Send document comments to nexus7k-docfeedback@cisco.com

Cisco Nexus 7000 Series NX-OS Release Notes, Release 4.2

Date: August 16, 2011
Part Number: OL-20020-07 C0
Current Release: 4.2(8)
Deferred Releases: 4.2(1), 4.2(2)

This document describes the features, caveats, and limitations for Cisco NX-OS software for use on the Cisco Nexus 7000 Series switches. Use this document in combination with documents listed in the "Related Documentation" section on page 77.

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 7000 Series NX-OS Release Notes, Release 4.2* Release Notes:
http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_2/nx-os/release/notes/42_nx-os_release_note.html

Table 1 shows the online change history for this document.

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

Table 1 Online History Change

Part Number	Revision	Date	Description
OL-20020-01	A0	August 10, 2009	Created release notes for Release 4.2(1).
	B0	August 21, 2009	• Added open Caveat CSCta96278. • Added open Caveat CSCtb31933. • Added the 1000BASE-T transceiver that is supported in Release 4.2(1) to Table 3.
	C0	August 25, 2009	Added a description of Border Gateway Protocol (BGP) enhancements to the New Software Features section.
OL-20020-02	A0	September 23, 2009	Created release notes for Release 4.2(2).
	B0	September 25, 2009	Added open Caveat CSCtc17493. Added a statement that Cisco DCNM Release 4.2(1) is compatible with Cisco NX-OS Release 4.2(2).
	C0	September 26, 2009	Moved Caveat CSCtb01813 from resolved to open.
OL-20020-03	A0	September 29, 2009	Created release notes for Release 4.2(2a).
	B0	October 2, 2009	Added a Note to the Upgrade Information for Caveat CSCtc17493 in the Resolved Caveats section.
	C0	October 9, 2009	Corrected the Conditions and Workaround for Caveat CSCtb67491.
	D0	October 19, 2009	Added the Documentation Updates section.
OL-20020-04	A0	December 18, 2009	Created release notes for Release 4.2(3).
	B0	February 5, 2010	Added open Caveat CSCtd41676.
OL-20020-05	A0	February 24, 2010	Created release notes for Release 4.2(4).
	B0	March 4, 2010	Added Resolved Caveat CSCte05048.
OL-20020-06	A0	August 1, 2010	Created release notes for Release 4.2(6).
	B0	August 2, 2010	Added Resolved Caveat CSCtf25126.
	C0	August 11, 2010	Added Open Caveat CSCti14627.
OL-20020-07	A0	August 16, 2011	Created release notes for Release 4.2(8).
	B0	September 13, 2011	Removed the Orphan Port Suspend Enhancement from the New Software Features section for Cisco NX-OS Release 4.2(8)
	C0	September 15, 2011	Added Open Caveat CSCts70896.

Contents

This document includes the following sections:

Introduction

The Cisco NX-OS software for the Cisco Nexus 7000 Series switches fulfills the routing, switching, and storage networking requirements of data centers and provides an Extensible Markup Language (XML) interface and a command-line interface (CLI) similar to Cisco IOS software.

System Requirements

This section includes the following topics:

Hardware Supported

The Cisco NX-OS software supports the Cisco Nexus 7000 Series chassis. You can find detailed information about supported hardware in the *Cisco Nexus 7000 Series Hardware Installation and Reference Guide*.

Memory Requirements

The Cisco NX-OS software requires 4 GB of memory.

Supported Device Hardware

Cisco NX-OS Release 4.2(1) and later releases support management and monitoring of the Cisco Nexus 7010 switch and Cisco Nexus 7018 switch. Although you can use Cisco NX-OS Release 4.0 to manage a Cisco Nexus 7010 switch, you must use Cisco NX-OS Release 4.1(2) or later releases to manage a Cisco Nexus 7018 switch, the 7.5-kW AC power supply unit, and the 48-port 1-Gigabit SFP I/O module. Table 2 shows the hardware features supported by Cisco NX-OS Release 4.0 software, Cisco NX-OS Release 4.1 software, and Cisco NX-OS Release 4.2 software.

Table 3 shows the transceivers supported by each release; many new optics are supported with the Cisco Release 4.2(x).

Table 2 Hardware Features Supported by Cisco NX-OS Software Releases

Hardware	Part Number	Cisco NX-OS Release 4.0 Support	Cisco NX-OS Release 4.1(2) through 4.2(8) Support
Cisco Nexus 7010 chassis	N7K-C7010	X	X
Cisco Nexus 7018 chassis	N7K-C7018	–	X
Supervisor module	N7K-SUP1	X	X
Fabric module, Cisco Nexus 7000 Series 10-slot	N7K-C7010-FAB-1	X	X
Fabric module, Cisco Nexus 7000 Series 18-slot	N7K-C7018-FAB-1	–	X
48-port 10/100/1000 Ethernet I/O module	N7K-M148GT-11	X	X
48-port 1-Gigabit Ethernet SFP I/O module	N7K-M148GS-11	–	X
32-port 10-Gigabit Ethernet SFP+ I/O module	N7K-M132XP-12	X	X
System fan tray for the Cisco Nexus 7010 chassis	N7K-C7010-FAN-S	X	X
Fabric fan tray for the Cisco Nexus 7010 chassis	N7K-C7010-FAN-F	X	X
Fan tray for the Cisco Nexus 7018 chassis	N7K-C7018-FAN	–	X
6-kW AC power supply unit	N7K-AC-6.0KW	X	X
7.5-kW AC power supply unit	N7K-AC-7.5KW-INT N7K-AC-7.5KW-US	– –	X X

Table 3 Transceivers Supported by Cisco NX-OS Software Releases

I/O Module	Transceiver Type	Product ID	Minimum Software Version
N7K-M148GS-11	1000BASE-CWDM	CWDM-SFP-1470	4.2(1)
		CWDM-SFP-1490	4.2(1)
		CWDM-SFP-1510	4.2(1)
		CWDM-SFP-1530	4.2(1)
		CWDM-SFP-1550	4.2(1)
		CWDM-SFP-1570	4.2(1)
		CWDM-SFP-1590	4.2(1)
		CWDM-SFP-1610	4.2(1)

Table 3 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Transceiver Type	Product ID	Minimum Software Version
N7K-M148GS-11	1000BASE-DWDM	DWDM-SFP-6141	4.2(1)
		DWDM-SFP-6061	4.2(1)
		DWDM-SFP-5979	4.2(1)
		DWDM-SFP-5898	4.2(1)
		DWDM-SFP-5817	4.2(1)
		DWDM-SFP-5736	4.2(1)
		DWDM-SFP-5655	4.2(1)
		DWDM-SFP-5575	4.2(1)
		DWDM-SFP-5494	4.2(1)
		DWDM-SFP-5413	4.2(1)
		DWDM-SFP-5332	4.2(1)
		DWDM-SFP-5252	4.2(1)
		DWDM-SFP-5172	4.2(1)
		DWDM-SFP-5092	4.2(1)
		DWDM-SFP-5012	4.2(1)
		DWDM-SFP-4931	4.2(1)
		DWDM-SFP-4851	4.2(1)
		DWDM-SFP-4772	4.2(1)
		DWDM-SFP-4692	4.2(1)
		DWDM-SFP-4612	4.2(1)
		DWDM-SFP-4532	4.2(1)
		DWDM-SFP-4453	4.2(1)
		DWDM-SFP-4373	4.2(1)
		DWDM-SFP-4294	4.2(1)
		DWDM-SFP-4214	4.2(1)
		DWDM-SFP-4134	4.2(1)
		DWDM-SFP-4056	4.2(1)
		DWDM-SFP-3977	4.2(1)
		DWDM-SFP-3898	4.2(1)
		DWDM-SFP-3819	4.2(1)
		DWDM-SFP-3739	4.2(1)
		DWDM-SFP-3661	4.2(1)
		DWDM-SFP-3582	4.2(1)
		DWDM-SFP-3504	4.2(1)
		DWDM-SFP-3425	4.2(1)
		DWDM-SFP-3346	4.2(1)
		DWDM-SFP-3268	4.2(1)

Table 3 Transceivers Supported by Cisco NX-OS Software Releases (continued)

I/O Module	Transceiver Type	Product ID	Minimum Software Version
		DWDM-SFP-3190	4.2(1)
		DWDM-SFP-3112	4.2(1)
		DWDM-SFP-3033	4.2(1)
N7K-M148GS-11	1000BASE-SX	SFP-GE-S	4.1(2)
		GLC-SX-MM	4.1(2)
	1000BASE-LX	SFP-GE-L	4.1(2)
		GLC-LH-SM	4.1(2)
	1000BASE-ZX	SFP-GE-Z	4.1(2)
		GLC-ZX-SM	4.1(2)
	1000BASE-T	GLC-T	4.2(1)
		SFP-GE-T	4.2(1)
N7K-M132XP-12	10GBASE-SR	SFP-10G-SR	4.0(1)
	10GBASE-LR	SFP-10G-LR	4.0(3)
	10-Gbps SFP+	SFP-10G-ER	4.2(6)

Upgrade/Downgrade Caveats

The following caveats apply to the Cisco NX-OS Release 4.2(1) or later for the Cisco Nexus 7000 Series devices:

- Do not change any configuration settings or network settings during the upgrade. Any changes in the network settings may cause a disruptive upgrade.
- Release 4.2(8) is ISSU-compatible with the following releases:
  - Release 4.2(6)
  - Release 4.2(4)
  - Release 4.2(3)
  - Release 4.2(2a)
  - Release 4.2(2)
  - Release 4.2(1)
  - Release 4.1(5)
  - Release 4.1(4)
  - Release 4.1(3)
  - Release 4.1(2)
  - Release 4.0(4)
  - Release 4.0(3)
- You can nondisruptively downgrade from Cisco NX-OS Release 4.2(8) to any of the following releases:

  - Release 4.2(6)
  - Release 4.2(4)
  - Release 4.2(3)
  - Release 4.2(2a)
  - Release 4.2(2)
  - Release 4.2(1)

Note If your switch has a standby supervisor with 4 GB of memory and an active supervisor with 8 GB of memory, when you perform an ISSD from Cisco NX-OS Release 4.2(8), the system powers down the standby supervisor and displays a syslog message.

Note If you need to downgrade to Cisco NX-OS Release 4.2(1), you will experience CSCtb76572, which is an Open Caveat in Cisco NX-OS Release 4.2(1). The symptom of this issue is that the interface index is not set correctly. The symptom might be seen in a vPC scenario when you have an HSRP router in a standby-standby state. To work around the issue, you can enter the **shut** command followed by the **no shut** command on the affected switched virtual interface (SVI), or temporarily change the state of the HSRP.

- You can nondisruptively downgrade from Cisco NX-OS Release 4.2(2a) or Release 4.2(2) to Release 4.2(1).

CMP Images

Cisco NX-OS Release 4.2(8) includes a new image for the CMP. The CMP is upgraded to version 4.2(8) on a successful ISSU of Cisco NX-OS to Release 4.2(8).

Cisco NX-OS Release 4.2(6), 4.2(4), Release 4.2(3), Release 4.2(2a), and Release 4.2(2) do not have a new image for the CMP. The CMP image version remains at Release 4.2(1).

Cisco NX-OS Release 4.2(1) includes a new image for the CMP. The CMP is upgraded to version 4.2(1) on successful ISSU of Cisco NX-OS to Release 4.2(1).

Cisco DCNM

Cisco Data Center Network Manager (DCNM) Release 4.2(3) supports Cisco NX-OS 4.2(8).

Note The release number of Cisco DCNM and Cisco NX-OS do not have to be the same. Cisco DCNM Release 4.2(3) is fully compatible with lower release versions of Cisco NX-OS.

There is no Cisco Data Center Network Manager Release 4.2(2a) or Release 4.2(2). Cisco DCNM Release 4.2(1) is fully compatible with Cisco NX-OS Release 4.2(2a) and Release 4.2(2).

New Software Features

This section briefly describes the new features introduced in Cisco NX-OS Release 4.2 for the Cisco Nexus 7000 Series switches. For detailed information about the features listed, see the documents listed in the "Related Documentation" section on page 77. The "New and Changed Information" section in each of these books provides a detailed list of all new features and includes links to the feature description or new command.

This section includes the following topics:

Cisco NX-OS Release 4.2(8)

This section briefly describes new enhancements in Cisco NX-OS Release 4.2(8) for the Cisco Nexus 7000 Series switches and includes the following topics:

Duplicate ARP Detection Suppression for HSRP IP in a DCI Topology

This enhancement allows you to suppress duplicate IP address detection when hosts use ARP for the HSRP active router, or when the HSRP active router sends a GARP for its own virtual IP address. In such a topology, there are two active HSRP virtual IP addresses (one in each site).

New CLI Command to Handle Multicast Traffic

The new **hardware fabric flow-control multicast** command enables the Cisco Nexus 7000 Series switch to handle multicast traffic more efficiently in microbursting environments. In large multicast networks where microbursts are frequent, it is possible to overfill certain multicast egress buffers for short periods of time (microseconds), which causes packets to be dropped. This new command, which includes a *forced* option and a *modules* option, can be used to mitigate the problem of egress buffers overflowing by allowing flow-control across the fabric and utilizing larger ingress buffers.We do not recommend using this command where bursting is prolonged, as it can lead to head-of-line blocking scenarios. The **show system internal xbar fabric-flow-control-info** command is a related new command.

Per-VLAN Type-1 Consistency Check

When spanning-tree VLANs that are enabled on vPC peers do not match, it is a global type-1 inconsistency. Cisco NX-OS Release 4.2(8) includes an enhancement to check for type-1 inconsistencies. With this enhancement, spanning-tree VLANs that do match on both peers will be brought down on all vPCs and the peer link. Other VLANs will stay up. There is no CLI command to enable or disable this enhancement; it is enabled by default. The per-VLAN type-1 consistency check does not apply in MST mode.

Cisco NX-OS Release 4.2(6)

This section briefly describes the new feature introduced in Cisco NX-OS Release 4.2(6) for the Cisco Nexus 7000 Series switches and includes the following topics:

Address Resolution Protocol Table Sync

The Address Resolution Protocol (ARP) table sync feature overcomes the delay involved in ARP table restoration that can be triggered when one of the switches in the vPC domain goes offline and comes back online and also when there are peer-link port channel flaps. Performance improvement in convergence times for unicast traffic is the result of this feature.

To improve performance, we suggest that you turn on the ARP sync feature. By default, it is not enabled.

To check whether or not ARP sync is enabled, enter the following command:

```
switch# show running
```

To enable ARP sync, enter the following command:

```
switch(config-vpc-doman)# ip arp synchronize
```

CoPP Enhancements

New Control Plane Policing (CoPP) class maps have been defined to classify known and unknown Layer 2 packets, and to police those packets.

vPC Fail-Safe

The vPC peer-switch feature has been enhanced to not change the STP role when the primary vPC switch reloads.

Cisco NX-OS Release 4.2(4)

Cisco NX-OS Release 4.2(4) for the Nexus 7000 Series switches has no new software features.

Cisco NX-OS Release 4.2(3)

Cisco NX-OS Release 4.2(3) for the Nexus 7000 Series switches has no new software features.

Cisco NX-OS Release 4.2(2a)

Cisco NX-OS Release 4.2(2a) for the Nexus 7000 Series switches has no new software features.

Cisco NX-OS Release 4.2(2)

Cisco NX-OS Release 4.2(2) for the Nexus 7000 Series switches has no new software features.

Cisco NX-OS Release 4.2(1)

This section briefly describes the new feature introduced in Cisco NX-OS Release 4.2(1) for the Cisco Nexus 7000 Series switches and includes the following topics:

Port Profiles

Port profiles allow you to easily apply a repetitive configuration to several interfaces. You configure a port profile and then attach it to an interface or a range of interfaces. Each port profile can be applied only to a specific type of interface; the choices are as follows:

- Ethernet
- VLAN network interface
- Port channel

Additionally, you can have one port profile inherit the settings from another port profile. Inheriting another port profile allows the initial port profile to assume all of the commands of the second, inherited, port profile that do not conflict with the initial port profile. Four levels of inheritance are supported. The same port profile can be inherited by any number of port profiles.

Port profiles support the following features in Cisco NX-OS Release 4.2(1):

- Port commands (such as speed, bandwidth, duplex, and so forth), and Layer 2 commands (such as switchport, port channels, STP, and so forth)
- dot1x, port security, and UDLD
- DHCP and NetFlow
- Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP)

- SPAN and QoS/ACL

WCCPv2

Web Cache Communication Protocol version 2 (WCCPv2) specifies interactions between one or more Cisco NX-OS routers and one or more cache engines. Only Layer 2 redirect WCCP is supported; the GRE method of WCCP is not supported. WCCPv2 transparently redirects selected types of traffic through a group of routers. The selected traffic is redirected to a group of cache engines to optimize resource usage and lower response times.

WCCP for the Cisco Nexus 7000 Series devices are used to integrate the Wide Area Application Service (WAAS) appliances with the switch.

IPv6 Support for Policy-Based Routing

Policy-based routing uses the Route Policy Manager to create policy route filters. These policy route filters can forward a packet to a specified next hop based on the source of the packet or other fields in the packet header. Cisco NX-OS Release 4.2(1) adds IPv6 support for policy-based routing.

IPv6 Support for BGP

The Border Gateway Protocol (BGP) is an inter-autonomous system routing protocol. A BGP router advertises network reachability information to other BGP routers. The network reachability information includes the destination network prefix, a list of autonomous systems that needs to be traversed to reach the destination, and the next-hop router. Cisco NX-OS Release 4.2(1) adds IPv6 support for BGP.

