Cisco Nexus 3000 Series NX-OS Release Notes, Release 7.0(3)I7(3)

This document describes the features, caveats, and limitations for Cisco Nexus 3000 Series and Cisco Nexus 3100 Series switches. Use this document in combination with documents listed in the *Obtaining Documentation and Submitting a Service Request* section.

Note: Starting with Cisco NX-OS Release 7.0(3)I2(1), the Cisco NX-OS image filename has changed to start with "nxos" instead of "n3000."

Table 1 shows the online change history for this document.

Table 1 Online History Change

Date	Description
February 12, 2018	Created NX-OS Release 7.0(3)I7(3) release notes.
February 21, 2018	Revised the Known Behaviors list.
March 07, 2017	Updated the open bug lists to include CSCvi02501 and CSCvi01072.
March 9, 2018	Added a limitation for IGMP snooping.
March 22, 2018	Updated the hardware list.
April 20, 2018	Updated the upgrade section to include the upgrade from Cisco NX-OS Release 6.0(2)U6(7) and Cisco NX-OS Release 6.0(2)U6(8) to Cisco NX-OS Release 7.0(3)I7(3).
August 10, 2018	Updated the upgrade path.
November 17, 2018	Replaced instances of Cisco NX-OS Release 6.0(2)U6(2) and 6.0(2)U6(3) with Cisco NX-OS Release 6.0(2)U6(2a) and 6.0(2)U6(3a).
December 18, 2018	Added Licensing Information.

Contents

Introduction

Several new hardware and software features are introduced for the Cisco Nexus 3000 Series and Cisco Nexus 3100 Series devices to improve the performance, scalability, and management of the product line. Cisco NX-OS Release 7.x also supports all hardware and software supported in Cisco NX-OS Release 6.x, Cisco NX-OS Release 5.1, and Cisco NX-OS Release 5.0.

Cisco NX-OS offers the following benefits:

- Cisco NX-OS runs on all Cisco data center switch platforms: Cisco Nexus 9000, Nexus 7000, Nexus 5000, Nexus 4000, Nexus 3000, Nexus 2000, and Nexus 1000V Series switches.
- Cisco NX-OS software interoperates with Cisco products that run any variant of Cisco IOS software and also with any networking operating system that conforms to common networking standards.
- Cisco NX-OS modular processes are triggered on demand, each in a separate protected memory space. Processes are started and system resources are allocated only when a feature is enabled. The modular processes are governed by a real-time preemptive scheduler that helps ensure timely processing of critical functions.
- Cisco NX-OS provides a programmatic XML interface that is based on the NETCONF industry standard. The Cisco NX-OS XML interface provides a consistent API for devices. Cisco NX-OS also provides support for Simple Network Management Protocol (SNMP) Versions 1, 2, and 3 MIBs.
- Cisco NX-OS enables administrators to limit access to switch operations by assigning roles to users. Administrators can customize access and restrict it to the users who require it.

This section includes the following:

- Cisco Nexus 3000 Series Switches
- Cisco Nexus 3100 Series Switches
- Cisco Nexus 3500 Series Switches

Cisco Nexus 3000 Series Switches

The Cisco Nexus 3000 Series switches are high-performance, high-density, ultra-low-latency Ethernet switches that provide line-rate Layer 2 and Layer 3 switching. The Cisco Nexus 3000 Series includes the following switches:

- The Cisco Nexus 3064 switch is a 1 RU switch that supports 48 1- or 10-Gigabit downlink ports, four Quad Small Form-Factor Pluggable (QSFP+) ports that can be used as a 40 Gigabit Ethernet port or 4 x10-Gigabit Ethernet ports, one 10/100/1000 management port, and one console port.
- The Cisco Nexus 3048 switch is a 1 rack unit (RU) switch that supports 48 10/100/1000 Ethernet server-facing (downlink) ports, four 10-Gigabit network-facing (uplink) ports, one 100/1000 management port, and one console port.
- The Cisco Nexus 3016 is a 1 RU, 16-port QSFP+ switch. Each QSFP+ port can be used as a 40-Gigabit Ethernet port or 4 x10-Gigabit Ethernet ports.

Each switch includes one or two power supply units and one fan tray module, and each switch can be ordered with either forward (port-side exhaust) airflow or reverse (port-side intake) airflow for cooling. All platforms support both AC and DC power supplies. All combinations of power (AC/DC) and airflow (forward/reverse) are available. The Cisco Nexus 3000 Series switches run the Cisco NX-OS software.

For information about the Cisco Nexus 3000 Series, see the Cisco Nexus 3000 Series Hardware Installation Guide.

Cisco Nexus 3100 Series Switches

The Cisco Nexus 3100 Series switches are high-performance, high-density, ultra-low-latency Ethernet switches that provide line-rate Layer 2 and Layer 3 switching. In Cisco NX-OS Release 7.0(3)I7(3), the Cisco Nexus 3100 Series includes the Cisco Nexus 3132, Nexus 3172, Nexus 3132Q-V, Nexus N31108PC-V, Nexus N31108TC-V, Nexus C3264Q-S, and Nexus C3232C switches.

The Cisco Nexus 3172PQ switch is a 10-Gbps Enhanced Small Form-Factor Pluggable (SFP+)–based ToR switch with 48 SFP+ ports and 6 Enhanced Quad SFP+ (QSFP+) ports.

The Cisco Nexus 3172TQ switch is a 10GBASE-T switch with 48 10GBASE-T ports and 6 Quad SFP+ (QSFP+) ports.

Each SFP+ port can operate in 100-Mbps, 1-Gbps, or 10-Gbps mode, and each QSFP+ port can operate in native 40-Gbps or 4 x 10-Gbps mode. This switch is a true physical-layer-free (phy-less) switch that is optimized for low latency and low power consumption.

The Cisco Nexus 3132Q switch is a 1RU, 40-Gbps QSFP-based switch that supports 32 fixed 40-Gbps QSFP+ ports. It also has 4 SFP+ ports that can be internally multiplexed with the first QSFP port. Each QSFP+ port can operate in the default 40-Gbps mode or 4 x 10-Gbps mode, up to a maximum of 104 10-Gbps ports.

