Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes,

Cisco NX-OS Release 5.1(3)N1(1a) and Cisco NX-OS Release 5.1(3)N1(1)

Release Date: February 9, 2012
Part Number: OL-25823-02 I0
Current Release: NX-OS Release 5.1(3)N1(1a)

This document describes the features, caveats, and limitations for Cisco Cisco Nexus 5000 Series switches and the Cisco Nexus 2000 Series Fabric Extenders. Use this document in combination with documents listed in the "Related Documentation" section on page 30.

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 Cisco Nexus 5000 Series and Cisco Nexus 2000 Series release notes: http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/release/notes/Nexus_5000_Release_Notes.html

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

Table 1 Online History Change

Part Number	Revision	Date	Description
OL-25823-01	A0	December 7, 2011	Created NX-OS Release 5.1(3)N1(1) release notes.
	B0	December 18, 2011	Added additional Resolved Caveats to Table 6.

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

Table 1 Online History Change

Part Number	Revision	Date	Description
OL-25823-02	A0	February 9, 2012	Created NX-OS Release 5.1(3)N1(1a) release notes.
	B0	March 27, 2012	Updated upgrade and downgrade paths for Release 4.1(x) and 4.2(x) in Table 4.
	C0	April 3, 2012	Added CSCty92945 to a downgrade limitation in the "Limitations" section.
	D0	May 4, 2012	Added CSCtq18819.
	E0	June 28, 2012	Added CSCtc06276 to the "Limitations" section.
	F0	July 11, 2012	Added the Cisco Nexus B22HP FEX.
	G0	July 31, 2012	Updated Supported Upgrade and Downgrade Paths.
	H0	November 6, 2012	Updated the SFP+ Optics information in Table 2.
	I0	November 13, 2012	Added a note following Table 4 about the upgrade path from Cisco NX-OS Release 4.2(x) to Release 5.1(3)x. Added a note following Table 4 about the addition of the vlan configuration to the running configuration following an upgrade to Cisco NX-OS Release 5.1(3)N1(1a).

Contents

This document includes the following sections:

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 MDS 9000 SAN-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 5000 Series switch and the Cisco Nexus 2000 Series Fabric Extender (FEX) to improve the performance, scalability, and management of the product line. Cisco NX-OS Release 5.1 also supports all hardware and software supported in Cisco NX-OS Release 5.0 and Cisco NX-OS Software Release 4.2.

Cisco Nexus 5000 Series Switches

The Cisco Nexus 5000 Series switches include a family of line-rate, low-latency, lossless 10-Gigabit Ethernet, Cisco Data Center Ethernet, Fibre Channel over Ethernet (FCoE), and native Fibre Channel switches for data center applications. The Cisco Nexus 5000 Series includes the Cisco Nexus 5500 Platform and the Cisco Nexus 5000 Platform.

For information about the Cisco Nexus 5000 Series, see the *Cisco Nexus 5000 Series and Cisco Nexus 5500 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 5000 Series switches to provide high-density and low-cost connectivity for server aggregation. Scaling across 1-Gigabit Ethernet, 10-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 5000 Series switch 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 5000 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 5000 Series Layer 2 Switching Configuration Guide*.

System Requirements

This section includes the following topics:

Hardware Supported

The Cisco NX-OS software supports the Cisco Nexus 5000 Series. You can find detailed information about supported hardware in the *Cisco Nexus 5000 Series Hardware Installation Guide*.

Table 2 shows the hardware supported by Cisco NX-OS Release 5.1(x) software.

Table 2 Hardware Supported by Cisco NX-OS Release 5.1(x) Software

	Cisco NX-OS Release Support					
Hardware	**Part Number**	**5.1(3)N1(1a) 5.1(3)N1(1)**	**5.0(3)N2(2a) 5.0(3)N2(2) 5.0(3)N2(1)**	**5.0(3)N1(1)**	**5.0(2)N2(1)**	**5.0(2)N1(1)**
Cisco Nexus 5000 Series						
Cisco Nexus 5596UP switch	N5K-C5596UP-FA	X	X	X	—	—
Cisco Nexus 5548UP switch	N5K-C5548UP-FA	X	X	X	—	—
Cisco Nexus 5548P switch	N5K-C5548P-FA	X	X	X	X	X
Cisco Nexus 5020P switch	N5K-C5020P-BF	X	X	X	X	X
Cisco Nexus 5010P switch	N5K-C5010P-BF	X	X	X	X	X
Cisco Nexus 2000 Series						
Cisco Nexus B22HP FEX[1]	N2K-B22HP-P	X	X	—	—	—
Cisco Nexus 2232TM FEX	N2K-C2232TM-10GE	X	X	—	—	—
Cisco Nexus 2232PP FEX	N2K-C2232PP-10GE	X	X	X	X	X
Cisco Nexus 2248TP E FEX	N2K-C2248TP-E-1GE	X	—	—	—	—
Cisco Nexus 2248TP FEX	N2K-C2248TP-1GE	X	X	X	X	X
Cisco Nexus 2224TP FEX	N2K-C2224TP-1GE	X	X	X	X	X
Cisco Nexus 2148T FEX	N2K-C2148T-1GE	X	X	X	X	X
Expansion Modules						
16-port Universal GEM	N55-M16UP(=)	X	X	X	—	—
N5596 Layer 3 GEM	N55-M160L3(=)	X	X	X	—	—
N5548 Layer 3 daughter card	N55-D160L3(=)	X	X	X	—	—
Layer 3 GEM	N55-M160L3-V2	X				
Version 2 Layer 3 daughter card	N55-D160L3-V2	X				
16-port SFP+ Ethernet	N55-M16P(=)	X	X	X	X	X
8 10-Gigabit Ethernet and 8 10-Gigabit FCoE ports	N55-M8P8FP(=)	X	X	X	X	X
Transceivers						
Fabric Extender Transceivers						
10-Gigabit Ethernet SFP (for Cisco Nexus 2000 Series to Cisco Nexus 5000 Series connectivity)	FET-10G(=)	X	X	X	X	X
SFP+ Optical						
10-Gigabit Ethernet—short range SFP+ module	SFP-10G-SR(=)	X	X	X	X	X
10-Gigabit Ethernet—long range SFP+ module	SFP-10G-LR(=)	X	X	X	X	X

Table 2 Hardware Supported by Cisco NX-OS Release 5.1(x) Software (continued)

		Cisco NX-OS Release Support				
Hardware	**Part Number**	**5.1(3)N1(1a) 5.1(3)N1(1)**	**5.0(3)N2(2a) 5.0(3)N2(2) 5.0(3)N2(1)**	**5.0(3)N1(1)**	**5.0(2)N2(1)**	**5.0(2)N1(1)**
10-Gigabit Ethernet—extended range SFP+ module	SFP-10G-ER(=)	X				
1000BASE-T standard	GLC-T(=)	X	X	X	—	—
Gigabit Ethernet SFP, LC connector SX transceiver (MMF)	GLC-SX-MM(=)	X	X	X	—	—
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF)	GLC-LH-SM(=)	X	X	X	—	—
SFP+ Copper						
10GBASE-CU SFP+ Cable (1 meter)	SFP-H10GB-CU1M(=)	X	X	X	X	X
10GBASE-CU SFP+ Cable (3 meters)	SFP-H10GB-CU3M(=)	X	X	X	X	X
10GBASE-CU SFP+ Cable (5 meters)	SFP-H10GB-CU5M(=)	X	X	X	X	X
10GBASE-CU SFP+ Cable (7 meters)	SFP-H10GB-ACU7M(=)	X	X	X	X	X
10GBASE-CU SFP+ Cable (10 meters)	SFP-H10GB-ACU10M(=)	X	X	X	X	X
Fibre Channel						
8-Gbps Fibre Channel—short wavelength	DS-SFP-FC8G-SW(=)	X	X	X	X	X
8-Gbps Fibre Channel—long wavelength	DS-SFP-FC8G-LW(=)	X	X	X	X	X
4-Gbps Fibre Channel—short wavelength	4DS-SFP-FC4G-SW(=)	X	X	X	X	X
4-Gbps Fibre Channel—long wavelength	4DS-SFP-FC4G-LW(=)	X	X	X	X	X
Extended Temperature Range						
1000BASE-T SFP, extended temperature range	SFP-GE-T(=)	X	X	X	X	X
Gigabit Ethernet SFP, LC connector SX transceiver (MMF), extended temperature range and digital optical monitoring (DOM)	SFP-GE-S(=)	X	X	X	X	X

Table 2 Hardware Supported by Cisco NX-OS Release 5.1(x) Software (continued)

		Cisco NX-OS Release Support				
Hardware	**Part Number**	**5.1(3)N1(1a) 5.1(3)N1(1)**	**5.0(3)N2(2a) 5.0(3)N2(2) 5.0(3)N2(1)**	**5.0(3)N1(1)**	**5.0(2)N2(1)**	**5.0(2)N1(1)**
Gigabit Ethernet SFP, LC connector LX/LH transceiver (SMF), extended temperature range and DOM	SFP-GE-L(=)	X	X	X	X	X
Converged Network Adapters						
Generation-1 (Pre-FIP) CNAs[2]		X	X	X	X	X

1. The Cisco Nexus B22HP FEX is supported starting with Cisco NX-OS Release 5.0(3)N2(2).
2. Generation-1 (Pre-FIP) CNAs are supported on the Nexus 5000 Platform switches; however, they are not supported on the Nexus 5500 Series.