Support for Static Router MAC Addresses

You can statically configure a static MAC address on the following Layer 3 interfaces:

- VLAN interfaces
- Layer 3 interfaces
- Layer 3 subinterfaces

Port Security for Layer 2 Port-Channel Interfaces

You can enable port security on a Layer 2 port channel to restrict the access to the port-channel interface by limiting and identifying source MAC addresses in either trunk or access mode. When you configure a Layer 2 port-channel interface as a secure interface and the maximum number of secure MAC addresses is reached, a security violation occurs when the MAC address of a workstation attempting to access the port-channel interface is different from any of the identified secure MAC addresses.

When you enable port security on a Layer 2 port channel in trunk mode, the MAC address restrictions apply on each VLAN in the entire port channel and the system maintains all the port security functionalities as on a regular trunk port.

Port security on the port channel has no effect on the control traffic going through the port channel. The control packets bypass the port security check without incurring any violations. Port security on port channels also supports aging as it does for regular a physical port.

Layer 2 NetFlow

Cisco NX-OS Release 4.2(1) adds support for Layer 2 NetFlow. Layer 2 NetFlow offers the ability to collect traffic statistics based on the packet's Layer2 header fields; this allows MAC-address-based accounting. Layer2 NetFlow can match and create flows based on the following:

- Source and destination MAC addresses
- VLAN
- EtherType
- Any combination of the above fields

Layer 2 NetFlow can be configured on all Layer 2 interfaces (that is, switchports--access and trunk switchports--and Layer2 port channels).

Dynamic FIB TCAM Allocation

The Layer 3 forwarding information base (FIB) Ternary Content Addressable Memory (TCAM) is designed to support routing information for multiple-address families, in particular:

- IPv4 unicast
- IPv4 multicast
- IPv6 unicast
- IPv6 multicast

Before Cisco NX-OS Release 4.2(1), the maximum number of entries for each of these classes was fixed to a predefined value. Beginning with Cisco NX-OS Release 4.2(1), the address families can be dynamically carved to a user-configurable maximum number of entries, within the overall maximum of the FIB TCAM. This feature provides users with greater flexibility when managing the various address families.

Object-Tracking Enhancements

Cisco NX-OS Release 4.2(1) adds support for object track lists, which use thresholds, weights, and Boolean expressions to combine multiple tracked objects into a single tracked state. Object tracking allows you to track specific objects on the network such as the interface line protocol state, IP routing, and route reachability, and to take action when the tracked object's state changes.

VRRP adds support for multiple objects tracking.

VDC and VRF Enhancements

You can now put the tunnel interfaces into a nondefault virtual device contexts (VDCs) and virtual routing and forwarding instances (VRFs).

VDC Enhancements

With Cisco NX-OS Release 4.2(1), you can restart nondefault VDCs that are in the active or failed state. You can also suspend and resume nondefault VDCs.

Beginning in Cisco NX-OS Release 4.2(1), you can change the command-line interface (CLI) prompt for nondefault VDCs.

Security Enhancements

Cisco NX-OS Release 4.2(1) supports the following security enhancements:

- The CoPP has been updated to include system protection from the control-plane traffic generated by WCCP and from the control-plane traffic generated by the Source Group Tag (SGT) Exchange Protocol, which is known as SXP.
- Provides support for creating and removing authenticator port access entity (PAE) instances on interfaces.
- Provides support for command authorization for TACACS+.
- Allows you to clear the statistics for RADIUS and TACACS+.
- Provides support for MSCHAPv2 for AAA authentication.

Load Interval

You can configure the collection interval for interface statistics. This interval is used for calculating other interface input/output traffic. You can configure up to three independent intervals per interface.

vPC Enhancements

Cisco NX-OS Release 4.2(1) supports the vPC enhancements listed in the following sections:

vPC Object Tracking

The vPC object tracking enhancement tracks uplinks and vPC peer link as an object list. When vPC object tracking is enabled, a vPC peer detects the tracked object going-down state (simultaneous failure of peer-link and uplinks interfaces) and locally suspends vPCs. The feature targets a topology where peer-link and uplinks are located on the same card (that is, a single point of failure) or a case where simultaneous failure of these interfaces is cause for a concern. In this scenario, suspending local vPCs through the vPC object tracking feature allows you to avoid potential traffic silent discards.

vPC Exclude Interface-VLAN

When a dual active condition is detected in vPC (that is, a peer-link fails and peer-keepalive is operational), SVIs and vPCs on the secondary vPC peer are suspended and only the primary vPC peer continues data plane and control plane functionalities. The vPC exclude interface-VLAN feature ensures that a configurable list of SVIs are not suspended on the secondary vPC peer when the vPC peer-link goes down. Consequently, for non-vPC ports that carry VLANs which are also present on the vPC peer-link, Layer 3 connectivity is maintained even in a dual active condition.

vPC Peer-Gateway

vPC peer-gateway functionality allows a vPC switch to act as the active gateway for packets that are addressed to the router MAC address of the vPC peer. This feature enables local forwarding of such packets without the need to cross the vPC peer-link. In this scenario, the feature optimizes use of the peer-link and avoids potential traffic loss.

vPC Orphan Port Listing

Single attached devices that are not connected via a vPC but still carry vPC VLANs are also known as orphan ports. In case of a peer-link shut or restoration, an orphan port's connectivity may be bound to the vPC failure or restoration process. For this reason, Cisco NX-OS Release 4.2(1) introduces support of a **show** command to monitor and list orphan ports in the system along with impacted VLANs.

vPC Delay Restore

This enhancement delays vPCs bringup after a vPC device reload (SVI bringup timing is unchanged), which allows for Layer 3 routing protocols to converge and FIB programming to complete for a more graceful restoration. The default timer for vPC restoration is set to 30 seconds and, if required, can be tuned according to the specific number of SVIs per routes.

GOLD Enhancements

The Cisco Generic Online Diagnostics (GOLD) is extended in the following ways:

- The GOLD PortLoopback test is enabled by default as health monitoring.
- The Cisco NX-OS Release 4.2(1) adds support for the StandbyFabricLoopback test, which is a health monitoring test that is enabled by default, designed to verify the integrity of the data path between the Standby supervisor and the Fabric. The diagnostic has the flexibility to define the action on failure: syslog (default action), onboard diagnostic failure logging, supervisor switchover. Multiple actions can be simultaneously triggered. Before the Cisco NX-OS Release 4.2(1), such a health monitoring test was supported only for the active supervisor in the chassis.
- The GOLD PortLoopback test is enabled as part of the module bootup sequence. Any ports that fail the loopback test stay in the error-disabled state and are not available for configuration.

Note In Cisco NX-OS Release 4.2(1), the PortLoopback test is deprecated on the N7K-M148GS-11 module.

Multicast Enhancements

The following multicast commands support the **route-map** keyword:

- ip pim ssm-range
- ip pim rp-address
- ip igmp join-group
- ip igmp static-group
- ip igmp static-oif

HSRP Enhancements

The Hot Standby Router Protocol (HSRP) is extended in the following ways:

- Added support for CISCO-HSRP-MIB
- Added support for Extended Non-stop Forwarding

Autocheckpoint for Configuration Rollback

The autocheckpoint functionality protects against any unintended loss of configuration, for example in the following situations, which may lead to deleted configurations:

- The user enters the **no feature** command.
- The license expires for a given feature.

Before these events are executed, the system automatically takes a a snapshot of the system configuration and creates checkpoints. These automatic checkpoints are termed system checkpoints; user checkpoints are created when the user enters the **checkpoint** command.

Increased Support for vPCs and Port Channels

Beginning with Cisco NX-OS Release 4.2(1), the system supports 256 virtual port channels (vPCs) and port channels.

IPv6 Support for Management Applications

Beginning with Cisco NX-OS Release 4.2(1), the system supports IPv6 for the following management applications:

- SNMP
- SSH
- Telnet
- syslog
- AAA (RADIUS and TACAS+)
- Call Home

Support for SNMP ACLs

Beginning with Cisco NX-OS Release 4.2(1), the system supports filtering SNMP requests with a particular community name using ACLs.

Border Gateway Protocol Enhancements

Cisco NX-OS Release 4.2(1) includes the following Border Gateway Protocol (BGP) enhancements:

- Advertisement map

- Scalability enhancements
- Support for 4-byte autonomous system number (ASN) plain-number format
- Support for 4-byte ASN communities
- Next-hop tracking enhancements
- Graceful low-memory handling

Limitations

This section describes the limitations in Cisco NX-OS Release 4.2(1) for the Cisco Nexus 7000 Series switches.

This section includes the following topics:

vPCs

Cisco NX-OS Release 4.2(1) for Cisco Nexus 7000 Series switches supports up to 256 vPCs per device.

The Cisco NX-OS software for Cisco Nexus 7000 Series switches does not support PIM SSM or BIDIR on vPCs; PIM ASM is fully supported.

XML Management Interface

You must enable the Secure Shell (SSH) server on the device to use the XML management interface because this is a mandatory requirement of the NETCONF Configuration Protocol (RFC 4741).

QoS

The Cisco NX-OS software does not support Quality of Service (QoS) policing on Layer 2 interfaces in the egress direction, only ingress.

Rollback

In Cisco NX-OS Release 4.1(4) and later releases, if you configure the Cisco NX-OS device while an atomic rollback is in progress, the rollback operation fails.

Port Profiles

In Cisco NX-OS Release 4.2(1), port profiles do not support Layer 3 (routing and routing protocol) commands nor CTS commands.

A maximum of 512 interfaces can inherit a single port profile.

The system allows only one level of inheritance for all commands for the following functions:

- switchport private-vlan mapping
- private-vlan mapping

To inherit port profiles, you must have the same configuration settings for the following:

- switchport
- medium p2p

GOLD

In Cisco NX-OS Release 4.2(1), the PortLoopback test is deprecated on the N7K-M148GS-11 module.

Multicast over Tunnel Interfaces

In Cisco NX-OS Release 4.2(1) and later releases, tunnel interfaces do not support Protocol-Independent Multicast (PIM).

Caveats

This section includes the following topics:

Open Caveats—Cisco NX-OS Release 4.2

This section includes the following open caveats:

- CSCta65195

  Symptom: The **ping** command to a First Hop Redundancy Protocol (FHRP) virtual IP address from an external device may fail.

Conditions: This problem occurs when you enable Strict Unicast RPF on FHRP interfaces, and the response from the **ping** command is forced to take the path using a standby/listen or backup router. To confirm if this symptom exists in your system, enter the **ping** command to a virtual IP address from the same source with unicast RPF disabled on FHRP-enabled interfaces; check if the **ping** command succeeds.

Workaround: Disable Unicast RPF on interfaces where FHRP is enabled, or reconfigure RPF as loose RPF.

- CSCts70896

  Symptom: Cisco Trusted Security (CTS) frames might be dropped in the next hop switch.

  Conditions: This symptom might be seen when CTS is enabled on a 32-port 10-Gigabit Ethernet SFP+ I/O module (N7K-M132XP-12).

  Workaround: None.

Resolved Caveats—Cisco NX-OS Release 4.2(8)

- CSCsm22329

  Symptom: QoS statistics require a policing action to allow marking actions to produce statistics.

  Conditions: When you define a QoS service policy with only marking actions, the statistics do not work. The statistics feature works only when the service policy has a policing action defined also.

  Workaround: This issue is resolved.

- CSCtb50133

  Symptom: If a service writes to the shared database more frequently than expected, it is possible that the shared database counter might roll over, which causes a kernel failure.

  Conditions: This symptom might be seen if the supervisor module is up for a few months or longer, and there a large number of writes to any shared database.

  Workaround: This issue is resolved.

- CSCtc86471

  Symptom: After a supervisor failover on a Cisco Nexus 7000 Series switch, the switch fails to recognize power supply 4. The **show environment power** command does not show the module 4 power supply, but does show an actual output value:

```
switch# sh environment power
Power Supply:
Voltage: 50 Volts
Power                                Actual        Total
Supply    Model                      Output     Capacity    Status
                                   (Watts )     (Watts )
-------  -------------------  -----------  -----------  --------------
1        N7K-AC-7.5KW-US            853 W       7500 W     Ok
2        N7K-AC-7.5KW-US            835 W       7500 W     Ok
3        N7K-AC-7.5KW-US            860 W       7500 W     Ok
4                                                840 W             0 W     Ok
```

  Conditions: This symptom might be seen following a supervisor switchover.

Workaround: This issue is resolved.

- CSCtd59280

  Symptom: Following a restart, OSPFv3 fails to generate an intra-area Link Service Advertisement (LSA) from the IPv6 loopback interface if there are no IPv4 addresses on the interfaces.

  Conditions: You might see this symptom if you do not have any IPv4 addresses on the loopback interfaces.

  Workaround: This issue is resolved.

- CSCtd84148

  Symptom: When you update an existing remark entry in an access list, the following message appears:

  ```
  "ERROR: Object not found"
  ```

  Conditions: This symptom might be seen when an existing remark entry in an access list is updated using a sequence number.

  Workaround: This issue is resolved.

- CSCtf04254

  Symptoms: The timestamp for sysuptime is incorrect on NetFlow export packets.

  Conditions: This symptom might be seen when a Cisco Nexus 7000 Series switch is configured for NetFlow Data Export (NDE).

  Workaround: This issue is resolved.

- CSCtf27037

  Symptom: In a vPC setup that is running Cisco NX-OS Release 4.2(x), the L2fm process fails during an ISSU or a switchover. Other symptoms include the L2fm process exchanging a lot of messages through CFS.

  Condition: This symptom might be seen in this situation:

  - An ISSU occurs with a peer vPC switch that is running Cisco NX-OS Release 4.2(x).
  - When the switchover occurs during the ISSU, the L2fm process recovers MAC addresses from modules and the peer switch. If the last MAC address has a particular flag set, the MAC address recovery process gets into a loop and eventually fails.

  Workaround: This issue is resolved.

- CSCtf94368

  Symptom: An SNMP walk of the OSPF MIB shows OSPF Area 0 as importNoExternal(2), which is incorrect.

  ```
  .1.3.6.1.2.1.14.2.1.3.0.0.0.0 =
  ```

  Conditions: This symptom might be when you do an SNMP walk of the OSPF MIB. The **show ip ospf** command shows the area as normal.

Workaround: This issue is resolved.

- CSCtg10624

  Symptom: An Ethernet interface on a Cisco Nexus 7000 32-port 10-Gigabit Ethernet SFP+ I/O module (N7K-M132XP-12) might go down. When you enter the **shut** command followed by the **no shut** command, the interface does not come back up.

  Conditions: This symptom might be see if the interface is configured for CTS encryption. The problem is intermittently triggered during the CTS rekey operation, which is a normal function of CTS.

  Workaround: This issue is resolved.

- CSCtg83771

  Symptom: The CMP-MGMT port becomes unreachable although the link is up and the address and subnet are correct.

  Conditions: This symptom might be seen when both of the following conditions are true:

  - The connected port is 100 M or 10 M.
  - The link is down (the connected port is administratively shut or the cable is unplugged) while the Connectivity Management Processor (CMP) is booting.

  Workaround: This issue is resolved.

- CSCtg89227

  Symptom: Following a supervisor switchover on a Cisco Nexus 7000 Series switch, the following Border Gateway Protocol (BGP) error from the BGP peer router appears:

  ```
  "%TCP-6-BADAUTH: No MD5 digest from"
  ```

  Conditions: This symptom might be seen when the BGP peer is established with the MD5 password.

  Workaround: This issue is resolved.

- CSCtg95103

  Symptom: The configuration of per-packet load sharing on an interface does not take effect.

  Conditions: This symptom might be seen when per-packet load sharing is not configured on all modules.

  Workaround: This issue is resolved.

- CSCth07851

  Symptom: All packets are dropped for the Fast Ethernet port when broadcast storm control is configured.

  Conditions: This symptom might be seen when broadcast storm control is configured on a 100-MB (Fast Ethernet) port and the control level is set to any value below 4 percent. The storm control drops all packets even when the limit is not reached.

  Workaround: This issue is resolved.

- CSCth33356

  Symptom: In very rare situations, a watchdog may be triggered that results in a failover or reboot.

  Conditions: This symptom might be seen under normal operating conditions on a Cisco Nexus 7000 Series switch running either Cisco NX-OS Release 4.x or Release 5.x software.

  Workaround: This issue is resolved.

- CSCth37883

  Symptom: A rare failure of an internal process (12fm) occurred.

  Conditions: This symptom might be seen after shutting down a port channel.

  Workaround: This issue is resolved.

- CSCth43966

  Symptom: The output of the **show mac address-table** command on a VLAN does not show a specific MAC address even though the Cisco Nexus 7000 Series switch is continuously receiving traffic through the interface.

  The **show mac address-table** command might delete the entry if the same MAC address and affected VLAN are present on both peer switches.

  Conditions: This symptom might be seen if the affected VLAN is not allowed on the vPC peer link.

  Workaround: This issue is resolved.

- CSCth53445

  Symptom: A supervisor 1 module that is running Cisco NX-OS Release 5.0(2) fails because of the adjmgr service. The following message appears:

  ```
  2010 Jun 16 03:45:57.736 N7K-B %SYSMGR-STANDBY-2-SERVICE_CRASHED:
  Service "adjmgr" (PID 4366) hasn't caught signal 6 (core will be saved)
  ```

  Conditions: This symptom might be on a supervisor 1 module that is running Cisco NX-OS Release 5.0(2).

  Workaround: This issue is resolved.

- CSCth62480

  Symptom: The peer-gateway MAC address of a vPC peer is learned on a peer link for a disallowed VLAN.

