



Cisco Nexus 1000V Release Notes, Release 4.0(4) SV1(3a)

Updated: June 23, 2011
OL-23098-01-G0

This document describes the features, limitations, and caveats for the Cisco Nexus 1000V software Release 4.0(4) SV1(3b). Use this document in combination with documents listed in the “[Available Documents](#)” section on page 12. The following is the change history for this document.

Part Number	Revision	Date	Description
OL-21663-01	A0	7/23/10	Created release notes for Release 4.0(4) SV1(3b).
	B0	8/23/10	Added open caveat CSCth99337 .
	C0	9/16/10	Added open caveat CSCti62879 .
	D0	9/17/10	Added open caveat CSCth01949 .
	G0	11/10/10	Moved CSCtg79060 from resolved to open caveat.

Contents

This document includes the following sections:

- [Introduction](#), page 2
- [Software Compatibility](#), page 2
- [New and Changed Information](#), page 2
- [Limitations and Restrictions](#), page 2
- [Caveats](#), page 10
- [Available Documents](#), page 12
- [Obtaining Documentation and Submitting a Service Request](#), page 13



[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

Introduction

The Cisco Nexus 1000V provides a distributed, layer 2 virtual switch that extends across many virtualized hosts. The Cisco Nexus 1000V manages a data center defined by the vCenter Server. Each server in the data center is represented as a line card in Cisco Nexus 1000V and can be managed as if it were a line card in a physical Cisco switch.

Cisco Nexus 1000V consists of the following two components:

- Virtual Supervisor Module (VSM), which contains the Cisco CLI, configuration, and high-level features.
- Virtual Ethernet Module (VEM), which acts as a line card and runs in each virtualized server to handle packet forwarding and other localized functions.

Software Compatibility

The servers that run the Cisco Nexus 1000V VSM and VEM must be in the VMware Hardware Compatibility list. This is a requirement for running the ESX 4.0 software.

For additional compatibility information, see the *Cisco Nexus 1000V Compatibility Information, Release 4.0(4)SV1(3b)*.

New and Changed Information

This section provides the following information about this release:

- [Changed Software Features, page 2](#)
- [New Software Features, page 2](#)

Changed Software Features

No software features were changed in this release.

New Software Features

No new software features were added in this release.

Limitations and Restrictions

The Cisco Nexus 1000V has the following limitations and restrictions:

- [Configuration Limits, page 3](#)
- [Vmotion of VSM, page 4](#)
- [VMware Lab Manager, page 4](#)
- [Virtual Service Domain, page 5](#)

[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

- [Upgrade, page 5](#)
- [Access Lists, page 6](#)
- [NetFlow, page 6](#)
- [Port Security, page 6](#)
- [Port Profile, page 7](#)
- [Telnet Enabled by Default, page 7](#)
- [SSH Support, page 7](#)
- [Cisco NX-OS Commands May Differ from Cisco IOS, page 7](#)
- [Layer 2 Switching, page 7](#)
- [Cisco Discovery Protocol, page 8](#)
- [DHCP Not Supported for the Management IP, page 9](#)
- [LACP, page 9](#)
- [MTU Mismatch After ESX Reboot, page 9](#)

Configuration Limits

The Cisco Nexus 1000V has the following configuration limits shown in [Table 1](#):

Table 1 Configuration Limits for Cisco Nexus 1000V

Component	Supported Limit	
Maximum Modules	66	
Virtual Ethernet (VEM)	64	
Virtual Supervisor (VSM)	2	
Hosts	64	
Active VLANs across all VEMs	512	
MACs over VLAN within a VEM	1024 (1K)	
vEthernet interfaces per port profile	1024 (1K)	
PVLAN	512	
Distributed Virtual Switches (DVS) per vCenter	12	
	Per DVS	Per Host
Virtual Service Domains (VSDs)	64	6
VSD interfaces	2048	214
vEthernet interfaces	2K	216
Port profiles	256	—
System port profiles	—	16
Port channel	256	8
Physical trunks	512	—
Physical NICs	—	32

[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

Table 1 Configuration Limits for Cisco Nexus 1000V (continued)

