Cisco Nexus 6000 Series Release Notes, Release 7.x

Release Date: January 29, 2014
Date Last Modified: February 3, 2014
Part Number: OL-30899-01 A1
Current Release: NX-OS Release 7.0(0)N1(1)

This document describes the features, caveats, and limitations for the Cisco Nexus 6000 Series devices and the Cisco Nexus 2000 Series Fabric Extenders. Use this document in combination with documents listed in the "Obtaining Documentation and Submitting a Service Request" section on page 20.

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 6000 and Cisco Nexus 2000 Series release notes:
http://www.cisco.com/en/US/docs/switches/datacenter/nexus6000/sw/release/notes/Nexus_6000_Release_Notes.html

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

Table 1 Online History Change

Part Number	Revision	Date	Description
OL-30899-01	A0	January 29, 2014	Created NX-OS Release 7.0(0)N1(1) release notes.
	A1	February 3, 2014	Removed Fibre Channel and Fibre Channel Over Ethernet Slow Drain from New Features list.

Contents

This document includes the following sections:

- Introduction, page 2

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

- System Requirements, page 3
- New and Changed Features, page 8
- Online Insertion and Removal Support, page 8
- Upgrading or Downgrading to a New Release, page 13
- Limitations, page 14
- Caveats, page 17
- MIB Support, page 19
- Obtaining Documentation and Submitting a Service Request, page 20

Introduction

The Cisco NX-OS software is a data center-class operating system built with modularity, resiliency, and serviceability at its foundation. Based on the industry-proven Cisco NX-OS software, Cisco NX-OS helps ensure continuous availability and sets the standard for mission-critical data center environments. The highly modular design of Cisco NX-OS makes zero-effect operations a reality and enables exceptional operational flexibility.

Several new hardware and software features are introduced for the Cisco Nexus 6000 Series device and the Cisco Nexus 2000 Series Fabric Extender (FEX) to improve the performance, scalability, and management of the product line.

Cisco Nexus 6000 Series Devices

The Cisco Nexus 6000 Series includes 10- and 40-Gigabit Ethernet density in energy-efficient compact form factor switches. The Cisco Nexus 6000 Series Layer 2 and Layer 3 set allow for multiple scenarios such as direct-attach 10- and 40-Gigabit Ethernet access and high-density Cisco Fabric Extender (FEX) aggregation deployments, leaf and spine architectures, or compact aggregation to build scalable Cisco Unified Fabric in the data centers.

Cisco Nexus 6000 Series products use the same set of Cisco application-specific integrated circuits (ASICs) and a single software image across the products within the family, which offers feature consistency and operational simplicity. Cisco Nexus 6000 Series switches support robust Layer 2 and Layer 3 functions, industry-leading FEX architecture with Cisco Nexus 2000 and Cisco Nexus B22 Blade FEX, in-service software upgrades (ISSUs), and Cisco FabricPath. Operational efficiency and programmability are enhanced on the Cisco Nexus 6000 Series through advanced analytics, PowerOn Auto Provisioning (POAP), and Python/Tool Command Language (Tcl) scripting.

For information about the Cisco Nexus 6000 Series, see the *Cisco Nexus 6000 Series Platform Hardware Installation Guide*.

Cisco Nexus 2000 Series Fabric Extenders

The Cisco Nexus 2000 Series Fabric Extender (FEX) is a highly scalable and flexible server networking solution that works with the Cisco Nexus 6000 Series devices to provide high-density and low-cost connectivity for server aggregation. Scaling across 1-Gigabit Ethernet, 10-Gigabit Ethernet, and 40-Gigabit Ethernet, unified fabric, rack, and blade server environments, the FEX is designed to simplify data center architecture and operations.

The FEX integrates with its parent Cisco Nexus device, which allows zero-touch provisioning and automatic configuration. The FEX provides a single point of management that supports a large numbers of servers and hosts that can be configured with the same feature set as the parent Cisco Nexus 6000 Series switch, including security and quality of service (QoS) configuration parameters. Spanning Tree Protocol (STP) is not required between the Fabric Extender and its parent switch, because the Fabric Extender and its parent switch allow you to enable a large multi-path, loop-free, active-active topology.

Software is not included with the Fabric Extender. Cisco NX-OS software is automatically downloaded and upgraded from its parent switch. For information about configuring the Cisco Nexus 2000 FEX, see the "Configuring the Fabric Extender" chapter in the *Cisco Nexus 6000 Series Layer 2 Switching Configuration Guide*.

System Requirements

This section includes the following topics:

- Hardware Supported, page 3
- Online Insertion and Removal Support, page 8

Hardware Supported

The Cisco NX-OS software supports the Cisco Nexus 6000 Series switch. You can find detailed information about supported hardware in the *Cisco Nexus 6000 Series Hardware Installation Guide*.

Table 2 shows the hardware supported by Cisco NX-OS Release 7.x software.