  Conditions: In some rare conditions, this symptom might be seen when the peer-gateway MAC address is incorrectly synchronized to a VPC peer after a VLAN is removed from the peer link.

  Workaround: This issue is resolved.

- CSCth67182

  Symptom: The standby supervisor in a Cisco Nexus 7000 Series system might not take over as the active supervisor.

Conditions: This symptom might be seen if there is an online insertion and removal (OIR) of the active supervisor before the standby supervisor is in a full HA state. While in this state, both Layer 2 and Layer 3 instability can occur.

Workaround: This issue is resolved.

- CSCth76379

  Symptom: Under certain conditions, the OSPF internal message queue can fill up and can eventually prevent further messaging into OSPF until the conditions are cleared by a reload or supervisor switchover.

  Conditions: This symptom might be seen when the internal messaging queue is full, and there is a large number of updates coming into OSPF. In that situation, it is possible that an OSPF neighbor relationship is not be formed with this router.

  Workaround: This issue is resolved.

- CSCth84134

  Symptom: Buffer leaks can occur in the Messages and Transactional Services (MTS).

  Conditions: This symptom might be seen because there was no message leaking detection mechanism in place.

  Workaround: This issue is resolved.

- CSCti14627

  Symptom: When you perform an ISSU from Cisco NX-OS Release 4.2(3) to NX-OS Release 4.2(6), certain VPC related scenarios can cause duplicate Layer 3 multicast packets across the VPC peer link.

  Conditions: This symptom might be seen when you perform a successful ISSU from Cisco NX-OS Release 4.2(3) to NX-OS Release 4.2(6) on a Cisco Nexus 7000 Series switch with a VPC configured. Layer 3 multicast flows that traverse the VPC peer link can have duplicate packets.

  Workaround: This issue is resolved.

- CSCti19285

  Symptom: When you change the Spanning Tree Protocol (STP) priority for the VLANs on a Cisco Nexus 7000 Series switch, the priority for the private VLANs configured on the switch might not change as expected.

  Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch running Cisco NX-OS Release 4.2(3) or Release 4.2(4).

  Workaround: This issue is resolved.

- CSCti20263

  Symptom: When you add a new VLAN on a peer link with HSRP or VRRP, there is a short traffic interruption of 2 to 7 seconds.

  Conditions: This symptom might be seen on a Cisco Nexus 7000 Series device running Cisco NX-OS Release 4.2(4) when a VLAN is created on a vPC peer node. Some traffic might be lost while VRRP or HSRP is configured and a new VLAN is added in the peer vPC.

Workaround: This issue is resolved.

- CSCti20899

  Symptom: An internal component repeatedly reports the status of transceivers, even if there are no changes in the status. As a result, the cIfXcvrMonStatusChangeNotif trap is repeatedly sent.

  Conditions: This symptom might be seen when an internal component is configured to send a trap for every interval for all ports.

  Workaround: This issue is resolved.

- CSCti22016

  Symptom: After you delete a TACACS server, a Cisco Nexus 7000 Series switch might fail and display the following message:

  ```
  %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service "Tacacs Daemon"
  ```

  If you enter the **show system reset-reason** command, the switch shows the following reset reason:

  ```
  Reason: Reset triggered due to HA policy of Reset , Service: Tacacs Daemon hap reset.
  ```

  Conditions: This symptom might be seen when there is a TACACS configuration change.

  Workaround: This issue is resolved.

- CSCti69843

  Symptom: A username and password can still work when ACS fails.

  Conditions: This symptom might be seen under normal operating conditions of a Cisco Nexus 7000 Series switch.

  Workaround: This issue is resolved.

- CSCti73121

  Symptom: The vrrp_engine process might restart if you periodically enter the **show running vrrp** command or the **show running** command.

  Conditions: This issue might be seen because of a memory leak in the vrrp_engine process of the VRRP service. The problem corrects itself. When the memory leak exceeds thresholds, the process restarts and recovers gracefully.

  Workaround: This issue is resolved.

- CSCti76031

  Symptom: Forwarding ports are incorrectly counted in the system.

  Condition: This symptom might be seen when there are vPC switches in Multiple Spanning Tree (MST) mode.

  Workaround: This issue is resolved.

- CSCti76477

Symptom: After a supervisor switchover in scale setups, the following syslog messages are displayed for some port channels which indicate that specific VLANs are blocked:

```
2010 Sep  4 05:05:44 n7k3-2-Agg %STP-2-LOOPGUARD_BLOCK: Loop guard blocking port
port-channel100 on VLAN1035.

2010 Sep  4 05:05:44 n7k3-2-Agg %STP-2-LOOPGUARD_BLOCK: Loop guard unblocking port
port-channel100 on VLAN1035.
```

Condition: This symptom might be seen when a switchover takes more than 6 seconds to complete and can lead to a momentary traffic drop. The **show logging logfile** command can be used to verify the time taken for the switchover.

Workaround: This issue is resolved.

- CSCti78744

  Symptom: When multiple egress ACLs are applied, and each ACE has a TCP connection attribute, there is a possibility of a netstack process restart if any of the following commands are executed:

  - **sh ip internal acl status**
  - **sh tech netstack**
  - **sh tech**

  The **sh tech netstack** command and the **sh tech** command include the **sh ip internal acl status** command in them so they can trigger this issue.

  Conditions: This symptom might be seen under normal operating conditions of a Cisco Nexus 7000 Series device.

  Workaround: This issue is resolved.

- CSCti92073

  Symptom: An IP multicast packet is not replicated for some interfaces in the outgoing interface list.

  Conditions: When a module reloads, some outgoing interfaces might not receive multicast packets. This situation might occur when an RPF interface for the groups is on the module being reloaded. While the module is still in the process of coming up, a control plane receives a join request for that group (via PIM or IGMP) on an interface on a different module. It is possible that the route update to include this newly added interface is missed. As a result, the newly added interface never receives traffic for this group.

  You can identify this issue by entering the **show forwarding distribution multicast route** command to show the outgoing interface where the packet is not replicated for that interface.

  Workaround: This issue is resolved.

- CSCtj21232

  Symptom: The following log messages might be seen on a Cisco Nexus 7000 Series switch, even after all IDS checks have been disabled through the command-line interface:

  ```
  %EEM_ACTION-6-INFORM: Packets dropped due to IDS check
  ```

  Conditions: This symptom might be seen on a Cisco Nexus 8-port 10-Gigabit Ethernet I/O module XL with ingress traffic. It is not specific to a particular IDS check.

  Workaround: This issue is resolved.

- CSCtj32600

  Symptom: When the resource manager process fails, it does not include all data required in a core file.

  Conditions: This symptom is rare and might be seen only when the resource manager process fails.

  Workaround: This issue is resolved.

- CSCtj42985

  Symptom: Upon applying configuration commands copied from the output of the **show run all** command, Layer 2 broadcast or multicast packets like ARP, HSRP, and so on, do not get switched correctly. Similarly, the port-security feature might not work.

  Conditions: This symptom might be seen because the Layer 2 storm control rate-limiter prevents Layer 2 broadcast or multicast packets from being switched. The **show hardware rate-limit** command indicates that packets are dropped by this rate-limiter.

  Port-security packets will also be dropped, in a similar fashion.

  By default, the Layer 2 storm control and port-security rate-limiters are disabled.

  The reason for this issue is that the **show run all** command incorrectly displays the following output for the default configuration:

  ```
  hardware rate-limiter layer-2 storm-control 0
  hardware rate-limiter layer-2 port-security 0
  ```

  This output shows that the rate-limiter is enabled with 0 pps.

  The output should be displayed as follows:

  ```
  no hardware rate-limiter layer-2 storm-control
  no hardware rate-limiter layer-2 port-security
  ```

  Workaround: This issue is resolved.

- CSCtj54465

  Symptom: The default originate configuration does not work correctly with the redistribute static configuration.

  Conditions: This symptom might be seen when default originate is configured and there is a default route in the BGP RIB and at least one other route.

  Workaround: This issue is resolved.

- CSCtj56827

  Symptom: If flash media is removed during I/O access on a Cisco Nexus 7000 Series switch, a kernel failure might occur.

  Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch running Cisco NX-OS Release 5.0(x) software.

  Workaround: This issue is resolved.

- CSCtj56845

Symptom: When Reverse Path Forwarding (RPF) changes, instability in various processes can occur.

Conditions: This symptom might be seen when the system has a vPC and more than 5000 S,G entries change RPF from one interface to the other.

Workaround: This issue is resolved.

- CSCtj57726

  Symptom: A Cisco Nexus 7000 Series switch might fail because of an ascii-cfg hap-reset. The following message appears:

  ```
  2010 Oct 19 03:52:07 Nexus7000 %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service
  "ascii-cfg" (PID 3769) hasn't caught signal 6 (core will be saved)
  ```

  Conditions: This symptom might be seen if the **rollback** command or the **show diff** command is incorrectly executed without specifying the checkpoint file.

  The following commands have the incorrect syntax where no file is specified, which triggers the failure:

  ```
  switch# rollback running-config file bootflash:
  switch# sh diff rollback-patch running-config file bootflash:
  ```

  Workaround: This issue is resolved.

- CSCtj65960

  Symptom: High CPU usage is seen in the OSPF process.

  Conditions: This symptom might be seen when SNMP polling is used.

  Workaround: This issue is resolved.

- CSCtj80413

  Symptom: Following a downgrade from Cisco NX-OS Release 5.1(1) to NX-OS Release 4.2(4) and a system switchover, the diagnostics manager cored.

  Conditions: This symptom might be seen under normal operating conditions of a Cisco Nexus 7000 Series device.

  Workaround: This issue is resolved.

- CSCtk02812

  Symptom: A ping fails between switch virtual interfaces (SVIs) on Cisco Nexus 7000 Series switches.

  Conditions: This symptom might be seen when vPC track interfaces are flapped and then the orphan port is used for the traffic path.

  Workaround: This issue is resolved.

- CSCtk82138

  Symptom: A Cisco Nexus 7000 Series switch might export NetFlow packets that have some records with high flow duration, high packet count, and zero byte count.

Conditions: This symptom might be seen when there are a high number of NetFlow entries being created or deleted.

Workaround: This issue is resolved.

- CSCtl62218

  Symptom: When an STP Topology change (TCN) occurs, IGMP general queries that are triggered by the querier in the VLAN are sent with a maximum-response-time (MRT) of 1 second. IGMP join reports for all groups in the VLAN are generated within the 1 second period, which causes a short burst that leads to reports being dropped and results in convergence delays for multicast groups. In addition, multiple queries were generated which caused multiple bursts of reports.

  Conditions: This symptom might be seen when there are STP topology changes in a VLAN.

  Workaround: This issue is resolved.

Resolved Caveats—Cisco NX-OS Release 4.2(6)

- CSCta03634

  Symptom: All member objects of a track list are lost after a configuration rollback.

  Conditions: This symptom occurs only when tracking objects of type “track list.” The sequence of events that trigger this symptom is as follows:

  1. Create a track list with some number of objects configured as members of the track list.
  2. Create a checkpoint.
  3. Roll back to the created checkpoint.

  Workaround: This issue is resolved.

- CSCta32738

  Symptom: Under certain conditions, TrustSec 802.1AE security negotiations between ports may not complete successfully.

  Conditions: You might see this symptom if you have 10-Gbps ports running in full rate dedicated mode as part of a port channel with the Cisco TrustSec 802.1AE Encryption/Authentication feature enabled.

  Workaround: This issue is resolved.

- CSCtb79720

  Symptom: The **show ip arp** command does not show the physical interface.

  Conditions: This symptom might be seen under normal operating conditions for the Cisco Nexus 7000 Series switch.

  Workaround: This issue is resolved.

- CSCtc81997

Symptom: If you remove a port channel that is part of a VLAN where ARP entries are leaned, and then packets are sent with a different MAC address in a frame header and ARP header, all the IP traffic is silently discarded.

Conditions: In a VLAN, if ARP request packets are sent with a different MAC address in the frame header and ARP header destined to the IP addresses of the switch, ARP entries are learned for the MAC address in the ARP header. If the physical interface is a port channel and the port channel is removed, then this symptom might be seen.

Workaround: This issue is resolved.

- CSCtd32469

  Symptom: Incorrect syslog messages that indicate a flap or state change are displayed during a supervisor switchover in an ISSU.

  Conditions: This symptom might be seen when a supervisor switchover takes place.

  Workaround: This issue is resolved.

- CSCtd46903

  Symptom: When a Cisco Nexus 7000 Series switch forwards IP unicast packets with a multicast destination MAC address, these packets are erroneously counted by Control Plane Protection (COPP) as if they have been policed by COPP.

  Conditions: This symptom might be seen under normal operating conditions for the Cisco Nexus 7000 Series switch.

  Workaround: This issue is resolved.

- CSCte18771

  Symptom: A static default route is added when a specific static route already exists.

  Conditions: This symptom might be seen when a static default route exists and there are also multiple static routes for a given prefix. If one of the static routes goes down, the static default-route next-hop also gets added as a next hop to the prefix.

  Workaround: This issue is resolved.

- CSCte36301

  Symptom: The **show env power detail** command has been enhanced to display inputs and voltages for power supplies.

  Conditions: Before this enhancement, the input and voltage information was not directly available.

  Workaround: This issue is resolved.

- CSCte66502

  Symptom: Memory threshold configuration commands are available in the nondefault VDC, but they should only be available in the default VDC.

  Conditions: This symptom might be seen under normal operating conditions for the Cisco Nexus 7000 Series switch.

  Workaround: This issue is resolved.

- CSCte78552

  Symptom: There was a problem where you could not log in to a Cisco Nexus 7000 Series switch from SSH or from the console.

  Conditions: This symptom was seen when the / filesystem was full.

  Workaround: This issue is resolved.

- CSCte81687

  Symptom: The Cisco Nexus 7000 Series switch may respond to SNMP queries for CDP information, even though the responses are explicitly blocked using the role configuration.

  Conditions: This symptom might be seen under normal operating conditions for the Cisco Nexus 7000 Series switch.

  Workaround: This issue is resolved.

- CSCte87291

  Symptom: Hosts that are connected to a Cisco Nexus 7000 Series switch isolated or community private VLAN ports might be able to communicate via multicast to hosts on other isolated ports or community ports in a different community VLAN.

  Conditions: This symptom might be seen under normal operating conditions for the Cisco Nexus 7000 Series switch.

  Workaround: This issue is resolved.

- CSCte91297

  Symptom: For a vPC, an IGMP process might take a long time to dequeue the Messages and Transactional Services (MTS) messages, which can result in an expiry state.

  Conditions: This symptom might be seen under normal operating conditions for the Cisco Nexus 7000 Series switch.

  Workaround: This issue is resolved.

- CSCtf02958

  Symptom: After you enter the **no feature netflow** command to disable the netflow feature, flow utilization might be kept high.

  Conditions: This symptom might be seen when the NetFlow feature is disabled on a Cisco Nexus 7000 Series switch.

  Workaround: This issue is resolved.

- CSCtf04254

  Symptom: The time stamp for sysuptime is incorrect on NetFlow export packets.

  Conditions: This symptom might be seen when the Cisco Nexus 7000 Series switch is configured for NDE.

  Workaround: This issue is resolved.

- CSCtf07305

  Symptom: After you apply a port profile to a port, the **show run int e<x/x> all** command no longer displays the default configuration.

  Conditions: This symptom might be seen when the port profile is applied to a port.

  Workaround: This issue is resolved.

- CSCtf11989

  Symptom: The output of the **show system resources** command displays incorrect values for memory buffers and cache.

  Conditions: This symptom might be seen under normal operating conditions for the Cisco Nexus 7000 Series switch.

  Workaround: This issue is resolved.

- CSCtf14732

  Symptom: Policing for an interface is not functional even when there is a QoS policy applied to the interface with a policing configuration.

  Conditions: This symptom might be seen when “match cos” is applied as an additional classifier to a class-map that is already part of a service policy applied to an interface. The hardware does not support the additional classifier and the attempt to add “match cos” fails with a warning message. After this, configured policing parameters are not restored, packets are not policed, and policing is no longer functional for the class.

  Workaround: This issue is resolved.

- CSCtf21920

  Symptom: Traffic on a port-channel subinterface is silently discarded.

  Conditions: This symptom might be seen when port-channel subinterfaces are configured and the module that contains at least one of the members of the port channel is removed and then reinserted. The VLAN is not reprogrammed in the hardware on the module.

  Workaround: This issue is resolved.

- CSCtf25126

  Symptom: The Cisco Nexus 7000 Series switch forwards DHCP requests from clients to the DHCP server. Because the source IP address of the forwarded packet is rewritten with the output (egress) interface IP address of the router instead of with the input interface on which the DHCP request was received, the forwarded DHCP packets may be dropped before they reach the DHCP server.

  Conditions: This symptom might be seen because some firewall rules do not allow only internal IP addresses.

  Workaround: This issue is resolved.

- CSCtf36535

  Symptom: The CSL command should be a hidden command as it used for debugging.

Conditions: This enhancement might be seen on the supervisor module where the command is hidden.

Workaround: This issue is resolved.

- CSCtf56714

  Symptom: Prior to removing the **vpc xx** command for a vPC member link port channel, a warning should be displayed.

  Conditions: This enhancement can be seen in configuration mode.

  Workaround: This issue is resolved.

- CSCtf63878

  Symptom: Following an ISSU from Cisco NX-OS Release 4.2(3) to NX-OS Release 4.2(4), an internal process failed.