Online Insertion and Removal Support

Table 3 shows the hardware and Cisco NX-OS Release 5.0(x) software that supports online insertion and removal (OIR).

Table 3 Online Insertion and Removable Support by Cisco NX-OS Release 5.0(x) Software

		Cisco NX-OS Release Support				
Hardware Part Number		**5.1(3)N1(1a) 5.1(3)N1(1)**	**5.0(3)N2(2a) 5.0(3)N2(2) 5.0(3)N2(1)**	**5.0(3)N1(1)**	**5.0(2)N2(1)**	**5.0(2)N1(1) and earlier releases**
Cisco Nexus 5000 Series						
Cisco Nexus 5596UP switch	N5K-C5596UP-FA	X	X	—	—	—
Cisco Nexus 5548UP switch	N5K-C5548UP-FA	X	X	—	—	—
Cisco Nexus 5548P switch	N5K-C5548P-FA	X	X	X	X	—
Expansion Modules						
16-port Universal GEM	N55-M16UP(=)	X	X	—	—	—
Layer 3 GEM	N55-M160L3-V2[1]	X				
Version 2 Layer 3 daughter card	N55-D160L3-V2[1]	X				
16-port SFP+ Ethernet	N55-M16P(=)	X	X	X	—	—
8-port SFP+ Ethernet ports and 8-port SFP+ Fibre Channel ports	N55-M8P8FPL(=)	X	X	X	—	—
N5596 Layer 3 GEM	N55-M160L3(=)		—	—	—	—
N5548 Layer 3 daughter card	N55-D160L3(=)		—	—	—	—

1. Does not support online insertion and removal.

New and Changed Features

This section describes the new features introduced in Cisco NX-OS Release 5.1(3)N1(1). This section includes the following topics:

New Features in Cisco NX-OS Release 5.1(3)N1(1a)

Cisco NX-OS Release 5.1(3)N1(1a) is a patch release that provides bug fixes. It does not include new software or hardware features.

New Hardware Features

This section describes the following new hardware:

Cisco Nexus 2248TP-E Fabric Extender

The new Cisco Nexus 2248TP-E Fabric Extender is a 1-RU, general purpose 100-Mb/1-G FEX that is optimized for specialized data center workloads such as data, distributed storage, distributed computing, market data, and video editing. The Cisco Nexus 2248TP-E FEX has 48x1 Gigabit Ethernet host ports and 4x10 Gigabit Ethernet uplinks. It supports all of the existing features and topologies as the Cisco Nexus 2248 and the Cisco Nexus 2148 support. In addition, the Cisco Nexus 2248TP-E offers rich counters for troubleshooting and capacity monitoring. It has a user-configurable shared buffer, and it has a per-port ingress and egress queue limit.

For detailed information about the Cisco Nexus 2248TP-E FEX, see the *Cisco Nexus 2000 Series Hardware Installation Guide.*

Cisco Nexus 5000 Series Expansion Modules

Two new Generic Expansion Modules (GEM) are being released:

- Layer 3 GEM, N55-M160L3-V2
- Layer 3 I/O Module, N55-D160L3-V2

ER Optics Support

The 10-Gigabit Ethernet, extended range SFP+ module (SFP-10G-ER) supports a link length of up to 40 kilometers on standard single-mode fiber (SMF, G.652). All Cisco Nexus 5500 switches and all Cisco FEX models support the new SFP-10G-ER optic.

Note Cisco Nexus 2232 FEX does not support the SFP+ module on the HIF port.

New Software Features—Cisco Nexus 5500 Switch

Cisco NX-OS Release 5.1(3)N1(1) supports the following new software features only on the Cisco Nexus 5500 switch:

Cisco FabricPath

Cisco FabricPath is a set of multipath Ethernet technologies that combine the reliability and scalability benefits of Layer 3 routing with the flexibility of Layer 2 networks, which enables it to build scalable data centers. Cisco FabricPath offers a topology-based Layer 2 routing mechanism that provides an equal-cost multipath (ECMP) forwarding model. Cisco NX-OS Release 5.1(3)N1(1) supports one FabricPath topology.

The FabricPath feature provides the following:

- Allows Layer 2 multipathing in the FabricPath network.
- Provides built-in loop prevention and mitigation with no need to use the Spanning Tree Protocol (STP).
- Provides a single control plane for unknown unicast, unicast, broadcast, and multicast traffic.
- Enhances mobility and virtualization in the FabricPath network.

The FabricPath network uses the Layer 2 Intermediate System-to-Intermediate System (IS-IS) protocol to forward traffic in the network using the FabricPath headers. Layer 2 IS-IS is different than Layer 3 IS-IS; the two protocols work independently. Layer 2 IS-IS requires no configuration and becomes operational when you enable FabricPath on the device. The frames carry the same FTag that is assigned at ingress throughout the FabricPath network, and Layer 2 IS-IS allows all devices to have the same view of all the trees built by the system. Known unicast traffic uses the Equal Cost Multipath Protocol (ECMP) to forward traffic throughout the network. The system automatically load balances traffic throughout the FabricPath network by using ECMP and the trees.

Cisco FabricPath is supported on all Cisco Nexus 5500 switches (N5K-C5596UP-FA, N5K-C5548UP-FA, and N5K-C5548P-FA). The switch must be running Cisco NX-OS Release 5.1(3)N1(1). In addition, Cisco FabricPath requires the Enhanced Layer 2 license. For licensing information, see the *License and Copyright Information for Cisco NX-OS Software* document.

For detailed information about Cisco FabricPath, see the *Cisco Nexus 5000 Series NX-OS FabricPath Configuration Guide.*

Cisco TrustSec

The Cisco TrustSec security architecture builds secure networks by establishing clouds of trusted network devices. Cisco TrustSec also uses the device information acquired during authentication for classifying, or coloring, the packets as they enter the network. This packet classification is maintained by tagging packets on ingress to the Cisco TrustSec network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path. The tag, also called the security group tag (SGT), allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT to filter traffic.

For more information about Cisco TrustSec, see the *Cisco Nexus 5000 Series NX-OS Security Configuration Guide.*

Adapter FEX

Cisco is introducing Adapter-FEX support on the Cisco Nexus 5500 platform and on Cisco Nexus 2200 FEXes that are connected to a Cisco Nexus 5500 parent switch. The Cisco NX-OS Adapter-FEX feature provides the advantages of the FEX Link architecture with that of server I/O virtualization to create multiple virtual interfaces over a single Ethernet interface. This allows the deployment of a dual port NIC on the server and the ability to configure more than two virtual interfaces that the server sees as a regular Ethernet interface. The advantage of this approach is a reduction of power and cooling requirements and a reduction of the number of network ports.

The Adapter-FEX implementation is designed to work on a variety of FEX-capable adapters including the Cisco adapter for Cisco UCS C-Series Platform (UCS P81E VIC) and third-party adapters that implement VNTag technology. For additional, see Cisco UCS C-Series documentation.

Adapter-FEX supports FCoE when a VIC-enabled adapter is attached to a Cisco Nexus 2000 FEX or directly to a Cisco Nexus 5000 Series switch.