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software

Cisco NX-OS Release Support		
Hardware	**Part Number**	**7.0(0)N1(1)**
Cisco Nexus 6000 Series		
Cisco Nexus 6004-EF switch	N6K-C6004	X
Cisco Nexus 6001P switch	N6K-C6001-64P	X
Cisco Nexus 6001T switch	N6K-C6001-64T	X
Cisco Nexus 6004 switch	N6K-C6004-96Q	X
Cisco Nexus 2000 Series		
Cisco Nexus B22 DELL FEX	N2K-B22DELL-P	X
Cisco Nexus 2232TM-E FEX	N2K-C2232TM-E-10GE	X
Cisco Nexus B22F FEX	N2K-B22FTS-P	X

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support		
Hardware	**Part Number**	**7.0(0)N1(1)**
Cisco Nexus B22HP FEX	N2K-B22HP-P	X
Cisco Nexus B22IBM FEX [1] [2]	N2K-B22IBM-P	—
Cisco Nexus 2232TM FEX	N2K-C2232TM-10GE	X
Cisco Nexus 2232PP FEX	N2K-C2232PP-10GE	X
Cisco Nexus 2248TP-E FEX	N2K-C2248TP-E-1GE	X
Cisco Nexus 2248TP FEX	N2K-C2248TP-1GE	X
Cisco Nexus 2248PQ FEX[3]	N2K-C2248PQ-10GE	X
Cisco Nexus 2224TP FEX	N2K-C2224TP-1GE	X
Cisco Nexus 2148T FEX	N2K-C2148T-1GE	—
Expansion Modules		
12Q 40-Gigabit Ethernet FCoE ports	N6K-C6004-M12Q	X
Transceivers		
QSFP Transceivers		
Cisco QSFP40G BiDi Short-reach Transceiver	QSFP-40G-SR-BD	X
Cisco QSFP 40GBASE-LR4 Transceiver Module, LC, 10KM	QSFP-40GE-LR4	X
40GBASE-SR4 QSFP Transceiver	QSFP-40G-SR4	X
QSFP 4x10GBASE-SR Transceiver	QSFP-40G-CSR4	X
QSFP 40GBASE-LR4 Transceiver, LC, 10KM	QSFP-40G-LR4	X
Cisco 40GBase-AOC QSFP direct-attach Active Optical Cable, 1-meter	QSFP-H40G-AOC1M	X

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support		
Hardware	**Part Number**	**7.0(0)N1(1)**
Cisco 40GBase-AOC QSFP direct-attach Active Optical Cable, 2-meter	QSFP-H40G-AOC2M	X
Cisco 40GBase-AOC QSFP direct-attach Active Optical Cable, 3-meter	QSFP-H40G-AOC3M	X
Cisco 40GBase-AOC QSFP direct-attach Active Optical Cable, 5-meter	QSFP-H40G-AOC5M	X
Cisco 40GBase-AOC QSFP direct-attach Active Optical Cable, 7-meter	QSFP-H40G-AOC7M	X
Cisco 40GBase-AOC QSFP direct-attach Active Optical Cable, 10-meter	QSFP-H40G-AOC10M	X
SFP+ Optical		
QSFP to 4xSFP 10G Passive Copper Splitter Cable, 1M	QSFP-4SFP10G-CU1M	X
QSFP to 4xSFP 10G Passive Copper Splitter Cable, 3M	QSFP-4SFP10G-CU3M	X
QSFP to 4xSFP 10G Passive Copper Splitter Cable, 5M	QSFP-4SFP10G-CU5M	X
QSFP to 4xSFP10G Active Copper Splitter Cable, 7M	QSFP-4SFP10G-ACu7M	X
QSFP to 4xSFP10G Active Copper Splitter Cable, 10M	QSFP-4X10G-AC10M	X
QSFP to 4xSFP10G Active Copper Splitter Cable, 7M	QSFP-4X10G-AC7M	X
Cisco 40GBASE-CR4 QSFP+ to 4 10GBASE-CU SFP+ direct-attach breakout 10-meter cable, active	QSFP-4X10G-AC10M	X

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support		
Hardware	**Part Number**	**7.0(0)N1(1)**
10-Gigabit Ethernet SFP (for Cisco Nexus 2000 Series to Cisco Nexus 6000 Series connectivity)	FET-10G(=)	X
40-Gigabit Ethernet QSFP+ (for Cisco Nexus 2000 Series to Cisco Nexus 6000 Series connectivity)	FET-40G	X
Gigabit Ethernet SFP, LH transceiver	GLC-LH-SMD	X
Gigabit Ethernet SFP, EX transceiver	GLC-EX-SMD	6.0(2)N1(2) and later
Cisco GE SFP, LC connector SX transceiver	GLC-SX-MM	X
40-Gigabit CU QSFP module	QSFP-H40G-CU1M	X
40-Gigabit CU QSFP module	QSFP-H40G-CU3M	X
40-Gigabit CU QSFP module	QSFP-H40G-CU5M	X
40-Gigabit CU QSFP module	QSFP-H40G-ACu7M	X
40-Gigabit CU QSFP module	QSFP-H40G-ACu10M	X
Cisco 10GBASE-AOC SFP+ Cable 1 Meter	SFP-10G-AOC1M	X
Cisco 10GBASE-AOC SFP+ Cable 2 Meter	SFP-10G-AOC2M	X
Cisco 10GBASE-AOC SFP+ Cable 3 Meter	SFP-10G-AOC3M	X
Cisco 10GBASE-AOC SFP+ Cable 5 Meter	SFP-10G-AOC5M	X
Cisco 10GBASE-AOC SFP+ Cable 7 Meter	SFP-10G-AOC7M	X
Cisco 10GBASE-AOC SFP+ Cable 10 Meter	SFP-10G-AOC10M	X