  Conditions: The issue might be seen if some Layer 2 interfaces are changed to Layer 3 interfaces prior to the ISSU. Following the ISSU, the interfaces go down.

  Workaround: This issue is resolved.

- CSCtf65013

  Symptom: On a Cisco Nexus 7000 Series switch with the 48-port Gigabit Ethernet I/O module XL module installed, nonfatal interrupt messages were seen following an ISSU.

  Conditions: This symptom might be seen if you enter the s**how module internal exception log** command on the 48-port Gigabit Ethernet I/O module XL module following an ISSU.

  Workaround: This issue is resolved.

- CSCtf67626

  Symptom: Outgoing interfaces (OIFs) between the Multicast Routing Information Base (MRIB) and the Internet Group Management Protocol (IGMP) become unsynchronized.

  Conditions: This symptom might be seen under normal operating conditions for the Cisco Nexus 7000 Series switch.

  Workaround: This issue is resolved.

- CSCtf87006

  Symptom: A warning should be displayed before you delete a port profile that has active members associated with it.

  Conditions: This symptom might be seen under normal operating conditions for the Cisco Nexus 7000 Series switch.

  Workaround: This issue is resolved.

- CSCtf94815

  Symptom: On recovery from a dual-active scenario (that is, when a keep-alive switch and a peer-link switch come back up), STP puts some of the vPC port channels into the blocking state.

Conditions: The symptom might be seen when a peer-link switch and a peer keep-alive switch go down, but both the vPC peer switches and port channels are still up and running. Due to the dual failure, both the vPC peer switches assume that the other side is not functioning. They both take over the role of Master and keep their vPC port channels up. On recovery from such a scenario (that is, when the keep-alive switch and the peer-link switch come back up), STP goes into an inconsistent state and puts some of the vPC port channels into a blocking state. The symptom occurs only when the vPC pair switch is not the STP root.

Workaround: This issue is resolved.

- CSCtg11847

  Symptom: During an ISSU from Cisco NX-OS Release 4.2(3) to NX-OS Release 4.2(4), port-profile configurations were lost, and all the commands for inheriting ports became individual commands.

  Conditions: This symptom was seen when performing an ISSU from Cisco NX-OS Release 4.2(3) to NX-OS Release 4.2(4).

  Workaround: This issue is resolved.

- CSCtg17663

  Symptom: Failures of the internal L2FM process caused orphaned Adjmgr threads.

  Conditions: This symptom might be seen under normal operating conditions for the Cisco Nexus 7000 Series switch.

  Workaround: This issue is resolved.

- CSCtg19983

  Symptom: If you enter the **system-priority** command for a config-vpc-domain, the peer-link is flapped even when the entered value is the same as the currently configured value. When this command is entered noninteractively, such as with the **copy** command, there is no warning prompt and the peer-link is unexpectedly flapped.

  Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch that has the nondefault system-priority value configured.

  Workaround: This issue is resolved.

- CSCtg25657

  Symptom: When default queuing is congested, 10-Mbps ports can cause packet losses on higher speed ports.

  Conditions: This symptom might be seen when a 10-Mbps port is on the same port ASIC as the higher speed ports.

  Workaround: This issue is resolved.

- CSCtg30388

  Symptom: When a **tac-pac** or **show tech** command executes, the system occasionally cannot send control plane packets.

Conditions: This symptom might be seen when an internal process has high utilization and the **show tech** command runs at the same time.

Workaround: This issue is resolved.

- CSCtg31112

  Symptom: When a Cisco Nexus 7000 Series switch has the Hot Standby Router Protocol (HSRP) configured to track prefix reachability and this prefix goes down, HSRP does not state change if there is a less specific prefix tracking the more specific one.

  Conditions: This symptom might be seen when HSRP is configured to track prefix reachability and this prefix goes down.

  Workaround: This issue is resolved.

- CSCtg36399

  Symptom: When you copy and paste the EEM SNMP policy configuration output from a **show running-config** command, the configuration fails when applied to a device.

  Conditions: This symptom might be seen if you configure a SNMP trap action as part of an EEM policy as follows:

  ```
  action 1.0 snmp-trap intdata1 10 intdata2 20 strdata "hello"
  ```

  When you enter the **show running-config eem** command, the display shows extra text:

  ```
  action 1.0 snmp-trap intdata1 10 intdata2 20 strdata "hello" event-type
$_event_type policy-name $_policy_name
  ```

  If you copy and paste this output from the **show running-config** command, it fails for each a**ction <x> snmp-trap** command.

  Workaround: This issue is resolved.

- CSCtg37200

  Symptom: When configuring a threshold for a broadcast storm suppression on the 32-port 10-Gigabit Ethernet SFP+ I/O module, N7K-M132XP-12, and the traffic on that interface breaches the upper threshold and drops later, the Cisco Nexus 7000 Series switch should generate the following two syslog messages, one for above the threshold and one for below the threshold:

  ```
  %ETHPORT-5-STORM_CONTROL_ABOVE_THRESHOLD
  %ETHPORT-5-STORM_CONTROL_BELOW_THRESHOLD
  ```

  When the N7K-M132XP-12 module is immediately reloaded, only the first syslog message displays. Following that, the Cisco Nexus 7000 Series switch does not display either syslog message, even though the storm suppression packets are increasing and stopping correctly

  Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch with a N7K-M132XP-12 module installed and storm suppression configured.

  Workaround: This issue is resolved.

- CSCtg53101

  Symptom: Core files are constantly copied from logflash:core to slot0.

Conditions: This symptom might be seen only when the default path for core files is changed from logflash:core to slot0:

Workaround: This issue is resolved.

- CSCtg58565

  Symptom: Specific routes are leaked to the neighbor, along with the summary route.

  Conditions: This symptom might be seen when a stateful switchover occurs on a switch with EIGRP summarization configured.

  Workaround: This issue is resolved.

- CSCtg66190

  Symptom: A packet that should be sent over a peer link, as a local member of a vPC channel that is down, is dropped on the egress module.

  Conditions: This symptom might be seen only when the vPC port channel is down (administratively down or all members are down) and the module is reloaded. This issue does not affect traffic that is sent over a peer link to orphan ports.

  Workaround: This issue is resolved.

- CSCtg66487

  Symptom: The **show running-configuration** command or the **copy running-configuration startup-configuration** command may fail and the following error displays:

  ```
  switch# show run
  The following SAPs did not respond within the expected timeframe
  Pending SAPS:32
  Printing Ascii configuration for remaining SAPs
  ```

  Conditions: This symptom might be seen when there is temperature fluctuation around the minor threshold and it is logged frequently. You can see this information when you enter the following commands:

  - **show environment temperature**
  - **show log**

  Workaround: This issue is resolved.

- CSCtg69067

  Symptom: High CPU utilization was seen on a Cisco Nexus 7000 Series switch.

  Conditions: This symptom might be seen when a shell process causes high CPU utilization.The Embedded Event Manager may spawn a virtual shell that may freeze and cause high CPU utilization.

  In addition, you might see this symptom if you enter the **show vlan** command. The command may freeze before completion. Press Ctrl+C to interrupt the command.

  Workaround: This issue is resolved.

- CSCtg70629

  Symptom: Following the replacement of a Cisco Nexus 7000 Series chassis, a Layer 3 routed MAC address may be automatically replaced by the system MAC address of the previous chassis.

  Conditions: This symptom might be seen when a Cisco Nexus 7000 Series chassis is replaced.

  Workaround: This issue is resolved.

- CSCtg71428

  Symptom: A Cisco Nexus 7000 Series switch may not export flows properly after you enter the **install all** command and the upgrade or downgrade completes. The rate and amount of flows that are exported are drastically reduced.

  Conditions: This symptom might be seen after you enter the **install all** command and the upgrade or downgrade completes.

  Workaround: This issue is resolved.

- CSCtg74537

  Symptom: A VLAN interface does not go to the UP/UP state when ports in the VLAN are using Spanning Tree Protocol (STP) forwarding.

  Conditions: This symptom might be seen if a new VLAN is created and you enter the **shut** command followed by the **no shut** command on the VLAN (not on the switch virtual interface (SVI)).

  Workaround: This issue is resolved.

- CSCtg76473

  Symptom: The Web Cache Control Protocol (WCCP) does not come up on a Cisco Nexus 7000 Series switch.

  Conditions: This symptom might be seen when BlueCoat with WCCP is used on a Cisco Nexus 7000 Series switch.

  Workaround: This issue is resolved.

- CSCtg77204

  Symptom: A way is needed to identify the source IP address of incomplete ARP entries from the IP event history. To address this symptom, the following new commands were added:

  - **debug ip arp-miss**
  - **show ip internal event-history arp-miss**

  Conditions: This is an enhancement request.

  Workaround: This issue is resolved.

- CSCtg79818

  Symptom: Under a very strict set of circumstances, ACLs may not be programmed in the hardware on Layer 3 subinterfaces.

Conditions: This symptom might be seen when the following very strict set of circumstances are present:

- You must have a parent Layer 3 interface or a port channel without any ACLs applied.
- You must have a number of Layer 3 subinterfaces and there is at least one subinterface with an ACL configured.
- A switchover must have occurred prior to any configuration change.
- If you try to configure an ACL on a previous subinterface that did not have an ACLs configured or any new subinterfaces are created where an ACL is configured, the ACL will fail to program in the hardware. You can confirm this issue if you enter the **show access-list** *name or number* **summary** command.

Workaround: This issue is resolved.

- CSCtg86021

  Symptom: Protocol Independent Multicast (PIM) neighbors lose adjacency when connected through a Cisco Nexus 7000 Series switch.

  Conditions: This symptom might be seen when an ingress port to a Cisco Nexus 7000 Series switch is a trunk, and IGMP snooping is enabled.

  Workaround: This issue is resolved.

- CSCtg91404

  Symptom: A recovery of the vPC process may occur, and the following message might be seen:

  ```
  %SYSMGR-2-SERVICE_CRASHED: Service "vpc" (PID <PID>) hasn't caught signal 11 (core
  will be saved).
  ```

  Conditions: This symptom was seen in Cisco NX-OS Release 4.2(4) in a vPC configuration when the **show vpc orphan-ports** command was entered.

  Workaround: This issue is resolved.

- CSCtg92807

  Symptom: A Cisco Nexus 7000 Series switch fails for the service igmp. The following message might be seen:

  ```
  %SYSMGR-2-SERVICE_CRASHED: Service "igmp" (PID 5472) hasn't caught signal 11 (core
  will be saved).
  %IGMP-3-RESTART_REASON: igmp [18520] IGMP process has restarted, restart reason:
  crashed, will preserve routes
  ```

  Conditions: This symptom was seen after IGMP V3 was configured for a switch virtual interface (SVI) and the Cisco NX-OS was still processing the IGMP V3 report.

  Workaround: This issue is resolved.

- CSCtg97904

  Symptom: On a port ACL, packets were flooding the frame.

  Conditions: This symptom was seen when RDT was not set for multicast packets and the packets were not dropped.

Workaround: This issue is resolved.

- CSCtg99418

  Symptom: A Cisco Nexus 7000 Series switch will have two hostnames: one before login (which is the old name) and one after login (which is the new name).

  Conditions: This symptom might be seen when the new hostname has a period (.) in it.

  Workaround: This issue is resolved.

- CSCth00183

  Symptom: The **show interface transceiver** command does not display the correct SFP type. GLC-LH-SM is displayed as 1000base-BX.

  Conditions: This symptom might be seen when Cisco NX-OS software reads a certain segment in the SFP SPROM to identify the SFP type. The segments in the GLC-LH-SM and the 1000BASE-BX SFP are identical, which leads to the incorrect display of the SFP type.

  Workaround: This issue is resolved.

- CSCth02484

  Symptom: In Cisco NX-OS Release 4.2.x and NX-OS Release 5.0(2), there might be some conditions that cause the Netstack process to fail while collecting details for a **show tech** command or while executing the **show ip internal ppf** command.

  Conditions: This symptom might be seen when the Netstack database is dumped. If there is any corruption in the database, the process might fail.

  Workaround: This issue is resolved.

- CSCth05382

  Symptom: The system.sysname is a standard MIB and when an SNMP walk is done in Cisco IOS or in the Catalyst operating system, the fully qualified domain name (FQDN) is returned. Cisco NX-OS does not support returning the FQDN.

  Conditions: This symptom might be seen when you do an snmp-walk on the system.sysname MIB for the Cisco Nexus 7000 Series switches.

  Workaround: This issue is resolved.

- CSCth14197

  Symptom: A LACP lag mismatch caused port channels to flap.

  Conditions: This symptom was seen after a reload, when a vPC secondary node was restored.

  Workaround: This issue is resolved.

- CSCth18037

  Symptom: The logging server displays the use-vrf default in the configuration even though it is the default.

Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch with a dual supervisor configuration.

Workaround: This issue is resolved.

- CSCth21869

  Symptom: An internal Layer 2 process failed.

  Conditions: This symptom was seen when the router reloads and the switch does not boot up.

  Workaround: This issue is resolved.

- CSCth24137

  Symptom: When a Cisco Nexus 7000 Series switch is configured as Anycast-RP and is also a vPC peer, some multicast groups may be silently discarded because the rendezvous point IP address belongs to the local loopback in the Anycast-RP advertisement being used as a reverse path forwarding NBR.

  Conditions: This symptom is seen intermittently.

  Workaround: This issue is resolved.

- CSCth31712

  Symptom: Some CPU values on the Cisco NX-OS process may spike to more than 100 percent.

  Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch running Cisco NX-OS.

  Workaround: This issues is resolved.

- CSCth32903

  Symptom: The logging level for an interface VLAN disappears after a switchover, and then the configuration does not appear in the running configuration.

  Conditions: This symptom might be seen following a supervisor switchover.

  Workaround: This issue is resolved.

- CSCth37833

  Symptom: An internal Layer 2 process failed.

  Conditions: This symptom was seen while shutting down a port channel.

  Workaround: This issue is resolved.

- CSCth38852

  Symptom: A supervisor failed on a Cisco Nexus 7000 Series switch when an SNMP configuration was applied following an upgrade to Cisco NX-OS Release 5.0(2a).

  Conditions: This symptom was seen following an upgrade to Cisco NX-OS Release 5.0(2a).

  Workaround: This issue is resolved.

- CSCth48500

  Symptom: SNMP counters for a port-channel subinterface are not available.

  Conditions: This symptom might be seen under normal operating conditions for a Cisco Nexus 7000 Series switch.

  Workaround: This issue is resolved.

- CSCth50290

  Symptom: On a Cisco Nexus 7000 Series switch, when an IGMPv3 report is sent to the device with at least one address in the link-local 224.x.x.x range, all addresses within the report will be ignored and not added to the IGMP snooping table.

  The following message will be seen in the debug:

  ```
  igmp: SNOOP: <vlan ID1> Group record for link-local group 224.0.0.251 is ignored
  ```

  Conditions: This symptom is seen only when IGMPv3 is in use. The groups are only ignored if the first address is link-local. For example, if a report is sent with the first group not in the link-local range, this group will be added.

  Workaround: This issue is resolved.

- CSCth54452

  Symptom: In some rare situations, VRRP may send a packet with an invalid type (type 15) from the backup peer that is sourced with the group's virtual MAC address. This may cause all Layer 2 switches on this VLAN to learn this MAC address on the incorrect port.

  Conditions: This symptom might be triggered if a group level **shut** command/**no shut** command is performed over a range of interfaces, such as in the following example:

  ```
  switch(config)# interface vlan 1-200
    vrrp 1
      shut
      no shut
  ```

  Workaround: This issue is resolved.

- CSCth61111

  Symptom: A DHCP relay agent on a Cisco Nexus 7000 Series switch may corrupt DHCP discovery packets.

  Conditions: This symptom might be seen only in NX-OS Release 5.0(2a). It occurs in two cases:

  - If the payload of DHCP is larger than 512 bytes. For example, if the DHCP clients adds 600+ bytes of padding (0x00) behind the end option (0xFF).
  - If the don't fragment bit in the IP header of the DHCP discover packet is set.

  Workaround: This issue is resolved.

- CSCth69876

  Symptom: When a switchover occurs on a vPC primary switch, Spanning Tree Protocol (STP) is not able to generate a bridge protocol data unit (BPDU) on time. As a result, ports get blocked by a loop guard on connected switches.

Conditions: This symptom might be seen when a switchover occurs on a vPC primary switch.

Workaround: This issue is resolved.

- CSCth73939

  Symptom: When you configure the DHCP IP relay command along with WCCP redirect statements on the same interface, the configuration does not allow WCCP to redirect packets.

  Conditions: This symptom might be seen under normal operating conditions for a Cisco Nexus 7000 Series switch.

  Workaround: This issue is resolved.

- CSCth85625

  Symptom: After the active supervisor online insertion (OIR), the OSPF process failed to register with netstack. The neighbor Cisco Nexus 7000 Series switch was sending out hellos, but the affected Cisco Nexus 7000 Series switch did not process them.

  Conditions: This symptom might be seen when the OSPF process failed to register with netstack following the active supervisor OIR.

  Workaround: This issue is resolved.

- CSCth88120

  Symptom: If traffic is restarted just before the Source, Group (S,G) expires, traffic takes longer to converge for certain flows.

  Conditions: You might see this symptom if traffic stops for 3.5 minutes and then resumes.

  Workaround: This issue is resolved.

- CSCth89291

  Symptom: When you add a second instance of an IPv6 static route to a configuration, but the second instance points to a different interface, the second IPv6 static route does not appear in the running configuration or in the startup configuration, but is present in the routing table.

