Send document comments to nexus7k-docfeedback@cisco.com.

Cisco Nexus 7000 Series NX-OS Release Notes, Release 4.1

Date: June 18, 2009
Part Number: OL-17764-04 E0

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 33.

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 4.1* Release Notes: *http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_1/nx-os/release/notes/41_nx-os_release_note.html*

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

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

Send document comments to nexus7k-docfeedback@cisco.com.

Table 1 Online History Change

Part Number	Revision	Date	Description
	A0	December 18, 2008	Created release notes for Release 4.1(2). **Note** Cisco NX-OS Release 4.1(1) is for use only on the Cisco MDS 9000 Series switches.
OL-17764-02	A0	February 6, 2009	Created release notes for Release 4.1(3).
	B0	February 20, 2009	Added reference to EPLD RNs for vPCs.
	C0	February 23, 2009	• Updated the maximum number of port channels supported in Release 4.1(2). • Added per-packet load balancing to the new features for Release 4.1(2).
OL-17764-03	A0	March 16, 2009	Created release notes for Release 4.1(4).
	B0	March 23, 2009	Modified limitations section for Release 4.1(4).
	C0	March 25, 2009	Added CMP section for Release 4.1(4).
OL-17764-04	A0	April 3, 2009	Created release notes for Release 4.1(5).
	B0	April 21, 2009	Corrected PIM information for Release 4.1(2), 4.1(3), 4.1(4), and 4.1(5): PIM SSM and BIDR are not supported on vPCs.
	C0	April 24, 2009	Added open Caveat CSCsz25152.
	D0	June 18, 2009	Added open Caveat CSCta17139.
	E0	September 14, 2009	Added a Limitation about multicast over tunnel interfaces.

Contents

This document includes the following sections:

- Introduction, page 3
- System Requirements, page 3
- New Hardware Features, page 4
- Upgrade/Downgrade Caveats, page 5
- CMP Images, page 6
- New Software Features, page 6
- Limitations, page 9
- Caveats, page 10
- Related Documentation, page 33
- Obtaining Documentation and Submitting a Service Request, page 34

Send document comments to nexus7k-docfeedback@cisco.com.

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, page 3
- Memory Requirements, page 3
- Supported Device Hardware, page 3

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 4.1(2) and later supports 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 a later release) 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(2) software, and Cisco NX-OS Release 4.1(3) software, and Table 3 shows the transceivers supported by each release.

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 4.1(5) 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

Send document comments to nexus7k-docfeedback@cisco.com.

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

Hardware	Part Number	Cisco NX-OS Release 4.0 Support	Cisco NX-OS Release 4.1(2) through 4.1(5) Support
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-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)
N7K-M132XP-12	10GBASE-SR	SFP-10G-SR	4.0(1)
	10GBASE-LR	SFP-10G-LR	4.0(3)

New Hardware Features

The Cisco NX-OS Release 4.1(2) is initially released at the same time that the following hardware is released for the Cisco Nexus 7000 Series switches:

- Cisco Nexus 7018 switch, which includes the new fabric module. The switch supports two supervisor modules, up to 16 I/O modules, up to five fabric modules, and up to four power supply units.
- Cisco Nexus 7018 fabric module, which provides up to 230 Gbps of fabric bandwidth for each I/O and supervisor module installed on the Cisco Nexus 7018 switch.
- 48-port, 1-Gigabit Ethernet SFP I/O module, which is supported by the Cisco Nexus 7010 switch and the Cisco Nexus 7018 switch.

Send document comments to nexus7k-docfeedback@cisco.com.

- 7.5-kW AC power supply unit, which is supported by the Cisco Nexus 7010 switch and the Cisco Nexus 7018 switch. You can install up to three of these power supply units in the Cisco Nexus 7010 switch and up to four of these power supply units in the Cisco Nexus 7018 switch.
- Cisco Nexus 7018 fan tray, which provides cooling for the supervisor, I/O, and fabric modules.

Note The new hardware requires that you have the Cisco NX-OS Release 4.1(2) or later operating system installed on your switch.

Upgrade/Downgrade Caveats

The following caveats apply to the Cisco NX-OS Release 4.1(2) or later for the Cisco Nexus 7000 Series switches:

- Do not change any configuration settings or network settings during the upgrade. Any changes in the network settings may cause a disruptive upgrade.
- Release 4.1(5) is ISSU-compatible with the following releases:
  - Release 4.1(4)
  - Release 4.1(3)
  - Release 4.1(2)
  - Release 4.0(4)
  - Release 4.0(3)
- Release 4.1(4) is ISSU-compatible with the following releases:
  - Release 4.1(3)
  - Release 4.1(2)
  - Release 4.0(4)
  - Release 4.0(3)
- Release 4.1(3) is ISSU-compatible with the following releases:
  - Release 4.1(2)
  - Release 4.0(4)
  - Release 4.0(3)
- Release 4.1(2) is ISSU-compatible with the following releases:
  - Release 4.0(4)
  - Release 4.0(3)
- If you are running Release 4.0(1) or 4.0(2), take the following steps:
  - Upgrade to Release 4.0(3) or Release 4.0(4)
  - Upgrade to Release 4.1(3)
- When you downgrade from Release 4.1(2) to 4.0(3), you will experience a disruptive downgrade.

Send document comments to nexus7k-docfeedback@cisco.com.

- When you are upgrading or downgrading Release 4.1(2) to 4.1(3) on a Cisco Nexus 7000 Series chassis with a single supervisor module, you may see an CMP upgrade failure although the rest of the system will upgrade or downgrade properly. If you see this condition, explicitly upgrade or downgrade the CMP by entering the **install module** *active-slot* **cmp system** *location* command and the **reload cmp module** command.

CMP Images

Cisco NX-OS Releases 4.1(5) and 4.1(4) for the Nexus 7000 Series device do not have a new image for the CMP. The CMP image version remains at Release 4.1(3).

New Software Features

Note Cisco NX-OS Release 4.1(1) is for use only on the Cisco MDS 9000 Series switches.

This section briefly describes the new features introduced in the releases of the Cisco NX-OS software 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 33. 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 4.1(5), page 6
- Cisco NX-OS Release 4.1(4), page 6
- Cisco NX-OS Release 4.1(3), page 7
- Cisco NX-OS Release 4.1(2), page 7

Cisco NX-OS Release 4.1(5)

Cisco NX-OS Release 4.1(5) for the Nexus 7000 Series switches has no new software features.

Cisco NX-OS Release 4.1(4)

This section briefly describes the new feature introduced in Cisco NX-OS Release 4.1(4) for the Cisco Nexus 7000 Series switches and includes the following topic:

- Increase vPC Limit, page 6

Increase vPC Limit

The Cisco NX-OS software supports a maximum of 192 virtual port channels (vPCs) on the Cisco Nexus 7000 Series switches.

Send document comments to nexus7k-docfeedback@cisco.com.