Component	Supported Limit	
vEthernet trunks	256	8
ACL	128	16 ¹
ACEs per ACL	128	16 ¹
ACL Interfaces	2048	256
NetFlow policies	32	8
NetFlow interfaces	256	32
SPAN/ERSPAN sessions	64	4
QoS policy map	128	16
QoS class map	1024	128
QoS interfaces	2048	256
Port security	1600	216
MultiCast groups	512	64

1. This number can be exceeded if VEM has available memory.

Vmotion of VSM

Vmotion of VSM has the following limitations and restrictions:

Vmotion of a VSM is supported for both the active and standby VSM VMs. For high availability, it is recommended that the active VSM and standby VSM reside on separate hosts. To achieve this, and prevent a host failure resulting in the loss of both the active and standby VSM, it is recommended that distributed resource scheduling (DRS) be disabled for both the active and standby VSMs.

If you do not disable DRS, then you must use the VMware anti-affinity rules to ensure that the two virtual machines are never on the same host, and that a host failure cannot result in the loss of both the active and standby VSM.

- VMware Vmotion does not complete when using an open virtual appliance (OVA) VSM deployment if the ISO is still mounted. To complete the Vmotion, either click **Edit Settings** on the VM to disconnect the mounted ISO, or power off the VM. No functional impact results from this limitation.

VMware 4.0 to 4.1 Online Bundle Missing From Online Portal

The software package for upgrading from VMware 4.0 to 4.1 is not available from the VMware online portal. For this reason, VUM does not automatically download the VIB from the VMware online portal. To upgrade from VMware 4.0 to 4.1, you must first import the offline bundle (ESX 4.1 and Cisco Nexus 1000V VIB) into VUM.

VMware Lab Manager

VMware Lab Manager does not support using the Cisco Nexus 1000V.

Send document comments to nexus1k-docfeedback@cisco.com.

Virtual Service Domain

The Virtual Service Domain (VSD) has the following limitations and restrictions:

- Vmotion is not supported for the service virtual machine (SVM) and should be disabled.
- To prevent loops in the network, configure the following before assigning an SVM to a port profile on the vCenter Server:
 - Inside port
 - Outside port
 - VSD
- To prevent it from flooding the network with packets, make sure to configure the inside or outside VSD port profile with a service port.
- To prevent loops in the network, when making any changes to the SVM port profile, do the following:
 - First shut down the SVM.
 - Make the changes to the SVM port profile.
 - Verify that the changes to the SVM port profile were applied.
 - Restart the SVM.
- You must remove the control and packet VLANs from the allowed VLAN lists for an inside or outside VSD port profile, such as that used for Vshield.

For more information about VSD, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)*.

Upgrade

Upgrading the software has the following limitations and restrictions:

- After the VSM feature support level is upgraded to support features in the new release, you cannot downgrade it again to a previous release.
- Connectivity to the VSM can be lost during a VEM upgrade when the VSM VM interfaces connect to its own DVS.
- Connectivity between the active and standby VSM can be lost during a VEM upgrade when the VEM that is being upgraded provides interface connectivity to one of the VSMs in the pair. In this case, both VSMs become active and lose connectivity. Use the following workaround:
 - Power off the VSM that is connected to the VEM.
 - Manually upgrade the VEM that provides interface connectivity to one VSM in the pair.
- If you use a proxy server to connect VMware Update Manager (VUM) to the Internet, you may need to disable the proxy before starting a VUM upgrade of your VEMs. In the VMware versions before VUM Update 1, the proxy prevents VUM from communicating locally with the VSM. Automatic VEM upgrades may fail if the proxy is not disabled first.

For more information about upgrades, see the *Cisco Nexus 1000V Software Upgrade Guide, Release 4.0(4)SV1(3b)*.

Send document comments to nexus1k-docfeedback@cisco.com.

Access Lists

ACLs have the following limitations and restrictions:

Limitations:

- IPV6 ACL rules are not supported.
- VLAN-based ACLs (VACLs) are not supported.
- ACLs are not supported on port channels.

Restrictions:

- IP ACL rules do not support the following:
 - fragments option
 - addressgroup option
 - portgroup option
 - interface ranges
- Control VLAN traffic between the VSM and VEM does not go through ACL processing.