Each switch includes dual redundant power supply units, four redundant fans, one 10/100/1000 management port, and one console port. Each switch can be ordered with either forward (port-side exhaust) airflow or reverse (port-side intake) airflow for cooling. It supports both AC and DC power supplies. All combinations of power (AC/DC) and airflow (forward/reverse) are available. The Cisco Nexus 3100 Series switches run the Cisco NX-OS software.

For information about the Cisco Nexus 3100 Series, see the Cisco Nexus 3000 Series Hardware Installation Guide.

Cisco Nexus 3500 Series Switches

The Cisco Nexus 3500 platform is an extension of the Cisco Nexus 3000 Series of 100M, 1, 10, and 40 Gigabit Ethernet switches built from a switch-on-a-chip (SoC) architecture. Switches in the Cisco Nexus 3500 series include Algorithm Boost (or Algo Boost) technology that is built into the switch application-specific integrated circuit (ASIC). Algo Boost allows the Cisco Nexus 3548 switch to achieve Layer 2 and Layer 3 switching latencies of less than 200 nanoseconds (ns). In addition, Algo Boost contains several innovations for latency, forwarding features, and performance visibility, including two configurable modes for low latency:

- Normal mode: This mode is suitable for environments needing low latency and high scalability.
- Warp mode: This mode consolidates forwarding operations within the switching ASIC, lowering latency by up to an additional 20 percent compared to normal operation.

Active buffer monitoring accelerates the collection of buffer utilization data in hardware, allowing significantly faster sampling intervals. Even on the lowest-latency switches, data packets can incur a millisecond or more of latency during periods of congestion. Previous buffer utilization monitoring techniques were based entirely on software polling algorithms with polling with higher polling intervals that can miss important congestion events.

Cisco Nexus 3548 Switch

The Cisco Nexus 3548 switch is the first member of the Cisco Nexus 3500 platform. As a compact one-rack-unit (1RU) form-factor 10 Gigabit Ethernet switch, the Cisco Nexus 3548 switch provides line-rate Layer 2 and Layer 3 switching at extremely low latency. The switch runs Cisco NX-OS software that has comprehensive features and functions that are widely deployed globally. The Cisco Nexus 3548 contains no physical layer (PHY) chips, which allows low latency and low power consumption. The switch supports both forward and reversed airflow and both AC and DC power inputs.

Cisco Nexus 3524 Switch

The Cisco Nexus 3524 switch is a Cisco Nexus 3548 switch, but with only 24 ports active and can be upgraded to use all 48 ports. As a compact one-rack-unit (1RU) form-factor 10 Gigabit Ethernet switch, the Cisco Nexus 3548 switch is the lowest entry point for main-stream top-of-rack (TOR) data center deployments which offers line-rate Layer 2 and Layer 3 switching with a comprehensive feature set, including Algo Boost technology, and ultra-low latency.

For information about the Cisco Nexus 3500 Series, see the *Cisco Nexus 3000 Series Hardware Installation Guide*.

Licensing Requirements

Temporary licenses with an expiry date are available for evaluation and lab use purposes. They are strictly not allowed to be used in production. Please use a permanent or subscription license that has been purchased through Cisco for production purposes.

For more information, see the Cisco NX-OS Licensing Guide.

System Requirements

This section includes the following topics:

- Memory Requirements
- Hardware Supported
- Twinax Cable Support on Cisco Nexus 3000 Switches
- Cisco QSFP 40-Gbps Bidirectional Short-Reach Transceiver

Memory Requirements

The Cisco NX-OS Release 7.0(3)I7(3) software requires 1 GB of flash memory.

Hardware Supported

Table 2 lists the Cisco Nexus 3000 and Cisco Nexus 3500 Series hardware that Cisco NX-OS Release 7.0(3)I7(3) supports. For additional information about the supported hardware, see the *Cisco Nexus 3000 Series Hardware Installation Guide*.

Table 2 Hardware Supported by Cisco NX-OS Release 7.0(30I7(3) Software.

Hardware	Part Number
Cisco Nexus 3548 switch	N3K-C3548P-10G
Cisco Nexus 3548x switch, 48 SFP+	N3K-C3548P-10GX
Cisco Nexus 3548-XL	N3K-C3548P-XL
Cisco Nexus 3524 switch	N3K-C3524P-10G
Cisco Nexus 3524 switch, 24 SFP+	N3K-C3524P-10GX
Cisco Nexus 3524-XL switch	N3K-C3524P-XL
Cisco Nexus 3132Q-X switch	N3K-C3132Q-40GX
Cisco Nexus C3172TQ-XL switch	N3K-C3172TQ-XL
Cisco Nexus C3172PQ-XL switch	N3K-C3172PQ-XL
Cisco Nexus C3132Q-XL switch	N3K-C3132Q-XL
Cisco Nexus 3172TQ switch	N3K-C3172TQ-10GT
Cisco Nexus 3172PQ switch	N3K-C3172PQ-10GE

Hardware	Part Number
Cisco Nexus 3132Q-V switch	N3k-C3132Q-V
Cisco Nexus 3132Q switch	N3K-C3132Q-40GE
Cisco Nexus 31108TC-V	N3K-C31108TC-V
Cisco Nexus 31108PC-V switch	N3K-C31108PC-V
Cisco Nexus 3064-X switch	N3K-C3064PQ-10GX
Cisco Nexus 3064-X reversed airflow (port-side intake) AC power supply	N3K-C3064-X-BA-L3
Cisco Nexus 3064-X forward airflow (port-side intake) DC power supply	N3K-C3064-X-BD-L3
Cisco Nexus 3064-X forward airflow (port-side exhaust) DC power supply	N3K-C3064-X-FD-L3
Cisco Nexus 3064-X forward airflow (port-side exhaust) AC power supply	N3K-C3064-X-FA-L3
Cisco Nexus 3064-TQ switch	N3K-C3064TQ-10GT
Cisco Nexus 3064-T 500W reverse airflow (port-side intake) AC power supply	NXA-PAC-500W-B
Cisco Nexus 3064-T 500W forward airflow (port-side exhaust) AC power supply	NXA-PAC-500W
Cisco Nexus 3064-E switch	N3K-C3064PQ-10GE
Cisco Nexus 3064 switch	N3K-C3064PQ
Cisco Nexus 3064 fan module with reverse airflow (port-side intake); also used in the Cisco Nexus 3016	N3K-C3064-FAN-B
Cisco Nexus 3064 fan module with forward airflow (port-side exhaust); also used in the Cisco Nexus 3016	N3K-C3064-FAN
Cisco Nexus 3048 switch	N3K-C3048TP-1GE
Cisco Nexus 3048 fan module with reverse airflow (port-side intake)	N3K-C3048-FAN-B