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support		
Hardware	**Part Number**	**7.0(0)N1(1)**
Cisco 40GBase-AOC QSFP to 4 SFP+ Active Optical breakout Cable, 1-meter	QSFP-4X10G-AOC1M	X
Cisco 40GBase-AOC QSFP to 4 SFP+ Active Optical breakout Cable, 2-meter	QSFP-4X10G-AOC2M	X
Cisco 40GBase-AOC QSFP to 4 SFP+ Active Optical breakout Cable, 3-meter	QSFP-4X10G-AOC3M	X
Cisco 40GBase-AOC QSFP to 4 SFP+ Active Optical breakout Cable, 5-meter	QSFP-4X10G-AOC5M	X
Cisco 40GBase-AOC QSFP to 4 SFP+ Active Optical breakout Cable, 7-meter	QSFP-4X10G-AOC7M	X
Cisco 40GBase-AOC QSFP to 4 SFP+ Active Optical breakout Cable, 10-meter	QSFP-4X10G-AOC10M	X
SFP+ Copper		
Cisco 1000 BASE-T SFP transceiver module for Category 5 copper wire, extended operating temperature range, RJ-45 connector	SFP-GE-T(=)	
Cisco 10GBASE-CU SFP+ cable 1 meter, passive	SFP-H10GB-CU1M	X
10GBASE CU SFP+ cable, 1.5 meter, passive	SFP-H10GB-CU1.5M	X
10GBASE CU SFP+ cable, 2 meters, passive	SFP-H10GB-CU2M	X
10GBASE CU SFP+ cable, 2.5 meters, passive	SFP-H10GB-CU2.5M	X

Table 2 Hardware Supported by Cisco NX-OS Release 7.x Software (continued)

Cisco NX-OS Release Support		
Hardware	**Part Number**	**7.0(0)N1(1)**
Cisco 10GBASE-CU SFP+ cable, 3 meters, passive	SFP-H10GB-CU3M	X
Cisco 10GBASE-CU SFP+ Cable, 5 meters, passive	SFP-H10GB-CU5M	X

1. The Cisco Nexus B22IBM FEX is supported with Cisco NX-OS Release 6.0(2)N2(1b)
2. The Cisco Nexus B22IBM FEX is not supported with Cisco NX-OS Release 6.0(2)N2(2)
3. The Cisco Nexus 2248PQ FEX does not support Gen1 cables.

Online Insertion and Removal Support

Table 3 shows the hardware and Cisco NX-OS Release 7.x software that supports online insertion and removal (OIR)

Table 3 Online Insertion and Removable Support by Cisco NX-OS Release 7.x Software

		Cisco NX-OS Release Support
Hardware	**Part Number**	**7.0(0)N1(1)**
Cisco Nexus 6000 Series		
Cisco Nexus 6004 switch	N6K-C6004	—
Cisco Nexus 6001P switch	N6K-C6001-64P	—
Cisco Nexus 6001T switch	N6K-C6001-64T	—
Cisco Nexus 6004 switch	N6K-C6004-96Q	X
Expansion Modules		
Nexus 6004 module 12Q 40-Gigabit Ethernet/FCoE, spare	N6K-6004-M12Q	X

New and Changed Features

This section describes the new features introduced in Cisco NX-OS Release 7.x.

- New Software Features in Cisco NX-OS Release 7.0(0)N1(1), page 9

- New Hardware Features in Cisco NX-OS Release 7.0(0)N1(1), page 13

New Software Features in Cisco NX-OS Release 7.0(0)N1(1)

Cisco NX-OS Release 7.0(0)N1(1) is a major release that includes bug fixes and the following software features and enhancements:

- FabricPath Anycast HSRP, page 9
- Data Analytics, page 9
- Dynamic Fabric Automation, page 10
- Early Warning for FIB Exhaustion, page 10
- ECN with WRED, page 10
- ERSPAN with ACL Filtering, page 10
- FabricPath Operations, Administration, and Management, page 11
- Intermediate System to Intermediate System Protocol, page 11
- Layer 2 Bidirectional Forwarding Detection, page 11
- Multi-Destination Switch Port Analyzer, page 11
- Multi-Destination Tree, page 11
- OpenFlow v1.0, page 11
- Overload Bit, page 12
- Port Channel Max Links, page 12
- Q-in-Q VLAN Tunneling, page 12
- Sampled NetFlow, page 12
- Switch Port Analyzer with ACL Filtering, page 12
- Static/Dynamic Network Address Translation, page 12
- TCAM Carving, page 12
- VN-Segment, page 13

FabricPath Anycast HSRP

Anycast HSRP is a FabricPath-based feature in which the traditional HSRP can be extended to an n-Gateway solution with all the gateways actively forwarding traffic. This feature supports active load balancing of traffic among all the gateways configured apart for redundancy. A maximum of 4 Gateways is supported.