  Conditions: This symptom might be seen if you enter the following configuration:

```
vrf context test1
   ip route 0.0.0.0/0 Ethernet1/9.803 10.174.28.161
   ip route 0.0.0.0/0 Ethernet1/1.802 10.174.28.165
   ipv6 route 0::/0 fc00::226:98ff:fe01:9841 Ethernet1/1.807
   ipv6 route 0::/0 fc00::226:98ff:fe01:9ec1  Ethernet1/9.805
```

  When you enter a **show running** command, one of the IPv6 routes is missing from the configuration, but is in the routing table.

```
switch#sh run | beg "vrf context test1"
 vrf context test1
   ip route 0.0.0.0/0 Ethernet1/9.803 10.174.28.161
   ip route 0.0.0.0/0 Ethernet1/1.802 10.174.28.165
   ipv6 route 0::/0 fc00::0226:98ff:fe01:9ec1 Ethernet1/9.805
                                                < missing 2nd ipv6 static router
```

When you reload of the switch, you will lose the second IPv6 static route.

Workaround: This issue is resolved.

- CSCth98949

  Symptom: When the switch boots up, all Layer 3 feature commands are removed.

  Conditions: This symptom might be seen when an internal race condition occurs between the command-line interface and the license manager.

  Workaround: This issue is resolved.

- CSCti00529

  Symptom: The Ethernet port-channel manager failed when the following command was entered:

  ```
  switch#snmpwalk -v 2c -c public <ip>  .1.3.6.1.4.1.9.9.225.1.3.1.1.1.<port-channel instance>
  ```

  Conditions: This symptom might be seen when you enter the preceding command.

  Workaround: This issue is resolved.

Resolved Caveats—Cisco NX-OS Release 4.2(4)

- CSCsw16354

  Symptom: The device does not process IPv6 packets on the management interface of nondefault VDCs properly.

  Conditions: You will see this symptom because IPv6 protocols such as Neighbor Discovery do not work on the management interface of nondefault VDCs.

  Workaround: This issue is resolved.

- CSCtb01898

  Symptom: When you enter the **show run all** command, the management interface displays shutdown as well as no shutdown.

  Workaround: This issue is resolved.

- CSCtb89376

  Symptom: A FHRP VMAC address is missing on one of the vPC peer switches as a dynamic MAC address after the SVI is shut in a particular order on both Cisco Nexus 7000 Series switches. FHRP is also configured on these VPC switches.

  Conditions: This symptom might be seen in a standard vPC setup where you have two Cisco Nexus 7000 Series switches running vPC, and a third switch. HSRP is configured on all three switches. The two Cisco Nexus 7000 Series switches are not active.

  Workaround: This issue is resolved.

- CSCtc52133

Symptom: Following an ISSU, the logflash: partition might end up not mounted. Attempts to access this partition produce the following error:

```
switch# dir logflash:
compact flash is either not present or not formatted
```

The unavailability of the logflash does not affect packet forwarding but affects serviceability aspects of the device. Core files for process failures and log messages will not be saved if logflash is unavailable.

Conditions: This symptom occurs rarely following an ISSU.

Workaround: This issue is resolved.

- CSCtc88713

  Symptom: When syslog level configuration for the interface-vlan component are modified, the changes are correctly seen when you enter the **show running-configuration** command. After you copy the running configuration to the startup configurations logging configuration is not displayed when you enter the **show startup-configuration** command.

  Conditions: This symptom might be seen when the logging configuration is modified for an interface-vlan component. This is a display issue, where the **show startup-configuration** command does not show the logging configuration for an interface-vlan component.

  Workaround: This issue is resolved.

- CSCtd14622

  Symptom: The UDLD process may fail continuously during an ISSU upgrade.

  Conditions: The symptom might be seen under normal operating conditions of a Cisco Nexus 7000 Series device.

  Workaround: This issue is resolved.

- CSCtd30007

  Symptom: Under certain conditions, there can be between 10-60 seconds of duplicate traffic in the receiver VLANs, depending on the scale of mroutes.

  Conditions: This symptom is seen in the following topology: two or more Cisco Nexus 7000 Series switches acting as routers in the aggregation layer are participating in a LAN scenario. The setup used is an inter-VLAN setup with two redundantly connected Cisco Nexus 7000 Series switches being the L2-L3 boundary, with a Cisco Nexus 7000 Series switch and Catalyst 4948 access switches with receivers behind the access network.

  When one of the aggregation switches is restored after being brought down (like a router reload), there can be between 10-60 seconds of duplicate traffic in the receiver VLANs, depending on the scale of mroutes (higher scales mean potentially longer duration of duplicates).

  Workaround: This issue is resolved.

- CSCtd41676

  Symptom: If a new channel-group number is configured on a physical interface that already has a service-policy applied, the following error will be displayed:

  ```
  switch(config)# int e1/1
  ```

```
switch(config-if)# service-policy type queuing output 10G-qing-out
switch(config-if)# channel-group 1 mode on
command failed: port not compatible [port egress queuing policy]
```

Conditions: This symptom might be seen if you configure a channel-group in this sequence:

1. Configure channel-group 1 on interface E1/1-2.
2. Configure interface E1/1-2 with an egress queueing service-policy that, as expected, will copy the service-policy to E1/1-8 and Po1.
3. Configure channel-group 2 on E1/3-4.

The configuration fails because E1/3-4 already has a service-policy configured from Step 2.

Workaround: This issue is resolved.

- CSCtd50082

  Symptom: If you enter a command in a super-profile, but the sub-profile is not enabled, the command it still executes on the interface.

  Conditions: This symptom might be seen on switch when you enter the following commands:

```
switch(config)# port-profile type port-channel pc1
switch(config-ppm)# state enabled
switch(config-ppm)# port-profile type port-channel pc2
switch(config-ppm)# inherit port-profile pc1
switch(config-ppm)# interface port-channel 1
switch(config-if)# inherit port-profile pc1
switch(config-if)# interface port-channel 2
switch(config-if)# inherit port-profile pc2
switch(config-if)# port-profile type port-channel pc1
switch(config-ppm)# mtu 2000
switch(config-ppm)# sh run int port-channel 2
```

  The output is as follows:

```
!Command: show running-config interface port-channel2
!Time: Thu Nov 26 10:46:10 2009

version 4.2(1)

interface port-channel2
  inherit port-profile pc2
  mtu 2000

switch(config-ppm)# sh run int port-channel 2 expand-port-profile

!Command: show running-config interface port-channel2 expand-port-profile
!Time: Thu Nov 26 10:46:17 2009

version 4.2(1)

interface port-channel2
  mtu 2000

switch(config-ppm)# show port-profile name pc2

port-profile pc2
 type: Port-channel
 description:
 status: disabled
 max-ports: 512
 inherit:
```

```
 pc1
config attributes:
evaluated config attributes:
 mtu 2000
assigned interfaces:
 port-channel2
```

Workaround: This issue is resolved.

- CSCtd57465

  Symptom: Occasionally, loss of traffic through an EtherChannel can be seen for 2-5 seconds.

  Conditions: This issue occurs on a device running Cisco NX-OS 4.2(x) when the following three conditions are met:

  - The EtherChannel has ports on different modules.
  - One of the modules is physically removed.
  - The ejectors are not disabled in the configuration.

  Workaround: This issue is resolved.

- CSCtd58071

  Symptom: MAC addresses on different modules are pointing to different DIs.

  Conditions: This symptom might be seen under the following conditions:

  - MAC-entry points to DI-1.
  - The MAC address moves and points to DI-2. An FF updates entries in other modules.
  - Before l2FMC scans for NL or Move, the MAC address moves back to DI-1. If FF misses, then entries in other modules point to DI-2.

  Workaround: This issue is resolved.

- CSCtd69558

  Symptom: When a Cisco Nexus 7000 switch sends a log to the syslog server that shows how many times the last message was repeated, the log does not match the logs in the logging buffer.

  Conditions: This symptom might be seen in Cisco NX-OS Release 4.2(2a) and later.

  Workaround: This issue is resolved.

- CSCtd73631

  Symptom: On a Cisco Nexus 7000 Series switch with a copper SFP installed, the link status may be declared up, even if there is no cable attached to the transceiver.

  Conditions: This symptom only occurs if the speed is hard-coded and autonegotiation is disabled.

  Workaround: This issue is resolved.

- CSCtd82425

  Symptom: When Global Load Balancing Protocol (GLBP) is configured, a MAC flap may occur on virtual MAC addresses on the access switch connected to Cisco Nexus 7000 Series switches.

A message similar to the following may be displayed:

```
%SW_MATM-4-MACFLAP_NOTIF: Host 0007.b400.4502 in vlan 100 is
flapping between port Te1/0/1 and port Te2/0/1
```

The MAC address 0007.b400.4502 is the vMAC of the GLBP group.

Conditions: This symptom might be seen in a topology where a Layer 2 access switch is dual-connected to two Cisco Nexus 7000 Series switches with GLBP enabled. Both the links from the access switch have to be in Layer 2 spanning tree forwarding state for this problem to occur. Under this configuration, the access switch may see MAC flaps for GLBP vMACs.

Workaround: This issue is resolved.

- CSCtd95226

  Symptom: When there are multiple EIGRP processes associated with an SVI, and the device reloads, some of the EIGRP processes will not be associated with the SVI after the reload.

  Conditions: This symptom occurs in Cisco NX-OS Release 4.2(2a) when there are multiple EIGRP processes associated with the interface:

  ```
  interface Vlan10
    no shutdown
    ip address 10.10.10.2/30
    ip router eigrp 1
    ip router eigrp 2
  ```

  In this example, EIGRP 1 will not be associated with the interface after a reload.

  Workaround: This issue is resolved.

- CSCtd95259

  Symptom: A stub router connected to a Cisco Nexus 7000 Series device does not get updated when you remove an interface from EIGRP on the device.

  Conditions: This symptom might be seen if one or more neighbors are configured as an EIGRP stub router. For example, a loopback is in the EIGRP AS, and you enter the **no ip router eigrp** *name* command for that interface to turn off EIGRP, a neighbor connected on a different interface that is configured as an EIGRP stub will not get an update about this change, and the route will persist on that router unless the EIGRP neighbor is flapped.

  Workaround: This issue is resolved.

- CSCte00702

  Symptom: The **attach** command works from a nondefault VDC, but it should not work in that configuration.

  Conditions: This symptom might be seen under normal operating conditions in Cisco NX-OS Release 4.2(3).

  Workaround: This issue is resolved.

CSCte05048

Symptom: If both redistribute static and default-information originate are configured in EIGRP, the default route (0.0.0.0/0) becomes unreachable in EIGRP.

Conditions: This symptom might be seen when both redistribute static and default-information originate are configured in EIGRP.

Workaround: This issue is resolved.

- CSCte07894

  Symptom: Routing protocols may flap during heavy FIB-miss or glean traffic.

  Conditions: This symptom is seen on neighbors that are known through Layer 3 ports or Layer 2 ports where the IP DSCP is not mapped to the appropriate CoS value in the 802.1p bits of the 802.1Q header.

  Workaround: This issue is resolved.

- CSCte16928

  Symptom: ARP replies sent by a Cisco Nexus 7000 Series device may come from random MAC addresses (including invalid MAC addresses) when the ARP request is a nonstandard size (60 bytes).

  Conditions: This symptom might be seen under normal operating conditions in Cisco NX-OS Release 4.2(1), Release 4.2(1), or Release 4.2(3).

  Workaround: This issue is resolved.

- CSCte17092

  Symptom: The diag_port_lb service may restart following an upgrade to Cisco NX-OS Release 4.2(3).

  Conditions: This symptom be seen under normal operating conditions in Cisco NX-OS Release 4.2(3). This service is diagnostic in nature and there is no functional impact to the normal operation of the system.

  Workaround: This issue is resolved.

- CSCte41190

  Symptom: In Cisco NX-OS Release 4.2(3) and earlier, some Layer 3 interface types save the system default MAC address into the configuration. As a result, if you enter the **copy running-config startup-config** command and move the supervisor module into a new chassis, these Layer 3 interfaces will use the MAC address from the old chassis.

  Conditions: This symptom is seen on all physical Ethernet or port-channel interfaces and their subinterfaces.

  Workaround: This issue is resolved.

- CSCte48168

  Symptom: When one side of a routed interface is shut down, and the link protocol on the other side is down, you can still ping the down interface on the other side if the ping is received on the link protocol on the router that is down, through another route, such as a default route.

  Conditions: This symptom be seen under normal operating conditions in Cisco NX-OS Release 4.2(3).

  Workaround: This issue is resolved.

- CSCte50841

  Symptom: A Cisco Nexus 7000 Series device may fail when SNMP polling sends a malformed SNMPGet for a CeDisplayColor message without appropriate table and index values. The following message appears:

  ```
  %SYSMGR-2-SERVICE_CRASHED: Service "Platform Manager" will lead to HA failover or
  complete switch reset.
  ```

  Conditions: This symptom may occur on a Cisco Nexus 7000 Series device with SNMP enabled and the NMS manager polling the ciscoEntityDisplayMIB.

  Workaround: This issue is resolved.

- CSCte53580

  Symptom: High CPU and packet loss may be exhibited on a Cisco Nexus 7000 Series device when switching Layer 3 traffic to hosts that are directly connected or to a valid next-hop router.

  Conditions: The issue is that ARP is resolved, but there is no resolved host route in the URIB or the FIB. Hardware will forward packets for the destination to the CPU for processing.

  Workaround: This issue is resolved.

- CSCte53614

  Symptom: A Cisco Nexus 7000 Series device that runs Cisco NX-OS Release 4.2.x may run out of memory due to a memory leak in the MTS module under specific conditions. A continuous memory leak can eventually cause the active supervisor module to fail and a switchover to occur. This issue does not affect the standby supervisor module.

  To confirm the memory leak, enter the **show system internal kernel malloc-stats** command. In the last column of klm_mts entry, the number will be very large (more than 100,000) and will increase over time. The following example shows the displayed information:

  ```
  switch# show system internal kernel malloc-stats
   Module           kmalloc       kcalloc      kfree         diff ...
   klm_mts          860524980      00000000     845560260      14964720
  ```

  Conditions: When the following specific SNMP walk or query is performed, a 32-byte memory block will be leaked:

  ```
  snmpwalk on 'CdpCacheEntry' and 'cdpInterfaceTable' tables.
  snmp-get/get-next on
         'CdpCacheEntry' table objects:
           (cdpCacheAddressType ,  cdpCacheAddress,  cdpCacheVersion,
  cdpCacheDeviceId ,
            cdpCacheDevicePort , cdpCachePlatform,  cdpCacheCapabilities ,
            cdpCacheVTPMgmtDomain,  cdpCacheNativeVLAN ,  cdpCacheDuplex,
            cdpCacheApplianceID,  cdpCacheVlanID ,  cdpCachePowerConsumption,
            cdpCacheMTU, cdpCacheSysName, cdpCacheSysObjectID,
            cdpCachePrimaryMgmtAddrType ,     cdpCachePrimaryMgmtAddr,
            cdpCacheSecondaryMgmtAddrType, cdpCacheSecondaryMgmtAddr,
            cdpCachePhysLocation, cdpCacheLastChange )

  cdpInterfaceTable table objects:
           (cdpInterfaceEnable,   cdpInterfaceGroup, cdpInterfacePort)

         Snmp query on the following objects:
           (cdpGlobalHoldTime, cdpGlobalDeviceId, cdpGlobalDeviceIdFormatCpb,
  ```

```
cdpGlobalRun,
          cdpGlobalDeviceIdFormat, cdpGlobalLastChange, cdpGlobalMessageInterval)
```

When you enter the following commands, a 32-byte memory block will be leaked:

- show cdp global
- show cdp interface
- show cdp all
- show cdp entry
- show cdp traffic

Workaround: This issue is resolved.

- CSCte57721

  Symptom: When you use SNMP EEM event publishing with OIDs, the event gets published continuously, which causes the actions to be triggered continuously.

  Conditions: This symptom might be seen under normal operating conditions in Cisco NX-OS Release 4.2(3).

  Workaround: This issue is resolved.

- CSCte58502

  Symptom: A Cisco Nexus 7000 Series device is unable to ping the VRRP master Virtual IP (VIP) address. The master VRRP router does not respond to ARP requests to VIP address.

  Conditions: The issue occurs when a configuration with a large number of VLANs and VRRP groups is applied to a running configuration either from a file or through a script.

  If this issue occurs on the master VRRP router, the registered VIP is not shown in the output of the **show ip process** *vrf* command but is visible in the output of the **show ip route** *vrf* command for the corresponding VRF.

  Workaround: This issue is resolved.

- CSCte69252

  Symptom: A Cisco Nexus 7000 Series device shows the following log messages

```
> 2010 Jan 14 22:05:59.898512 wccp: WCCP-EVNT: vrf  TRUSTED service 92:
> Here_I_Am packet from 10.134.150.89 w/bad recive_id  0x4386
> 2010 Jan 14 22:06:07.073311 wccp: WCCP-EVNT: vrf TRUSTED service 92:
> Here_I_Am packet from 10.134.150.90 w/bad recive_id 0x4385
> 2010 Jan 14  22:06:09.899774 wccp: WCCP-EVNT: vrf TRUSTED service 92:
> Here_I_Am packet from  10.134.150.89 w/bad recive_id 0x4386
```

  Conditions: This symptom might be seen if you enable virtual routing and forwarding instances (VRF) and Web Cache Communication Protocol (WCCP) on a Cisco Nexus 7000 Series device and a McAfee Proxy Server.

  Workaround: This issue is resolved.