Adapter-FEX at the access layer needs a FEX-enabled adapter in a server that connects to a parent switch that supports Adapter-FEX functionality. There are two adapters that support Adapter-FEX functionality:

- Cisco UCS P81E Virtual Interface Card
- Broadcom NIV Adapter

Note Adapter FEX does not support SPAN and cannot be used as a SPAN source.

For detailed information about Adapter-FEX, see the *Cisco Nexus 5000 Series NX-OS Adapter-FEX Configuration Guide.*

VM-FEX

The VM-FEX is an extension of the FEX that extends to the VIC virtual interface card (VIC) in the server. It simulates ports and enables a high-speed link between the switch and the server. The VM-FEX consolidates the virtual and physical network. Each VM gets a dedicated port on the switch. In addition, the VM-FEX provides for vCenter management of Adapter-FEX interfaces.

The VM-FEX solution provides the following benefits:

- Policy-based VM connectivity
- Mobility of network and security properties
- A nondisruptive operation model

VM-FEX does not support SPAN and cannot be used as a SPAN source.

VM-FEX does not support FCoE in NPV mode. Support for this feature will be available when CSCts09434 is resolved, which is expected in the next maintenance release of VMware ESX 5.0.

For more information about VM-FEX, see the *Cisco Nexus 5000 Series NX-OS Layer2 Switching Configuration Guide.*

Support for FCoE on a Dual Homed FEX

The Cisco Adapter FEX with FCoE feature allows you to create an FCoE connection to a Cisco Nexus 2000 Series Fabric Extender (FEX), which can then establish an FCoE connection to a server with a virtual interface card (VIC) adapter. The switch connects to the FEX through a virtual port channel (vPC) while the FEX connects to the server using a standard FCoE link between the FEX and the VIC adapter.

If you are using Enhanced vPC, the FEX can be associated with one and only one Cisco Nexus 5000 fabric for FCoE forwarding.

If you are using FabricPath, you must use a dedicated link for FCoE traffic.

If you are using a Cisco UCS C-Series Rack-Mount Server with a Cisco UCS P81E Virtual Interface Card (VIC):

- The VIC must be configured in Network Interface Virtualization (NIV) mode, which makes the two unified ports appear to the system as virtual host bus adapters (vHBAs).
- The VIC cannot be connected to the FEX through a VNP port. If this type of connection is used, NIV mode cannot be enabled on the VIC.
- The NIC mode on the Cisco UCS C-Series Rack-Mount Server must be set to active-standby.
- If you deploy FCoE over Adapter FEX on a server with a Cisco UCS P81E Virtual Interface Card (VIC) and that is running Windows 2008, you must install new versions of software drivers.

For more information about support for FCoE on Dual Homed FEX, see the *Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide.*

CoPP

Control Plane Policing (CoPP) provides QoS-based prioritization and protection of control plane traffic that arrives at the switch in the data plane, which ensures network stability, reachability, and packet delivery.

Cisco NX-OS Release 5.1(3)N1(1) provides several predefined CoPP policies that administrators can deploy for different environments. In these predefined CoPP policies, the classification of flows is predetermined and the policing rates for the flows is fixed. In addition, there is one flexible CoPP policy for cases where predefined policies do not address the needs of the deployment.

The CoPP implementation on Cisco Nexus 5500 Series switches provides three predefined COPP policies for different deployment environments.

- Default
- Scaled-Layer 2
- Scaled-Layer 3

- Customized Policy

The CoPP policies can be changed at run time like any other QoS configuration. Classification of flows is predetermined and cannot be modified. Policing rates for the flows is fixed and cannot be modified.

For additional information about CoPP, see the *Cisco Nexus 5000 Series NX-OS Security Configuration Guide.*

Enhanced vPC Support

Enhanced vPC (EvPC) provides a uniform access layer for any server to any FEX in hybrid deployments. In addition, EvPC provides data, control plane, and management plane redundancy. A new vPC option allows port channel connectivity to dual-homed FEXes.

The Cisco Nexus 2000 Series Fabric Extender (FEX) that contains the port assigned to the vPC must be associated with the Cisco Nexus switch.

The CNA must be attached to the Cisco Nexus 2000 Series FEX rather than directly to the Cisco Nexus 5000 Series switch.

If you want to ensure backward compatibility for all previous configurations and supported topologies, you must configure the FEX in a straight-through FEX topology that does not use Enhanced vPC.

Note Enhanced vPC does not support SPAN and cannot be used as a SPAN source.

For more information about EvPC, see the *Cisco Nexus 5000 Layer 2 Switching Configuration Guide.*

IP ARP Synchronization

Cisco NX-OS Release 5.1(3)N1(1) introduces the **ip arp synchronize** command.When this command is enabled, faster convergence of address tables between the vPC peers is possible. This convergence is designed to overcome the delay involved in ARP table restoration when the peer-link port channel flaps or when a vPC peer comes back online.

Enabling ARP synchronization improves convergence times during the restart of a vPC peer when a Cisco Nexus 5000 Series switch acts as a default gateway. By default, ARP synchronization is not enabled.

For more information about IP ARP sync, see the *Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide.*

Management SVI

A switch virtual interface (SVI) is a VLAN of switch ports represented by one interface to a routing or bridging system. The SVI can be configured for routing, in which case it supports Layer 3 protocols for processing packets from all switch ports associated with the VLAN, or for in-band management of the switch.

Starting with Release 5.1(3)N1(1), the NX-OS switch has specific support for management SVIs. Having different SVIs for routing and management separates data traffic from management traffic, which can reduce competition for routing resources. If you are using an SVI for management purposes, we recommend that you specifically configure your SVI for management using the **management** command so that you can take advantage of this added functionality.

With this change, there are new guidelines and limitations for routed SVIs:

- Although the CLI does not prevent you from configuring routing protocols on a management SVI, we recommend that you do not configure them on management SVIs.
- Routed SVIs that are being used for management (that is, routed SVIs that have not been specifically configured for management using the **management** command) can still be used for management as long as the Layer 3 license is not installed.
- Management SVIs do not support configuration synchronization mode (config-sync). Configuration synchronization is performed using the mgmt 0 interface.
- RACL is not supported. Use VACL to filter the management traffic.

For more information about management SVIs, see the *Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide.*

New Software Features—Cisco Nexus 5000 Series Switches

Cisco NX-OS Release 5.1(3)N1(1) supports the following new software features on all Cisco Nexus 5000 Series switches:

ERSPAN

Encapsulated Remote Switched Port Analyzer (ERSPAN) introduces an additional level of flexibility to the powerful network monitoring capabilities of SPAN and RSPAN. ERSPAN allows the analyzer to be placed on one location and multiple switches can send mirrored traffic to this analyzer. Traffic from any port on the network on any remote switch can be analyzed without physically moving the analyzer tool.

- ERSPAN encapsulates SPAN traffic to IP-GRE frame format and allows remote monitoring traffic over an IP network.
- All Cisco Nexus 5000 Series switches, including Cisco Nexus 5500 switches, support ERSPAN.
- Cisco NX-OS Release 5.1(3)N1(1) supports an ERSPAN source session only; there is no support for an ERSPAN destination session. The Cisco Nexus 5000 Series switch hardware cannot deencapsulate an ERSPAN frame.
- ERSPN does not require a Layer 3 module and Layer 3 license.
- The Cisco Nexus 5010 and Nexus 5020 switches support two active ERSPAN sessions. The Cisco Nexus 5548P, Nexus 5548UP, and Nexus 5596UP switch support four active ERSPAN sessions.

For more information about ERSPAN, see the *Cisco Nexus 5000 Series NX-OS System Management Configuration Guide.*

Multicast VLAN Registration

Multicast VLAN Registration (MVR) allows a Layer 2 switch to deliver a multicast packet received from one VLAN to multiple receivers that reside in different VLANs, without Layer 3 replication.

MVR offers the following advantages:

- It reduces the overhead of Layer 3 multicast replication on a multicast router.
- It reduces the bandwidth consumption for the link between the Layer 2 switch and the multicast router.
- It reduces the multicast forwarding table size on the Layer 2 switch.

All models of Cisco Nexus 5000 Series switches support MVR.

