-limit** command enables an automatic recovery of the port after a pre-defined interval of recovery time (if the port was error-disabled as a result of the pause-rate-limiting function). By default, this recovery mechanism is not enabled.

The following command allows configuration of the timeout value for automatic recovery. The default value is 300 seconds.

```
switch(config)# errdisable recovery interval ?
  <30-65535>  Timer-interval (sec)
```

Kickstart Break Sequence

Press the **Ctrl-]** key sequence from the console port session when the switch begins the Cisco NX-OS software boot sequence to enter the boot prompt mode.

```
Ctrl-]
switch(boot)#
```

Release 4.0(1a)N1(1a) Upgrade and Downgrade Issues

This section describes issues that you may encounter when you upgrade or downgrade the Cisco NX-OS software release on the Cisco Nexus 5000 Series switch. It provides examples of configuration syntax differences for some of these changes.

Upgrade and downgrade is supported between the following versions of the Cisco NX-OS software on the Cisco Nexus 5000 Series switches:

- 4.0(0)N1(2a)
- 4.0(1a)N1(1)
- 4.0(1a)N1(1a)

Upgrade and downgrade is not supported between the following versions of the Cisco NX-OS software on the Cisco Nexus 5000 Series switches:

- 4.0(1a)N1(1a)
- 4.0(1a)N2(1)

All the documented behavior for upgrade and downgrade between 4.0(0)N1 based releases and 4.0(1a)N1(1) also applies to upgrade and downgrade between 4.0(0)N1 based releases and 4.0(1a)N1(1a).

The following upgrade and downgrade issues occur as a result of CSCsy37432, CSCsy53275, CSCsy09062, CSCsy08516 (For details see, Resolved Caveats—Cisco NX-OS Release 4.0(1a)N1(1a), page 18 and Resolved Caveats—Cisco NX-OS Release 4.0(1a)N1(1), page 19):

- If the startup-config has an RBAC role configured with more than 35 rules, then after a downgrade to the 4.0(0)N1(2a) release, the **show running-config** command causes the vshd process to core dump. This is due to a caveat (CSCsy37432). The workaround is to remove rules from the roles configuration in a way that a role does not have more than 35 rules before downgrading to the 4.0(0)N1(2a) release.
- If the startup-config has an RBAC role configured with more than 20 roles with 20 rules each, then after a downgrade to the 4.0(0)N1(2a) release, **show running-config** will make the roles feature work incorrectly. This is due to caveat CSCsy53275. The workaround is, before you downgrade to the 4.0(0)N1(2a) release, remove rules from the roles configuration to limit the configuration so it does not exceed the previously mentioned numbers.
- After an upgrade or downgrade, if the **show startup security** command is issued before performing **copy running-config startup-config**, the security process could crash. This is due to caveat CSCsy09062. You can avoid a core dump by issuing a **copy running-config startup-config** command after an upgrade or downgrade and before issuing the **show startup <feature>** command.
- After an upgrade or downgrade, when the system comes up users are assigned a default role of network-operator. This is due to caveat CSCsy08516. To avoid the problem, reload the switch after an upgrade or a downgrade and after the system comes up. You can then perform a **copy running-config startup-config** to save the correct configuration.

For more information about the features listed, refer to the documentation set listed in the"Related Documentation" section on page 26.

This section includes the following topics:

EtherChannel® Upgrade/Downgrade Changes

The following table describes the changes to the security ACLs for EtherChannel members.

4.0(0)-based releases	Configuration is allowed on member ports (but not used while the port is a member of the EtherChannel).
4.0(1a)N1(1a)	No configuration is allowed on member ports. All member ports follow the configuration on the EtherChannel.
Upgrade	Member port ACL configuration, if any, is lost; EtherChannel configuration is preserved. No impact on the functional behavior while the port is a member of the EtherChannel. When the member port leaves the EtherChannel, you have to recreate the ACL configuration on the physical interface.
Downgrade	No issue.