Data Analytics

This feature provides the capability of advanced analytics for network visibility and management. Critical analytics for network monitoring is supported including Latency Based SPAN, SPAN on Drop, Micro-Burst Monitor and Switch Latency.

Latency-based SPAN can be used to monitor any packet from an interface when the latency on that interface exceeds the configured threshold.

SPAN on Drop can be used to configure SPAN on particular packets which would otherwise get dropped due to congestion, and is used for known unicast packets.

Micro-Burst Monitoring is supported per port both in ingress and egress direction and can be selectively enabled or disabled in either direction.

Switch Latency provides instantaneous latency and histogram data between a pair of ports and provides minimum, average, and maximum latency between the slected pairs of ports.

Dynamic Fabric Automation

This software release is the first release to support Cisco's Evolutionary Data Center Fabric solution called Dynamic Fabric Automation (DFA). DFA is evolutionary and is based on the industry leading Unified Fabric solution.

DFA focuses on simplifying, optimizing and automating data center fabric environments by offering an architecture based on four major pillars namely Fabric Management, Workload Automation, Optimized Networking and Virtual Fabrics. Each of these pillars provide a set of modular functions which can be used together or independently for easiness of adoption of new technologies in the data center environment.

Complete details on the DFA architecture can be found at: http://www.cisco.com/go/dfa.

Early Warning for FIB Exhaustion

When the Forwarding Information Base (FIB) table is 90% full, the following messages is displayed:

FIB_TCAM_RESOURCE_EXHAUSTION:FIB TCAM exhausted

ECN with WRED

Currently, the congestion control and avoidance algorithms for Transmission Control Protocol (TCP) are based on the idea that packet loss is an appropriate indication of congestion on networks transmitting data using the best-effort service model. When a network uses the best-effort service model, the network delivers data if it can, without any assurance of reliability, delay bounds, or throughput. However, these algorithms and the best-effort service model are not suited to applications that are sensitive to delay or packet loss (for instance, interactive traffic including Telnet, web-browsing, and transfer of audio and video data). Weighted Random Early Detection (WRED), and by extension, Explicit Congestion Notification (ECN), solves this problem.

ERSPAN with ACL Filtering

With ERSPAN traffic the destination is remote and the overall impact of bandwidth congestion can be significant. The ERSPAN with ACL filtering feature allows you to filter ERSPAN traffic so that you can reduce bandwidth congestion. To configure ERSPAN with ACL filtering, you use ACL's for the session to filter out traffic that you do not to span. An ACL is a list of permissions associated to any entity in the system; in the context of a monitoring session, an ACL is a list of rules which results in the spanning of traffic that matches the ACL criteria, saving bandwidth for more meaningful data. The filter would apply on all sources in the session (VLAN or interface).

FabricPath Operations, Administration, and Management

Support for Fabric Path Operations, Administration and Management has been added in this software release.

Intermediate System to Intermediate System Protocol

Intermediate System to Intermediate System (IS-IS) is an Interior Gateway Protocol (IGP) based on Standardization (ISO)/International Engineering Consortium (IEC) 10589. Cisco Nexus 6000 Series switches supports Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). IS-IS is a dynamic link-state routing protocol that can detect changes in the network topology and calculate loop-free routes to other nodes in the network. Each router maintains a link-state database that describes the state of the network and sends packets on every configured link to discover neighbors. IS-IS floods the link-state information across the network to each neighbor. The router also sends advertisements and updates on the link-state database through all the existing neighbors.

Layer 2 Bidirectional Forwarding Detection

The Bidirectional Forwarding Detection (BFD) provides fast forwarding-path failure detection times for media types, encapsulations, topologies, and routing protocols. You can use BFD to detect forwarding path failures at a uniform rate, rather than at variable rates for different protocol hello mechanisms. BFD makes network profiling and planning easier and reconvergence time consistent and predictable.

Multi-Destination Switch Port Analyzer

Local Switch Port Analyzer (SPAN) and SPAN-on-Drop sessions can support multiple destination ports. This allows traffic in a single local SPAN session or a SPAN-on-Drop session also to be monitored and sent to multiple destinations.

Multi-Destination Tree

A Multi-Destination Tree (MDT), also referred to as a forwarding tag or ftag, is a spanning-tree used for forwarding packets within a topology. By default, a topology has two MDTs/ ftags: topology 0 has ftag 1 and 2, topology 1 has ftag 3 and 4, topology 2 has ftag 5 and 6, up to a maximum supported 64 topologies.

OpenFlow v1.0

The OpenFlow feature is a specification from the Open Networking Foundation (ONF) that defines a flow-based forwarding infrastructure (L2-L4 Ethernet switch model) and a standardized application programmatic interface (protocol definition) to learn capabilities, add and remove flow control entries and request statistics. OpenFlow allows a controller to direct the forwarding functions of a switch through a secure channel.