For more information about MVR, see the *Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide.*

Port Security

Port security is a simple Ethernet MAC-based security feature that can restrict input to an interface by limiting and identifying MAC addresses of the end host that are allowed to access the port. Cisco NX-OS Release 5.1(3)N1(1) adds port security to the Cisco Nexus 5000 Series and Cisco Nexus 2000 Series, and it is available on both Cisco Nexus 5000 and Nexus 5500 switches. Port security supports the following features:

- It supports both physical ports and port channels.
- It supports vPC ports for the first time in Cisco NX-OS, and only in the Cisco Nexus 5000 Series. (Port security support for vPC ports is not available in the Cisco Nexus 7000 Series, although the port security feature itself is supported on that platform.)
- It supports EvPC ports.
- It does not support NIV ports.

A device maximum of 8192 secure MAC addresses in addition to one MAC address per port is supported. The interface maximum is 1025 MAC addresses per interface.

For additional information about the port security feature, see the *Cisco Nexus 5000 NX-OS Security Configuration Guide.*

Boot from SAN with vPC

Cisco Nexus Series 5000 switches support SAN boot with vPC. A VFC interface must be bound to a vPC member physical interface (and not to the vPC port-channel interface itself) for a SAN boot to occur.

For more information about SAN boot with vPC, see the *Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide.*

Config-Sync Enhancements

Config-sync allows you to synchronize the configuration between a pair of vPC switches. It eliminates downtime due to vPC inconsistencies, simplifies vPC operations, and reduces administrative overhead.

The enhancements to config-sync in Cisco NX-OS Release 5.1(3)N1(1) remove the port channel configuration restriction that previously existed. All port channels and member interfaces should be configured inside a switch profile.

For more information about config-sync enhancements, see the *Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide.*

SNMP over IPv6

Cisco NX-OS Release 5.1(3)N1(1) supports SNMP over IPv6.

For more information, see the *Cisco Nexus 5000 Series NX-OS System Management Configuration Guide.*

Support for Eight Syslog Servers

In Cisco NX-OS Release 5.1(3)N1(1), you can configure up to eight syslog servers. You use the Cisco Fabric Services (CFS) to distribute the syslog server configuration; however, CFS distribution of the syslog server configuration is limited to three servers.

For more information, see the *Cisco Nexus 5000 Series NX-OS System Management Configuration Guide.*

Upgrading or Downgrading to a New Release

This section describes the upgrade and downgrade paths that are supported for Cisco NX-OS Release 5.1(3)N1(1a) and Release 5.1(3)N1(1) on the Cisco Nexus 5000 Series switch.

This section includes the following topics:

Upgrade and Downgrade Guidelines

The following guidelines apply to Cisco NX-OS Release 5.1(3)N1(1a) and Release 5.1(3)N1(1) for the Cisco Nexus 5000 Series switches:

- When a Layer 3 license is installed, the Cisco Nexus 5500 Platform does not support an ISSU. Hot swapping a Layer 3 module is not supported.

Supported Upgrade and Downgrade Paths

Table 4 shows the upgrade and downgrade possibilities for Cisco NX-OS Release 5.1(3)N1(1a) and Release 5.1(3)N1(1).

Table 4 Cisco NX-OS Release 5.1(3)N1(1a) and Release 5.1(3)N1(1) Supported Upgrade and Downgrade Paths

Current Cisco NX-OS Release	Upgrade to NX-OS Release 5.1(3)N1(1a)	Upgrade to NX-OS Release 5.1(3)N1(1)	Downgrade from NX-OS Release 5.1(3)N1(1a)	Downgrade from NX-OS Release 5.1(3)N1(1)
5.0(3)N2(2b) 5.0(3)N2(2a) 5.0(3)N2(2) 5.0(3)N2(1)	Nondisruptive upgrade (ISSU)	Nondisruptive upgrade (ISSU)	Disruptive downgrade	Disruptive downgrade
5.0(3)N1(1c)	Nondisruptive upgrade (ISSU)	Nondisruptive upgrade (ISSU)	Disruptive downgrade	Disruptive downgrade
5.0(2)N2(1)	Nondisruptive upgrade (ISSU)	Nondisruptive upgrade (ISSU)	Disruptive downgrade	Disruptive downgrade
5.0(2)N1(1)	Nondisruptive upgrade (ISSU)	Nondisruptive upgrade (ISSU)	Disruptive downgrade	Disruptive downgrade

Note An upgrade from Cisco NX-OS Release 4.2(x) to Release 5.1(x) is disruptive. This upgrade path requires that you upgrade in steps from Cisco NX-OS Release 4.2(x) to Release 5.0(3)x to Release 5.1(3)x.

Note Following an upgrade to Cisco NX-OS Release 5.1(3)N1(1a) on a Cisco Nexus 5000 or 5500 Series switch, the vlan configuration is added to the running configuration. This change appears if the upgrade is nondisruptive or disruptive. The addition of the vlan configuration is the result of the conversion of some CLI commands in an older version of Cisco NX-OS software to a newer version. The operation of the switch is not affected by the vlan configuration being a part of the running configuration.

Limitations

This section describes the limitations for Cisco NX-OS Release 5.1(3)N1(1).

- When upgrading from Cisco NX-OS Release 4.2(1)N1(1) and earlier releases to any release, the policy description is lost. This problem does not occur when upgrading from Cisco NX-OS Release 4.2(1)N1(1) and later releases. After an upgrade, we recommend that you reconfigure the policy description. For details, see CSCth14225.
- Starting with Cisco NX-OS Release 4.2(1)N2(1), LACP fast timers are supported. If you downgrade to an earlier release that does not support this feature, entering the **install all** command displays the following warning:

```
"Configuration not supported - Lacp fast rate is enabled",
  "Use \"lacp rate normal\" on those interfaces"
```

  Before downgrading to an earlier release, change the LACP rate to normal. If you ignore the warning and force the installation, then it is possible that the leftover LACP rate fast configuration would still be active with previous releases of software but the behavior would be unpredictable and link flap might occur. We recommend that you change the LACP rate setting to normal. For details, see CSCth93787.

- When an FC SPAN destination port is changed from SD to F mode and back to SD mode on a NPV switch, the port goes into an error-disabled state. Perform a shut/no-shut after the mode change recovers the port. This issue occurs only in NPV mode. For details, see CSCtf87701.
- 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 a 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.
- Given the implementation of a single CPU ISSU, the STP root on the PVST region with switches on an MST region is not supported. The PVST simulation on the boundary ports go into a PVST SIM inconsistent blocked state that breaks the STP active path. To work around this issue, move all STP roots to the MST region. However, the workaround causes a nondisruptive ISSU to fail because non-edge designated forwarding ports are not allowed for an ISSU. For additional information, see CSCtf51577. For information topologies that a nondisruptive upgrade is supported, see to the *Cisco Nexus 5000 Series NX-OS Upgrade and Downgrade Guide*.
- IGMP queries sent in CSCtf94558 are group-specific queries that are sent with the destination IP/MAC address as the group's address.

  GS queries are sent for IP address: 224.1.14.1 to 224.1.14.100 [0100.5E01.0E01 to 0100.5E01.0E64]

  These are not link-local addresses. By default, they are not flooded by the hardware into the VLAN. They are sent only to the ports that have joined this group.

  This is expected behavior during an ISSU.

  In another scenario, the IGMP global queries [dest IP 224.0.0.1] get flooded correctly in the VLAN.

  Group-specific queries are not forwarded to ports other than the one that joined the group during ISSU. The reason to forward group-specific queries toward hosts is to avoid having them leave the group. However, if a port has not joined the group, then this is not an issue. If there is an interface that has joined the group, then the queries are expected to make it to the host. While the behavior is different when ISSU is not occurring, it is sufficient and works as expected and there is no impact to traffic. For details, see CSCtf94558.
- The meaning of an MTU configuration has changed in Cisco NX-OS Release 4.2(1)N1(1) and earlier releases. In releases earlier than Cisco NX-OS Release 4.2(1)N1(1), the configured MTU included the Ethernet payload and Ethernet headers. In Cisco NX-OS Release 4.2(1)N1(1), the configured MTU includes only the Ethernet payload and not the Ethernet headers. When upgrading or downgrading between Cisco NX-OS Release 4.2(1)N1(1) and earlier releases, Cisco NX-OS automatically converts the configuration to address this semantic change by adding or subtracting 38 to the MTU to address the Ethernet header size.