Hardware	Part Number
Cisco Nexus 3048 fan module with forward airflow (port-side exhaust)	N3K-C3048-FAN
Cisco Nexus 3016 switch	N3K-C3016Q-40GE
Cisco Nexus 3000 power supply with reverse airflow (port-side intake)	N2200-PAC-400W-B
Cisco Nexus 3000 power supply with forward airflow (port-side exhaust)	N2200-PAC-400W
Cisco Nexus 2000 power supply with forward airflow (port-side exhaust)	N2200-PDC-400W
Cisco Nexus 2000 DC power supply with reverse air-flow (port-side intake)	N3K-PDC-350W-B
Cisco Nexus 2000 or Nexus 3000 individual fan, for-ward airflow (port side exhaust	NXA-FAN-30CFM-F
Cisco Nexus 2000 or Nexus 3000 individual fan, re-versed airflow (port side intake)	NXA-FAN-30CFM-B
Cisco Nexus 2000 or Nexus 3000 400W AC power supply, forward airflow (port side exhaust)	N2200-PAC-400W
Cisco Nexus 2000 or Nexus 3000 400W AC power supply, reversed airflow (port side intake)	N2200-PAC-400W-B
Cisco Nexus 2000 or Nexus 3000 400W DC power supply, forward airflow (port side exhaust)	N2200-PDC-400W
Cisco Nexus 2000 or Nexus 3000 350W DC power supply, reversed airflow (port side intake)	N3K-PDC-350W-B
Transceivers	
10-Gigabit	
10GBASE-ZR SFP+ module (single-mode fiber [SMF])	SFP-10G-ZR
10GBASE-CU SFP+ cable 1.5 m (Twinax cable)	SFP-H10GB-CU1-5M
10GBASE-CU SFP+ cable 2 m (Twinax cable)	SFP-H10GB-CU2M

Hardware	Part Number
10GBASE-CU SFP+ cable 2.5 m (Twinax cable)	SFP-H10GB-CU2-5M
Active optical cable 1 m	SFP-10G-AOC1M
Active optical cable 3 m	SFP-10G-AOC3M
Active optical cable 5 m	SFP-10G-AOC5M
Active optical cable 7 m	SFP-10G-AOC7M
10GBASE-DWDM long-range transceiver module 80 km with single mode duplex fiber	DWDM-SFP10G-C
10GBASE-DWDM long-range transceiver module 80 km with single mode duplex fiber	DWDM-SFP10G
10GBASE-SR SFP+ module (multimode fiber [MMF])	SFP-10G-SR
10GBASE-LR SFP+ module (single-mode fiber [SMF])	SFP-10G-LR
Cisco 10GBASE-ER SFP+ Module for SMF	SFP-10G-ER
10GBASE-CU SFP+ cable 1 m (Twinax cable)	SFP-H10GB-CU1M
10GBASE-CU SFP+ cable 3 m (Twinax cable)	SFP-H10GB-CU3M
10GBASE-CU SFP+ cable 5 m (Twinax cable)	SFP-H10GB-CU5M
Active Twinax cable assembly, 7 m	SFP-H10GB-ACU7M
Active Twinax cable assembly, 10 m	SFP-H10GB-ACU10M
1-Gigabit Ethernet	
1000BASE-T SFP	GLC-TE
Gigabit Ethernet SFP, LC connector EX transceiver (MMF)	GLC-EX-SMD
Gigabit Ethernet SFP, LC connector ZX transceiver (MMF)	GLC-ZX-SMD
1000BASE-T SFP	GLC-T
Gigabit Ethernet SFP, LC connector SX transceiver (MMF)	GLC-SX-MM

Hardware	Part Number
Gigabit Ethernet SFP, LC connector SX transceiver (MMF)	GLC-SX-MMD
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF)	GLC-LH-SM
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF)	GLC-LH-SMD
100-Megabit Ethernet	
1000BASE-T SFP transceiver module with extended operating temperature range	SFP-GE-T
100BASE-FX SFP module for Gigabit Ethernet ports GLC-GE-100FX	GLC-GE-100FX

Twinax Cable Support on Cisco Nexus 3000 Switches

Starting with Cisco Release NX-OS 5.0(3)U1(1), the following algorithm is used to detect copper SFP+ twinax, QSFP+ twinax, and QSFP+ splitter cables on Cisco Nexus 3000 Series switches.

If the attached interconnect (transceiver) is a copper SFP+ twinax or QSFP+ twinax cable:

- Verify the transceiver SPROM to match the Cisco magic code.
- If the check succeeds, bring up the interface. Otherwise, print the following warning message appears stating that a non-Cisco transceiver is attached and that you should try to bring up the port.

  2009 Oct 9 01:46:42 switch %ETHPORT-3-IF_NON-CISCO_TRANSCEIVER: Non-Cisco transceiver on interface Ethernet1/18 is detected.

If the attached transceiver is a QSFP+ splitter cable, then no special check is performed. The Cisco NX-OS software tries to bring up the port.

The following disclaimer applies to non-Cisco manufactured and non-Cisco certified QSFP copper splitter cables:

If a customer has a valid support contract for Cisco Nexus switches, Cisco TAC will support twinax cables that are a part of the compatibility matrix for the respective switches. However, if the twinax cables are not purchased through Cisco, a customer cannot return these cables through an RMA to Cisco for replacement.

If a twinax cable that is not part of the compatibility matrix is connected into a system, Cisco TAC will still debug the problem, provided the customer has a valid support contract on the switches. However TAC may ask the customer to replace the cables with Cisco qualified cables if there is a situation that points to the cables possibly being faulty or direct the customer to the cable provider for support. Cisco TAC cannot issue an RMA against uncertified cables for replacement.