NetFlow

The NetFlow configuration has the following support, limitations, and restrictions:

- Layer 2 match fields are not supported.
- NetFlow Sampler is not supported.
- NetFlow Exporter format V9 is supported
- NetFlow Exporter format V5 is not supported.
- Multicast traffic type is not supported. Cache entries are created for multicast packets, but the packet/byte count does not reflect replicated packets.
- NetFlow is not supported on port channels.

The NetFlow cache table has the following limitation:

- Immediate and permanent cache types are not supported.



Note The cache size that is configured using the CLI defines the number of entries, not the size in bytes. The configured entries are allocated for each processor in the ESX host and the total memory allocated depends on the number of processors.

Port Security

Port security has the following support, limitations, and restrictions:

- Port security is enabled globally by default.
The **feature/no feature port-security** command is not supported.
- In response to a security violation, you can shut down the port.

[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

- The port security violation actions that are supported on a secure port are **Shutdown** and **Protect**. The **Restrict** violation action is not supported.
- Port security is not supported on the PVLAN promiscuous ports.

Port Profile

Port profiles have the following restrictions or limitations:

- If you attempt to remove a port profile that is in use, that is, one that has already been auto-assigned to an interface, the Cisco Nexus 1000V generates an error message and does not allow the removal.
- When you remove a port profile that is mapped to a VMware port group, the associated port group and settings within the vCenter Server are also removed.
- Policy names are not checked against the policy database when ACL/NetFlow policies are applied through the port profile. It is possible to apply a nonexistent policy.

Telnet Enabled by Default

The Telnet server is enabled by default.

For more information about Telnet, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)*.

SSH Support

Only SSH version 2 (SSHv2) is supported.

For more information, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)*.

Cisco NX-OS Commands May Differ from Cisco IOS

Be aware that the Cisco NX-OS CLI commands and modes may differ from those used in the Cisco IOS software.

For information about CLI commands, see the *Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)*.

For more information about the CLI command modes, see the *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(3)*.

Layer 2 Switching

This section lists the Layer 2 switching limitations and restrictions and includes the following topics:

- [No Spanning Tree Protocol, page 8](#)
- [MAC Address Table, page 8](#)
- [Maximum Allowed VLANs and MAC Addresses per VLAN, page 8.](#)

For more information about Layer 2 switching, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(3)*.

[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

No Spanning Tree Protocol

The Cisco Nexus 1000V forwarding logic is designed to prevent network loops so it does not need to use the Spanning Tree Protocol. Packets that are received from the network on any link connecting the host to the network are not forwarded back to the network by the Cisco Nexus 1000V.

MAC Address Table

In the MAC address table, the forwarding table for each VLAN in a VEM can store up to 1024 MAC addresses.

For more information about the Cisco Nexus 1000V MAC address table, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(3)*.

Maximum Allowed VLANs and MAC Addresses per VLAN

Table 1-2 lists the allowable number of VLANs and MAC addresses per VLAN that can be configured.

Table 1-2 Allowable VLANs and MAC Addresses Per VLAN

Feature	Maximum Limit
VLANs across all VEMs	512
MAC addresses per VLAN within a VEM	1024 (1K)

For more information about the Cisco Nexus 1000V VLAN configuration, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(3)*.

Cisco Discovery Protocol

The Cisco Discovery Protocol (CDP) is enabled globally by default.

CDP runs on all Cisco-manufactured equipment over the data link layer and does the following:

- Advertises information to all attached Cisco devices.
- Discovers and views information about those Cisco devices.
 - CDP can discover up to 256 neighbors per port if the port is connected to a hub with 256 connections.

If disabled globally, then CDP is also disabled for all interfaces.

For more information about the Cisco Discovery Protocol, see the *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)*.

Send document comments to nexus1k-docfeedback@cisco.com.

DHCP Not Supported for the Management IP

DHCP is not supported for the management IP. The management IP must be configured statically.

LACP

The Link Aggregation Control Protocol (LACP) is an IEEE standard protocol that aggregates Ethernet links into an EtherChannel.

Cisco Nexus 1000V has the following restrictions for enabling LACP on ports carrying the Control and Packet VLANs:



Note

These restrictions do not apply to other data ports using LACP.

- At least two ports must be configured as part of the LACP channel.
- The upstream switch ports must be configured in spanning-tree portfast mode. The LACP negotiation causes upstream switch ports to bounce, as per protocol, before starting the port aggregation process.