  In a vPC configuration, the MTU per class needs to be consistent on both switches in the vPC domain for the vPC peer link to come up. When upgrading/downgrading a working vPC setup between pre-4.2(1)N1(1) and 4.2(1)N1(1) releases, the MTU is adjusted to make sure that the MCT peer-link always comes up.

  However if you add a peer-link between two switches in a vPC domain that are identically configured (MTU in particular) with one switch running Cisco NX-OS Release 4.2(1)N1(1) and another switch running an earlier release, then the vPC peer link does not come up because the MTU is inconsistent between the two switches.

This is not an issue when upgrading or downgrading peer switches in a vPC domain; this is only an issue when adding a peer link between two switches running Cisco NX-OS Release 4.2(1)N1(1) and earlier releases that were not previously in the same vPC domain.

To resolve this issue, upgrade or downgrade one switch to match the version on the other switch and reconfigure the MTU to be consistent on both sides. For details, see CSCtg27538.

- The channel-group configuration is not applied to the Cisco Nexus 2000 Series downlink interface after downgrading to the Cisco NX-OS Release 4.1(3)N1(1) software. This issue occurs if the **speed 1000** command is present under the context of the port channel. To work around this issue, reconfigure the **channel-group** command after the system comes up and reapply the configuration from the saved configuration in the bootflash. For details, see CSCtc06276.
- 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 may 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 5000 Series switch, and 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 2000 Fabric Extender does not support PVLANs over VLAN trunks used to connect to another switch. The PVLAN trunks are used only on inter-switch links but the FEX ports are only meant to connect to servers. Because it is not a valid configuration to have an isolated secondary VLAN as part of a Fabric Extender port configured as a VLAN trunk, all frames on isolated secondary VLANs are pruned from going out to a FEX.
- Egress scheduling is not supported across the drop/no-drop class. Each Fabric Extender host port does not support simultaneous drop and no drop traffic. Each Fabric Extender host port can support drop or no drop traffic.
- The Cisco Nexus 2148 Fabric Extender does not support frames with the dot1p 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 remove an expansion module with Fibre Channel ports, and the cable is still attached, the following FCP_ERRFCP_PORT errors are displayed:

```
2008 May 14 15:55:43 switch %KERN-3-SYSTEM_MSG: FCP_ERRFCP_PORT:
gat_fcp_isr_ip_fcmac_sync_intr@424, jiffies = 0x7add9a:Unknown intr src_id 42 - kernel
2008 May 14 15:55:43 switch %KERN-3-SYSTEM_MSG: FCP_ERRFCP_PORT:
gat_fcp_isr_ip_fcmac_sync_intr@424, jiffies = 0x7add9a:Unknown intr src_id 41 - kernel
```

  These messages are informational only, and result in no loss of functionality.
- If you configure Multiple Spanning Tree (MST) on a Cisco Nexus 5000 Series switch, we do not recommend that you partition the network into a large number of regions.
- A downgrade from Cisco NX-OS Release 5.1(3)N1(1) to any 5.0(3)N1(x) image can cause the Cisco Nexus 5000 Series switch to fail. For details, see CSCty92945.

- If you upgrade a vPC Peer switch from Cisco NX-OS Release 5.0(3)N2(1) to Cisco NX-OS Release5.1(3)N1(1) and feature-set fabricpath is enabled on the upgraded switch, the vPC Peer-Link enters STP Bridge Assurance Inconsistency which affects all VLANs except VLAN 1 and affects traffic forwarding for vPC ports.

  To avoid this issue, upgrade the peer switch that is running Cisco NX-OS Release 5.0(3)N2(1) switch also to Cisco NX-OS Release 5.1(3)N1(1) or higher and then enable feature-set fabricpath on the switch or switches. If you accidentally enable feature-set fabricpath in Cisco NX-OS Release 5.1(3)N1(1) when the peer vPC switch is running Cisco NX-OS Release 5.0(3)N2(1), disable the feature-set fabricpath and the vPC will resume STP forwarding state for all VLANs.
- By design, vEth interfaces do not share the underlying behavior of a vPC port. As a result, a VLAN does not get 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 is up as it is an active VLAN on the secondary switch.
- RBACL policy enforcement is performed on VLANs on which CTS enforcement is not configured. This situation occurs when there is at least one VLAN in the switch where CTS is enforced. On a VLAN where CTS is not enforced, RBACL policy lookup occurs for ingress packets and the packet is denied or permitted according to the policies in the system. To work around this issue, make sure that all VLANs on which SGT tagged packets ingress enforce CTS.
- 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. This situation can occur whenever the MTU value that is configured in an ERSPAN or SPAN session is smaller than the SPAN packet, such as when the packet is truncated. The IP GRE packet is truncated to a value that differs by -2 to 10 bytes from the expected MTU.
- When you configure a Layer 3 interface as an ERSPAN source, and configure the ERSPAN termination on a Catalyst 6000 switch or a Cisco Nexus 7000 Series switch, you cannot terminate the Layer 3 interface ERSPAN source on the Cisco Nexus 7000 Series switch or the Catalyst 6000 switch. To work around this issue, configure VLAN 1 to 512 on the Cisco Nexus 7000 Series switch or the Catalyst 6000 switch.
- 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 5000 Series switch increments the interface counter based on the outer FabricPath header. As a result, multicast counters are incremented. In the case of a Cisco Nexus 7000 Series switch, Unicast counters are incremented as they are based on an inner Ethernet header. There is no workaround for this issue.
- If you configure a speed of 1 G on a base or GEM port and then check for compatibility with a Cisco NX-OS Release 5.0(2) image, no incompatibility is shown. However, because 1 G was not supported in the Cisco NX-OS Release 5.0(2), an incompatibility should be shown. To work around this issue, manually remove the 1 G configuration from the ports before downgrading to Cisco NX-OS Release 5.0(2) or an earlier release.
- In an emulated switch setup, 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 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.
- Fabricpath requires 802.1q tagging of inner Ethernet header of the packet. Native VLAN packets that are sent by a Cisco Nexus 7000 Series switch are not tagged. As a result, a Cisco Nexus 5000 Series switch drops packets due to packet parsing errors. To work around this issue, enable **vlan dot1q tag native** on the Cisco Nexus 7000 Series switch to force 802.1q tagging of native VLAN packets.
- Cisco Nexus 5548UP and Cisco Nexus 5598UP switches with a fibre-channel connection to HP Virtual Connect modules experience link destabilization and packet loss when the speed is set to 8GB. To work around this issue, leave the speed set to 4GB. For details, see CSCtx52991.

Configuration Synchronization Limitation

When you remove a switch profile using the **no switch-profile** *name* **[all-config | local-config]** command, the configuration in the switch profile is not immediately removed from the running configuration. The following warning message appears:

```
WARNING: Deleting switch-profile will remove all commands configured under
switch-profile. Are you sure you want to delete all switch-profile commands from the
system ?

Are you sure? (y/n)  [n]
```

For current information about this issue, refer to CSCtl87260.

Limitations on the Cisco Nexus 5010 and Cisco Nexus 5020

The limitations on the Cisco Nexus 5010 switch and the Cisco Nexus 5020 switch are as follows:

- Traffic going out the Ethernet SPAN destination is always tagged. The SPAN destination can be in the access or trunk mode and frames on the SPAN source port can be tagged or untagged. Frames are always tagged internally as they travel through the system. Information about whether the frame was originally tagged or untagged, as it appeared in the SPAN source, is not preserved in the SPAN destination. The spanned traffic exiting the SPAN destination port always has the VLAN tag on it. The correct VLAN tag is applied on the frame as it goes out the SPAN destination. The only exception is if frames ingress on a SPAN source port on an invalid VLAN. In this case, **vlan 0** is applied on a spanned frame.
- Spanned FCoE frames do not preserve original SMAC and DMAC fields. The Ethernet header gets modified as the frame is spanned to the destination. The modified header fields are displayed when monitored on the SPAN destination.
- The CoS value in spanned FCoE frames on the Ethernet SPAN destination port does not match with the CoS value in the SPAN FCoE source frame. The CoS value on the captured SPAN FCoE frame should be ignored.
- The class-fcoe cannot be removed even if Fibre Channel is not enabled on a switch.
- If a port drains traffic at a rate less than 100 Kbps, it is error-disabled in 10 seconds to avoid buffer exhaustion. However, if the drain rate is larger than 100 Kbps, the port may not be consistently error-disabled within 10 seconds which exhaust ingress buffers and discard frames. Use the **shut** command to disable the slow-draining port.
- The multicast storm control functionality in the Cisco Nexus 5000 Series does not distinguish between IP, non-IP, registered, or unregistered multicast traffic. All multicast traffic is subject to a single-multicast storm control policer when configured.