Cisco QSFP 40-Gbps Bidirectional Short-Reach Transceiver

The Cisco QSFP 40-Gbps Bidirectional (BiDi) transceiver is a short-reach pluggable optical transceiver with a duplex LC connector for 40-GbE short-reach data communications and interconnect applications by using multimode fiber (MMF). The Cisco QSFP 40-Gbps BiDi transceiver offers a solution that uses existing duplex MMF infrastructure for 40-GbE connectivity. With the Cisco QSFP 40-Gbps BiDi transceiver, customers can upgrade their network from 10-GbE to 40-GbE without incurring any fiber infrastructure upgrade cost. The Cisco QSFP 40-Gbps BiDi transceiver can enable 40-GbE connectivity in a range of up to 100 meters over OM3 fiber, which meets most data center reach requirements. It complies with the Multiple Source Agreement (MSA) QSFP specification and enables customers to use it on all Cisco QSFP 40-Gbps platforms and achieve high density in a 40-GbE network. It can be used in data centers, high-performance computing (HPC) networks, enterprise and distribution layers, and service provider transport applications.

New and Changed Information

This section lists the new and changed information in Release 7.0(3)I7(3):

- New Supported Hardware
- New Software Features

New Supported Hardware

Cisco NX-OS Release 7.0(3)I7(3) supports the following hardware:

- Cisco Nexus 3524-XL
- Cisco Nexus 3548-XL

New Software Features

Cisco NX-OS Release 7.0(3)I7(3) supports the following new software features:

Fundamentals Feature

- POAP − Added the ability to enable POAP during each reload and disable the POAP process during boot up for all Cisco Nexus 3000 Series switches.

  For more information, see the Cisco Nexus 3000 Series NX-OS Fundamentals Configuration Guide, Release 7.x.

Interfaces Features

- NAT − Support to NAT for all Cisco Nexus 3100 Series switches.
- Q-in-Q - Double Tagging: Added the ability for the Cisco Nexus 3000 Series switches to allow multi-tagged BPDUs on a tunnel port.

  For more information, see the Cisco Nexus 3000 Series NX-OS Interfaces Configuration Guide, Release 7.x .

Label Switching Features

- ISIS over Segment Routing – Added support to Cisco Nexus 3172, Cisco Nexus 3132, Cisco Nexus C31128PQ-10GE, and Cisco Nexus N3K-C3164Q-40GE switches.
- SR-APP – Added the segment routing application which helps configuring the segment routing functionality. This reserves the SRGB range and notifies the clients about while maintaining the prefix to the SID mappings.

  For more information, see the Cisco Nexus 3000 Series NX-OS Label Switching Configuration Guide, Release 7.x .

Layer 2 Switching Feature

- MAC learn disable and MAC address loop detect – Added support to disable MAC learning and detect loop port down.

  For more information, see the Cisco Nexus 3000 Series NX-OS Layer 2 Switching Configuration Guide, Release 7.x.

Security Feature

- Legacy SSH Algorithm – Added the ability to configure support for legacy SSH security algorithms, message authentication codes (MACs), key types, and ciphers.

  For more information, see the Cisco Nexus 3000 Series NX-OS Security Configuration Guide, Release 7.x.

System Management Feature

- Config Replace – Added the ability for the Cisco Nexus 3000 Series switches to replace the running configuration with user provided configuration, without reloading the Cisco NX-OS switch.

  For more information, see the Cisco Nexus 3000 Series NX-OS System Management Configuration Guide, Release 7.x.

NX-API REST Features

- See the "New and Changed Information" section of the *Cisco Nexus 3000 and 9000 Series NX-API REST SDK User Guide and API Reference* for a detailed list of the updates for Cisco NX-OS Release 7.0(3)I7(3).

Section Name	Subsection
Additional Configuration	Configuring POAP ■ Added commands for enabling POAP
Configuring BGP	Configuring an IPv4 Address Family ■ Added commands for configuring and deleting label allocations Configuring an IPv4 Labeled Unicast Address ■ Added commands for configuring and deleting: ▪ Receive capability for additional paths ▪ To advertise only active routes to the peer ▪ A route map to selectively unsuppress suppressed routes ▪ A conditioned route-map to advertise only when a prefix in condition exists ▪ A route map for conditional advertisement ▪ A route map to specify criteria for originating the default ▪ A site-of-origin extended community under VRF default and IPv4 labeled unicast Configuring an IPv6 Address Family ■ Added commands for configuring and deleting: ▪ The label allocation to all routes ▪ The label allocation to a route map ▪ Additional paths to install the backup path Configuring an IPv6 Labeled Unicast Address ■ Added commands for configuring and deleting: ▪ To advertise only active routes to the peer ▪ Receive capability for additional paths ▪ A third-party nexthop ▪ A route-map to selectively unsuppress suppressed routes ▪ A conditioned route map to advertise only when prefix in condition exists ▪ A route map for conditional advertisement ▪ A route map to specify criteria for originating the default Configuring an IPv4 Labeled Unicast Address ■ Added commands for configuring and deleting: ▪ Overriding route-target's ASN field for EBGP EVPN sessions (values inherited from a peer template) ▪ A default site-of-origin extended community (values inherited from a peer template)Configuring a Link-State Address Family Configuring a Link-State Address Family

Section Name	Subsection
	■ Added commands for configuring and deleting target VPN extended communities Configuring a VPNv4 Unicast Address Family ■ Added commands for configuring and deleting: ▪ Multipath for EBGP and IBGP paths ▪ The peering address as nexthop Configuring a VPNv6 Unicast Address Family ■ Added commands for configuring and deleting: ▪ Multipath for EBGP and IBGP paths ▪ The peering address as nexthop
Configuring the Clock	Added commands for configuring: ■ The NTP clock protocol