The following table describes the changes to the interface level QoS service policy,

4.0(0)-based releases	Interface level QoS service policy is not aware of the EtherChannel. QoS strictly follows a per-member port configuration. The only service policy supported on the interface level is egress queue scheduling.
4.0(1a)N1(1a)	No configuration is allowed on member ports. All member ports follow the configuration on the EtherChannel.
Upgrade	If any member port has a modified egress scheduling policy and the EtherChannel is explicitly configured, then the egress scheduling configuration for the port is lost. A EtherChannel has a default egress scheduling policy.
Downgrade	This capability needs to be reconfigured after the downgrade. Otherwise, egress queue scheduling configuration on the EtherChannel will be lost after the downgrade.

The following table describes the changes to the priority flow control configuration.

4.0(0)-based releases	Priority flow control is an interface level configuration. This CLI option is used to override results of DCBX negotiation. Priority flow control function is not aware of the EtherChannel. It strictly follows a per-member port configuration.
4.0(1a)N1(1a)	No configuration allowed on member ports. All member ports follow the configuration on the EtherChannel.
Upgrade	If a member port has modified priority flow control configuration and the EtherChannel is explicitly configured, then port configuration is lost. The EtherChannel has default priority flow control configuration.
Downgrade	This capability needs to be reconfigured after the downgrade. Otherwise, the priority flow control configuration on the EtherChannel will be lost.

The following table describes the changes to the syntax of the Ethernet load-balancing commands.

4.0(0)-based releases	The following command is used to set the load-balancing method in a channel-group bundle:
	`switch(config)# port-channel load-balance ethernet source-destination-?`
	`  source-destination-ip    Source & Destination IP address`
	`  source-destination-mac   Source & Destination MAC address`
	`  source-destination-port  Source & Destination TCP/UDP port`
	Note The keyword **source-destination** is used in this release.

4.0(1a)N1(1a)	The following command is used to set the load-balancing method in a channel-group bundle:
	`switch(config)# port-channel load-balance ethernet source-dest-?`
	`  source-dest-ip    Source & Destination IP address`
	`  source-dest-mac   Source & Destination MAC address`
	`  source-dest-port  Source & Destination TCP/UDP port`
	Note The keyword **source-dest** is used in this release.

Upgrade	The load-balancing configuration is lost.
Downgrade	This capability needs to be reconfigured after the downgrade. Otherwise, the load-balancing configuration on the EtherChannel will be lost.

When an Ethernet interface joins a EtherChannel, the following interface level parameters are disabled:

```
bandwidth              Set bandwidth informational parameter
delay                  Specify interface throughput delay
duplex                 Enter the port duplex mode
flowcontrol            Configure interface flowcontrol
ip                     Configure IP features
ipv6                   Configure IPv6 features
mac                    MAC configuration commands
priority-flow-control  Configure interface priority-flowcontrol
service-policy         Configure QoS service policy
spanning-tree          Spanning Tree Subsystem
speed                  Enter the port speed
storm-control          Configure Interface storm control
```

Fibre Channel Port Shutdown

The following table describes the changes to the interface shutdown command syntax.

4.0(0)-based releases	The **system default switchport shutdown** command causes all Fibre Channel ports, virtual or physical, to default to shutdown.
4.0(1a)N1(1a)	The **system default switchport shutdown** command now configures the administrative state for all Ethernet ports as down. To configure the Fibre Channel ports to shutdown state, use the **system default switchport shutdown san** command.
Upgrade	Ethernet ports will default to shutdown instead of Fibre Channel ports.
Downgrade	This capability needs to be reconfigured after the downgrade. Otherwise, the switch will flag the **system default switchport shutdown san** command as invalid.

Switched Port Analyzer (SPAN)

The following table describes the changes to SPAN sessions.