Cisco NX-OS Release 4.1(3)

This section briefly describes the new feature introduced in Cisco NX-OS Release 4.1(3) for the Cisco Nexus 7000 Series switches and includes the following topic:

- vPCs, page 7

vPCs

A virtual port channel (vPC) allows links that are physically connected to two different Cisco Nexus 7000 Series switches to appear as a single port channel by a third downstream device. The third device can be a switch, server, or any other networking device that supports IEEE 802.3ad port channels.

Note You may need to upgrade the EPLDs to run vPC. For complete information on EPLDs and vPCs, see the following:
http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_1/epld/epld_rn.html

vPCs increase usable bandwidth by eliminating STP blocked ports in common dual-homed designs. The vPC is transparent to the neighbor devices, and those neighbors need only to support port channels using static or LACP configuration. Each device in the vPC retains it own independent control and data planes. vPC provides supports for dual supervisors on each device.

Note If you are attempting to configure the vPC on an incorrect version of the N7K-M148GT-11 module, the screen displays an error message. Contact your Cisco Account Team if you see this message.

Cisco NX-OS Release 4.1(2)

This section briefly describes the new features introduced in Cisco NX-OS Release 4.1(2) for the Cisco Nexus 7000 Series switches and includes the following topics:

- VTP Transparent, page 7
- IPv6, page 8
- PKI, page 8
- CFSoIP, page 8
- File-Based Checkpoint/Rollback, page 8
- Per-Packet Load Balancing, page 8

VTP Transparent

In the Cisco Nexus 7000 Series switches, the VLAN Trunking Protocol (VTP) works in transparent mode, allowing you to extend a VTP domain across the device. Layer 2 trunk interfaces, Layer 2 trunk over physical interfaces, and Layer 2 port channels support VTP transparent functionality.

This feature relays all VTP protocol packets that the device receives on a trunk port onto all other trunk ports. When the VTP feature is disabled, VTP protocol packets are not relayed.

Send document comments to nexus7k-docfeedback@cisco.com.

IPv6

The Cisco Nexus 7000 Series NX-OS software supports IPv6 addressing for the following routing protocols:

- MLD v2
- PIM SSM
- PIM BIDR
- EIGRP

The following features support IPv6:

- QoS
- uRPF
- ACLs—PACLs, VACLs, and RACLs
- CoPP matching packets
- NetFlow

PKI

The Public Key Infrastructure (PKI) allows the Cisco Nexus 7000 Series device to obtain and use digital certificates for secure communication in the network; it also provides manageability and scalability.

CFSoIP

Cisco Fabric Services (CFS) is a distribution protocol that supports a rich set of features. Using CFSoIP, applications can distribute and synchronize configuration and/or runtime data in a network. CFSoIP is part of the core CFS (CFS over FC), in which the transport media is IP. Applications can register with CFS in IP scope and exchange information with their peers. This feature provides consistent and, in most cases, identical configurations and behavior within a network.

Cisco NX-OS supports CFSoIP for Call Home and several security features, such as AAA, RADIUS, TACAS+, and user roles.

File-Based Checkpoint/Rollback

This feature allows you to save a checkpoint to a storage location of your choice, such as bootflash memory. It also allows you to roll back from a checkpoint file that is residing in bootflash.

Rollback is not supported for checkpoints across software versions.

Per-Packet Load Balancing

The per-packet load balancing feature allows data traffic to be evenly distributed in an IP network over multiple equal-cost connections. Per-packet load balancing uses round-robin techniques to select the output path without basing the choice on the packet content.

Send document comments to nexus7k-docfeedback@cisco.com.

Limitations

This section describes the limitations in Cisco NX-OS Release 4.1(2), Release 4.1(3), and Release 4.(4) for the Cisco Nexus 7000 Series switches.

This section includes the following topics:

- vPCs, page 9
- XML Management Interface, page 9
- Cisco TrustSec, page 9
- QoS, page 9
- Tunnel Interfaces and VRFs, page 10
- VRFs, page 10
- Multicast over Tunnel Interfaces, page 10

vPCs

Cisco NX-OS Release 4.1(4) for Cisco Nexus 7000 Series switches supports up to 192 vPCs per device. Cisco NX-OS Release 4.1(3) for Cisco Nexus 7000 Series switches supports up to 50 vPCs per device.

The Cisco NX-OS software for Cisco Nexus 7000 Series switches does not support PIM SSM or BIDR on vPCs; PIM 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).

Cisco TrustSec

Cisco TrustSec (CTS) does not fully support the following commands:

- **clear cts cache**
- **clear cts policy**
- **cts cache**
- **cts l3 spi** (global configuration)
- **cts l3 spi** (interface configuration)
- **show cts l3 interface**
- **show cts l3 mapping**

QoS

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

Send document comments to nexus7k-docfeedback@cisco.com.

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.

Tunnel Interfaces and VRFs

The Cisco NX-OS software supports assigning tunnel interfaces only to the default VDC and the default VRF instance.

VRFs

The Cisco NX-OS software supports a maximum of 200 Virtual Routing and Forwarding instances (VRFs).

Multicast over Tunnel Interfaces

In Cisco NX-OS Release 4.1(5) and earlier releases, tunnel interfaces do not support Protocol-Independent Multicast (PIM).

Caveats

Note Cisco NX-OS Release 4.1(1) is for use only on the Cisco MDS 9000 Series switches.

This section includes the following topics:

- Open Caveats, page 10
- Resolved Caveats—Cisco NX-OS Release 4.1(5), page 13
- Resolved Caveats—Cisco NX-OS Release 4.1(4), page 15
- Resolved Caveats—Cisco NX-OS Release 4.1(3), page 20
- Resolved Caveats—Cisco NX-OS Release 4.1(2), page 22

Open Caveats

- CSCsm22329

  Symptom: QoS statistics require a policing action in order for 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: You can get statistics for a marking-only policy by applying a dummy policing action to the policies. For example, in addition to the marking actions, you should define a policing action that permits 100 percent traffic. Configure the violate and conform action as transmit.

Send document comments to nexus7k-docfeedback@cisco.com.

- CSCsm75863

  Symptom: Logging to an external syslog server using an IPv6 address does not work.

  Conditions: If you configure IPv6 addresses for an external syslog server, then logging does not work for the server.

  Workaround: No workaround.

- CSCsm98733

  Symptom: After a rollback, one checkpoint is missing after a supervisor module switchover.

  Conditions: If the ascii-cfg-server process restarts or if the active supervisor module switches over to the standby supervisor module while a checkpoint operation is in progress, then the checkpoint operation may not complete.

  Workaround: Recreate the checkpoint after a supervisor module switchover if the checkpoint is missing.

- CSCso03889

  Symptom: Address Resolution Protocol (ARP) ACLs are not supported on private VLANs.

  Conditions: If you configure an ARP ACL on a primary VLAN using the **ip arp inspection filter** *vlan-id* command, it is not propagated to the secondary VLAN.

  Workaround: No workaround.