- CSCte72124

Symptom: A Cisco Nexus 7000 Series device may have routes installed in the unicast routing table for different VRFs and in the global table that are marked in a pending state, which means that the routes are in the URIB but have not been pushed to the FIB and are not programmed in hardware.

Conditions: This symptom may occur if there is a link flap of a route advertised by an EIGRP neighbor. After the link flap, the route looks as follows:

```
192.168.210.10/32, ubest/mbest: 1/0, pending <<<<<<
      *via 192.168.10.2, Eth10/1.10, [90/128512], 00:00:20, eigrp-200, internal
  switch#
```

Workaround: This issue is resolved.

- CSCte81951

  Symptom: The **show system resources** command shows high CPU usage even when there is not much activity on the switch. In one instance, the CPU utility (user and kernel) was always 100 percent.

  Conditions: You might see this symptom 248 days after the system came up.

  Workaround: This issue is resolved.

- CSCte85821

  Symptom: A Cisco Nexus 7000 Series device that runs Cisco NX-OS Release 4.1(5) displays the following error message:

  ```
  2010 Feb  5 05:04:20.672 MTN-GDC-AGG-N7018A-1
  %SYSMGR-2-TMP_DIR_FULL: System temporary directory usage is unexpectedly high at 87%.
  ```

  Conditions: This symptom might be seen under the following conditions:

  ```
  fscm_status.log filling up /tmp
  show system internal dir /var/tmp
  fscm_status.log    236269152
  ```

  Workaround: This issue is resolved.

- CSCte98663

  Symptom: If you use the **distance** command to modify the administrative distance, and if the external path is preferred over the internal path, Cisco NX-OS EIGRP does not include the AD in its path calculation.

  Conditions: You might see this symptom if the same prefix is redistributed in the EIGRP domain in multiple routers.

  Workaround: This issue is resolved.

Resolved Caveats—Cisco NX-OS Release 4.2(3)

- CSCsy48440

  Symptom: Duplicate multicast packets are sent to receivers in a vPC access network when sources are also in the vPC access network.

Conditions: With both multicast sources and receivers behind vPC access switches in different VLANs and multicast routing is involved, and when a vPC member-link goes down on one switch, packet duplication occurs for any receivers behind the vPC link.

Workaround: This issue is resolved.

- CSCsy91621

  Symptom: A delay that is returned by an SVI interface is different than what is displayed in the output of the **show interface** command. If a protocol uses this value for a metric calculation, then the final metric could be affected.

  Conditions: This symptom might be seen under normal operating conditions.

  Workaround: This issue is resolved.

- CSCsz52347

  Symptom: If you configure a SPAN session to monitor a routed interface, only the received traffic is captured, even if the session is configured for both directions.

  Conditions: This symptom is only for traffic that enters a Layer 2 interface (with SVI as a Layer 3 interface) and then exits a routed (physical Layer 3) interface, which is the source of the monitor session. If traffic enters a routed (physical Layer 3) interface and exits another routed (physical Layer 3) interface which is the source of the monitor session, then the destination port of the monitor session captures traffic in both directions. A SPAN session captures traffic in both directions if traffic entering the routed port is destined to an IP address (SVI) on the switch.

  Workaround: This issue is resolved.

- CSCsz67416

  Symptom: With vPC configured, if one of the vPC peer devices fails, the remaining operational vPC primary device is unable to properly handle operational changes (such as a temporary disconnect or power cycle) on any of the vPC neighboring devices that are connected to one of the vPC member ports. In most cases, the vPC moves into the suspended state.

  Conditions: You might see this symptom if one of the vPC peer devices fails.

  Workaround: This issue is resolved.

- CSCsz86472

  Symptom: When RADIUS authentication is used to authenticate the AAA user via IAS, the switch ignores the user-to-role binding information specified in IAS. The user gets logged in with the default role which is network-operator for any new user, and network-admin for the admin user.

  Conditions: This symptom might be seen when the user-role binding attribute is configured on IAS as follows:

  ```
  "shell:roles*network-admin"
  ```

  Workaround: This issue is resolved.

- CSCta32322

  Symptom: Ethernet interfaces that are a part of a vPC port channel could be error disabled with the following reason: request prohibited by current state.

Conditions: This symptom can be observed because of a race condition between two system processes that are responsible for vPC that get out of sync.

Workaround: This issue is resolved.

- CSCtb17904

  Symptom: Under rare conditions, EIGRP neighbors may flap once after an ISSU.

  Conditions: You might see this symptom when you perform an ISSU with a large number of L3 interfaces in the configuration.

  Workaround: This issue is resolved.

- CSCtb20242

  Symptom: Following an upgrade from Cisco NX-OS Release 4.1(x) to Cisco NX-OS Release 4.2(1), and a peer-link port channel flap, the port goes into a suspended state.

  Conditions: You might see this symptom following an upgrade to Cisco NX-OS 4.2(1) and a peer-link port channel flap.

  Workaround: This issue is resolved.

- CSCtb39514

  Symptom: During initial configuration, a vPC may fail the consistency check with this reason:

```
switch# sh vpc
<snip>
vPC status
----------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- -------------------------- ------------
2    Po2    up     failed      vpc port channel           -
                                mis-config due to vpc
                                links in the 2 switches
                                connected to different
                                partners
```

  The **show vpc consistency-parameters vpc** *vpc_id* command will show different MAC addresses in the lag ID between the local and peer Nexus.

  Conditions: This symptom might be seen if the same physical interface is initially configured with a vPC port channel, and then the configuration is removed and the interface is reconfigured with another vPC port channel. The issue occurs due to the lag ID not matching the lag ID last sent to the vPC manager.

  Workaround: This issue is resolved.

- CSCtb56106

  Symptom: Routes in EIGRP can become stuck-in-action (SIA), which causes some links between neighbors to flap.

  Conditions: This symptom might be seen when you have full mesh topologies with more than 4000 prefixes in the topology table. Parallel links between neighbors increase the probability of hitting this issue.

Workaround: This issue is resolved.

- CSCtb67370

  Symptom: After you physically remove a module from a system that has a switch attached through a vPC, some traffic will not reach its destinations on the switch.

  Conditions: This symptom might be seen when the vPC peer link consists of multiple interfaces across two or modules, and one of the modules is removed, and the removed module contains the only local member of the vPC where traffic loss occurs.

  Workaround: This issue is resolved.

- CSCtb73645

  Symptom: A Cisco Nexus 7000 switch would not allow an SSH connection.

  Conditions: This symptom may have been related to not using a graceful disconnect method.

  Workaround: This issue is resolved.

- CSCtb81656

  Symptom: The output of the **show policy-map interface** command might show the counter values as zero when the policy map has a class that matches on DSCP or precedence.

  Conditions: This symptom might be seen in Cisco NX-OS Release 4.2(2).

  Workaround: This issue is resolved.

- CSCtb84144

  Symptom: The following log message occurs intermittently for admin down ports with SFPs inserted:

  ```
  %ETHPORT-3-IF_SFP_ALARM: Interface Ethernet10/2, Low Rx  Power Alarm
  %ETHPORT-3-IF_SFP_ALARM: Interface Ethernet10/2, Low Rx  Power Alarm cleared
  ```

  Conditions: This symptom might be seen on a switch that is running Cisco NX-OS Release 4.2(2). The interface is administratively down and an SFP is inserted.

  Workaround: This issue is resolved.

- CSCtb89155

  Symptom: All ports in a module are not able to transmit any frames because of an error in the virtual queue index (VQI) allocation.

  Conditions: When a module insertion fails for some reason, the VQIs for that module do not get deallocated, which may result in multiple VQIs being assigned to the same module. In this situation, the packets sent to the module may never be transmitted out.

  Workaround: This issue is resolved.

- CSCtb94236

Symptom: The Access Control Server (ACS) returns the error code "External DB reports error condition," and Cisco NX-OS authenticates the user locally and interprets the error as meaning ACS is unreachable.

Conditions: Cisco NX-OS is configured for TACACS authentication, and the user account exists both locally and in the external database.

Workaround: This issue is resolved.

- CSCtb95529

  Symptom: IP Protocol Independent Multicast (PIM) is not supported over tunnel interfaces in Cisco NX-OS 4.x releases.

  Conditions: PIM can be configured on tunnel interfaces, but the configuration does not take effect.

  Workaround: This issue is resolved.

- CSCtb98654

  Symptom: EIGRP neighbors in a non-default virtual routing and forwarding instance (VRF) may not come up after an ISSU.

  Conditions: You might see this symptom in an EIGRP configuration in a nondefault VRF.

  Workaround: This issue is resolved.

- CSCtc01675

  Symptom: EIGRP routes learned from redistribution may get stuck in the topology table.

  Conditions: Routes learned from redistribution are removed by the other protocol being redistributed. When this occurs, the routes may remain in the topology table. The redistribution source protocol must also have ECMPs to the destinations for this issue to occur.

  Workaround: This issue is resolved.

- CSCtc02698

  Symptom: In rare conditions, a Nexus 7000 Series switch may not install routes from certain OSPF neighbors in the routing table.

  Conditions: This symptom might be seen following an OSPF process restart or an ISSU.

  Workaround: This issue is resolved.

- CSCtc10316

  Symptom: The routing table installs an external EIGRP route instead of the internal route.

  Conditions: You might see this symptom when EIGRP learns an external route and an internal route for the same prefix. The external route needs to be a better metric than the internal one.

  Workaround: This issue is resolved.

- CSCtc11159

  Symptom: The Interface Manager process fails during a VDC suspend operation.

Conditions: This symptom might be seen when a VDC that contains many switched virtual interfaces (SVIs) is either suspended or reloaded.

Workaround: This issue is resolved.

- CSCtc13255

  Symptom: If you configure two stop bits for the serial console parameter and copy the running-config to the startup-config and then reload the supervisor, the supervisor does not boot.

  Conditions: You might see this symptom when two stop bits are configured.

  Workaround: This issue is resolved.

- CSCtc15107

  Symptom: The Access Control Server (ACS) becomes unresponsive after some time and ACS 2.3.6 fails on Solaris.

  Conditions: When per command authorization is enabled on a Cisco Nexus 7000 Series switch and the corresponding TACACS+ server used is ACS 2.3.6(2) on Solaris, then ACS becomes unresponsive and eventually fails.

  Workaround: This issue is resolved.

- CSCtc20038

  Symptom: An HSRP engine process restarts.

  Conditions: This symptom might be seen in rare conditions when the reload timer is configured, and then gets triggered. This typically happens when a Cisco Nexus 7000 Series switch comes up with HSRP in the startup configuration, or an interface with an HSRP configuration is enabled with the **no shut** command after a reload. This condition will happen only if the HSRP group reaches the "listen" state, and the configured reload delay timer gets triggered in this state.

  Workaround: This issue is resolved.

- CSCtc22126

  Symptom: VLANs may become errdisabled on trunks. The following error message may be displayed:

  ```
  ERROR:   Module 7 returned status "feature combination is not supported  in tcam"
  ```

  Entering the **no switchport** command followed by the **switchport** command may cause the module to fail.

  Conditions: This symptom might be seen when the following features are configured:

  - SVI: Netflow, ACL
  - VLAN: policy-map and VACL.

  Workaround: This issue is resolved.

- CSCtc28760

  Symptom: There is a traffic interruption of up to 30 seconds when an HSRP state changes in a vPC environment, such as when reloading the HSRP primary peer with preempt enabled.

Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch configured as a vPC cluster with HSRP. This issue may depend on the HSRP timers, preempt configuration, and number of vPCs or HSRP groups; it is not seen in all environments.

Workaround: This issue is resolved.

- CSCtc29293

  Symptom: In certain network topologies, an intermittent internal event can cause EIGRP neighbor flaps.

  Conditions: This symptom might be seen in certain network topologies with a large number of routes, such as a full mesh topology with thousands of routes.

  Workaround: This issue is resolved.

- CSCtc32803

  Symptom: A link goes down on a switch-PC connection with MDIX disabled.

  Conditions: This symptom can be seen when you connect a device to the switch with the following configuration:

  - There is no MDIX on the interface
  - The speed and duplex are hard-coded on the interface and PC
  - A straight-through cable is used

  Workaround: This issue is resolved.

- CSCtc34401

  Symptom: EIGRP failed after the **show ip eigrp topology active** command was entered.

  Conditions: This symptom was seen after the **show ip eigrp topology active** command was entered on a switch running Cisco NX-OS Release 4.2(2).

  Workaround: This issue is resolved.

- CSCtc36424

  Symptom: On a Cisco Nexus 7000 switch that is routing traffic between VLANs using a switched virtual interface (SVI), there is a possibility that some packets may be routed in the software path instead of in the hardware.

  Conditions: The problem occurs when the next-hop device's MAC address on the egress VLAN is the same as the destination MAC address of the packet on the ingress VLAN, and that MAC address is programmed as a local MAC address on the Cisco Nexus 7000 switch with the destination index pointing to 0x400 (the CPU interface).

  Workaround: This issue is resolved.

- CSCtc46435

  Symptom: A VDC may become stuck and show an updating status, as in the following example:

```
switch# show vdc
vdc_id             vdc_name         state               mac
 ------              -------         -----               ----------
```

```
1               N7k-1           updating            00:24:98:ea:9a:41
2               N7K-2            active              00:24:98:ea:9a:42
```

In this situation, you cannot allocate a physical interface to a VDC that is stuck.

Conditions: This symptom is rarely seen.

Workaround: This issue is resolved.

- CSCtc48208

  Symptom: After BGP flap changes are made in the routing table, routes that have the same prefix but a different mask are not always redistributed to OSPF.

  Conditions: This symptom might be seen with routes that have the same prefix, but a different mask, and is triggered by a BGP flap or changes in the BGP routing table.

  Workaround: This issue is resolved.

- CSCtc51606

  Symptom: When there is traffic oversubscription on a Cisco Nexus 7000 Series switch, the output drop counter may not work.

  Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch running Cisco NX-OS Release 4.2.

  Workaround: This issue is resolved.

- CSCtc55019

  Symptom: EIGRP does not readvertise an external route when an internal route with the same prefix is lost.

  Conditions: The route must be learned as both an external route (using the **redistribute static** command) and an internal route.

  Workaround: This issue is resolved.

- CSCtc55490

  Symptom: Protocol Independent Multicast (PIM) neighbors were lost over a congested Layer 2 link.

  Conditions: There are various conditions that could cause this:

  - PIM neighbors are on a VLAN where Cisco NX-OS is running with IGMP Snooping enabled
  - PIM neighbors are on a VLAN with no SVI and Cisco NX-OS is running with IGMP Snooping disabled

  Workaround: This issue is resolved.

- CSCtc57821

  Symptom: EIGRP neighbors may flap when you enter the **show tech-support eigrp detail** command.

  Conditions: This symptom might be seen when the event-log-size is greater than 100000.

  Workaround: This issue is resolved.

- CSCtc58755

  Symptom: A tracking object feature fails to be triggered.

  Conditions: This symptom occurs only when the tracking object is of type track-list that tracks multiple objects, and the following sequence of events occurs:

  - The running configuration is saved to the startup configuration.
  - The switch is reloaded.

  After the reload, track-list stops tracking the individual objects.

  Workaround: This issue is resolved.

- CSCtc59804

  Symptom: The PIM hello authentication does not match any class in the default CoPP configuration on the Cisco Nexus 7000 Series switch.

  Conditions: This symptom might be seen with the default CoPP.

  Workaround: This issue is resolved.

- CSCtc66732

  Symptom: An SVI interface goes down when a vPC link goes down.

  Conditions: A vPC pair of two Cisco Nexus 7000 Series switches, such as N7k-a and N7k-b are connected to another switch with VPC(Po101). N7k-a and N7k-b are running NS-OS Release 4.2(2a). Po101 is a trunk link and has allowed VLAN 100-101,103. VPC peer-link(Po1) has allowed VLAN 100-104,999. SVIs (VLAN 100-104,999) are configured and are up.

  When vPC link (eth7/1 of N7k-a) of N7k-a goes down, VLAN 100,101,103 of N7k-a also go down although the VPC peer link is still up and the trunk includes these VLANs.

  Workaround: This issue is resolved.

- CSCtc73726

  Symptom: Routes in EIGRP can occasionally become SIA, which causes neighbor flaps.

  Conditions: This condition happens with full mesh topologies in large EIGRP networks.

  Workaround: This issue is resolved.

- CSCtc77820

  Symptom: EIGRP did not process unreachable external routes with a matching router ID. This may result in stale paths in the topology table.

  Conditions: This symptom might be seen when an external path as a feasible successor is promoted to a successor.

  Workaround: This issue is resolved.

- CSCtc79421

Symptom: An SNMP walk on interface number 0 returns the total number of physical interfaces only. The port channel interfaces and the VLAN interfaces are not taken into account.

Conditions:

Workaround: This issue is resolved.

- CSCtc79515

  Symptom: The following message is displayed:

  ```
  %NETSTACK-3-NO_SH_MEM: netstack [3160] Failed to allocate shared memory
  Shared memory mallet failed in MRIB notification handler
  ```

  Conditions: The memory leak may occur when interfaces are moved between VRFs or when the IP address mask length is changed.

  Workaround: This issue is resolved.

- CSCtc79580

  Symptom: When a third party SNMP application is used to do an SNMP walk, the responsible process may restarted.

  Conditions: This symptom might be seen in a configuration where a specific VLAN is fragmented across a large number of ports (more than64 ports) such as when the following range of ports in a VLAN is counted as 2 ranges: 1/1-32, 2/1-32

  Workaround: This issue is resolved.