4.0(0)-based releases	The default is to keep session in an open state. To shut a session, use the following command: `switch(config)# monitor session session-number suspend`
4.0(1a)N1(1a)	The default is to keep session state shut. To open a session, use the following command: `switch(config)# no monitor session session-number shut` **Note** The syntax of the command has also changed. The **suspend** keyword has been changed to **shut**.
Upgrade	SPAN session will be in shut state after the upgrade.
Downgrade	If you do not execute a specific **shut** or **no-shut** command on the SPAN session, the SPAN session will be in a no suspend state after the downgrade.

Changes to the FCoE Model and Related Configuration

In the previous Cisco NX-OS 4.0(0)-based releases, the FCoE model allowed Ethernet and FCoE to co-exist on the interface. The virtual interfaces, virtual Ethernet and virtual Fibre Channel (VFC), did not affect each other. For example, if the virtual Ethernet interface was errdisabled, the VFC interface could still be up.

With Cisco NX-OS Release 4.0(1a)N1(1), the CLI implementation was changed to provide forward compatibility with the forthcoming T11 FCoE Initialization Protocol (FIP). In this new FCoE model, the following is changed:

- FCoE traffic is passed over Ethernet; the Ethernet STP controls port status.
- FCoE traffic for a VSAN is transported over a single dedicated FCoE-enabled VLAN.

  Although the CLI implementation requires a VLAN-to-VSAN mapping, the FCoE frames are expected to be untagged or priority-tagged. The FCoE VLAN is not expected to be carried in the FCoE frames. This will change in a future release once FIP-based FCoE is supported.

The changes to the virtual interfaces are described in the following topics:

- Virtual Interface Groups, page 8
- Virtual Ethernet Interfaces, page 8
- Virtual Fibre Channel Interfaces, page 8
- VSAN-to-VLAN Mapping, page 9

Virtual Interface Groups

In previous Cisco NX-OS 4.0(0)-based releases, a virtual interface group allowed you to bind virtual interfaces to a physical Ethernet interface, as shown in the following example:

```
switch# configure terminal
switch(config)# interface vig 1
switch(config-if)# bind interface ethernet 1/1
```

Virtual interface groups have been deprecated in release 4.0(1a)N1(1a).

Virtual Ethernet Interfaces

Cisco NX-OS Release 4.0(1a)N1(1a) does not support virtual Ethernet interfaces. All Ethernet features previously configured at the virtual Ethernet interface now need to be configured at the bound Ethernet interface.

The following configuration statements must be explicitly configured on the Ethernet interface to keep behavior the same as virtual Ethernet interface:

```
spanning-tree bpduguard enable
spanning-tree port type edge trunk
```

All other features (for example, ACLs, SPAN etc.) that were previously configured at the virtual Ethernet interface would need to be applied to the bound Ethernet interface.

Virtual Fibre Channel Interfaces

In previous Cisco NX-OS 4.0(0)-based releases, a virtual Fibre Channel interface was attached to a virtual interface group, which then bound it to the physical Ethernet interface.

Each virtual Fibre Channel interface is bound directly to an FCoE-enabled physical Ethernet interface in Release 4.0(1a)N1(1a). This change simplifies the **interface vfc** command as shown in the following example:

```
switch# configure terminal
switch(config)# interface vfc 1
switch(config-if)# bind interface ethernet 1/1
```

The Ethernet interface that you bind the virtual Fibre Channel interface to must be configured as follows:

- It must be a trunk port (use the **switchport mode trunk** command).
- The FCoE VLAN that corresponds to virtual Fibre Channel's VSAN must be in the allowed VLAN list.
- FCoE VLAN must not be configured as the native VLAN of the trunk port.
- The Ethernet interface must be configured as PortFast (use the **spanning-tree port type edge trunk** command).

VSAN-to-VLAN Mapping

In previous Cisco NX-OS 4.0(0)-based releases, FCoE had no dependence on the VLANs defined on the switch.