- CSCsq66001

  Symptom: The tunnel interface is not detected when you are processing an SNMP MIB walk.

  Conditions: This situation occurs under all conditions and does not affect functionality.

  Workaround: No workaround.

- CSCsr68326

  Symptom: If the Netstack process restarts, the IPv6 protocol packets are not delivered to OSPFv3.

  Conditions: After the Netstack process restarts for any reason, OSPFv3 does not receive protocol packets and does not establish neighbors.

  Workaround: Restart the affected IPv6 unicast protocol.

- CSCsy31214

  Symptom: If you create a VRF, delete it, and then add the VRF again, you may see problems with the syslog if you use the **use-vrf** keyword to log in the VRF.

  Conditions: You see this symptom when you delete an existing VRF and reload the device.

  Workaround: After the reload, remove the correct configuration and then add it again.

Send document comments to nexus7k-docfeedback@cisco.com.

- CSCsy50070

  Symptom: During an in-service software upgrade (ISSU), the following error message may display for VDC 1:

  ```
  %RES_MGR-4-RES_MGR_RES_ALREADY_EXCEEDED_BUT_NOT_ENFORCED: RES_MGR Warning: The VDC 1
  is currently already using more u4route-mem resources than the desired new maximum
  limit. You may experience some route loss upon switchover, when the new limits will
  actually take effect.
  ```

  : This situation may occur during a supervisor module switchover but does not impact functionality.

  : No workaround.

- CSCsz25152

  : 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.

  : 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 and this results in this situation.

  : Ensure that the vPC port channel is up on the primary vPC peer device before you bring down the vPC port channel on the secondary vPC peer device.

  If the downstream vPC peer device reloads, bring the vPC peer link down and up on the vPC primary device by entering the and commands. This will not trigger an STP topology change because the vPC port channel is already up on the secondary vPC peer device, and STP sees vPC as a single logical port unit.

- CSCta17139

  : You may see high CPU usage on directly connected switches running VTP.

  : VTP transparent mode does not work in a redundant Layer 2 topology with physical loops.

  : Eliminate redundant physical loops by putting redundant links in port channels when possible. Otherwise, disable VTP.

Send document comments to nexus7k-docfeedback@cisco.com.

Resolved Caveats—Cisco NX-OS Release 4.1(5)

All the caveats listed in this section are resolved in Cisco NX-OS Release 4.1(5) for the Cisco Nexus 7000 Series switches:

- CSCsx69941

  : ARP packets may be duplicated when DHCP is enabled.

  : When the DHCP feature is enabled, the ARP packets on the VLAN interfaces may be flooded through the hardware and another time in the software, resulting in duplicate ARP packets.

  : This issue is resolved.

- CSCsy36733

  : When you delete a VRF, the interfaces that are running EIGRP may lose their EIGRP adjacencies.

  : You may see this symptom when more than one EIGRP instance is running in a particular VDC and you move an EIGRP-enabled interface from one VRF to another by entering the **vrf member** command.

  Workaround: This issue is resolved.

- CSCsy53158

  Symptom: If the Unicast IPv6 RIB goes down, the system may switch over to the standby supervisor.

  Conditions: You may see this symptom when the system detects an IPv6 route loop in the Unicast IPv6 RIB.

  Workaround: This issue is resolved.

- CSCsy57525

  Symptom: The L2FM process may go down, and you will see a message on the syslog.

  Conditions: You may see this symptom when the system is programming a large number of MAC addresses and the same time it is running other processes that require communication with the modules.

  Workaround: This issue is resolved.

- CSCsy57564

  Symptom: The L2FM process may go down, and you will see a message on the syslog.

  Conditions: You may see this symptom when you are running vPC, which is adding a large number of MAC addresses, and you shut down the vPC peer link.

  Workaround: This issue is resolved.

- CSCsy58563

  Symptom: You may see a module in the Cisco Nexus 7000 Series chassis take an exception, and reset.

Send document comments to nexus7k-docfeedback@cisco.com.

Conditions: You may see this symptom when you have configured VLANs and VLAN interfaces with the same flow monitor, and you reconfigure the VLAN to have a different flow monitor.

Workaround: This issue is resolved.

- CSCsy77856

  Symptom: If you remove the VRF configuration from under the routing process and then add it back, then all of the neighbor relationships in the VRF may never recover.

  Conditions: You may see this symptom when you are using VRF with EIGRP on a Cisco Nexus 7000 Series device.

  Workaround: This issue is resolved.

- CSCsy78904

  Symptom: After you reboot the device, redistribution into an EIGRP may fail.

  Conditions: You may see this symptom if all the interfaces in the routing context are down at the time of redistribution.

  Workaround: This issue is resolved.

- CSCsy83394

  Symptom: If you are running NX-OS Release 4.1(4) or earlier and have configured either the DHCP server or relay on the Cisco Nexus 7000 Series device, UDP fragments may not be forwarded.

  Conditions: You may see this symptom when the DHCP feature is enabled on the system, when DHCP snooping or DHCP relay is configured.

  Workaround: This problem has been fixed in Cisco NX-OS Release 4.1(5). However, this fix is not automatically applied when you do an ISSU upgrade to Release 4.1(5) from an earlier release. If you reload the system, the system applies the fix automatically.

  To ensure that this fix is applied after you perform an ISSU, do one of the following:
  1. For DHCP relay, enter the **no service dhcp** command and then the **service dhcp** command.
  2. For DHCP snooping, enter the **no feature dhcp** command and then the **feature dhcp** command; the reconfigure the DHCP policies.

- CSCsy84185

  Symptom: You may see spanning-tree instabilities because of improper CBL programming, which is a result of a SPAN misconfiguration.

  Conditions: You may see this symptom when you configure SPAN to source-span multiple VLANs, some of which have not been created in the system. The SPAN session is up, and if an interface moves from up to down to up rapidly several times, you may see this symptom.

  Workaround: This issue is resolved.

- CSCsy84202

  Symptom: The system may not apply the commands to end the SPAN session.

Send document comments to nexus7k-docfeedback@cisco.com.

Conditions: You may see this symptom when you configure SPAN to source-span multiple VLANs, some of which have not been created in the system. The SPAN session is up, and the command to end the SPAN session may not get applied.

Workaround: This issue is resolved.

Resolved Caveats—Cisco NX-OS Release 4.1(4)

All the caveats listed in this section are resolved in Cisco NX-OS Release 4.1(4) for the Cisco Nexus 7000 Series switches:

- CSCsl16405

  Symptom: Some static routes may be lost after you reload the system on a Cisco Nexus 7000 Series device that is configured with IP static routes.

  Conditions: You may see this symptom after you reload the system 8 to 10 times. This symptom is purely a software timing issue and may happen more or less often than the typical scenario.

  Workaround: This issue is resolved.

- CSCsu85189

  Symptom: No VLANs are shown as Up on the vPC peer link or vPCs. Although the compatibility status displays as success, all the VLANs are in the errored state when you enter the **show system internal ethpm info interface port-channel** *x* command, where x is the peer link. When you enter the **show interface port-channel** *x* **status error-vlans** command, the display shows a timeout as the reason for the suspension.