One Platform Kit (OnePK)

Support has been added for One Platform Kit (onePK) Turbo API. OnePK is a cross-platform API and software development kit that enables you to develop applications that interact directly with Cisco networking devices. onePK provides you access to networking services by using a set of controlled APIs that share the same programming model and style. For more information, see the following URL:

http://www.cisco.com/en/US/partner/prod/iosswrel/onepk.html

Overload Bit

Intermediate System to Intermediate System (IS-IS) uses the overload bit to tell other routers not to use the local router to forward traffic but to continue routing traffic destined for that local router.

Port Channel Max Links

The Port Channel Max Links feature defines the maximum number of bundled ports allowed in an LACP port channel.

Q-in-Q VLAN Tunneling

A Q-in-Q VLAN tunnel enables a service provider to segregate the traffic of different customers in their infrastructure, while still giving the customer a full range of VLANs for their internal use by adding a second 802.1Q tag to an already tagged frame.

Sampled NetFlow

The Sampled NetFlow feature samples incoming packets on an interface. The packets sampled then qualify to create flows. Sampled NetFlow reduces the amount of export data sent to the collector by limiting the number of packets that create flows and the number of flows. It is essential when flows are created on a line card or external device, instead of on the forwarding engine.

Switch Port Analyzer with ACL Filtering

The Switch Port Analyzer (SPAN) with Access Control List (ACL) filtering feature allows you to filter SPAN traffic so that you can reduce bandwidth congestion. To configure SPAN with ACL filtering, you use ACL's for the session to filter out traffic that you do not want to span. An ACL is a list of permissions associated to any entity in the system; in the context of a monitoring session, an ACL is a list of rules which results in spanning only the traffic that matches the ACL criteria, saving bandwidth for more meaningful data. The filter can apply to all sources in the session.

Static/Dynamic Network Address Translation

Network Address Translation (NAT) enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a device, usually connecting two networks, and translates private (not globally unique) IP addresses in the internal network into legal IP addresses before packets are forwarded to another network. You can configure NAT to advertise only one IP address for the entire network to the outside world. This ability provides additional security, effectively hiding the entire internal network behind one IP address.

TCAM Carving

You can create and administer up to 16 templates to resize the regions in ternary content-addressable memory (TCAM).

VN-Segment

The VN-Segment feature defines a new way to "tag" packets on the wire replacing the traditional 802.1Q VLAN tag. This feature uses a 24-bit tag also referred to as a Virtual Network Identifier (VNI). CE links (access and trunk) carry traditional VLAN tagged/untagged frames. These are the VN-Segment Edge ports.

Web Cache Control Protocol v2

WCCPv2 specifies interactions between one or more Cisco NX-OS routers and one or more cache engines. WCCPv2 transparently redirects selected types of traffic through a group of routers. The selected traffic is redirected to a group of cache engines to optimize resource usage and lower response times.

New Hardware Features in Cisco NX-OS Release 7.0(0)N1(1)

Cisco NX-OS Release 7.0(0)N1(1) supports the following new optics:

- QSFP-H40G-AOCxM (1/2/3/5/7/10m)
- QSFP-40G-SR-BD
- SFP-10G-AOCxM (1/2/3/5/7/10m)
- QSFP-40G-LR4
- PSF1PXA3.5MBU
- PSF1PXA4MBU
- QSFP-4X10G-AOC xM (1/2/3/5/7/10m)

Upgrading or Downgrading to a New Release

This section describes the upgrade and downgrade paths that are supported for Cisco NX-OS Release 7.0(0)N1(1) on the Cisco Nexus device.

This section includes the following topics:

- Upgrade and Downgrade Guidelines, page 13
- Supported Upgrade and Downgrade Paths, page 13

Upgrade and Downgrade Guidelines

The following guidelines apply to Cisco NX-OS Release 7.0(0)N1(1) for the Cisco Nexus devices:

Supported Upgrade and Downgrade Paths

Table 4 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 7.0(0)N1(1). For more information, see the *Cisco Nexus 6000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.0*.

Table 4 Cisco NX-OS Release 7.0(0)N1(1) Supported Upgrade and Downgrade Paths

Current Cisco NX-OS Release	Upgrade to NX-OS Release 7.0(0)N1(1)	Downgrade from NX-OS Release 7.0(0)N1(1)
6.0(2)N2(2) 6.0(2)N2(1) 6.0(2)N1(2) 6.0(2)N1(1a) 6.0(2)N1(1)	Nondisruptive upgrade [1]	Disruptive downgrade

1. Disruptive upgrade when operating in 10G fabric mode.

Limitations

This section describes the limitations for Cisco NX-OS Release 7.0(0)N1(1).