In Release 4.0(1a)N1(1a), each virtual Fibre Channel interface is associated with only one VSAN. Any VSAN with associated virtual Fibre Channel interfaces must be mapped to a dedicated FCOE-enabled VLAN as shown in the following example:

```
switch# configure terminal
switch(config)# vlan 200
switch(config-vlan)# fcoe vsan 2
switch(config-vlan)# exit
switch(config)# interface ethernet 1/1
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk native vlan 1
switch(config-if)# switchport trunk allowed vlan 1,200
switch(config-if)# exit
switch(config)# interface vfc 1
switch(config-if)# bind interface ethernet 1/1
switch(config-if)# exit
switch(config)# vsan database
switch(config-vsan)# vsan 2 interface vfc 1
```

Note The FCoE VLAN must be exclusively reserved for FCoE traffic; it must not be used for non-FCoE Ethernet forwarding.

Example of Virtual Interface Configuration Changes

Cisco NX-OS 4.0(0)-based Release Configuration

```
interface vig 1
bind interface Ethernet 1/1

interface vethernet 1/1
switchport access vlan 2
```

```
interface vfc 1/1
no shutdown

vsan database
vsan 1 interface vfc 1/1
```

Release 4.0(1a)N1(1a) Converted Configuration

```
vlan 101
fcoe vsan 1

interface Ethernet 1/1
switchport mode trunk
switchport trunk native vlan 2
switchport trunk allowed vlan 2,101
spanning-tree bpduguard enable
spanning-tree port type edge trunk

interface vfc 1
no shutdown

vsan database
vsan 1 interface vfc 1
```

Upgrading from Cisco NX-OS 4.0(0)-Based Releases

When you upgrade your Cisco Nexus 5000 Series switch from Cisco NX-OS 4.0(0)-based releases, all virtual Fibre Channel and virtual Ethernet interface configuration will be lost because the applicable CLI is incompatible with the previous releases. We recommend that you backup your startup-config file prior to performing the upgrade. If your switch has an FCoE configuration you will need to reconfigure FCoE using the new FCoE CLI. Alternatively, you can contact Cisco Customer Support for help with upgrading and converting your configuration to the new format.

Downgrading to Cisco NX-OS 4.0(0)-Based Releases

Your FCoE configuration will be lost on downgrade. We recommend that you backup your original configuration prior to upgrading to Cisco NX-OS Release 4.0(1a)N1(1a). The backed up startup-config can be used to restore your original configuration after a downgrade.

Limitations

This section describes the limitations in Nexus 5000 Series switches, Release 4.0(1a)N1(1a).

- The untagged **cos** command is not supported in this release.
- 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.

- RADIUS and AAA startup configuration is lost when you upgrade from 4.0(0)N based releases to 4.0(1a)N based releases and later releases or when you downgrade to 4.0(0)N based releases. Save the startup configuration to bootflash memory before an upgrade or a downgrade, and restore it from bootflash memory after the upgrade or downgrade.
- 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.
- Ethernet and Fibre Channel frames with bad CRC or invalid SOF and EOF are not dropped. The Cisco Nexus 5000 Series switch operates in cut-through switching mode, so frames are forwarded through the system before they are completely received. The Ethernet and Fibre Channel CRCs are overwritten in the frame and the EOF code is set to EOFa. A downstream switch or the destination end station will drop the bad frames.
- 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 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.

Caveats

This section includes the following topics:

Open Caveats

This section lists the open caveats for this release.

- CSCtb56755

  Symptom: When a 750W power supply OIR is performed, following error message is generated:

  ```
  009 Aug 15 00:37:38 Switch-1 %$ VDC-1 %$ %NOHMS-2-NOHMS_DIAG_ERR_PS_RECOVERED:
  Recovered: System minor alarm on power supply 1: failed
  ```

  Workaround: There is no effect on functionality.

- CSCsy53718

  Symptom: If **errdisable recovery interval** is configured to the maximum value of 65535 (taking approximately 18hrs), when a port is errdisabled due to a recovery enabled cause, it takes four more hours for the recovery to take effect.

  Workaround: None.

- CSCsy05103

  Symptom: When an RBAC role is configured to deny a few commands within a specific interface, the **help** command falsely displays all commands as denied. This is only a help issue and the rules are enforced as configured.