  Conditions: You may see this symptom if more than 2,000 VLANs are enabled on the vPC peer link and the vPC because the message size exceeds the messaging infrastructure, which causes the handshake failure.

  Workaround: This issue is resolved.

- CSCsv40347

  Symptom: After a module or a switch reloads, some commands may be missing from the **show running-config** command output but the configurations are active on the switch.

  Conditions: During the module reload process, as the module comes online, the CLI server may not receive the responses from the protocol components for more that 10 seconds after it sends the configuration commands to those components. This delay causes the CLI server to remove the commands from the current configuration.

  Workaround: This issue is resolved.

- CSCsw64054

  Symptom: When the device does an SNMP SET on the RMON-MIB:statistics group objects or RMON-MIB:history, the SNMP agent crashes.

  Conditions: You may see this symptom under all conditions.

  Workaround: This issue is resolved.

Send document comments to nexus7k-docfeedback@cisco.com.

- CSCsx23179

  Symptom: The Cisco NX-OS software clears the BGP session upon receiving a prefix that has the AS4_PATH attribute with AS_CONFED_SEQUENCE in it.

  Conditions: A prefix with AS4_PATH attribute with AS_CONFED_SEQUENCE in it is received.

  Workaround: This issue is resolved.

- CSCsx35858

  Symptom: Command accounting is logged as a STOP record instead of as an UPDATE record.

  Conditions: This symptom can occur in all conditions.

  Workaround: This issue is resolved.

- CSCsx42110

  Symptom: OSPF flaps between a Cisco 7200 Series router and a Cisco Nexus 7000 Series switch.

  Conditions: When redistributed routes flap very frequently, the Cisco 7200 Series router flushes and reoriginates the type-5 external LSAs. If the flap is fast enough, the Cisco 7200 Series router reoriginates and flushes the LSA before the Cisco Nexus 7000 Series switch has a chance to delete the higher sequence numbered maxAged LSAs from its LSDB.

  Workaround: This issue is resolved.

- CSCsx42741

  Symptom: If multiple I/O modules or interconnected Cisco 7000 Series switches are restarted simultaneously, some of the member interfaces of an active port channel may toggle between the ‘I’ and ‘P’ states for a few seconds before stabilizing to the ‘P’ state. The port channels remain operationally up at all times.

  Conditions: This symptom occurs when you reload the swathes or modules several times.

  Workaround: This issue is resolved.

- CSCsx46214

  Symptom: DHCP clients that are on interfaces connected to slot 18 of the Cisco Nexus 7018 chassis may fail to obtain an IP address.

  Conditions: The host/client connected to interfaces on a module in slot 18 will fail to obtain IP addresses when the system comes up after you reload the system with DHCP disabled.

  Workaround: This issue is resolved.

Send document comments to nexus7k-docfeedback@cisco.com.

- CSCsx47787

  Symptom: ARP broadcast packets bound for the supervisor module may not be rate limited because we didn't have a CoPP policy to cover this situation. The default system-defined CoPP policy will be used to police supervisor-bound ARP packets and prevent an ARP broadcast storm from affecting the control plane traffic without affecting bridged packets.

  Conditions: You would see this symptom only with ARP broadcast packets that go to the supervisor module.

  Workaround: This issue is resolved.

- CSCsx51757

  Symptom: Tunnel packets ingressing on the module in slot 18 of the Cisco Nexus 7018 chassis will be dropped.

  Conditions: This symptom appears when you enter the **feature tunnel** command after the module in the 18th slot is online. If you enable the tunnel feature before you bring the module in slot 18 online, you will not see this symptom.

  Workaround: This issue is resolved.

- CSCsx57439

  Symptom: The addition and deletion of port-channel members followed by a change in the state of the associations of the trunked private VLANs may result in the private VLANs not being forwarded on the port channel.

  Conditions: This symptom occurs when the private VLANs (both primary and associated secondary) are trunked on port channels.

  Workaround: This issue is resolved.

- CSCsx60328

  Symptom: The **filter vlan**-*range* **include-untagged** command does not translate correctly to the running configuration.

  Conditions: After you enter the command, the **show running-config** command output shows that the **include-untagged** option becomes VLAN 0. Also, the Cisco NX-OS software does not allow you to remove the configuration.

  This example shows how to create the configuration:

```
switch(config)# monitor session 1
switch(config-monitor)# filter vlan 10-15 include-untagged
```

  This example shows the command output with the incorrect translation:

```
monitor session 1
  source interface sup-eth0 rx
  destination interface Ethernet3/32
  filter vlan 0,10-15     <-- This should be filter vlan 10-15 include-untagged
  no shut
```

  This example shows the syntax error when trying to remove the configuration:

```
switch(config)# monitor session 1
switch(config-monitor)# no filter vlan 0,10-15
                                       ^
```

Send document comments to nexus7k-docfeedback@cisco.com.

```
Invalid value/range at '^' marker.
```

: This issue is resolved.

- CSCsx60516

: The following syslog message can be sometimes seen:

```
DEVICE_TEST-2-ASIC_REG_CHECK_FAIL: Module 6 has failed test  ASICRegCheck 20 times on
device SantaCruzLocal instance 1  frontpanel  ports affected  due to error SCZ Asic is
not  accessible
```

Note The value of the instance number depends on the fabric module slot affected.

: This symptom is a timing issue when accessing the fabric module through the internal bus.

: This issue is resolved.

- CSCsx62030

: The maximum transmission unit (MTU) configured on a Layer 3 port-channel interface may not be applied correctly to the hardware and could prevent jumbo frame transmission over the interface.

: This symptom may occur with Layer 2 or Layer 3 port channels on 1-Gigabit or 10-Gigabit interfaces.

: This issue is resolved.

- CSCsx74326

: In a rare condition, an inconsistent adjacency could occur due to a MAC move.

: This symptom could occur in a loop topology where the MAC is first learned from one link, and then is stuck in that link even though the forwarding changes to the other link. When this situation happens, unicast forwarding does not occur through the link.

: This issue is resolved.

- CSCsx88140

: EIGRP failed to promote a path with better metrics when the maximum-paths limit had been reached.

: If the number of paths available is greater than the maximum-path configuration and if a best path comes in beyond the maximum configured, it is not promoted.

: This issue is resolved.

- CSCsx82805

: If you query the Cisco Nexus 7000 Series loopback IP using SNMP v2c, the device sources the response from the physical interface to which the SNMP Manager is connected rather than from the loopback IP itself.

Send document comments to nexus7k-docfeedback@cisco.com.

: You will see this symptom when you query the loopback IP using SNMPv2c.

: This issue is resolved.

- CSCsx94461

  : A rollback to a previous checkpoint may fail because of the route map.

  : This symptom may occur if the running-config file or the checkpoint contains more than one *name* [*seq*] command.