IGMP Snooping Limitation

On the Cisco Nexus 5010 switch and the Cisco Nexus 5020 switch with a Cisco Nexus 2000 Series Fabric Extender (FEX) installed, unregistered IP multicast packets on one VLAN are forwarded to other VLANs where IGMP snooping is disabled. We recommend that you do not disable IGMP snooping on the Cisco Nexus 5010 switch and the Cisco Nexus 5020 switch. A static IGMP join can be configured for devices intended to receive IP multicast traffic but not to send IGMP join requests. This limitation applies to the Cisco Nexus 5010 switch and the Cisco Nexus 5020 switch only.

SPAN Limitations on Fabric Extender Ports

The SPAN limitations on Fabric Extender ports are as follows:

- On a Cisco Nexus 5000 Series switch, if the SPAN source is a FEX port, the frames will always be tagged when leaving the SPAN destination.
- On a Cisco Nexus 5010 switch or a Nexus 5020 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 5500 Platform 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 4.0(1a)N2(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 the following error is displayed:

```
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 on all VLANs for which the tx-source port is a member, is spanned. 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, the broadcast, non-IGMP Layer-2 multicast, and unknown unicast frames originating from that port may 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.

Checkpoint and Configuration Rollback Limitation

When FCoE is enabled, the checkpoint and configuration rollback functionality is disabled.

Layer 3 Limitations

Asymmetric Configuration

In a vPC topology, two Cisco Nexus 5000 switches configured as vPC peer switches need to be configured symmetrically for Layer 3 configurations such as SVIs, 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 SVIs are shutdown.

Upgrading and Downgrading

When a Layer 3 license is installed, the Cisco Nexus 5500 platform does not support an ISSU. Layer 3 module hot swaps are not supported.

Cisco Nexus 5548P Daughter Card (N55-D160L3)

Before installing a Layer 3 daughter card (N55-D160L3) into a Cisco Nexus 5548P switch, you must upgrade to Cisco NX-OS Release NX-OS Release 5.0(3)N1(1c) or a later release, and then install the card into the chassis.

Caveats

This section includes the open and resolved caveat record numbers for this release. Links are provided to the Bug Toolkit where you can find details about each caveat.

This section includes the following topics:

Open Caveats

Table 5 lists descriptions of open caveats in Cisco NX-OS Release 5.1(3)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 5.1(3)N1(1) Open Caveats

Record Number	Open Caveat Headline
Open Caveats	
CSCtj85867	The switch might print an incorrect message when VLANs are added to or removed from the trunk.
CSCtk84182	The **show incompatibilities** command does not display an incompatible configuration.
CSCtl09648	The interface from the static IGMP group cannot be removed if it is part of a range.
CSCtl45495	After the license has been reinstalled, the Layer 3 DC remains offline until the switch is rebooted.
CSCtl51493	Information about IPv6 is not in the HSRP summary.
CSCtl53720	The service does not respond when you delete the Layer 3 port channel and SVI interfaces.
CSCtl87598	The QoS Type-2 inconsistency is not displayed in the **show vpc** command.
CSCtl87649	A commit failed when copying a configuration to the running configuration twice as per the recommended procedure.
CSCtl88086	On a host interface port in a straight-through topology, the channel-grp command displays an error due to “Slot in vpc A-A mode”
CSCtl94228	No IP load-sharing not reset to default mode
CSCtl95401	The FIB does not synchronize with the RIB after the FIB hit the hardware limit and the entries aged out.
CSCtl99388	A syntax error occurred after parsing the router-id and applying the saved configuration.
CSCtn00893	The **undebug all** command does not turn off CDP debugging logs.
CSCtn19504	The HIF port is stuck in the vpc-peer-link-down state during a switchover test.
CSCtn27125	Traffic leaking on SVI ACL during switch bootup
CSCtn31018	On a host interface port in a straight-through topology, the **channel-grp** command displays an error message indicating “Slot in vpc A-A mode”.
CSCtn40301	The syslog is consistently using more than 95% CPU after a switch upgrade.
CSCtn47093	The 32 entries that point to ECMP are not supported.
CSCtn50937	The (s,g) mroutes do not expire if the source stopped and (*,g) is still joined.
CSCtn51223	Pre-provisioning and port profile configurations are not supported on Layer 3 interfaces.
CSCtn52446	A problem occurs when adding routes in VRF.
CSCtn66859	A Cisco Nexus 5548P switch reboots after copying files from the bootlfash to USB flash.

Table 5 Cisco NX-OS Release 5.1(3)N1(1) Open Caveats (continued)

Record Number	Open Caveat Headline
CSCtn70380	Switch vPC member ports on the secondary switch go into a suspended-by-vpc state when configuring or removing configurations using config-sync mode.
CSCtn99894	When DHCP snooping is disabled globally but enabled in a VLAN, the boot-request packet is looped on the MCT in certain cases.
CSCtq84902	An ERSPAN packet has 4 extra bytes on a Cisco Nexus 5010 or 5020 switch.
CSCtq84910	An ERSPAN session state is incorrect if the egress port is shut.
CSCtr19103	Slot module-provisioning configuration should be removed if interfaces are configured for cts-manual.
CSCtr73654	Ports connected to a GEM in a peer switch are UDLD error disabled when the GEM module is powered off.
CSCts09424	A SPAN session remains down after a mode change of the destination interface.
CSCts26881	There is no CTS role-based enforcement on VLANs.
CSCts27285	ERSPAN or local SPAN truncated packets are a bit off in size.
CSCts51072	The SVI configuration is lost if CTS is enforced on the VLAN while configurations are copied from a file to the running configuration.
CSCts64671	CTS command rollback fails.
CSCts71048	VFCs connected to servers do not come up automatically after a delete or add VLAN or VSAN operation.
CSCtt02940	SPAN may not work if a VFC and port channel that are bound to the VFC are sources.
CSCtt96885	Static TGMP groups on an MVR VLANs do not work
CSCtu05349	CVL was not sent through a VFC over a EvPC when flapping a fabric port.
CSCtu14476	Remove the insert-before option in a COPP customized policy.
CSCtu21900	Traffic is not spanned correctly after an ISSU from Cisco NX-OS Release 5.0(3)N2 to Release 5.1(3)N1 or downgrade from Release 5.1(3)N1 to 5.0(3)N2.
CSCtu25289	RACLs on a subinterface are not applied when the saved configuration is applied to the running configuration.
CSCtu40226	An incorrect error message displays when configuring a distance command on a provisioned FEX.
CSCtu41247	The VLAN configuration on trunk interfaces fails with the **interface range** command in the switch profile.
CSCtu43469	The update-all message should be update to warn about MVR query timer change.
CSCtu81489	Configuring a Layer 3 port without a Layer 3 license followed by a GEM removal causes the switch to fail.
CSCtw47588	CPU utility by CTS process remains high when CTS sxp connection is not successfully established.
CSCtw57372	More that one UCS VIC P81E adapter on the host can cause multiple VIFs.
CSCtw62218	After conversion to FabricPath, Layer 3 Unicast traffic is dropped.
CSCtw65587	Fabric ports go to the hardware failure state after configuring a two-layer vPC as a SPAN source.

Table 5 Cisco NX-OS Release 5.1(3)N1(1) Open Caveats (continued)

Record Number	Open Caveat Headline
CSCtw76636	Delay during vPC failover with reload of primary switch.
CSCtw79225	Cannot manage switch via Telnet and console after an upgrade to Cisco NX-OS Release 5.1(3)N1(1).
CSCtw82571	Nexus 50x0: VLAN membership incorrect after an upgrade to Cisco NX-OS Release 5.1(3)N1(1).
CSCtw87601	Cannot configure IP prefix-list on a Cisco Nexus 55XX switch with NX-OS Release 5.1(3)N1(1).
Platform, Infrastructure	
CSCso01268	VDC-related syslog message appears when a module is hot-swapped.
CSCsv95478	On a FEX, the **fex pinn redist** command does not wait for a user prompt with a y/n.
CSCti11823	When upgrading from NX-OS Release 4.2(1)N1(1) to NX-OS Release 4.2(1)N2(1), the 1-Gb HIF LED blinks amber after an ISSU.