  Workaround: None.

- CSCsy16212

  Symptom: When an RBAC role is configured to deny a few commands, users within that role may incorrectly see a some disallowed commands in the help. This is only a help issue and commands are denied as per the configured rules.

  Workaround: None

- CSCsy28374

  Symptom: An RBAC role with rules denying commands for all interfaces of certain types using the wildcard * option, are not honored.

  Workaround: Configure rules with specific interface names.

- 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.

- 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 switches support 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
```

- CSCsu01188

  Symptom: No traps are sent when SFPs for GE and 10GE are removed or inserted.

  Workaround: None.

- 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.

- 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.

- 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.

- CSCsv02866

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

  Workaround: None.

- CSCsv10783

  Symptom: The s**how startup-config** 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.

- CSCsv00989

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

  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.

- 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.

- 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 gets into this state, subsequent VACL configurations fail.

  Workaround: A reload is needed to recover the configuration.

- CSCsu50589

  Symptom: If an invalid IP address is configured within a RADIUS configuration (such 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.

- 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.

- CSCsv00402

  Symptom: When you downgrade from the 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.

- 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.

- 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 (DM) displays in amber color even though the fan is working 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.

- 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.

- 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 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 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 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 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.

- 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.

- 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.

- 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.

- 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 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 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.

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

This section lists the resolved caveats for this release.

- CSCsy65407

  Symptom: In the Cisco NX-OS 4.0(1a)N1(1) release, if an RBAC role has more than 67 rules configured, **show running-config** causes the vshd process to core dump. This caveat exists in the 4.0(0)N1(2a) and 4.0(1a)N1(1) releases.

  Workaround: Before downgrading to the Cisco NX-OS 4.0(1a)N1(1) release, remove rules from the roles configuration such that a role does not have more than 67 rules.

- CSCsv55655

  Symptom: The Cisco Nexus 5000 Series switch 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 Nexus 5000 Series switches and does not enable flow control at its end.

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

- CSCsw39639

  Symptom: When a rule that refers to a specific interface name (Ethernet 1/1) is entered in the role definition CLI, the command could hang. Type **Ctrl-C** to return to the CLI prompt.

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

- CSCsy09062

  Symptom: This is an open caveat in 4.0(0)N1(2a) and 4.0(1a)N1(1) releases. After an upgrade or downgrade if the **show startup security** command is issued before performing a **copy running-config startup-config,** the security process could crash.

  Workaround: You can avoid a core dump by issuing a **copy running-config startup-config** command after an upgrade or downgrade and before issuing the **show startup <feature>** command.

- CSCsy08516

  Symptom: This is an open caveat in 4.0(0)N1(2a) and 4.0(1a)N1(1) releases. After an upgrade or a downgrade and when the system comes up, users are assigned a network-operator role by default.

  Workaround: To avoid the problem, reload the switch after an upgrade or a downgrade and after the system comes up. You can then perform the **copy running-config startup-config** operation to save the correct configuration.

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

This section lists the resolved caveats for this release.

- CSCsy37432

  Symptom: This is an open caveat in the Cisco NX-OS 4.0(0)N1(2a) release. On the 4.0(0)N1(2a) release if an RBAC role has more than 35 rules configured, **show running-config** and **copy running-config** cause the vshd process to core dump.

  Workaround: Before downgrading to the Cisco NX-OS 4.0(0)N1(2a) release, remove rules from the roles configuration such that a role does not have more than 35 rules.

- CSCsy53275