  : This issue is resolved.

- CSCsx95422

  : Packets sent from the supervisor module to nonexistent hosts is flooded with a MAC address that contains all zeros.

  : When the system forwards a packet addressed to a host that does not exist on the LAN, the system sends the packet to the supervisor module to trigger ARP resolution. The system adds a temporary adjacency entry MAC address of all zeros until the ARP resolution occurs and the adjacency then gets updated. Because the ARP resolution does not happen for a nonexistent host, packets destined for the nonexistent host are forwarded using the information in the adjacency entry, using the zero MAC address and the outgoing interface.

  : This issue is resolved.

- CSCsx97281

  : On Cisco NX-OS, GOLD detects hardware failures through periodic tests and compiles a reports. In some conditions, GOLD does not detect a partial failure in one of the ASICs. If this partial ASIC failure occurs, you may see the control protocols going up and down and the following syslog message appears:

  ```
  %OC_USD-SLOT1-2-RF_CRC: OC0 received packets with CRC error from XBAR <x>
  ```

  : You may see this symptom when a partial failure occurs in an ASIC.

  : This issue is resolved.

- CSCsy05849

  : Control packets for BGP and HSRP that are sourced by the device are sent with the Class of Service (CoS) value set to 0.

  : This situation occurs under all conditions.

  : This issue is resolved.

Send document comments to nexus7k-docfeedback@cisco.com.

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

All the caveats listed in this section are resolved in Cisco NX-OS Release 4.1(3) for the Cisco Nexus 7000 Series switches:

- CSCsm70593

  : An interface is disabled when more than 50,000 port-VLAN instances go down at the same time.

  : When more than 50,000 port-VLAN instances go down at the same time, the interface times out and becomes disabled. The following system message displays:

  ```
  %$ VDC-1 %$ %ETHPORT-2-SEQ_TIMEOUT: Component MTS_SAP_L2FM timed out on response to
  opcode:MTS_OPC_ETHPM_PORT_LOGICAL_CLEANUP (for:RID_PORT: Ethernet9/46)
  ```

  : This issue is resolved.

- CSCso02550

  : CoPP crashes with large policy maps.

  : CoPP crashes if you attach more than 300 classes to the policy map.

  : Ensure that the number of classes attached to the policy map is not more than 128.

- CSCso43538

  : IGMP packets and PIM hello packets received on a Layer 2 interface or VLAN interface cannot be policed with CoPP.

  : IGMP reports and queries and PIM hello packets received on a Layer 2 interface or VLAN interface are not subjected to control plane policing. The packets can only be rate limited tuning the receive rate limiter.

  : Enter the **hardware rate-limit layer-2 multicast-snooping** <*pps*> command to rate limit these packets.

  Note The receive rate limiter matches and also rate limits certain other data packets that are sent to the supervisor module. It does not differentiate IGMP/PIM hello packets from these data packets. You must take appropriate care when you tune the receive rate limiter.
  Please note that an ISSU to Release 4.1(3) or above automatically shifts to the use of this rate-limiter to a default value of 10,000.

- CSCsr90977

  Symptom: Ports may go into the error-disabled state when you apply a large ACL to a port channel with many interfaces and you reload the module with the interfaces.

  Conditions: This situation may occur when you restart a module with a large ACL applied to a port channel with many interfaces on that module. When the module restarts, the ACL policies may not reach that module and cause the related ports to remain down and move into the error-disabled state.

  Workaround: This issue is resolved.

Send document comments to nexus7k-docfeedback@cisco.com.

- CSCsu01048

  Symptom: You may see high CPU utilization on the Cisco Nexus 7000 Series device if the network is passing a lot of packets that require fragmentation or are hitting the TTL expiry time.

  Conditions: When the system receives an IP packet with a length longer than the configured MTU on the packet's egress interface, the system sends this packet to the control plane, which takes care of the fragmentation.

  In the current software releases, the rate limiter for this type of packet does not take effect, which may possibly overwhelm the software forwarding stack. This situation, in turn, may lead to the instability of the routing and the control protocols.

  Workaround: This issue is resolved.

- CSCsu87911

  Symptom: The following syslog may be seen:

  ```
  *_2008 Sep 30 07:33:37 ch1-x7x-1b %DAEMON-2-SYSTEM_MSG: fatal:
  > buffer_append_space: len 4294967295 not supported - sshd[16028]_*
  ```

  Conditions: This symptom occurs infrequently under all conditions.

  Workaround: This issue is resolved.

- CSCsv92355

  Symptom: When you are working with the Cisco Nexus 70 10 and 7018 chassis, you may see packet drops on other modules when you perform an online insertion and removal of the 32-port 10-Gigabit Ethernet module.

  Conditions: You see this symptom only if you do not power down the module before performing an online insertion and removal of the 32-port 10-Gigabit Ethernet module.

  Workaround: This issue is resolved.

- CSCsw46525

  Symptom: When you create a VDC after a switchover, one or more interfaces may come up in the error-disabled state with a hardware error.

  Conditions: You may see this symptom when you perform a system switchover with less than four VDCs in the system and you create a new VDC after the switchover.

  Workaround: This issue is resolved.

- CSCsw47736

  Symptom: When you are processing a **flow monitor** command on a large range of VLANs, you may see a NetFlow memory error.

  Conditions: You may see this symptom when you are working with a large range of VLANs.

  Workaround: This issue is resolved.

- CSCsw64054

Send document comments to nexus7k-docfeedback@cisco.com.

Symptom: When the device does an SNMP SET on the RMON-MIB:statistics group objects or RMON-MIB:history, the SNMP agent crashes.

Conditions: You may see this symptom under all conditions.

Workaround: This issue is resolved.

- CSCsw92524

  Symptom: To obtain the IEEE 802.1Q value for a specific VLAN when you are working with NetConf, you must use the show interface brief form of the command. But the resulting display is still difficult to use.

  Conditions: This symptom may occur when you are working on 802.1Q VLANs and NetConf.

  Workaround: This issue is resolved.

- CSCsw97701

  Symptom: If you have a faulty I/O or fabric module in your system when you upgrade between Cisco NX-OS releases and that upgrade requires a mandatory upgrade of hardware firmware for a component, the system gets stuck in a "system not ready" state and does not allow the configuration to be saved when you enter the **copy running-config startup-config** command.

  Conditions: This symptom can occur when you have a combination of a failed hardware component and a pending software upgrade.

  Workaround: This issue is resolved.

- CSCsw98383

  Symptom: After you reload one of the modules, you may see that the CoPP policies are missing.

  Conditions: You may see this symptom after you reload a module.

  Workaround: This issue is resolved.

- CSCsx01522

  Symptom: When you enter the **show tech** command, the Cisco Nexus 7000 Series device that has dual supervisor modules, the active supervisor may reload because of a watchdog timeout.

  Conditions: You may see this symptom if the standby supervisor module has been rebooted more than 20 times and you enter the **show tech** command on the active supervisor module.