CSCtj22747	On a failing type_check, GEMs do not recover from that state
Configuration Synchronization	
CSCti19892	Pressing Ctrl + Z does not interrupt a switch-profile deletion.
CSCti40833	Long failure detection times occur for the verify and commit (commands or actions?) in certain cases.
CSCti68764	Some spanning-tree commands are not supported in the switch profile.
CSCtj10460	A failure has occurred while deleting a switch profile.
CSCtj26673	A configuration synchronization import has failed for an implicitly generated QoS configuration.
CSCtl87260	A switch profile has been removed so as not to impact the running configuration.
Layer 2 Switching	
CSCso25966	The Catalyst 6500 Series LACP ports go to the err disable state when a peer Cisco Nexus 5000 Series switch PC has a configuration mismatch.
CSCso27446	The management port does not bring down/up a link when you enter the **shut/no shut** commands.
CSCso84269	An unsaved configuration warning appears even when there was no configuration change after a reload.
CSCsq35527	When doing IGMP snooping, the ip-mcast might take longer to converge on an STP top change.
CSCsr36661	Static IGMP groups with PVLAN host ports are not restored after a reload.
CSCsv56881	Inconsistent behavior occurs when duplicate IPv4/IPv6 addresses are configured.
CSCsv81694	A flap occurs when the dynamically learned port removes the auto-learn static mac entry.

Table 5 Cisco NX-OS Release 5.1(3)N1(1) Open Caveats (continued)

Record Number	Open Caveat Headline
CSCsv93922	If the modules operator "(%)" is used in a FEX description, the **show** command will not display information correctly.
CSCsx35870	If the modules operator "(%)" is used in a FEX description, the **show** command will not display information correctly.
CSCta77490	When you quickly toggle the primary VLAN type, a failure of the type change occurs.
CSCtb58641	Entering the **clear mac-address** command did not delete a MAC address.
CSCtc04213	The VLAN configuration doesn't get applied on a range of interfaces.
CSCtc36397	A vPC role switchover does not occur when the vPC role is a primary operational role.
CSCtc44231	When a VLAN is deleted from the switch, the LACP port channels that have that VLAN set as a native VLAN fail to come-up.
CSCtd31131	This caveat was superseded by CSCtb70565.
CSCtf79253	Multiple alternate ports results in a root port failover and transient loops in a vPC topology.
CSCtg33706	This caveat was superseded by CSCtc91532.
CSCth69160	An SVI over a secondary PVLAN is not working.
CSCti86007	When a peer-link comes up and vPC ports are in the process of coming up, if a peer switch reboots, there is a small window where vPC ports don't come up due to the peer-link down status.
CSCtj85867	Entering the **show run** command is not displaying the switchport trunk VLAN list when a port profile is inherited.
SAN Switching	
CSCso46345	The i10K interop 4 mode is not supported.
CSCsq35728	When creating a SAN port channel, a MAP_PARAM_FROM_CHANNEL syslog message is displayed.
CSCsr28868	When you disable FCoE, the untagged Ethernet packet type 0000 shows CRC errors.
CSCsv19979	The speed should be configured manually for Fibre Channel ports in SD mode.
CSCsx80279	Addresses are not learned when egress interfaces are only FEX-facing ports.
CSCsy02439	An FC port error message displays occasionally.
CSCsy99816	The wrong FEX serial number does not show as an Identity-Mismatch in the output of the **show interface fex** command.
CSCtb61197	There are inconsistent SAN-port member states in the output of the **show interface** and **show san-port** commands.
CSCth98138	The command output for the **show fc-port-security** command for some virtual Fibre Channel interfaces is wrong.
CSCti99872	This caveat was superseded by CSCtr66343.
FCoE	

Table 5 Cisco NX-OS Release 5.1(3)N1(1) Open Caveats (continued)

Record Number	Open Caveat Headline
CSCtc77180	When you enable FCoE, ports are error-disabled.
CSCti87913	When you upgrade from NX-OS Release 4.2(1)N to NX-OS Release 5.0(2)N1(1), FLOGI fails after an ISSU.
CSCtq18819	The FCoE Manager does not respond on enabling feature fcoe and the port manager process fails.
Installation/Upgrade/Downgrade	
CSCtd15304	A successful reset occurred during the upgrade of Release 4.1(3)N1(1) to Release 4.1(3)N2(1) using Fabric Manager.
CSCtd70554	The fc-port-security configuration did not get converted when downgrading from NX-OS Release 4.1(3)N2(1) to NX-OS Release 4.1(3)N1(1).
CSCtf98638	During an ISSU, the following message appears: %SYSMGR-5-SUBPROC_KILLED “System Manager (core-client)”
Pre-Provisioning	
CSCti84186	The output of the **show run all** command shows an inconsistent configuration for the pre-provisioned interface.
Security	
CSCsq64251	A directed request does not work with TACACS+.
CSCsr20499	During a configuration restore to the running configuration from a configuration file using the **copy** *file* **running-config** command, the aclmgr may leak memory.
CSCsv39939	Incorrect values are displayed for the interface capabilities for ports on a Cisco Nexus 2000 Series Fabric Extender connected to a Cisco Nexus 5000 Series switch.
CSCsz82199	When priority-flow-control is disabled between two Cisco Nexus 5000 Series switches, std.pause (interface flowcontrol) configuration does not take affect.
CSCtc62994	When combining RBAC roles (multiple roles assigned to the same user account), interface policies in those roles aren't working on a per-role basis.
CSCti15226	On Cisco Nexus 5500 platform switches, no error is identified when you configure an ACL-based qos policy for class-fcoe.
CSCti61513	The **match ip rtp** command is not supported in the match-all class.
Configuration Rollback	
CSCti77835	A rollback fails to revert to the earlier VLAN configuration.
CSCti87532	A rollback fails when changes are made in the buffer-size for class-fcoe.
CSCti97003	A rollback fails and the output of the **show rollback log exec** command displays “Deletion of switch profile failed”.
CSCtj16996	A rollback fails when the switch profile configuration involves a conditional feature.

Table 5 Cisco NX-OS Release 5.1(3)N1(1) Open Caveats (continued)

Record Number	Open Caveat Headline
System Management	
CSCsm03765	You cannot assign an IP address on the mgmt0 interface using Device Manager.
CSCso74872	When two SNMP walks are started simultaneously, one of them may fail with the following error - 'OID not increasing'.
CSCsq57558	The software does not support an EISL encapsulation on an SD port (VFT cannot be preserved).
CSCsq76688	A CDP neighbor is not removed immediately after the port is shut down.
CSCsq90423	In NPV mode, EISL encapsulation for an SD port is not supported.
CSCsr68690	When egress SPAN is configured on a port that is transmitting jumbo or large frames, the spanned frames are truncated to 2384 bytes.
CSCsx40562	When using a FEX, the ACL drop traffic is not reaching the SPAN destination in certain configuration cases.
CSCsx59489	When the switch and FEX bootup after entering the **reload all** command, the time of event for any environment Call Home event, such as temperature alarm, power supply or fan alarms, is set to 1970.
CSCsz81365	Even after private-vlan mapping is removed on a trunk port using the **no switchport private-vlan mapping trunk** command, traffic received over the VLAN continues to be SPANed.
CSCtb53820	The monitor session goes to the error state with VSAN as a source after a reload.
CSCtb84512	In a mixed SPAN mode where Ethernet port channels, vFCs, and FC ports are span sources and an Ethernet interface is a SPAN destination, a vFC flap causes the traffic coming in on the Ethernet port channel not to be spanned.
CSCtb94310	Removing or adding a SAN port member causes a monitor session to go into an error state.
CSCti10941	The destination port is wrong in the **show interface brief** command output.
CSCtj53287	Traffic received over Fibre Channel ports cannot be monitored on SPAN.
CFS	
CSCsl73766	RADIUS configuration distribution via CFS is unsupported.
CSCsm16222	Roles configuration distribution via CFS is unsupported.
CSCsr35452	CFS-based distribution of the NTP peer configuration does not work.
CSCtb34546	Peer switches gets stuck in CFS discovery when you enter the **deny all ip pkts mgmt0** command.