- CSCtc82869

  Symptom: When you have two Cisco Nexus 7000 Series switches that are connected via a port channel and that have a vPC configured between them, and you enter the **shut** command on the P0 interface on the primary vPC, the switch fails because of the PIM process. A core dump is generated.

  Conditions: This symptom might be seen when vPC is configured and there is a need to bounce the interface port channel.

  Workaround: This issue is resolved.

- CSCtc83165

  Symptom: And SNMP process may core when a specific SNMP configuration is applied to the configuration.

  Conditions: This symptom might be seen under normal operating conditions for a Cisco Nexus 7000 Series device.

  Workaround: This issue is resolved.

- CSCtc83746

  Symptom: A Solaris ACS machine may go into an unresponsive state during command authorization.

  Conditions: This symptom might be seen if command authorization has not been enabled on the Nexus device.

Workaround: This issue is resolved.

- CSCtc84869

  Symptom: A Cisco Nexus 7000 Series switch may fail when an EEM pallet is configured and an incorrect SNMP OID is configured. The service “snmp hap” will fail and cause a supervisor failover.

  Conditions: This symptom only occurs when an incorrect SNMP OID is entered. When a correct OID is used, there is no failure.

  Workaround: This issue is resolved.

- CSCtc97131

  Symptom: When an Cisco Nexus 7000 Series switch is ISSU upgraded from 4.2(1)E2 to 4.2(2a)E1, and if there are SVI interfaces that are in the shutdown mode part of OSPF, the network for the shutdown SVI will still be advertised by OSPF to its neighbors. Only some shutdown SVIs get advertised, and not all.

  Conditions: This symptom might be seen if there are SVI interfaces that are in the shutdown mode part of OSPF.

  Workaround: This issue is resolved.

- CSCtc94771

  Symptom: When flapping the peer link between two Cisco Nexus 7000 Series switches, a device connected via a non-vPC link to the secondary Cisco Nexus 7000 Series switch may stop receiving ARP replies from the primary Cisco Nexus 7000 Series switch.

  Conditions: This issue might be seen after flapping the link. It can be seen after one flap, but multiple flaps are typically required before the issue occurs.

  Workaround: This issue is resolved.

- CSCtd00583

  Symptom: A Cisco Nexus 7000 Series switch may experience high CPU usage due to a netstack process reaching above 100%.

  Conditions: This symptom is rarely seen.

  Workaround: This issue is resolved.

- CSCtd14544

  Symptom: A Cisco Nexus 7000 Series switch may experience an unexpected reload due to the Netstack process and the following message may be displayed:

  ```
  %SYSMGR-2-SERVICE_CRASHED: Service "netstack" (PID ####) hasn't caught
  signal 11 (core will be saved).
  ```

  Conditions: The Netstack failure may occur under some conditions while recovering the IP multicast addresses.

  Workaround: This issue is resolved.

- CSCtd16345

  Symptom: When you attempt to configure an interface with a CLI command on a Cisco Nexus 7000 Series switch, you might see the following error message:

```
switch(config)# int eth15/48
     switch(config-if)# description test
     ERROR: Writer failed to open the file
```

  At the same time, the switch may also experience a standby supervisor sync error as shown in the following message:

```
%SYSMGR-2-STANDBY_BOOT_FAILED: Standby supervisor failed to boot up.
  %SYSMGR-2-GSYNC_SNAPSHOT_SRVFAILED:
  Service "ppm" on active supervisor failed to store its snapshot (error-id
0x80480018).
```

  Conditions: You might see this symptom after configuring the port-profile feature and after entering multiple **show run** commands.

  Workaround: This issue is resolved.

- CSCtd16868

  Symptom: A Cisco Nexus 7000 Series switch detects a duplicate IPv6 address and displays the following message:

```
%ICMPV6-3-ND_LOG:  icmpv6 [3875]  Duplicate address detected on Ethernet1/1 from mac
xxxxxxx
```

  Conditions: This symptom might be seen if the link local address used by a neighbor is also used on any other Cisco Nexus 7000 Series switch interface.

  Workaround: This issue is resolved.

- CSCtd18772

  Symptom: A Cisco Nexus 7000 Series switch may not accept a port profile configuration, as shown in the following output:

```
switch(config)# int e14/48
switch(config-if)# inherit port-profile test
switch(config-if)# sh run int Eth14/48
  version 4.2(2a)
  interface Ethernet14/48
```

  Conditions: This symptom might be seen when you attempt to configure a port profile.

  Workaround: This issue is resolved.

- CSCtd19402

  Symptom: A process could restart while logging a syslog message.

  Conditions: The message has be logged in the time window when the Netstack process has failed and it is being restarted. Also, at least one external syslog server has to be configured.

  Workaround. This issue is resolved.

- CSCtd34841

  Symptom: The **snmp get** command shows wrong values for IP address and mask.

  Conditions: The **snmp get** command for the OID 1.3.6.1.2.1.4.1.3.*ip-address* returns the wrong values.

  Workaround: This issue is resolved.

- CSCtd55248

  Symptom: Users on a failed HSRP VIP will not be able to route out of the VLAN and will not be able to ping or reach the HSRP Active VIP on the subnet.

  Conditions: After a failover, the HSRP VIP on one of the subinterfaces or SVI might not be reachable.

  Workaround: This issue is resolved.

- CSCtd64167

  Symptom: A Cisco Nexus 7000 Series switch UDLD takes a large space in the /tmp directory and constantly uses it.

```
switch#sh system internal dir /var/tmp | i udld
                        udld_trace.txt.0x50e015c4    298921984
switch#sh system internal dir /var/tmp | i udld
                        udld_trace.txt.0x50e015c4    303652864
```

  The following error message might be displayed:

```
n7k-1 %SYSMGR-2-TMP_DIR_FULL: System temporary directory usage
is unexpectedly high at 100%.
```

  Conditions: This symptom might be seen on a Cisco Nexus 7000 Series switch running a Cisco NX-OS Release 4.1(2) system image.

  Workaround: This issue is resolved.

- CSCtd69947

  Symptom: The object tracking line protocol of an interface of the VPC peer link shows an incorrect status when you enter the **track object-id interface** *interface* **line-protocol** command.

  Conditions: This symptom might be seen when a vPC peer is down, but the interfaces are up.

  Workaround: This issue is resolved.

Resolved Caveats—Cisco NX-OS Release 4.2(2a)

- CSCtc06496

  Symptom: The XML subagent (xmlsa) process fails when you enter a combination of **show interface** commands.

Conditions: This symptom might be seen when you enter **show interface** commands in a certain order on an XML interface. For example, entering the **show interface capabilities** command followed by the **show interface flowcontrol** command triggers this issue. Cisco DCNM does run into this issue during discovery, but automatically re-opens a new connection and retries the last command.

As a result of this issue, three or fewer core files are occasionally created and they consume some memory. The failure instances are visible in syslog and when you enter a **show core** command.

Workaround: This issue is resolved.

- CSCtc17493

  Symptom: You might see an unexpected supervisor switchover or system reload.

  Conditions: Because of a slow resource leak, the Cisco NX-OS online diagnostic loopback process may core and cause the supervisor to switch over (in a dual-supervisor system) or the system to reload (in a single supervisor system).

  Workaround: This issue is resolved. If you upgrade to Cisco NX-OS Release 4.2(2a), follow the instructions in the Upgrade Information section that follows.

  Upgrade Information

  After upgrading from an earlier version to Cisco NX-OS Release 4.2(2a), issue the following hidden command to clean any stale resources left from previous images:

Note Perform this step only on a dual supervisor switch, after an ISSU. This step should not be done on a single supervisor system or after a reload.

```
switch# diagnostic pss shrink
```

On both single supervisor and dual supervisor switches, re-enable the online diagnostics tests if they were disabled earlier:

1. Enter the following command on each of the modules that are present on the device:

```
(config)# diagnostic monitor module <x> test 5,6
```

2. Enter the following command to enable the bootup diagnostics:

```
(config)# diagnostic bootup level complete
```

3. Enter the following command to save the configuration to startup-config:

```
(config)# copy running-config startup
```

Resolved Caveats—Cisco NX-OS Release 4.2(2)

All the caveats listed in this section are resolved in Cisco NX-OS Release 4.2(2) for the Cisco Nexus 7000 Series switches:

- CSCsz43535

  Symptom: The backup VRRP is not reachable from the master VRRP.

  Conditions: This symptom might be seen when VRRP is configured and the same IP address is used for both the VRRP IP address and the real address on the master VRRP.

  Workaround: This issue is resolved.

- CSCsz51037

  Symptom: If you configure a Cisco Nexus 7000 Level 5 password by entering the **username admin password 5 test role network-admin** command, you will be unable to log in to the switch.

  Conditions: This symptom might be seen on any Cisco Nexus 7000 Series switch. When Level 5 is used, the switch expects an encrypted password.

  Workaround: This issue is resolved.

- CSCta24404

  Symptom: When a module reloads or a port channel member flaps, a software inconsistency may cause the following issues with packet forwarding on port channels:

  - The egress virtual switch link (VSL) bit can be incorrectly programmed which results in loops.
  - The VLAN membership information in the software can be incorrect which results in the VLANs not being enabled on certain port channels. This issue in turn results in packet drops for these VLANs.

  Conditions: You might see this symptom after you perform an ISSU to Cisco NX-OS Release 4.2(1) from an earlier Cisco NX-OS release; however, the software inconsistency may not appear immediately after the ISSU, but may be seen after a module reload or port flaps.

  Workaround: This issue is resolved. If the problem existed in a system that was running a release earlier than Cisco NX-OS Release 4.2(2), the ISSU to Release 4.2(2) will fix the problem automatically.

- CSCta30863

  Symptom: You cannot apply the WCCP redirect in function and the redirect out function for a single service group on an interface at the same time.

  Conditions: This symptom appears when you are working with WCCP.

  Workaround: This issue is resolved.

- CSCta55476

  Symptom: After a vPC peer failure, learning breaks on non-vPC uplinks as follows:

  1. MAC address learning breaks on non-VPC L2 ports when the vPC peer is reloaded or the peer link goes down. This happens when the last member of a port channel on a module goes down. The packets are flooded, and therefore there is no packet loss.
  2. Following the occurrence of 1, if there is a port flap of non-vPC L2 ports, L2 learning on non-vPC L2 ports is restored, but MAC address learning happens on the vPC peer link, which can result in packet drops.

  Conditions: When the last member of a peer link port channel on a module goes down, learning is disabled on all non-vPC L2 ports on the module. If a flap occurs after this, learning on non-vPC L2 ports is restored, but learning is enabled on vPC peer-links.

  Although this problem did not exist in Cisco NX-OS Release 4.2(1), it did exist in the releases prior to Release 4.2(1), and an upgrade from an earlier Cisco NX-OS Release, such as Release 4.1(5) to Release 4.2(1) would not automatically fix the issue. An upgrade from any earlier Cisco NX-OS release to Release 4.2(2) automatically fixes the problem.

Workaround: This issue is resolved.

- CSCta96278

  Symptom: When you reload a VDC that has a vPC running in it, a heartbeat failure may occur for the vPC.

  Conditions: You might see this condition if the vPC that is running in the VDC that you reload has a peer-keep alive configuration under the vPC domain.

  Workaround: This issue is resolved.

- CSCtb01813

  Symptom: You might see an outage for Layer 2 traffic that traverses the device from a non-vPC link to a vPC link when the vPC peer link is down.

  Conditions: Traffic that traverses through the secondary vPC switch will have an outage.

  Workaround: This issue is resolved.

- CSCtb15386

  Symptom: A Cisco Nexus 7000 switch may send a unicast Address Resolution Protocol (ARP) reply from the wrong interface if the Ethernet source MAC address of the ARP request is different from the sender MAC address in the ARP payload.

  Conditions: This symptom only occurs when then the Ethernet source MAC address is not the same as the ARP sender address in the ARP payload.

  Workaround: This issue is resolved.

- CSCtb18456

  Symptom: The event manager service failed and the following message was displayed:

  ```
  Nexus Service "evms" crash when using % in event manager configuration:
  %SYSMGR-2-SERVICE_CRASHED: Service "evms"
  ```

  Conditions: This symptom might be seen when the percent sign (%) character is used in the active event manager configuration, and either the **show run eem** command or the **show run | i eem** command is entered.

  Workaround: This issue is resolved.

- CSCtb31933

  Symptom: On a cold boot of a Cisco Nexus 7000 Series switch, the following startup configurations are not applied: poweroff and power-supply redundancy-mode.

  Conditions: You might see this symptom when you power up a Cisco Nexus 7000 Series switch.

  Workaround: This issue is resolved.

- CSCtb35248

  Symptom: EIGRP routes that were removed from the EIGRP topology table were still present in the routing table.

Conditions: This symptom might be seen on any Cisco Nexus 7000 Series switch after a link flap.

Workaround: This issue is resolved.

- CSCtb35959

  Symptom: An ISSU upgrade from any Cisco NX-OS Release 4.1(x) release to Cisco NX-OS Release 4.2(1) release failed or aborted when one or more of the following behaviors were observed:

  - The standby and active supervisor were upgraded to the new software images, but the modules upgrade failed.
  - The **copy running-config startup-config** command entered from different VDCs timed out or aborted.
  - The **show running-config snmp** command or any other SNMP related commands, such as the **show interface counters snmp module** *slot* command, timed out.

  Conditions: This issue is related to an SNMP process not responding to a message that it does not handle because of SNMP polling by any external management application.

  Workaround: This issue is resolved.

- CSCtb39479

  Symptom: When you restart or suspend a VDC, traffic disruption can occur, and ports on neighboring switches may go into an errdisabled state.

  Conditions: This symptom might be seen when vPC or Unidirectional Link Detection (UDLD) is set to aggressive.

  Workaround: This issue is resolved.

- CSCtb39810

  Symptom: There is a 100 percent packet duplication for packets that hit the adjacency. The second copy will have a time to live of one less than the first copy.

  Conditions: This symptom might be seen if you configure a static ARP entry with a multicast MAC address, such as: ip arp 10.55.55.2 0100.5E01.0101.

  Workaround: This issue is resolved.

- CSCtb44730

  Symptom: During a EIGRP stuck-in-action (SIA), you might see the following message:

  ```
  %EIGRP-4-UNEQUAL_METRICS:  eigrp-1 [5257](default-base) EIGRP: Unequal metric
  (10.196.0.92/30),delay [128512/4294967295], bandwidth [2560/2560], mtu [1500/1500],
  hopcount [2/2],reliability [255/255], load [1/1]
  ```

  Conditions: This informational message might be seen during a storm of EIGRP messages.

  Workaround: This issue is resolved.

- CSCtb52260

  Symptom: OSPF configured with MD5 authentication returns bad authentication errors after a module reloads.

Conditions: This issue might be seen under the following conditions:

- If you enter the **area** *area-id* **authentication [message-digest]** command or any other area level authentication command, followed by any authentication type such as md5.
- If no other area level command such as NSSA/stub (area *id* nssa/stub), cost (area *id* default-cost) or address-range is configured.

The issue will be triggered if either one of the following events occur:

- If you unconfigure all interfaces that belong to that area, and then configure any interface(s) in that area, then those interfaces will not inherit the authentication command from the area and there will be authentication errors for the new interfaces.
- If all interfaces that belong to the area are on a particular module, and the module reloads, then there will be authentication errors seen on those interfaces once they come up again.

Workaround: This issue is resolved.

- CSCtb52573

  Symptom: A vPC domain with Hot Standby Router Protocol (HSRP) configured and routers or switches attached that share the same HSRP group might discard traffic after HSRP state changes.

  Conditions: This symptom might be seen in a topology where two vPC domains (1 and 2) are connected back-to-back using a vPC. All four switches share the same HSRP group. Initial programming of the HSRP MAC address is done in domain 1 (based on HSRP priority). Domain 2 learns the HSRP MAC address over the vPC. After an HSRP state change that is caused by a configuration change or tracking object, the active HSRP can move to domain 2. In this case, switches in domain 1 might keep stale entries and will not forward traffic to domain 2. Duplicate HSRP MAC entries can be observed in the MAC address table.

  Workaround: This issue is resolved.

- CSCtb54403

  Symptom: The **write erase** command was not accepted for non-default VDCs.

  Conditions: This symptom might be seen when you enter the **write erase** command under non-default VDCs.

  Workaround: This issue is resolved.

- CSCtb62617

  Symptom: If you apply ACLs in software to small TCP or UDP fragments, the Netstack process may fail.

  Conditions: This symptom might be seen when the total length of the fragment that is processed is less than the minimum size of IP and TCP or UDP headers.

  Workaround: This issue is resolved.

- CSCtb64914

  Symptom: The **no hardware ejector enable** command displays as part of the **show running-configuration** command.

  Conditions: This symptom might be seen when you enter the **no hardware ejector enable** command.

Workaround: This issue is resolved.

- CSCtb67618

  Symptom: After a module reload or an ISSU, the following messages are displayed:

  L2PD_IF_TO_HWIDX_FAILED

  These messages may indicate incorrect forwarding on one or more modules.

  Conditions: This symptom might be seen if state changes of the FHRP have previously occurred, and if an ISSU or a module reload was triggered.

  Workaround: This issue is resolved.

- CSCtb69155

  Symptom: MAC addresses are not cleared correctly on a vPC.

  Condition: This symptom might be seen when there are extra VLANs in the configuration that are not allowed on a peer link. For example, if you have 20 VLANS on both peer switches, but allow 10 VLANs on the peer link, the vPC will not carry VLANs 11-20.

  Workaround: This issue is resolved.

- CSCtb72710

  Symptom: If you enter commands that produce long output, a Telnet or SSH session with a Cisco Nexus 7000 vPC peer might stop responding.