  Workaround: This issue is resolved.

Resolved Caveats—Cisco NX-OS Release 4.1(2)

All the caveats listed in this section are resolved in Cisco NX-OS Release 4.1(2) for the Cisco Nexus 7000 Series switches:

- CSCsm13589

  Symptom: Record-route does not work correctly when Policy Based Routing (PBR) is configured.

Send document comments to nexus7k-docfeedback@cisco.com.

Conditions: Any IP traffic redirected due to PBR is not sent to the supervisor module. As a result, record-route does not work for packets redirected due to PBR.

Workaround: This issue is resolved.

- CSCsm63331

  Symptom: The on-demand diagnostics for the port loopback test are not supported on the 32-port 10-Gbps Ethernet modules.

  Conditions: The **show diagnostic result module command** output indicates untested (U) for the 32-port 10-Gbps Ethernet modules after on-demand diagnostic testing of the port loopback feature with the **diagnostic start module** command.

  Workaround: This issue is resolved.

- CSCsm98229

  Symptom: A checkpoint creation or rollback operation can fail when an in-service software upgrade (ISSU) is in progress.

  Conditions: If you roll back the configuration or create a checkpoint while an ISSU is in progress, then the rollback or checkpoint creation operation can fail.

  Workaround: This issue is resolved.

- CSCso09082

  Symptom: The “use burn-in address (BIA)” feature for HSRP is not automatically applied to the main interface and all subinterfaces.

  Conditions: If you configure HSRP to use the BIA for an interface or subinterface using the **hsrp use-bia** command, the configuration is only applied to that interface or subinterface. The configuration is not, then, also applied to the main interface and all subinterfaces.

  Workaround: This issue is resolved.

- CSCso27690

  Symptom: The device name does not display with the login prompt.

  Conditions: If you configure a device name using the **switchname** command, the name does not display at the login prompt on the standby.

  Workaround: This issue is resolved.

- CSCso31974

  Symptom: If you open the ejector levers on the supervisor and reload the chassis, the supervisor module attempts to come up and as the ejector levers are detected as open, the system reloads the supervisor module again. This situation results in the standby supervisor module going through repeated reboot cycles.

  Conditions: This symptom occurs when you attempt to reload the chassis with the supervisor module still seated but with the ejector levers open.

  Workaround: This issue is resolved.

Send document comments to nexus7k-docfeedback@cisco.com.

- CSCso40446

  Symptom: You may see the Network Time Protocol (NTP) commands that hang for several minutes, and the related CLI commands do not take effect.

  Conditions: You may see this symptom when you are working with NTP.

  Workaround: This issue is resolved.

- CSCso43922

  Symptom: You may see lost OSPF adjacencies.

  Conditions: ICMP redirect is enabled by default on all Layer 3 interfaces. If the device receives a significant amount of traffic that triggers ICMP redirect, this situation can affect OSPF control traffic. If OSPF packets are dropped due to data packets being copied to the supervisor module for ICMP redirect, you can see an adjacency loss.

  Workaround: This issue is resolved.

- CSCsq25183

  Symptom: With more than 1000 interfaces or subinterfaces in the startup configuration, the device may fail.

  Conditions: If you are running an extremely large startup configuration, such as more than 1000 interfaces or subinterfaces, the configuration server may exhaust its memory and fail.

  Workaround: This issue is resolved.

- CSCsq28404

  Symptom: The IP EIGRP topology table does not show the next hop after changing the delay.

  Conditions: After you change the delay and enter the **show ip eigrp topology** command, the next hop information displayed is incorrect.

  Workaround: This issue is resolved.

- CSCsq29514

  Symptom: The current output of the Ethanalyzer read function resembles a UNIX cat command, where the output of a file is streamed without a pause or break. To add further functionality, add the following pipe operators:

  - **egrep**—Egrep
  - **grep**—Grep
  - **head**—Stream Editor
  - **last**—Display last lines
  - **less**—Stream editor
  - **no-more**—Turn-off pagination for command output
  - **sed**—Stream editor
  - **wc**—Count words, lines, or characters
  - **begin**—Begin with the line that matches

Send document comments to nexus7k-docfeedback@cisco.com.

  - **count**—Count number of lines
  - **exclude**—Exclude lines that match
  - **include**—Include lines that match

  Conditions: You may see this when you are using the Etheranalyzer on the Cisco Nexus 7000 Series switches.

  Workaround: This issue is resolved.

- CSCsq43292

  Symptom: Changing the LACP hello timers from normal to fast or from fast to normal may not work.

  Conditions: This symptom can occur in all conditions.

  Workaround: This issue is resolved.

- CSCsq73090

  Symptom: When you enter the **show interface tunnel** *number* command, the device displays the operational state of the tunnel as up when that tunnel source interface is down.

  Conditions: This situation occurs under all conditions.

  Workaround: This issue is resolved.

- CSCsq74911

  Symptom: The show blink function that displays the blink/beacon status for all devices is not available.

  Conditions: This symptom exists under all conditions.

  Workaround: This issue is resolved.

- CSCsq79703

  Symptom: NX-OS supports only prefix length; it does not support wildcard masks that have a 0 bit anywhere after the first 1 bit. You cannot have an ACL that offers the same granularity that Cisco IOS ACL provides.

  Conditions: This symptom occurs under all conditions.

  Workaround: This issue is resolved.

- CSCsq95595

  Symptom: The **clear counters** command does not clear the counters for tunnel interfaces.

  Conditions: This situation occurs under all conditions.

  Workaround: This issue is resolved.

- CSCsr09718

  Symptom: After IGMP multiple join and leave events, the Layer 2 multicast may stop functioning.

Send document comments to nexus7k-docfeedback@cisco.com.

Conditions: You may see this symptom after you enable IGMP snooping on a VLAN. A large number of receivers attached to this VLAN join and leave, which causes the outgoing list to be freed and reallocated multiple times. For example, if multiple join and leaves cause the multicast module to free and allocate a new set of outgoing interface list at least 64,000 times, the multicast module may fail to add a new outgoing list. Then, traffic is not forwarded to newly added receivers that require adding a new interface to the outgoing interface list.

Workaround: This issue is resolved.

- CSCsr21551

  Symptom: Cisco Nexus Series 7000 device failed to boot.

  Conditions: If the device receives an SNMP request when it is booting, the bootup fails.

  Workaround: This issue is resolved.

- CSCsr23521

  Symptom: The device may install only one route when the OSPF process receives two or more identical type-5 or type-7 LSAs with zero forwarding addresses. The device installs the last LSA received. According to RFC 3101, the OSPF process should install routes from all the identical LSAs to do ECMP routing.

  Conditions: You may see this symptom under all conditions.

  Workaround: This issue is resolved.

- CSCsr26385

  Symptom: Although the device sends the CMD accounting information, this information is not shown in the TACACS accounting log in the ACS server.

  Conditions: You have enabled TACACS cmd-accounting in the ACS server and set accounting to remote on the device, using a TACACS group, but the command configuration that you are doing on the device does not show on the server.