Fabric Extender	
CSCsv15775	The priority-tagged frames on FEX ports get dropped.
CSCsv93263	FEX port configurations are lost when a configuration restore is done after a write erase and reload.

Table 5 Cisco NX-OS Release 5.1(3)N1(1) Open Caveats (continued)

Record Number	Open Caveat Headline
CSCsx68778	Flow control configuration on the FEX ports may fail when the **range** command is used with interfaces that are spread across FEXs.
CSCta04383	The FEX should automatically revert to an older image if a second switch boots with the same version.
Transceiver	
CSCsv00989	Transceiver details are read as zeros even on DOM-capable 1G SFPs.
CSCsv02866	The **show interface ethernet transceiver details** command may show "invalid calibration" for DOM supported 1 G SFPs.

Resolved Caveats—Cisco NX-OS Release 5.1(3)N1(1a) and Release 5.1(3)N1(1)

Table 6 lists the caveats that are resolved in Cisco NX-OS Release 5.1(3)N1(1a) and Release 5.1(3)N1(1). The caveats may be open in previous Cisco NX-OS releases.

Table 6 Cisco NX-OS Release 5.1(3)N1(1a) and Release 5.1(3)N1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCsu77946	You cannot unconfigure statistics from an ACL in a configuration session.
CSCtf32340	An error occurs while changing the VSAN and Interface scope of an existing role name.
CSCtg93294	A Cisco Nexus 5000 Series switch mgmt0 MAC address is not learned on its own VRF default interfaces.
CSCti34155	The output for the **show run ipqos all** command does not show the default queuing class map.
CSCti63620	An import has failed verification for channel-group member interfaces.
CSCtj19861	Shutting down nontrunking SAN port channel members takes more than 30 seconds.
CSCtj94130	The Layer 3 traffic over an MCT link has dropped.
CSCtl46093	OSPF does not come up with a Layer 3 interface MTU of 9000 because the supervisor MTU is 2000.
CSCtl56470	No IGMP configuration in the running configuration with VTP server or client.
CSCtl66943	DHCP validation errors have occurred in the PVLAN setup.
CSCtn40667	A FEX does not recover after a failed hitless upgrade during an ISSU.
CSCtq13290	VPC PO goes to FWD after ISSU with MST multiple regions configured.
CSCtq14143	If you enable Layer 3 routing after an ISSU upgrade, Layer 3 routing protocols do not come up until the switch reloads.
CSCtq54750	Layer 2 multicast traffic gets flooded when a Layer 3 link to the core is brought up.
CSCtq61472	HSRP virtual MAC address with static router CAM entry on listen in vPC setup.
CSCtq64880	Not able to reach VRRP HSRP virtual address from a Cisco Nexus 5000 Series switch vPC peer VLAN SVI.

Table 6 Cisco NX-OS Release 5.1(3)N1(1a) and Release 5.1(3)N1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtq79377	IGMP reports are going to the supervisor when IGMP is disabled on an SVI-enabled VLAN.
CSCtq98473	DCNM - snmpd core is generated while creating VFC interface from DM.
CSCtr47060	Support needed for management SVI on Cisco Nexus 5500 platforms.
CSCts06174	A Cisco Nexus 5000 Series switch reloads due to CDP packet with TLV with a null pointer (invalid).
CSCts38112	ETHPORT-3-IF_NON_CISCO_TRANSCEIVER: Non-Cisco for Tyco SFP-H10GB-CU3M error is observed.
CSCts46521	The IGMP process fails @ igmp_snoop_orib_fill_source_update.
CSCts70215	The switch reloads after twice removing the peer-gateway.
CSCtt04661	The port-profile process fails during a **copy running-config startup-config** command.
CSCtt10736	Traffic from a peer-link is dropped after a secondary reload and peer keepalive reconnect.
CSCtt94612	LACP core occurs due to a process failure on a Cisco Nexus 5010 switch during a AA/ST flex port flap.
CSCtu06674	Following the **shut** command on a vPC peer link, a VLAN interface on a secondary Cisco Nexus 5000 Series switch remains up.
CSCtu28167	NETSTACK-3-LOCK_STACK_FULL message in the log.
CSCtu59645	Make Release 4.2(1)N1(1) and 4.2(1)N2(x) to 5.1(3)N1(1) upgrade and downgrade disruptive.
CSCtw82571	On a Cisco Nexus 5010 or 5020 switch, VLAN membership is incorrect after upgrade to Release 5.1(3)N1(1).
CSCtw87601	Cannot configure IP prefix-list on a Cisco Nexus 5500 Series switch with Release 5.1(3)N1(1).
CSCtw88352	Cisco NX-OS Release 5.1(3) does not accept a subnet-mask ACL.
CSCtw76636	A delay during a vPC failover occurs with a reload of the primary switch.
CSCtw79225	Cannot manage switch via Telnet and the console after an upgrade to NX-OS Release 5.1(3)N1(1).
CSCtx03844	The **show hardware internal cpu-mac** command cannot be executed by the non-admin user.
CSCtx08585	All ACE protocols other than ICMP, IGMP, TCP, UDP, and IP are displayed as IP protocols.
CSCtx09587	The hardware clock is missing in NX-OS Release 5.1(3)N1(1).
CSVtx11573	A process failure occurs in /isan/bin/port_mgr.
CSCtx15807	The Smart Call Home feature on the Cisco Nexus 5500 Series in not sending SMTP email notification.
CSCtx33661	The “VSAN not present” message is received during zone set activation from Cisco DCNM.
CSCtx35237	Following an upgrade to NX-OS Release 5.1(3)N1(1), there is a FWM failure.

Table 6 Cisco NX-OS Release 5.1(3)N1(1a) and Release 5.1(3)N1(1) Resolved Caveats

Record Number	Resolved Caveat Headline
CSCtx41358	Fabricpath: BPDUs are not sent from a vPC secondary upon link failure.
CSCtx45802	PLOGI to name server was dropped on Cisco Nexus 5500 Series with unified port (UP) switches.
CSCtx50264	A port profile that is inherited on a FEX interface using configuration sync causes the port-profile process to fail.
CSCtx62699	A Cisco Nexus 5000 Series switch running NX-OS Release 5.1(3)N1(1) might fail in the CDP process.
CSCtx64132	A username cannot be added or deleted.
CSCtx78040	A port profile hap reset occurs after a port channel is created with the force option.

Related Documentation

Documentation for Cisco Nexus 5000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders is available at the following URL:

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

The following are related Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Fabric Extender documents:

Release Notes

Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes

Cisco Nexus 5000 Series Switch Release Notes

Configuration Guides

Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 5.1(3)

Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 5.0(2)N1(1)

Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 4.2(1)N1(1) and Release 4.2(1)N2(1)

Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide

Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide

Cisco Nexus 5000 Series NX-OS Multicast Routing Configuration Guide

Cisco Nexus 5000 Series NX-OS Quality of Service Configuration Guide

Cisco Nexus 5000 Series NX-OS SAN Switching Configuration Guide

Cisco Nexus 5000 Series NX-OS Security Configuration Guide

Cisco Nexus 5000 Series NX-OS System Management Configuration Guide

Cisco Nexus 5000 Series NX-OS Unicast Routing Configuration Guide

Cisco Nexus 5000 Series Switch NX-OS Software Configuration Guide

Cisco Nexus 5000 Series Fabric Manager Configuration Guide, Release 3.4(1a)

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

Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide

Maintain and Operate Guides

Cisco Nexus 5000 Series NX-OS Operations Guide

Installation and Upgrade Guides

Cisco Nexus 5000 Series and Cisco Nexus 5500 Platform Hardware Installation Guide

Cisco Nexus 2000 Series Hardware Installation Guide

Cisco Nexus 5000 Series NX-OS Software Upgrade and Downgrade Guide

Regulatory Compliance and Safety Information for the Cisco Nexus 5000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders

Licensing Guide

Cisco NX-OS Licensing Guide

Command References

Cisco Nexus 5000 Series Command Reference

Technical References

Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Fabric Extender MIBs Reference

Error and System Messages

Cisco NX-OS System Messages Reference

Troubleshooting Guide

Cisco Nexus 5000 Troubleshooting Guide

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:

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

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

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)

©2012 Cisco Systems, Inc. All rights reserved.