  Conditions: This symptom might be seen when you have a session over a vPC link and the vPC member link that is directly connected to the destination is down.

  Workaround: This issue is resolved.

- CSCtc11044

  Symptom: After you enter a **reload** command for a VDC or a **no suspend** command for a VDC, you cannot enter a **copy running-config startup-config** command on the local VDC until you enter a **copy running-config startup-config** command again on the default VDC.

  Conditions: You might see this symptom whenever you enter a **reload** command for a VDC or **no suspend command** for a VDC.

  Workaround: This issue is resolved.

- CSCtc13628

  Symptom: When a vPC peer link comes up, a hardware index failure syslog is displayed.

  Conditions: You might see this symptom when a vPC peer link comes up on a switch and notifications get out of sync.

  Workaround: This issue is resolved.

- CSCtc20038

  Symptom: A Hot Standby Router Protocol (HSRP) engine restarts.

Conditions: The HSRP engine process may restart in rare conditions when the reload timer is configured and then get triggered. This situation typically occurs when a Cisco Nexus 7000 switch is brought up with HSRP in the startup-configuration, or an interface with an HSRP configuration is enabled (through the **no shut** command) after a reload. This symptom happens only if the HSRP group reaches the listen state, and the configured reload delay timer gets triggered.

Workaround: This issue is resolved.

- CSCtc32368

  Symptom: Traffic loss may occur for 60 seconds, which is the Protocol Independent Multicast (PIM) join/prune (JP) period, in a Anycast Rendezvous Point (RP) environment if the RP that the client joins then fails.

  Conditions: This symptom might be seen only when all the following conditions exist:

  - Anycast RP is used
  - The shortest-path tree (SPT) is along the shared tree
  - The shared tree switches to the new RP because of the failure of the old RP

  Workaround: This issue is resolved.

Resolved Caveats—Cisco NX-OS Release 4.2(1)

All the caveats listed in this section are resolved in Cisco NX-OS Release 4.2(1) for the Cisco Nexus 7000 Series switches:

- CSCso93210

  Symptom: When a DHCP server and client are on the same VLAN, the Cisco Nexus 7000 Series switch drops the DHCP request broadcast packets from the client.

  Conditions: You might see this symptom when you have DHCP service enabled and then any interface has DHCP relay enabled if your VLAN does not have DHCP relay enabled, then you might see this symptom.

  Workaround: This issue is resolved.

- CSCsv81041

  Symptom: When you enter an interface configuration from the CLI and nothing happens, the switch times out and displays a message similar to the following:

  ```
  % cli: interface Ethernet8/11 Command timed out
  ```

  Conditions: You might see this symptom if you press Ctrl-C before the **copy** <*URL:file*> **running-config** command completes.

  Workaround: This issue is resolved.

- CSCsx27608

  Symptom: Some OSPF routes may not be in the routing table, although the correct Link Service Advertisements (LSAs) are in the OSPF database.

Conditions: You might see this symptom when routes are learned from point-to-point network segments, and there are no direct routes.

Workaround: This issue is resolved.

- CSCsx40449

  Symptom: A vPC to a Catalyst 6500 Series switch goes down as the Catalyst error disables the port because of a misconfiguration.

  Conditions: You might see this symptom if both vPC switches become the primary vPC switch and the downstream switches get into an STP EtherChannel guard misconfiguration and the port channel and EtherChannel are error disabled.

  Workaround: This issue is resolved.

- CSCsy08304

  Symptom: During a best path promotion for EIGRP, the reported distance (RD) is sometimes used instead of the feasible distance (FD). Depending on the actual values, a suboptimal path might be selected.

  Conditions: You might see this symptom when the maximum paths are reached or ECMPs are available and the metrics between paths are set up so that a higher RD results in a lower cost.

  Workaround: This issue is resolved.

- CSCsy13155

  Symptom: Some unicast DHCP packets might be dropped.

  Conditions: When you configure DHCP and DHCP services with IP relay, the system sends all DHCP traffic to the CPU for processing.

  Workaround: This issue is resolved.

- CSCsy40411

  Symptom: You might see an active unconfigured VRRP virtual address. After you reconfigure a virtual address, ping and Telnet to the unconfigured address are still successful.

  Conditions: You might see this symptom when VRRP is active and running and you reconfigure the virtual address.

  Workaround: This issue is resolved.

- CSCsy59367

  Symptom: When there is a low rate of packet flow (that is, if you send one packet and allow it to age out based on the inactive timer), the exported packet is set with a duration value of 4096 in the exporter, although the default maximum timeout for active flows is 1800.

  Conditions: You might see this symptom when there is a low rate of packet flow.

  Workaround: This issue is resolved.

- CSCsy84448

  Symptom: The terminal may hang or become unresponsive for 60 seconds or more with error messages such as the following:

```
%ACLMGR-3-ACLMGR_PPF_ERROR: PPF error: DDB Error: 0x41170040
  (ddb_srv_ses_rmtsrv_dset_unln/1864)
%ETHPORT-2-IF_SEQ_ERROR: Error ("sequence timeout") while communicating with component
MTS_SAP_RPM_CTRL for opcode MTS_OPC_ETHPM_PORT_LOGICAL_CLEANUP (RID_PORT:
port-channel5)
  %ETHPORT-2-SEQ_TIMEOUT: Component MTS_SAP_RPM_CTRL timed out on response to opcode
MTS_OPC_ETHPM_PORT_LOGICAL_CLEAN
  %RPM-2-PPF_SES_VERIFY: rpm [4581] PPF session verify failed in client (Line card
1/VDC NONE/UUID  0) with an error 0x41170014(Operation timed out)
  %ETHPORT-2-IF_DOWN_ERROR_DISABLED: Interface Ethernet2/14 is down (Error disabled.
Reason: Internal Handshake Failure).
```

  Conditions: You might see this symptom under the conditions similar to those conditions in this example:

  - An ARP ACL named ARP 1 with deny rules is created.
  - An ARP ACL is applied on VLANs 11 and 12.
  - DHCP Snooping and DAI are enabled for VLAN 11 where both the DHCP client and server are located.
  - Traffic is not moving because of the deny rules.
  - The ARP ACL is deleted with the **no arp access-list arp1** command.
  - The VACL policy (to deny IP packets) still exists for VLAN 11 and traffic is disrupted.

  Workaround: This issue is resolved.

- CSCsy90318

  Symptom: A Cisco Nexus 7000 Series switch with vPCs loses traffic for 60 seconds after a reload caused by a LACP link flap toward a downstream device.

  Conditions: You might see this symptom after a reload caused by a LACP link flap toward a downstream device.

  Workaround: This issue is resolved.

- CSCsz01146

  Symptom: A vPC peer link inconsistency occurs when you shut down a vPC on both the primary and secondary device.

  Conditions: When a vPC is shutdown on the primary vPC peer device and is being shutdown on the secondary vPC peer device, you might see a vPC peer-link spanning tree inconsistency among those VLANs carried on the vPC that is going down.

  Workaround: This issue is resolved.

- CSCsz11092

  Symptom: When you are using VRRP, you might see one or both of the following:

  - When you are using a VRRP IP address as a source of a ping from the VRRP master, the ping fails with the following error:

```
ping: can't bind to address <ip-address-of-VRRP>
```

- A ping from an external device to VRRP VIP on the Cisco Nexus 7000 Series device fails.

Conditions: You might see this symptom when you reload the system and restore the VRRP configuration from the startup configuration. If this problem occurs, the forwarding data path is not affected; however, reachability to VIP is lost.

Workaround: This issue is resolved.

- CSCsz22390

  Symptom: Following an ISSU upgrade or a system switchover on a device running Cisco NX-OS software, local and direct routes may be missing from the routing table.

  Conditions: This symptom may occur when there is a VRF in the system, such as the management VRF, that is in the administratively shutdown mode, and this shutdown VRF has an interface with IP address configuration.

  Workaround: This issue is resolved.

- CSCsz25152

  Symptom: Even when the vPC peer link or some vPCs are still active in a VLAN on the primary vPC device, the VLAN interface on that VLAN may go down. In addition, all VLAN interfaces go down when the last vPC goes down.

  Conditions: You will see this symptom only on the vPC primary peer device and only when the primary vPC port channel is down and the vPC port channel also goes down on the secondary vPC peer device. This situation triggers an incorrect count of forwarding ports in a VLAN.

  Workaround: This issue is resolved.

- CSCsz27138

  Symptom: You might see a service L2FM failure or a port may fail to come up and the system displays the error message “internal handshake failure.”

  Conditions: You might see this symptom when you have configured a sparse number of noncontiguous VLANs (for example 1, 3, 5, and 7).

  Workaround: This issue is resolved.

- CSCsz30788

  Symptom: An unexpected virtual port channel (vPC) peer role change might occur and cause traffic disruption when the role priorities are within a certain range of values.

  Conditions: vPC role preemption is not supposed to occur.

  Workaround: This issue is resolved.

- CSCsz53108

  Symptom: For OSF NSSA ABR, the wrong default route may be programmed.

  Conditions: When OSPF Type 5 and Type 7 default routes are present in the Link Service database (LSDB), the NSSA ABR installs the Type 7 Default route in the RIB instead of the Type 5 default route.

Workaround: This issue is resolved.

- CSCsz55220

  Symptom: The IP load sharing distribution might change upon a reboot.

  Conditions: When the universal ID (seed) is not specified for the **ip load-sharing** command, a random value is used every time after the system restarts.

  Workaround: This issue is resolved.

- CSCsz54148

  Symptom: A system failure occurred in the TACACS+ process and the following messages were displayed:

  ```
  %TACACS-3-TACACS_ERROR_MESSAGE: All servers failed to respond
  %SYSMGR-2-SERVICE_CRASHED: Service "Tacacs Daemon" (PID 3929) hasn't caught signal 11
  (no core).
  ```

  Conditions: You might see this symptom when you enter the **sh run | vsh | grep interface** command.

  Workaround: This issue is resolved.

- CSCsz57729

  Symptom: The OSPF “default-info originate always” configuration can introduce routing loops in certain topologies.

  Conditions: You might see this symptom if you have two OSPF routers that use the “default-info originate always” configuration and there is no default route in the RIB.

  Workaround: This issue is resolved.

- CSCsz73619

  Symptom: Certain third-party file servers and appliances that are connected behind vPC might not be accessible by some devices in the network.

  Conditions: The filer is connected behind a vPC using FHRP as the default gateway. The filer default is to use the source MAC address in the received packet as the gateway MAC address instead of the FHRP group MAC address.

  Workaround: This issue is resolved.

- CSCsz79883

  Symptom: Virtual port channels experience packet loss during recovery of a peer link. In addition, virtual port channels experience spanning-tree fallback when root port goes down. If the primary Cisco Nexus 7000 Series switch has a root port for some VLANs and the secondary Cisco Nexus 7000 switch has an Alt port for those VLANs, when the root port down, the primary switch sends a proposal to the virtual port channels with system MAC address as the bridge identifier. The connected switches respond by agreement but this agreement is not accepted. Because the agreement is not accepted, the Spanning Tree Protocol (STP) fallback occurs on the virtual port channel.

  Conditions: This symptom might be seen under the following conditions:

- A packet loss will be seen during STP convergence when a vPC peer link is recovered and the standby vPC switch is operating as the primary switch. This situation occurs if the root port moves as a result of the peer link recovery.
- The system MAC address is a higher priority than that of the local MAC address and the Cisco Nexus 7000 Series switch needs to exchange a proposal and agreement with switches connected through a virtual port channel.

Workaround: This issue is resolved.

- CSCsz92775

  Symptom: If you have a vPC environment where you have two Cisco Nexus 7000 Series switches and a Catalyst 6500 Series switch running in VTP server mode with pruning enabled, in rare situations, traffic may stop between the Cisco Nexus 7000 switches and the Catalyst switch. This is caused by VTP packet floods from the Cisco Nexus 7000 Series switches to the Catalyst switch on both port-channel links.

  Conditions: You might see this symptom when you are in vPC mode and the Catalyst switch is running in VTP server mode with pruning enabled.

  Workaround: This issue is resolved.

- CSCsz98098

  Symptom: HSRP group states may flap during a supervisor switchover.

  Conditions: You might see this symptom when there are a few hundred Layer 3 interfaces with HSRP groups configured on the switch. The flaps may continue for a few seconds after the switchover.

  Workaround: This issue is resolved.

- CSCta00339

  Symptom: Traffic from a secure MAC address is dropped upon a MAC move security violation.

  Conditions: This symptom might be seen when the same MAC address on a secure port is learned on another port in the same VLAN.

  Workaround: This issue is resolved.

- CSCta04879

  Symptom: When certain active ACL configurations that have statistics per entry configured are modified, an aclqos exception might occur. Eventually, the modules associated with those ACLs might reset.

  Conditions: You might see this symptom if you modify an active ACL configuration that has statistics per entry configured.

  Workaround: This issue is resolved.

- CSCta17139

  Symptom: You might see high CPU usage on directly connected switches running the VLAN Trunking Protocol (VTP).

Conditions: You might see this symptom if you have two Cisco Nexus 7000 Series switches that are connected directly together via two or more independent links that are not in a port channel. In addition, you need to have a VTP server connected to each Cisco Nexus 7000 Series switch.

Workaround: This issue is resolved.

- CSCta47295

  Symptom: The **show mac address-table** command hangs during execution. The heading of the table is printed, but no entries are written to the table.

  Conditions: This symptom might be seen by clearing the dynamic entries of the MAC address table, and will only occur if the interface on which the entries are cleared is in a vPC, and that vPC is in a nondefault VDC.

  Workaround: This issue is resolved.

- CSCta48546

  Symptom: The management interface IP address is not reachable after an ISSU switchover.

  Conditions: This symptom might be seen when an ISSU switchover occurs and there is a change in the MAC address as the new supervisor takes over. The switch should send a gratuitous ARP to the gateway IP due to the change of a MAC address, but the ARP is not sent in a timely manner, which results in the management interface not being reachable.

  Workaround: This issue is resolved.

- CSCta48640

  Symptom: During the time a vPC primary switch reloads and then comes back, a packet loss can occur for up to 300 seconds.

  Conditions: This symptom might be seen when there are two Cisco Nexus 7000 Series switches running vPC and neither of them is the root of the spanning tree.

  Workaround: This issue is resolved.

- CSCta53273

  Symptom: A Cisco Nexus 7000 Series switch may have routes installed in the IPv4 RIB that are marked as pending, which means that the routes have not been pushed to the FIB and are therefore not installed in the hardware.

  Conditions: This symptom may occur under various conditions with any client; however, the only scenario where it has been seen is when an EIGRP prefix is withdrawn, such as when there is a peer neighbor down event.

  Workaround: This issue is resolved.

- CSCta55866

  Symptom: Under rare circumstances, when an active supervisor on a Cisco Nexus 7000 Series switch has multiple back-to-back, fatal hardware exceptions, it is possible that the standby supervisor will reset. As a result, the standby supervisor will not take over as the active supervisor.

  Conditions: This symptom might be seen when there are multiple back-to-back fatal hardware exceptions.

Workaround: This issue is resolved.

Documentation Updates

The following Caveats describe corrections that have been incorporated into Cisco Nexus 7000 Series product documentation. In some cases, the updated document may not be available yet on Cisco.com.

- CSCsz07437

  Description: Added the **show system resources** command to the *Cisco Nexus 7000 Series NX-OS System Management Command Reference, 4.1*. The *Cisco Nexus 7000 Series NX-OS Command Reference Master Index, Release 4.1* has not yet been updated.

- CSCtc40710

  Description: Added the following note to the "Configuring AAA" chapter in the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 4.2:*

  Note: If the AAA server fails, you cannot exit the vty session or execute any other commands unless you have previously configured the device to fall back to the local database.

- CSCtc46250

  Description: Changed the **platform rate-limit** command to the **hardware rate-limit** command in the "Configuration Rate Limits" chapter in the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 4.2.*

- CSCtc54732

  Description: Added "root" to the list of reserved usernames in the "Configuring User Accounts and RBAC" chapter of the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 4.2.*

- CSCtf06392

  Description: Updated the documentation with the following text:

  VLAN 1 is required on all trunk ports used for switch interconnects if VTP is supported in the network. Pruning VLAN 1 from any of these ports will prevent VTP from functioning.

  This information was added to the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide.*

Related Documentation

Cisco NX-OS documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html

The Release Notes for upgrading the FPGA/EPLD is available at the following URL:

http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_1/epld/epld_rn.html

The following are related Cisco NX-OS documents:

Cisco NX-OS Configuration Guides

Cisco Nexus 7000 Series NX-OS Getting Started with Virtual Device Contexts, Release 4.2

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

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

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.2

Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide, Release 4.2

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

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

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

Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.2

Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 4.2

Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.2

Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 4.2

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

Cisco Nexus 7000 Series NX-OS XML Management Interface User Guide, Release 4.2

Cisco NX-OS System Messages Reference

Cisco Nexus 7000 Series NX-OS MIB Quick Reference

Cisco NX-OS Command References

Cisco Nexus 7000 Series NX-OS Command Reference Master Index, Release 4.2

Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference, Release 4.2

Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 4.2

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.2

Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference, Release 4.2

Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.2

Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference, Release 4.2

Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.2

Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference, Release 4.2

Cisco Nexus 7000 Series NX-OS System Management Command Reference, Release 4.2

Other Software Document

Cisco Nexus 7000 Series NX-OS Troubleshooting Guide, Release 4.x

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.

Cisco Nexus 7000 Series NX-OS Release Notes, Release 4.2