Without spanning-tree portfast on upstream switch ports, it takes approximately 30 seconds to recover these ports on the upstream switch. Because these ports are carrying control and packet VLANs, VSM loses connectivity to the VEM.

The following commands are available to use on Cisco upstream switch ports in interface configuration mode:

spanning-tree portfast

spanning-tree portfast trunk

spanning-tree portfast edge trunk

MTU Mismatch After ESX Reboot

If you use an MTU other than 1500 (the default) for a physical NIC attached to the Cisco Nexus 1000V, then reboots of the ESX can result in a mismatch with the VMware kernel NIC and failure of the VSM and VEM. For example, in networks that use jumbo frames, you may manually configure an MTU of other than 1500. During a power cycle, the ESX reboots and the MTU of the physical NIC reverts to the default of 1500 but the VMware kernel NIC does not. To prevent this mismatch and preserve the MTU for the physical NIC across reboots of the ESX, you must configure the system MTU in the system port profile.

For information about configuring MTU in the system port profile, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)*.

For information about recovering from a loss of connectivity due to an MTU mismatch, see the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(3)*.

[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

Caveats

This section includes the following topics:

- [Open Caveats, page 10](#)
- [Resolved Caveats, page 11](#)

Open Caveats

The following are descriptions of the caveats in Cisco Nexus 1000V Release 4.0(4) SV1(3b). The ID links you into the Cisco Bug Toolkit.

ID	Open Caveat Headline
1. CSCsy15485	Domain ID change reboots primary active VSM.
2. CSCta09184	The show policy-map and show class-map commands are not compatible with XML API.
3. CSCta63359	Show interface show 10M when using Virtual Connect.
4. CSCte55714	Unable to change the service port action from forward to drop.
5. CSCte99459	VSM shows IGMP querier router port as the port of SVM.
6. CSCtf70582	Improve the error messages for VEM upgrades via VUM.
7. CSCtf75345	When the mode is changed from Layer 2 to Layer 3 without removing the hosts from VC, one of the ports in the LACP channel goes to suspended state.
8. CSCtg03760	Active VLANs on VSM programmed on VEM - post link flap.
9. CSCtg06894	Upgrade to software Release 4.0(4)SV1(3) may fail if you load Release 4.0(4)SV1(2) first immediately followed by Release 4.0(4)SV1(3).
10. CSCtg22241	VSM interfaces down on standby VSM VM NICs flap.
11. CSCtg37769	IGMP Leave message is not processed by VSM on switchover after 5 minutes.
12. CSCtg46514	LACP channel not formed during shut and no shut on upstream switch.
13. CSCtg79060	Virtual ports not pinned.
14. CSCtg82051	SNMP polling for certain MIBs may timeout on Cisco Nexus 1000V.
15. CSCth01949	pNIC ports missing from BD/DR during reconnect.
16. CSCth30738	Memory corrupted during Layer 3 Control setup with VLAN 1.
17. CSCth31100	Ethernet interfaces are not formed when module is attached.

Send document comments to nexus1k-docfeedback@cisco.com.

ID	Open Caveat Headline
18. CSCth46091	VSM is not receiving VMotion event during VEM migration.
19. CSCth72604	VEM Module is disconnected from VSM after upgrade.
20. CSCth76634	LACP member port goes into suspended state after VSM reload.
21. CSCth96579	Cisco Nexus 5000 vPC must be configured in specific sequence for LACP port channel to function on Cisco Nexus 1000V.
22. CSCth98132	Packet VLAN must be a system VLAN for LACP to function, even in L3 mode.
23. CSCth99230	Modules bounce after adding multiple modules to a DVS simultaneously.
24. CSCth99337	Host disconnect or PSOD on removal of KL.next beta host from DVS.
25. CSCti62879	vEth ports on VSM out of sync with VEMs after upgrade.

Resolved Caveats

The following are descriptions of caveats that were resolved in Cisco Nexus 1000V Release 4.0(4) SV1(3b). The ID links you into the Cisco Bug Toolkit.