Section Name	Subsection
Configuring DHCP	Configuring an IPv6 DHCP Guard Policy ■ Added commands for configuring and deleting: ▪ The maximum number for the allowed advertised server preference of an ipv6 dhcp guard policy ▪ The minimum number for the allowed advertised server preference of an ipv6 dhcp guard policy ▪ Trusted port (no policing) for an ipv6 dhcp guard policy Configuring IPv6 RA Guard Policies ■ Added commands for configuring and deleting: ▪ trusted port (no policing) for an IPv6 RA guard policy ▪ The maximum hop limit for an IPv6 RA guard policy ▪ The minimum hop limit for an IPv6 RA guard policy ▪ The verification of the advertised managed address configuration flag for an IPv6 RA guard policy ▪ The verification of the advertised other configuration flag for an IPv6 RA guard policy ▪ Discarding RAs with a router preference greater than high Configuring IPv6 Snooping Policies ■ Added commands for configuring and deleting: ▪ The role of the switch attached to the port for an IPv6 snooping policy ▪ The maximum addresses per port for an IPv6 snooping policy ▪ A list of protected prefixes to glean DHCP packets for an IPv6 snooping policy ▪ The security level to glean addresses for an IPv6 snooping policy ▪ Trusted port (no policing) for an IPv6 snooping policy Configuring an IPv6 Snooping Binding Table ■ Added commands for configuring and deleting: ▪ An IPv6 snooping binding table with a VLAN interface ▪ The maximum number of entries for an IPv6 snooping binding table ▪ The syslog logging of binding table events ▪ The interval time between two probings
Configuring DNS	Added commands for configuring: ▪ The name for an IPv4 host ▪ The name for an IPv6 host
Configuring Interfaces	Added commands for configuring and deleting: ▪ A NAT pool with network mask ▪ A NAT pool with prefix length

Section Name	Subsection
Configuring LACP	Added commands for configuring and deleting: ▪ The MAC address to be used for the LACP protocol exchanges (role: primary) ▪ The MAC address to be used for the LACP protocol exchanges (role: secondary) Resetting to use the default VDC MAC address

Section Name	Subsection
Configuring Multicast (IGMP)	Added commands for configuring: ■ Event history buffers ■ Group membership timeout in minutes ■ The IGMP snooping timeout to never expire ports from a group membership ■ Global link-local groups suppression ■ A vPC-peer-link as static Mrouter for all VLANs ■ The max-response-time for the switch's proxy general-queries ■ Enabling loopback packet to check and drop it ■ Disabling loopback packet to check and drop it ■ To exclude a vPC peer-link for routed multicast traffic ■ The initial hold-down period after switchover or restart ■ Entering MFDM congestion-control mode ■ Exiting MFDM congestion-control mode ■ IGMPv3 report suppression and proxy reporting for the VLAN ■ Snooping for VXLAN VLANs ■ The IGMP table syslog threshold ■ The filter policy for groups mentioned in a route-map ■ IGMPv1 or IGMPv2 report suppression for a VLAN ■ The group membership timeout in minutes (Under a VLAN) ■ The IGMP snooping timeout to never expire ports from a group membership (Under a VLAN) ■ VLAN link-local groups suppression (Under a VLAN) ■ A static group membership (Under a VLAN) ■ The number of omf route entries in m2rib buffer (Under a VLAN) ■ The number of groups that could be joined per interface (Under a VLAN) ■ The maximum number of omf entries in m2rib buffer (Under a VLAN) ■ The maximum number of route entries in m2rib buffer (Under a VLAN) ■ The max-response-time for the switch's proxy general-queries (Under a VLAN) ■ Explicit host tracking for VLAN (Under a VLAN) ■ Fast leave for the VLAN (Under a VLAN) ■ The interval between group-specific query transmissions (Under a VLAN) ■ IGMPv1 or IGMPv2 report suppression for the VLAN (Under a VLAN) ■ IGMPv3 report suppression and proxy reporting for the VLAN (Under a VLAN) ■ IGMP snooping (Under a VLAN) ■ An IGMP report policy with a prefix list (Under a VLAN) ■ An IGMP report policy with a route map (Under a VLAN) ■ An IGMP access group with a prefix list (Under a VLAN) ■ An IGMP report policy with a route map (Under a VLAN) ■ Querier timeout for IGMPv2 (Under a VLAN)

Section Name	Subsection
Configuring Multicast (MRIB)	Added commands for configuring event history buffers
Configuring Multicast (MSDP)	Added commands for configuring event history buffers
Configuring Multicast (NGMVPN)	Added commands for configuring and deleting: ■ A node as distributed-DR ■ L3-overlay SPT (Shortest-Path-Tree)
Configuring Multicast (PIM)	Added commands for configuring and deleting event history buffers
Configuring Power Modes	Added commands for configuring and deleting: ■ Power supply redundancy mode as combined (Forced) ■ Power supply redundancy mode as combined ■ Power supply redundancy mode as input source redundant ■ Power Su supply redundancy mode as PS redundant
Configuring Route Policy Manager	IPv4 Configuration Examples Added commands for configuring and deleting: ■ Next-hop order as per CLI configuration ■ Load sharing IPv6 Configuration Examples Added commands for configuring and deleting: ■ Next-hop order as per CLI configuration ■ Load sharing
Configuring Static MPLS and Segment Routing	Added sections for configuring: ■ Shutdown segment routing ■ Global block range for segment routing bindings ■ Interval for which SR will wait for SRGB cleanup ACK from clients ■ Interval for which SR will retry SRGB allocation with ULIB ■ Connected prefix segment identifier mappings ■ IPv4 address-family under connected prefix segment identifier mappings ■ IPv6 address-family under connected prefix segment identifier mappings ■ IP address for IPv4 address-family under connected prefix segment identifier mappings

Section Name	Subsection
Configuring Unicast RPF	IPv4 Configurations ■ Added commands for configuring: ▪ The source as reachable via the interface on which a packet was received ▪ The source as reachable via any interface with loose default route unicast reverse path forwarding IPv6 Configurations ■ Added commands for configuring and deleting: ▪ The source as reachable via the interface on which a packet was received ▪ The source as reachable via any interface with loose default route unicast reverse path forwarding
Configuring VLANs	Added commands for enabling MAC learning on all VLANs on an interface

Caveats

The open and resolved caveats and the known behaviors for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Note: You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. if you do not have one, you can register for an account.

This section includes the following topics:

- Resolved Caveats-Cisco NX-OS Release 7.0(3)I7(3)
- Open Caveats-Cisco NX-OS Release 7.0(3)I7(3)
- Known Behaviors-Cisco NX-OS Release 7.0(3)I7(3)

Resolved Caveats-Cisco NX-OS Release 7.0(3)I7(3)

Table 3 lists the resolved caveats in Cisco NX-OS Release 7.0(3)I7(3). Click the Bug ID to access the Cisco Bug Search Tool for additional information about the bug.