- The Server Virtualization Switch (SVS) connection is not deleted during a rollback when NIV is enabled. To resolve this issue, delete the current SVS connection and reapply the original SVS connection. For details, see CSCts17033.
- If you configure a Cisco Nexus 2248TP port to 100 Mbps instead of autonegotiation, then autonegotiation does not occur, which is the expected behavior. Both sides of the link should be configured to both hardwired speed or both autonegotiate.

  no speed—Autonegotiates and advertises all speeds (only full duplex).

  speed 1000—Autonegotiates only for an 802.3x pause.

  speed 100—Does not autonegotiate; pause cannot be advertised. The peer must be set to not autonegotiate and fix at 100 Mbps (similar to the N2248TP). For details, see CSCte81998.
- When a private VLAN port is configured as a TX (egress) SPAN source, the traffic seen at the SPAN destination port is marked with the VLAN of the ingressed frame. There is no workaround.
- In large-scale configurations, some Cisco Nexus 2000 Series Fabric Extenders might take up to 3 minutes to appear online after entering the **reload** command. A configuration can be termed large scale when the maximum permissible Cisco Nexus 2000 Series Fabric Extenders are connected to a Cisco Nexus 6000 Series switch, all host-facing ports are connected, and each host-facing interface has a large configuration that supports the maximum permissible ACEs per interface.
- The Cisco Nexus 2148 Fabric Extender does not support frames with the dot1q vlan 0 tag.
- VACLs of more than one type on a single VLAN are unsupported. Cisco NX-OS software supports only a single type of VACL (either MAC, IPv4, or IPv6) applied on a VLAN. When a VACL is applied to a VLAN, it replaces the existing VACL if the new VACL is a different type. For instance, if a MAC VACL is configured on a VLAN and then an IPv6 VACL is configured on the same VLAN, the IPv6 VACL is applied, and the MAC VACL is removed.
- A MAC ACL is applied only on non-IP packets. Even if there is a **match eth type = ipv4** statement in the MAC ACL, it does not match an IP packet. To avoid this situation, use IP ACLs to apply access control to the IP traffic instead of using a MAC ACL that matches the EtherType to IPv4 or IPv6.
- Multiple **boot kickstart** statements in the configuration are not supported.
- If you configure Multiple Spanning Tree (MST) on a Cisco Nexus 6000 Series switch, avoid partitioning the network into a large number of regions.
- By design, vEth interfaces do not share the underlying behavior of a vPC port. As a result, a VLAN is not suspended when the peer switch suspends it. For example, when you shut a VLAN on a primary switch, the VLAN continues to be up on the secondary switch when the vEth interface is

on a FEX. When the VLAN on the primary switch goes down, the VLAN on the vEth interface on the primary is suspended, but the vEth on the secondary switch remains up because it is an active VLAN on the secondary switch.

- The packet length in the IP GRE header of a packet exiting from the switch is not equal to the MTU value configured in the ERSPAN source session. This is true for SPAN or ERSPAN. The Cisco Nexus 6000 Series switch terminates in multiples of 16 bytes. If MTU is configured as 100 bytes, then the actual truncated packet is 96 bytes.
- Unknown unicast packets in FabricPath ports are counted as multicast packets in interface counters. This issue occurs when unknown Unicast packets are sent and received with a reserved multicast address (that floods to a VLAN) in the outer FabricPath header, and the Cisco Nexus 6000 Series switch increments the interface counter based on the outer FabricPath header. As a result, Multicast counters are incremented. There is no workaround for this issue.
- In an emulated switch setup, an inband keepalive does not work. The following steps are recommended for peer keepalive over SVI when a switch is in FabricPath mode:
  - Use a dedicated front panel port as a vPC+ keepalive. The port should be in CE mode.
  - Use a dedicated VLAN to carry the keepalive interface. The VLAN should be a CE VLAN.
  - Add the **management** keyword to the corresponding SVI so that the failure of a Layer 3 module will not bring down the SVI interface.
  - Enter the **dual-active exclude interface-vlan** *keepalive-vlan* command to prevent the SVI from going down on the secondary when a peer-link goes down.
- The limit of the table that holds the Router MAC and Virtual MAC entries for determining packet routing or switching is 500 entries. The Virtual MAC entries, the MAC used for HSRP/VRRP that is also programmed in this table, can be shared across multiple Layer 3 interfaces. If SVIs 1–100 all have the same group number configured, just one entry needs to be programmed in this table. We recommend that you configure the same group ID across all or multiple Layer 3 interfaces/SVIs. If multiple group IDs are configured on an Layer 3 interface, we recommend that you configure the same set of group IDs across all or multiple Layer 3 interfaces. This configuration supports HSRP/VRRP on more interfaces.
- The maximum IP MTU that can be set on Layer 3 interfaces running Layer 3 protocols is 9192 because of the internal header used inside the switch. The related network-qos policy must be set to 9216.

Limitations on the Cisco Nexus 6000

The limitations on the Cisco Nexus 6000 Series switch are as follows:

- SPAN Limitations on Fabric Extender Ports, page 15
- Layer 3 Limitations, page 16

SPAN Limitations on Fabric Extender Ports

The SPAN limitations on Fabric Extender ports are as follows:

- On a Cisco Nexus device, if the SPAN source is a FEX port, the frames will always be tagged when leaving the SPAN destination.
- On a Cisco Nexus 6000 Series switch, if the SPAN source is an access port on a switch port or FEX port, the spanned frames at the SPAN destination will be tagged.

- On a Cisco Nexus 6000 Series switch, if the SPAN source is on an access port on the switch port, the frames will not be tagged when leaving the SPAN destination.
- Ports on a FEX can be configured as a tx-source in one session only.

  If two ports on the same FEX are enabled to be tx-source, the ports need to be in the same session. If you configure a FEX port as a tx-source and another port belonging to the same FEX is already configured as a tx-source on a different SPAN session, an error is displayed on the CLI.