  Configuration for AAA server to see the accounting logs: Enable watchdog for that AAA client. Take the following steps to do that on the ACS server:

  1. Go to **Network Configuration**.
  2. In the AAA client's list, select the IP address of the device, which should be already configured.
  3. Check **Log Update/Watchdog Packets** from this AAA Client.
  4. Click **Submit+Apply**.

  The accounting is logged in the TACACS+ administration section.

  Workaround: This issue is resolved.

- CSCsr43915

  Symptom: You cannot work with EIGRP multi-instance MIBs without defining the SNMP context.

  Conditions: This symptom occurs when you are running more than one instance of EIGRP on a single device or operating an EIGRP process in a nondefault VRF.

  Workaround: This issue is resolved.

Send document comments to nexus7k-docfeedback@cisco.com.

- CSCsr46956

  Symptom: The Cisco Nexus 7000 Series device scales up to a maximum of 4000 VLANs across the entire system. These VLANs can be configured in single VDCs or across multiple VDCs. Problems can occur with multiple modules if the total number of VLANs configured on the device across all VDCs exceeds 4000.

  Conditions: This symptom can occur in all conditions.

  Workaround: This issue is resolved.

- CSCsr52252

  Symptom: After you upgrade to Release 4.0(4) from a previous release and you enter the **show eltm table** command from a module, the display may not show output for the module.

  Conditions: This symptom can occur in all conditions.

  Workaround: This issue is resolved.

- CSCsr75691

  Symptom: The device displays the CMP as operationally up, even when there is no cable connection to the CMP.

  Conditions: The output for the **show interface cmp-management** command shows the interface as up, even when there is no cable connection to the CMP.

  Workaround: This issue is resolved.

- CSCsr82153

  Symptom: When you are saving the configuration in a nondefault VDC using the **show running-config startup-config** command and you enter the **show startup-config** command in the default VDC, the device does not display the startup-config and returns the following error:

  ```
  configuration change in progress
  ```

  Conditions: If you enter the **show startup-config** command in the default VDC when there is an ongoing **show running-config startup-config** command in a nondefault VDC.

  Workaround: This issue is resolved.

- CSCsr87423

  Symptom: No syslog message is sent when you insert either the standby supervisor or the fabric module.

  Conditions: The device does not send a syslog message when you insert either the standby supervisor or the fabric module.

  Workaround: This issue is resolved.

Send document comments to nexus7k-docfeedback@cisco.com.

- CSCsr91565

  Symptom: After you reinitialize a module with port-channel subinterfaces that run Relay ACLs, the Relay ACL is removed from the port-channel interfaces.

  Conditions: You enabled the Relay function on the device by entering the **service dhcp** command. The module is configured with subinterfaces on a port channel with active members. After you reinitialize the module, some of the port-channel member interfaces are moved to a different VDC. The Relay ACL is removed from the port channel and port channel-subinterface on that module.

  Workaround: This issue is resolved.

- CSCsr93674

  Symptom: When you enter the **show ip arp vrf** *nondefault-vrf* | **last** *num* command for a nondefault, VRF, the device does not return the shell prompt.

  Conditions: When this situation occurs, you can press Ctrl- C to return the device to its normal state.

  Workaround: This issue is resolved.

- CSCsr96589

  Symptom: When you are replaying ASCII configuration scripts in nondefault VDCs, various private-vlan configuration commands fail.

  Conditions: When you replay ASCII configuration scripts in a nondefault VDC, the generated **feature private-vlan** command does not fall in the correct place. As a result, all other private-vlan commands fail.

  Workaround: This issue is resolved.

- CSCsr99927

  Symptom: If you configure a minimum MTU value for path-mtu-discovery that is greater than the actual value discovered, the device does not fall back to the default value until the default ager times out in 10 minutes.

  Conditions: If you configure a minimum MTU value for path-mtu-discovery that is greater than the actual value discovered. the device should immediately fall back to the default value. However, the device waits until the ager times out (the default is 10 minutes) before it falls back to the default minimum value.

  Workaround: This issue is resolved.

- CSCsu01052

  Symptom: If you configure a large number of port ACLS on a port-channel member, the member port may be set to the error-disabled or suspended state.

  Conditions: When you apply a large PACL policy for the first time, some of the affected port-channel members may be put into the error-disabled or suspended state during initialization. Note that ACL policies are applied only once during the first initialization and remain persistent in the hardware. Subsequent port initializations do not trigger the device to download policies to the hardware.

  Workaround: This issue is resolved.

Send document comments to nexus7k-docfeedback@cisco.com.

- CSCsu01596

  Symptom: After you enable the path-mtu-discovery process, the device may fragment tunneled packets, which may lead to packet drops at the tunnel destination because of rate limiters.

  Conditions: This situation occurs when the path MTU for two or more devices in the tunnel path are configured for a lower MTU than the tunnel destination MTU.

  Workaround: This issue is resolved.

- CSCsu01779

  Symptom: After you upgrade from the Cisco NX-OS Release 4.0(2) to the Release 4.0(3), the statistics for rate limiting may show incorrect values.

  Conditions: After you upgrade from the Cisco NX-OS Release 4.0(2) to the Release 4.0(3) and enter the **show hardware rate-limit** command, the resulting display may show incorrect values.

  Workaround: This issue is resolved.

- CSCsu05411

  Symptom: When there is more than one path to a prefix, the consistency checker may report an inconsistency, even though there is no inconsistency.

  Conditions: The consistency checker may report false positives for routes with ECMP.

  Workaround: This issue is resolved.

- CSCsu22036

  Symptom: Layer 3 multicast is not supported on port-channel subinterfaces.

  Conditions: Port-channel subinterfaces are not included in the Layer 3 multicast outgoing list.

  Workaround: This issue is resolved.

- CSCsu45752

  Symptom: When you insert or remove the compact flash (CF) of the logflash and enter the **dir logflash** command, the Cisco Nexus 7000 supervisor module may reload, which results in a switchover to the standby supervisor.

  Conditions: The Cisco Nexus 7000 supervisor module can switch over to the standby supervisor and return the following message when you insert or remove the compact flash of the logflash and enter the **dir logflash** command:

  ```
  N7K# Raw time read from Hardware Clock: Y=2008 M=8 D=29 11:17:25 writing reset reason
  34, Service "syslogd" in vdc 1
  ```

  Workaround: This issue is resolved.

- CSCsv07357

  Symptom: You may see a loss of routing adjacencies when the device is flooded with IP traffic with a time-to-live (TTL) of 1.

  Conditions: You may see this symptom when the Cisco Nexus Series 7000 device is flooded continuously with TTL 1 IP traffic on the control plane.

Send document comments to nexus7k-docfeedback@cisco.com.

Workaround: This issue is resolved.

- CSCsv21769

  Symptom: EIGRP may be unstable, such as neighbor ports are flapping, during congested or looped traffic conditions.