Table 3 Cisco NX-OS Release 7.0(3)I7(3) – Resolved Caveats

Bug ID	Description
CSCva08222	When the ethanalyzer is used to monitor the packets for more than 30 minutes, a syslog is generated to indicate the system temporary directory (\tmp) usage is full.
CSCvb08421	Due to an IGMP enhancement, the display for show ip igmp snooping command is changed.
CSCvb35966	MPLS label imposition statistics are not displayed correctly.

Bug ID	Description
CSCvb45258	When IGMP snooping is enabled, the NVE interface is added by default as a static mrouter port. This causes traffic to be received on all the remote VTEPs.
CSCvb45282	When IGMP report is received from only one NVE peer on an NVE interface, access to network traffic is replicated to all NVE peers even when those peers are not sending any IGMP join requests.
CSCvc95305	If you attempt to copy an image with compact option through SCP with the image name similar to the one already present in the DUT (compacted one), the copying will fail in spite of enabling the deletion of the image using allow delete boot-image command.
CSCve58167	Adding the SVI configuration in shutdown state via the config replace feature fails.
CSCvg96153	Feature needed for handling the double tagged control plane traffic (STP) to traverse via QnQ tunnel.
CSCvh10368	When the vPC local leg goes down, traffic exiting via vPC PL will have a complete drop.

Open Caveats-Cisco NX-OS Release 7.0(3)I7(3)

Table 4 lists the open caveats in the Cisco NX-OS Release 7.0(3)I7(3). Click the Bug ID to search the Cisco Bug Search Tool for additional information about the bug.

- Table 4 Cisco NX-OS Release 7.0(3)I7(3) –Open Bugs

Bug ID	Description
CSCuw97656	When ALPM is enabled on vPC devices, inconsistency is detected between the hardware and software MAC table on both vPC nodes after learning more than 32K MAC addresses. In ALPM mode, the supported MAC table limit is 32K. MAC tables on both vPC devices go out of sync.Old
CSCvf03400	To overcome timing issues, shut the system default switchport.
CSCvg48391	If PFC is received on a non-configured group, create log entry (track interface).
CSCvh19555	Resilient Hashing: flows on other ports are also rehashed if a port of ECMP group is shut.
CSCvh56804	When you set the l2protocol tunnel cos value to 0, the VLAN priority value on the outer VLAN tag, added as part of allow double tag feature is set to 7.
CSCvh74746	In the Cisco Nexus 3500 switches, the queue-limit CLI in the network-quos policy errors out.
CSCvi01072	When a CISCO QSA (active QSA) is inserted without a SFP and a port breakout is tried on it, then an error occurs. Error is: Breakout not supported with QSA Adapter
CSCvi02501	When a CISCO QSA (active QSA) is inserted with a SFP and a port breakout is tried on it, then an error occurs. Error is: Breakout not supported with SFP transceiver.

Known Behaviors-Cisco NX-OS Release 7.0(3)I7(3)

Table 5 lists the known behaviors in Cisco NX-OS Release 7.0(3)I7(3). Click the bug ID to search the Cisco Bug Search Tool for details about the bug.

Table 5 Cisco NX-OS Release 7.0(3)I7(3) –Known Behaviors

Bug ID	Description
CSCvg03567	With switchport mac-learn disable cli, mac's are still learnt on VNI enabled vlan.
CSCvg66442	In Cisco NX-OS Release 7.0(3)I7(3), the auto ECMP feature fails to fill all 256 ecmp entries in "show hardware profile status" and always shows 255 as one short though partial routes are present.
CSCvg68550	The MPLS SR outputs stats incremented for all FECs with same next-hop during POP(swap with 3).
CSCvg95733	When you upgrade to Cisco NX-OS Release 7.0(3)I7(3), the following BGP error message is displayed: "%BGP-2-FATAL: bgp- [27041] Fatal error: syntax error:: Usage: bgp [-d] [-h] -t <tagstring>".
CSCvh07154	PFC are generated for /24 routes in specific scenario on TH-EOR.
CSCvg99951	During ISSU from Cisco NX-OS Release 7.0(3)I6(1) to Cisco NX-OS Release 7.0(3)I7(3), the following error message is seen: [Cannot find device "eth1"]

Large core files are split into 3 or more files. For example:

- 1405964207_0x101_iftmc_log.3679.tar.gzaa
- 1405964207_0x101_iftmc_log.3679.tar.gzab
- 1405964207_0x101_iftmc_log.3679.tar.gzac

To decode the multiple core files, first club the files to a single file:

```
$ cat 1405964207_0x101_iftmc_log.3679.tar.gz* > 1405964207_0x101_iftmc_log.3679.tar.gz
```

Upgrading Cisco Nexus 3000 Series Switch

The upgrade process is triggered when you enter the install all command. This section describes the sequence of events that occur when you upgrade a single Cisco Nexus 3000 Series switch.

Note:

- If you have a release prior to Release 7.0(3)I2(1), upgrade to Cisco Nexus 3000 Release 6.0.2.U6(3a) first and then upgrade to Release 7.0(3)I2(1) or later releases.
- Beginning with the 7.0(3)I2(1) release, kickstart and system images are no longer used to install the Cisco NX-OS software image on Cisco Nexus 3000 and 3100 Series switches. Instead, a single binary image is used (for example, nxos.7.0.3.I4.1.bin). To install the software, you would use the install all nxos bootflash:nxos.7.0.3.I4.1.bin command.

To perform a software upgrade, follow the instructions in the Cisco NX-OS Software Upgrade and Downgrade Guide, Release 7.x.

This section includes the following topics:

Overview – Upgrade Process

This table provides an overview of the upgrade process. To perform a software upgrade, follow the instructions in the Cisco NX-OS Software Upgrade and Downgrade Guide, Release 7.x.

Process	Tasks
Upgrade Preparation	1. Log in to the first Cisco Nexus 3000 Series switch. We recommend that you log in to the console port. In vPC topologies, the first upgrade can be performed on either the primary or secondary switch in the topology. 2. Log in to Cisco.com to access the Software Download Center. To log in to Cisco.com, go to http://www.cisco.com/ and click Log In at the top of the page. Enter your Cisco username and password. 3. Choose and download the software image to the server. 4. Verify that the required space is available in the bootflash: directory for the image file(s) to be copied. 5. If you need more space in the bootflash: directory, delete unnecessary files to make space available. 6. Copy the Cisco NX-OS software image to the bootflash using a transfer protocol such as ftp:, http:, https:, tftp:, scp:, or sftp. 7. Compare the file sizes of the images that were transferred using the dir bootflash command. The file sizes of the images obtained from Cisco.com and the image sizes of the transferred files should be the same.7. 8. Complete the above Step 1 through Step 7 for each Cisco Nexus 3000 Series switch in the topology.