  In the following example, Interface Ethernet100/1/1 on a FEX 100 is already configured as a tx-source on SPAN session-1:

```
swor28(config-monitor)# show running-config monitor
      version 7.0(0)N1(1)
      monitor session 1
          source interface Ethernet100/1/1 tx
          destination interface Ethernet1/37
          no shut
```

  If you add an interface Ethernet100/1/2 as a tx-source to a different SPAN session (session-2) the following error appears:

```
swor28(config)# monitor session 2
swor28(config-monitor)# source interface ethernet 100/1/2 tx
ERROR: Eth100/1/2: Ports on a fex can be tx source in one session only
swor28(config-monitor)#
```

- When a FEX port is configured as a tx-source, the multicast traffic is spanned on all VLANs that the tx-source port is a member of. The FEX port sends out only multicast packets that are not filtered by IGMP snooping. For example, if FEX ports 100/1/1–12 are configured on VLAN 11 and the switch port 1/5 sends multicast traffic on VLAN 11 in a multicast group, and hosts connected to FEX ports 100/1/3–12 are interested in receiving that multicast traffic (through IGMP), then that multicast traffic goes out on FEX ports 100/1/3–12, but not on 100/1/1–2.

  If you configure SPAN Tx on port 100/1/1, although the multicast traffic does not egress out of port 100/1/1, the SPAN destination does receive that multicast traffic, which is due to a design limitation.
- When a FEX port is configured as both SPAN rx-source and tx-source, broadcast non-IGMP Layer-2 multicast frames as well as unknown unicast frames originating from that port might be seen twice on the SPAN destination: once on the ingress and once on the egress path. On the egress path, the frames are filtered by the FEX to prevent them from going out on the same port on which they were received. For example, if FEX port 100/1/1 is configured on VLAN 11 and is also configured as SPAN rx-source and tx-source and a broadcast frame is received on that port, the SPAN destination recognizes two copies of the frame, even though the frame is not sent back on port 100/1/1.
- A FEX port cannot be configured as a SPAN destination. Only a switch port can be configured and used as a SPAN destination.
- With a SPAN on Latency session, FEX ports cannot be configured as source or destination.

Layer 3 Limitations

Asymmetric Configuration

In a vPC topology, two Cisco Nexus 6000 Series switches configured as vPC peer switches need to be configured symmetrically for Layer 3 configurations such as SVIs, a peer gateway, routing protocol and policies, and RACLs.

Note vPC consistency check does not include Layer 3 parameters.

SVI

When a Layer 3 module goes offline, all non-management SVIs are shut down. To maintain connectivity when a Layer 3 module fails, you can configure an SVI as a management SVI using the command **management** under i**nterface vlan**. This prevents traffic to the management SVI from passing through the failed Layer 3 module.

Caveats

This section includes the open and resolved caveats for this release. Each caveat has a link to the Bug Toolkit, where you can find details.

This section includes the following topics:

- Open Caveats, page 17
- Resolved Caveats in Cisco NX-OS Release 7.0(0)N1(1), page 19

Open Caveats

Table 5 lists descriptions of open caveats in Cisco NX-OS Release 7.0(0)N1(1)

The record ID links to the Cisco Bug Toolkit where you can find details about the caveat.

Table 5 Cisco NX-OS Release 7.x Open Caveats

Record Number	Open Caveat Headline
CSCts71048	On an NPV switch, VFCs do not come up after delete/add VLAN/VSAN.
CSCty33678	MACs not synced after ISSU on AA HIF trink with PSEC;non-default timers.
CSCuf82183	In some scenarios, policy statistics are not enabled when a service policy is applied to ports.
CSCuh17828	On a Cisco Nexus 6000 Series switch, when the command sequence **copy file start** is used, copying the saved configuration to the running configuration takes too long.
CSCuh97761	MTU violated packets are not accounted as output errors in "show interface eth x counter detailed."
CSCug90859	N96-PBR is not working on PVLAN SVI.
CSCuc12211	Channel-group configuration missing after reload on HIF port.
CSCuc25187	Config-sync is unable to remove the VLAN QoS policy and offset configuration.
CSCuc43503	The IGMP vPC optimization knob does not work when the feature-set virtualization is configured.
CSCud43962	CDPv6 shows addresses of different interfaces and not the connected interfaces.
CSCud53059	DAI is blocking traffic for HIF ports.
CSCue22038	Unable to power on the module after powering off the module.