  Symptom: This is an open caveat in the Cisco NX-OS4.0(0)N1(2a) release. If there are 20 RBAC roles configured with 20 rules each, the RBAC feature becomes non-functional.

Workaround: Do not configure more than 20 rules in each role. The feature works fine if the numbers of rules are limited to 10 per role.

- CSCso91286

  Symptom: When TACACS+ authentication is used to authenticate AAA users using ACS, the Cisco Nexus 5000 Series switch ignores the user to role binding information specified in the ACS. 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 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

  Symptom: 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 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 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 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 Release 4.0(0)N1(2) from 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 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 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 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 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.

Cisco Fabric Manager

Beginning with Cisco Fabric Manager release 3.4(1a), Nexus 5000 Series switches are supported by Fabric Manager.

If you are deploying Nexus 5000 Series switches with FCoE, you should operate Fabric Manager in Display FCoE mode. Display FCoE mode displays additional tree nodes, menu items, toolbar buttons, and topology nodes and links related to FCoE. To convert to Display FCoE mode, edit the server.properties file to set the display FCoE property to true.

For additional information about Fabric Manager, see *Cisco Nexus 5000 Series Switch Fabric Manager Software Configuration Guide, Release 4.0*

The following sections apply to Fabric Manager support for Nexus 5000 series switches:

- Limitations, page 24
- Caveats, page 25

Limitations

This section lists the Cisco Fabric Manager limitations related to managing Nexus 5000 series switches.

Ethernet Configuration

You cannot configure physical Ethernet interfaces using Fabric Manager or Device Manager. You must configure physical Ethernet interfaces using CLI commands.

SPAN

You cannot use Device Manager to configure Ethernet or virtual Ethernet interfaces as SPAN source ports or to configure Ethernet interfaces as destination ports. The workaround is to configure SPAN using CLI commands.

Zoning

In the Edit Local Full Zone Database tool, virtual Fibre Channel interfaces must be specified using the Switch Port WWN method of adding members to a zone. In the Add Members to Zone dialog box, the Switch & Port method and the Domain & Port method are not supported for virtual Fibre Channel interfaces.

Caveats

This section lists the Cisco Fabric Manager caveats related to managing Nexus 5000 series switches.

Open Caveats

- CSCq57019

  Symptom: The Fabric Manager N-Port Virtualization (NPV) Wizard does not list the Nexus 5000 Series switches that are operating in NPV mode.

  Workaround: None.

- CSCsq06170

  Symptom: In Fabric Manager, only one power supply is displayed for a Nexus 5000 Series switch with two power supplies.

  Workaround: Use Device Manager, which displays the correct information when you use the Power Supplies menu item from the Physical menu.

- CSCso82992

  Symptom: When using the Roles dialog box in Device Manager, if you edit the role scopes for a role that already has role scopes defined, and then click the **Apply** button, an error message dialog box states that the entry already exists.

  Workaround: The changes are saved if you click the **Apply** button again.

- CSCsq23436

  Symptom: The load-balancing and traffic-engineering features are not supported on Nexus 5000 Series switches in NPV mode, but Fabric Manager does not disable the configuration of these features. In the Switches > NPV information pane, the Load Balancing tab provides a check box to enable the feature, and the Traffic Engineering tab provides a dialog box to create a traffic engineering session.

  Workaround: Ignore these configuration options for Nexus 5000 Series switches.

- CSCsq14828

  Symptom: The web client does not display flow statistics or the Ethernet interface statistics for initiators using Fibre Channel over Ethernet (FCoE) connections to the Nexus 5000 Series switch.

  Workaround: Use Flow Statistics in Fabric Manager, which displays the flow statistics correctly. The Device Manager displays the Ethernet interface statistics correctly.

- CSCsq32710

  Symptom: If you logged in to the Nexus 5000 Series switch using a user-defined role, you cannot retrieve the Fibre Channel interfaces using SNMP.

  Workaround: You can retrieve the information using CLI commands.

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, Release 4.0*
- *Cisco Nexus 5000 Series Switch Fabric Manager Software Configuration Guide, Release 4.0*
- *Cisco Nexus 5000 Series System Messages Reference, Release 4.0*
- *Cisco Nexus 5000 Series MIB Quick Reference, Release 4.0*
- *Cisco Nexus 5000 Series Command Reference, Release 4.0*
- *Cisco Nexus 5000 Series Hardware Installation Guide, Release 4.0*

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.