Pre-upgrade Checks	1. Enter the show incompatibility command to verify that the target image is feature-wise compatible with the current image. 2. Enter the show install all impact command to identify the upgrade impact. A BIOS incompatibility issue has been discovered on specific Cisco Nexus 3000 and 3100 Series switches. When you upgrade these switches from Cisco NX-OS Release 6.0(2)U6(8) or an earlier release to Cisco NX-OS Release 7.0(x), an MD5 mismatch error might occur and leave the switch at the loader prompt. We recommend that you view the field notice for this release to see if your software or hardware platforms are affected. You can find the field notice at the following URL: http://www.cisco.com/c/en/us/support/docs/field-notices/642/fn64233.html
Upgrade Process	1. Enter the install all command to update to the latest Cisco NX-OS software. 2. Peruse the installer impact analysis and accept to proceed. 3. Installer on Nexus 3000 upgrades the software – the switch will now run new version of the software.
Upgrade Verification	1. Enter the show install all status command to verify the status of the installation.

Upgrade Matrix

You can perform an In-Service Software Upgrade (ISSU) from the following release to Cisco NX-OS Release 7.0(3)I7(3):

- 7.0(3)I7(2)
- 7.0(3)I7(1)
- 7.0(3)I6(2)
- 7.0(3)I6(1)
- 7.0(3)I5(2)
- 7.0(3)I5(1)

The following upgrade path is supported and recommended:

- For All Cisco Nexus 3000 Series switches (except Cisco Nexus 3048 Switches):

  Cisco NX-OS Release 6.0(2)U5(1) > Cisco NX-OS Release 6.0(2)U6(10) > Cisco NX-OS Release 7.0(3)I7(3)

The following table shows the upgrade paths for Cisco NX-OS Release 7.0(3)I7(3) from Cisco NX-OS Release 6.0(2)U5(1) and later.

From	To	Limitations	Recommended Procedure
7.0(3)I2(1) or later	7.0(3)I7(3)	None	install all is the recommended upgrade method supported.

6.0(2)U6(7) and 6.0(2)U6(8)	7.0(3)I7(3)	First upgrade to Cisco NX-OS Release 6.0(2)U6(10). *A Cisco Nexus 3000 Series switch requires an additional step when you upgrade from Cisco NX-OS Release 6.0(2)U6(7) or Cisco NX-OS Release 6.0(2)U6(8) software version, otherwise the BGP sessions will flap after a fast-reload. You must first upgrade the switch to Cisco NX-OS Release 6.0(2)U6(10) before you upgrade it to Cisco NX-OS Release 7.0(3)I7(3).*	install all is the recommended upgrade method supported.
6.0(2)U6(3a)[1] and later	7.0(3)I7(3)	None	install all is the only upgrade method supported because of a BIOS upgrade requirement. Warning: Make sure that you store the pre-Release, 6.0(2)U6(3)'s configuration file. For more information, see the *Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.x*.

[1] Cisco NX-OS Release 6.0(2)U6(3) is no longer available for a software download through www.cisco.com. This software release has been replaced by Cisco NX-OS Release 6.0(2)U6(3a).

6.0(2)U6(2a)[2] or earlier	7.0(3)I7(3)	First, upgrade to Cisco NX-OS Release 6.0(2)U6(3a) or a later release. *A Cisco Nexus 3048 switch requires an additional step when you upgrade from a software version older than Cisco NX-OS 6.0(2)U6(2), otherwise the switch can fail to boot. You must first upgrade the switch to Cisco NX-OS Release 6.0(2)U6(2a), then to Cisco NX-OS Release 6.0(2)U6(a3), and finally to Cisco NX-OS Release 7.0(3)I7(3).*	install all is the only upgrade method supported because of a BIOS upgrade requirement. For more information, see the *Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.x*.

Guidelines and Limitations

Follow these guidelines and limitations while upgrading to Cisco NX-OS Release 7.0(3)I7(3):

- The only supported method of upgrading is install all from Release 6.0(2)U6(3a) or later due to the need to upgrade the BIOS. Without the Release 7.0(3)I7(3) BIOS, the 7.0(3)I7(3) image will not load.
- The no-save option is now required to downgrade from Release 7.x to Release 6.x. The bios-force is a hidden option that is only available on Cisco Nexus 3000 Series switches that are running 7.x releases.
- Cisco Nexus 3000 Series switches that use software versions older than Cisco NX-OS Release 5.0(3)U5(1) need to be updated to Cisco NX-OS Release 5.0(3)U5(1) before they are upgraded to Cisco NX-OS Release 6.0(2).

[2] Cisco NX-OS Release 6.0(2)U6(2) is no longer available for a software download through www.cisco.com. This software release has been replaced by Cisco NX-OS Release 6.0(2)U6(2a).

- Cisco NX-OS Release 5.0(3)U3(1) does not support a software upgrade from Cisco NX-OS Release 5.0(3)U2(2c). If you want to upgrade through this path, see CSCty75328 for details about how to work around this issue.

  Note: It is recommended that you upgrade to Cisco NX-OS Release 7.0(3)I7(3) by using Cisco NX-OS install procedures.

- In Cisco NX-OS Release 6.0(2)U2(2), the default interface name in LLDP MIB is in short form. To make it long form, you must set lldp portid-subtype to 1. In Cisco NX-OS Release 6.0(2)U2(3), this behavior was reversed. The default interface name in LLDP MIB is now in long form. To make it short form, you must set lldp portid-subtype to 0.

- If you have set lldp port-subtype to 1 and you are upgrading to Cisco NX-OS Release 6.0(2)U2(4), ensure that you set lldp port-subtype to 0.