Table 5 Cisco NX-OS Release 7.x Open Caveats (continued)

Record Number	Open Caveat Headline
CSCue33173	IPSG blocks traffic for private VLAN isolated trunk ports, even when a valid DHCP snooping binding entry exists.
CSCuh44777	Support should be available to log an enabled IP ACL as a class-map match.
CSCug66129	STP loops are detected when root re-selection is triggered in a nonconverged STP topology.
CSCug72465	A test harness does not properly treat closing of the TCP flow.
CSCug72464	The Cisco Nexus 6004 needs "purge module" cli to clean up the configuration properly following a LEM OIR.
CSCuf52331	Handle minimum suppression value in switch/HIF/NIF storm-control.
CSCuh04973	The **default-interface** command is not resetting the speed command in the HIF/switch interface.
CSCuf16457	On a Cisco Nexus 6000 Series switch, applying policy maps fails with the error %RPM-2-PPF_SES_VERIFY.
CSCug90859	On the Cisco Nexus 6004 switch, PBR does not work on a PVLAN SVI.
CSCuh23056	N96- The error %FWM-2-FIB_TCAM_RESOURCE_EXHAUSTIO- occurs with a non-default HRT template.
CSCug98105	Norcal96-BGPv6 peering is not coming up if the same address in a different VRF uses MD5.
CSCuh36797	N96- The remove/hide process restart CLI for PIM/IGMP is not supported.
CSCuh26111	N64P- Mroutes are not removed on LHR following an admin down receiver SVI.
CSCui56698	Slow drain: Need support for non-default CoS value for class-fcoe.
CSCuf47724	Carmel: SVI Counters show incorrect results.
CSCuj12958	U6RIB structure errors seen during withdraw/add routes.
CSCuj12998	FCOE/EEM - 100% CPU for EEM actions with low timeout/high pause rate.
CSCuj13018	FCoE/EEM - Only 18 actions are taken when 19 actions are accepted.
CSCuj43607	NAT: With same static and dynamic NAT policy, packets punted to CPU.
CSCuj58467	Router MAC is not getting installed when changing the ASID.
CSCuj69824	Python script is not working when called using the **python** *script_name* command.
CSCuj78048	Interface VLAN shows up in the **show run** command after creating a configuration profile.
CSCuj83153	POAP: Addition of python-run and python-exec files to bootflash.
CSCuj86321	Pause events not seen if slow drain is enabled before VFC is up.
CSCul23467	Port-monitor and FC slow drain configurable on NPV switch.
CSCul49154	Flow match statistics are displaying 0 for default frop flow.
CSCul51416	FCoE slowdrain - pause events not detected for bind MAC configuration.
CSCul81869	10Mb FEX:ISSU downgrade from 7.0(0)N1(1) to 6.0(2)N2(1) should be incompatible with Speed 10.
CSCul82850	While configuring no IPv6 access-list acl_pbrIpv6L3PO_N5K getting error.
CSCul99528	Openflow: default-miss cascade normal not working in pipeline 201.

Table 5 Cisco NX-OS Release 7.x Open Caveats (continued)

Record Number	Open Caveat Headline
CSCum08767	WCCP: Interfaces level CLI configurations removed after invalid ID to spm.
CSCum11052	MAC address out of sync between two switches.
CSCum64907	FCOE Slowdrain: Pause Events not triggered on sh/no shut PO mem.
CSCum68574	Do not advertise Anycast SID when overload asserted.
CSCum83908	Port-security is not learning all addresses upon changing the port mode.

Resolved Caveats in Cisco NX-OS Release 7.0(0)N1(1)

Table 6 Cisco NX-OS Release 7.0(0)N1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtu31087	BGP update generation blocked because of large number of idle/active peers.
CSCud48710	Layer 2 multicast traffic can be lost up to 1 to 2 minutes upon unshut of the fabric PO in an AA topology. This happens only under the following conditions: • AA topology. • The group is downgraded to V2 of a V3 receiver. • The FEX fabric port is shut on one side. • When the fabric port is unshut, Layer 2 multicast traffic loss may be seen until the next join comes in.
CSCud72942	When all the FEXs are reloaded at the same time, Layer 2 multicast traffic may not recover on one of the HIF ports.
CSCud73169	The policer stats are not enabled if police action is added after it is applied to the interface configuration.
CSCuh36961	A QoS policy with qos-group 1 cannot be applied on a non-FCoE class.
CSCui77868	Add support for 10M speed on FEX interfaces.
CSCum48119	MTU option in SOL throws an error message when configured.

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 6000 Series switch.

The MIB Support List is available at the following FTP site:

ftp://ftp.cisco.com/pub/mibs/supportlists/nexus6000/Nexus6000MIBSupportList.html

Related Documentation

Documentation for the Cisco Nexus 6000 Series Switch is available at the following URL:

http://www.cisco.com/en/US/products/ps12806/tsd_products_support_series_home.html

The documentation set is divided into the following categories:

Release Notes

The release notes are available at the following URL:

http://www.cisco.com/en/US/products/ps12806/prod_release_notes_list.html

Installation and Upgrade Guides

The installation and upgrade guides are available at the following URL:

http://www.cisco.com/en/US/products/ps12806/prod_installation_guides_list.html

Command References

The command references are available at the following URL:

http://www.cisco.com/en/US/products/ps12806/prod_command_reference_list.html

Technical References

The technical references are available at the following URL:

http://www.cisco.com/en/US/products/ps12806/prod_technical_reference_list.html

Configuration Guides

The configuration guides are available at the following URL:

http://www.cisco.com/en/US/products/ps12806/products_installation_and_configuration_guides_list.html

Error and System Messages

The system message reference guide is available at the following URL:

http://www.cisco.com/en/US/products/ps12806/products_system_message_guides_list.html

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus6k-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)