  Conditions: The device sets the dot1q CoS value to 0 for EIGRP packets, so these packets have a lower priority. During congested or looped traffic conditions, this situation may cause the symptom.

  Workaround: This issue is resolved.

- CSCsv35262

  Symptom: When an exporter has the source interface configured on a loopback interface in an ASCII config file, an error will occur when the ASCII configuration is applied to the running configuration.

  Conditions: This symptom may occur when an exporter has the source interface configured on a loopback interface.

  Workaround: This issue is resolved.

- CSCsv35626

  Symptom: VRRP groups that are in the active state with tracking enabled can change to the backup state after the supervisor module switches over.

  Conditions: The tracking state of VRRP groups can change from up to down after the supervisor module switches over, even though the underlying interface has not changed its state. The priority of the VRRP group is lowered and can change to the backup state for that group. The priority is not affected if tracking is not configured or if the tracked interface is in the down state already.

  Workaround: This issue is resolved.

- CSCsv35775

  Symptom: The ACL QoS process fails on the module.

  Conditions: When there are a large number of egress RACL entries in the ACL TCAM and you attach egress NetFlow with nonatomic updates enabled, the ACL QoS may fail and the policies may not be applied.

  Workaround: This issue is resolved.

- CSCsv40044

  Symptom: Reloading a module or the system may fail when you have configured a large number of ACLs with other features such as policy-based routing, DHCP snooping/relay, NetFlow, and so forth and you have not enabled the nonatomic update feature. This failure is due to insufficient resources.

  Conditions: This symptom may occur under all conditions.

  Workaround: This issue is resolved.

- CSCsv40258

Send document comments to nexus7k-docfeedback@cisco.com.

Symptom: Infrequently, after reloading the Cisco Nexus 7000 Series device, the direct routes for EIGRP-configured interfaces are not added to the EIGRP topology table. Instead, the topology entry is incorrectly shown as '0 successors' and 'Inaccessible.' Because the EIGRP prefix is not sent to the device's neighbors, the device is unreachable from the neighbors.

Conditions: This intermittent symptom may occur when the EIGRP-configured interface goes up immediately after going down.

Workaround: This issue is resolved.

- CSCsv40606

  Symptom: When you are interoperating with devices from vendors other than Cisco and you enter the **shutdown** and **no shutdown** commands operation on port-channel interfaces, the ports in the channel may move to the error-disabled state.

  Conditions: This symptom may occur when you are interoperating with devices from vendors other than Cisco.

  Workaround: This issue is resolved.

- CSCsv47908

  Symptom: When you are configuring a VRRP group, you may see virtual MAC address addition errors. The VRRP group remains in init state.

  Conditions: The insertion of the virtual MAC address into the hardware fails when you delete a VRRP group from an interface and you configure the same VRRP group number on a different interface. This situation causes the VRRP group to fail to come up. You may also see this symptom when you disable and reenable VRRP and then reconfigure the VRRP groups.

  Workaround: This issue is resolved.

- CSCsv49677

  Symptom: When you boot up the device with autorp announce or autorp discovery configured, PIM crashes.

  Conditions: You may see this symptom when you start up the device if the startup configuration has autorp announce or autorp discovery commands.

  Workaround: This issue is resolved.

- CSCsv63773

  Symptom: If a duplicate name exists for the user in both a non-default VDC and the default VDC and that user is logged in, you are unable to remove that user from the default VDC.

  Conditions: You will not see this problem with a duplicate username in two separate non-default VDCs. You may see this symptom under the following conditions:

  - The same username is configured in the default VDC and in a non-default VDC.
  - This user is logging into the non-default VDC.

  Workaround: This issue is resolved.

Send document comments to nexus7k-docfeedback@cisco.com.

- CSCsv75113

  Symptom: The device may display the incorrect outgoing interface in a non-default VDC after you enter the **show port-channel load-balance forwarding-path** command.

  Conditions: You may see this symptom when you are working in a non-default VDC.

  Workaround: This issue is resolved.

- CSCsv84522

  Symptom: During an ISSU, you may see some packet loss and memory/mts leak on VLAN network interfaces for First Hop Router Protocols (FHRP)—for example, Hot Standby Router Protocol (HSRP), VRRP, and Gateway Load Balancing Protocol (GLBP).

  Conditions: During an ISSU with an FHRP configured on a VLAN network interface, the protocol changes and interface flaps are queued up temporarily. These do not get processed later; this situation also results in mts buffer and memory leaks.

  Workaround: This issue is resolved.

- CSCsv85569

  Symptom: The Cisco Nexus 7000 Series device may create a duplicate copy of the packet when it receives a packet that requires an ICMP redirect.

  Conditions: When the device receives a packet that is routed back on the same interface—which is the condition required to send an ICMP redirect to the source—the hardware switches the packet and sends a copy of the packet to the supervisor for generating ICMP redirect. The supervisor then switches the copied packet using software, which creates a duplicate copy of the packet.

  Workaround: This issue is resolved.

- CSCsw17668

  Symptom: After you enter the **system default switchport** command and configure a loopback interface, you may see the following:

  - You cannot ping the loopback interface.
  - When you enter the **show ip interface** *x* command, the system returns the following message:

  ```
  IP is disabled on loopback
  ```

  Conditions: You may see this symptom after you configure a loopback interface and try to display the IP information for that interface after you have entered the **system default switchport** command.

  Workaround: This issue is resolved.

- CSCsw22423

  Symptom: After you modify an ACL set in an interface, some of the ACLs on the other interfaces may not work correctly. For example, after you make this modification, some Layer 4 applications like Telnet or SSH sessions cannot be filtered.

  Conditions: You may see this symptom right after you boot the device and modify an ACL configuration.

  Workaround: This issue is resolved.

Send document comments to nexus7k-docfeedback@cisco.com.

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:

NX-OS Configuration Guides

Cisco Nexus 7000 Series NX-OS Getting Started with Virtual Device Contexts, Release 4.1

Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.1

Cisco Nexus 7000 Series NX-OS XML Management Interface User Guide, Release 4.1

Cisco MDS 9000 Family and Nexus 7000 Series NX-OS System Messages Reference, Release 4.1

Cisco Nexus 7000 Series NX-OS MIB Quick Reference

NX-OS Command References

Cisco Nexus 7000 Series NX-OS Command Reference Master Index, Release 4.1

Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference, Release 4.1

Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 4.1

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.1

Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference, Release 4.1

Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.1

Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference, Release 4.1

Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.1

Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference, Release 4.1

Cisco Nexus 7000 Series NX-OS System Management Command Reference, Release 4.1

Send document comments to nexus7k-docfeedback@cisco.com.

Other Software Document

Cisco Nexus 7000 Series NX-OS Troubleshooting Guide, Release 4.1

Obtaining Documentation and Submitting a Service Request

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

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

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

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

Cisco Nexus 7000 Series NX-OS Release Notes, Release 4.1

© 2008-2009 Cisco Systems, Inc. All rights reserved.