- While performing a non-disruptive ISSU, VRRP and VRRPV3 will display the following messages:

  - If VRRPV3 is enabled:
    2015 Dec 29 20:41:44 MDP-N9K-6 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: ISSU ERROR: Service "vrrpv3" has sent the following message: Feature vrrpv3 is configured. User can change vrrpv3 timers to 120 seconds or fine tune these timers based on upgrade time on all Vrrp Peers to avoid Vrrp State transitions. – sysmgr

  - If VRRP is enabled:
    2015 Dec 29 20:45:10 MDP-N9K-6 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: ISSU ERROR: Service "vrrp-eng" has sent the following message: Feature vrrp is configured. User can change vrrp timers to 120 seconds or fine tune these timers based on upgrade time on all Vrrp Peers to avoid Vrrp State transitions. – sysmgr

- Packet loss may occur on Cisco Nexus 31108PC-V, 31108TC-V and 3132Q-V switches when they are in the default cut-through switching-mode and the default oversubscribed port mode. These packet losses are seen in hardware counters on the egress port as TERR and/or TFCS. One of the following workarounds can be implemented to address this issue without NX-OS upgrade. To view more details, see CSCvf87120.

- Change the port mode from oversubscribed to line-rate and then reload the switch:

  - On Nexus 31108PC-V and 31108TC-V switches, change from 48x10g+6x100g to 48x10g+4x100g+2x40g.

  - On Nexus 3132Q-V switches change from 32x40g or 26x40g to 24x40g.

- Change the switching-mode from cut-through to store-and-forward and then reload the switch.

- An error occurs when you try to perform an ISSU if you changed the reserved VLAN without entering the copy running-config save-config and reload commands.

- Subinterfaces cannot be used as network ports.

- Cisco Nexus 3000-XL platforms do not support breakout using speed 10000 CLI command. Use the interface breakout module 1 port <num> map 10g-4x CLI command instead.

- While installing the NXAPI https certificate that is present in the device, the following error message can appear if the user does not have the permission to install this certificate (See CSCup72219): Certificate file read error.Please re-check permissions.

- After configuring the NXAPI feature, the default http port (port 80) is still in the listening state even after we run the no nxapi http command. This results in the sandbox becoming accessible. Although the sandbox becomes accessible, HTTP requests from the sandbox to the device do not go through. Thus, the functionality is not affected. (See CSCup77051).

- Chunking is enabled while displaying XML output for any CLI, and html tags (& lt; and & gt;) are displayed instead of < and > both on the sandbox and while running the Python script (See CSCup84801).

  This is expected behavior. Each chunk should be in XML format for you to parse it and extract everything inside the <body> tag. This is done so that it can be later concatenated with similar output from all the chunks of the CLI XML output. After all the chunks are concatenated to get the complete XML output for the CLI, this complete XML output can be parsed for any parameter.

  The following workaround is recommended to address this issue:
  - Concatenate the <body> outputs from each chunk
  - Replace all the html tags (& lt; and & gt;) with < and >
  - Parse for any XML tag needed
- If you use the write erase command, you cannot view the output for the show startup *feature* command. To view the startup configuration, you must then use the show startup-config command. This limitation will remain until you run the copy running-config startup-config command. After that, the show startup-config feature command will display the feature-only configuration output as expected (See CSCuq15638).

- A Python traceback is seen while running the show xml command by using the Python shell. The exception type is httplib.IncompleteRead. This happens when you use Python scripts to leverage the NXAPI for retrieving switch data through XML or JSON. You should handle the exceptions in your Python scripts (See CSCuq19257).

- While upgrading to a new release, when you create a checkpoint without running the setup script, the checkpoint file does not contain the copp-s-mpls class. After you run the write erase command and reload the switch, the copp-s-mpls class is created when the default configuration is applied. When a rollback is done to this checkpoint file, it detects a change in the CoPP policy and tries to delete all class-maps. Because you cannot delete static class-maps, this operation fails and, in turn, the rollback also fails.

  This can also happen if you create a checkpoint, then create a new user-defined class and insert the new class before any other existing class (See CSCup56505).

  The following workarounds are recommended to address this issue:
  - Run setup after upgrading to a new release.
  - Always insert the new classes at the end before a rollback.

- When both the ip icmp-errors source and ip source *intf* icmp error commands are configured, then the command that is configured last takes effect.

  Thereafter, if the last configured command is removed, the switch does not get configured with the command that was configured first.

- Users who upgrade to 7.0(3)I7(3) need to run the set up script if they want to enable the MPLS static or the VRRpv3 feature.

- The following Cisco Nexus 9000 features are not supported on the Cisco Nexus 3100 Series switches in N3K or N9K mode:

- FEX
- Multicast PIM Bidir
- Port VLAN (PV) switching and routing support for VXLAN
- Auto-Config
- Secure login enhancements:
    - Ability to block login attempts and enforce a quiet period
    - Ability to restrict the maximum login sessions per user
    - Ability to restrict the password length
    - Ability to prompt the user to enter a password after entering the username
    - Ability to hide the shared secret used for RADIUS or TACACS+ authentication or accounting
    - SHA256 hashing support for encrypted passwords
- SHA256 algorithm to verify operating system integrity
- Non-hierarchical routing mode
- NX-API REST

- Link Level Flow Control (LLFC) is not supported on Cisco Nexus 3000 series and Cisco Nexus 3100 series switches.
- You can disable IGMP snooping either globally or for a specific VLAN.
- You cannot disable IGMP snooping on a PIM enabled SVIs. The warning message displayed is: IGMP snooping cannot be disabled on a PIM enabled SVIs. There are one or more VLANs with PIM enabled.

MIB Support

The Cisco Management Information Base (MIB) list includes Cisco proprietary MIBs and many other Internet Engineering Task Force (IETF) standard MIBs. These standard MIBs are defined in Requests for Comments (RFCs). To find specific MIB information, you must examine the Cisco proprietary MIB structure and related IETF-standard MIBs supported by the Cisco Nexus 3000 Series switch. The MIB Support List is available at the following FTP sites:

ftp://ftp.cisco.com/pub/mibs/supportlists/nexus3000/Nexus3000MIBSupportList.html

Related Documentation

The entire Cisco Nexus 3000 Series NX-OS documentation set is available at the following URL:

https://www.cisco.com/c/en/us/support/switches/nexus-3000-series-switches/tsd-products-support-series-home.html

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus3k-docfeedback@cisco.com. We appreciate your feedback.

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.