ID	Resolved Caveat Headline
1. CSCtb29215	The interface MIB does not display the control 0 interface.
2. CSCtf07382	The port profile FSM gets stuck while processing interface addresses.
3. CSCtf71880	The Cisco Nexus 1000V removes the 1q tag from packets which are dropped by the host.
4. CSCtg43391	Modules do not come up after shut/no shut on upstream port channel.
5. CSCtg46327	High Availability VSM redundancy driver (breakage) mismatch.
6. CSCtg49628	License system message updated.
7. CSCtg72137	VM traffic affected on VLANs; DR points at member.
8. CSCtg93995	Cisco Nexus 1000V port security error.
9. CSCth06558	Adding host causes ESX failure.
10. CSCth08677	ACL fails when applying QoS on port channel interface.
11. CSCth19998	Host ID not cleared.
12. CSCth22183	Private VLAN port says down (primary vlan is down).

Send document comments to nexus1k-docfeedback@cisco.com.

ID	Resolved Caveat Headline
13. CSCth37319	SNMP fails while reading corrupted PCM shared DB.
14. CSCth43614	Opaque data is sent without system port profiles
15. CSCth46897	NetFlow byte count is not correctly reflected in NetFlow Exporter tools.
16. CSCth48862	Private VLAN trunks do not trunk new VLANs without port
17. CSCth51527	Corrupt PCM SDB caused SNMP to fail.
18. CSCth53649	VEM may drop Cisco Nexus 1000V ARP request from VM.
19. CSCth54621	iSCSI Multipath setup on host fails in ESX/ESXi 4.0.
20. CSCth63194	VEM removal after channel port failure with Layer 3 Control configuration.
21. CSCth84295	File descriptor leak in interface MIB function.
22. CSCth86555	VSM and VEM are out of sync, VEM in headless mode and module online on VSM.

Available Documents

The following documents are used with the Cisco Nexus 1000 and are available on [Cisco.com](http://www.cisco.com) at the following url:

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

General Information

[Cisco Nexus 1000V Documentation Roadmap, Release 4.0\(4\)SV1\(3a\)](#)

[Cisco Nexus 1000V Release Notes, Release 4.0\(4\)SV1\(3a\)](#)

[Cisco Nexus 1000V Compatibility Information, Release 4.0\(4\)SV1\(3a\)](#)

[Cisco Nexus 1010 Management Software Release Notes, Release 4.0\(4\)SP1\(1\)](#)

Install and Upgrade

[Cisco Nexus 1000V Virtual Supervisor Module Software Installation Guide, Release 4.0\(4\)SV1\(3a\)](#)

[Cisco Nexus 1000V Software Upgrade Guide, Release 4.0\(4\)SV1\(3a\)](#)

[Cisco Nexus 1000V VEM Software Installation and Upgrade Guide, Release 4.0\(4\)SV1\(3a\)](#)

[Cisco Nexus 1010 Virtual Services Appliance Installation Guide](#)

Configuration Guides

[Cisco Nexus 1000V License Configuration Guide, Release 4.0\(4\)SV1\(3\)](#)

[Cisco Nexus 1000V Getting Started Guide, Release 4.0\(4\)SV1\(3\)](#)

[Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.0\(4\)SV1\(3\)](#)

Send document comments to nexus1k-docfeedback@cisco.com.

Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)
Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(3)
Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)
Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.0(4)SV1(3)
Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)
Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)
Cisco Nexus 1010 Software Configuration Guide, Release 4.0(4)SP1(1)

Programming Guide

Cisco Nexus 1000V XML API User Guide, Release 4.0(4)SV1(3)

Reference Guides

Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)
Cisco Nexus 1000V MIB Quick Reference
Cisco Nexus 1010 Command Reference, Release 4.0(4)SP1(1)

Troubleshooting and Alerts

Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(3a)
Cisco Nexus 1000V Password Recovery Guide
Cisco NX-OS System Messages Reference

Network Analysis Module Documentation

Cisco Network Analysis Module Software Documentation Guide, 4.2
Cisco Nexus 1000V NAM Virtual Service Blade Installation and Configuration Guide
Network Analysis Module Command Reference Guide, 4.2
User Guide for the Cisco Network Analysis Module Virtual Service Blades, 4.2
Cisco Network Analysis Module Software Release Notes, 4.2

Obtaining Documentation and Submitting a Service Request

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

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

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

Send document comments to nexus1k-docfeedback@cisco.com.

This document is to be used in conjunction with the documents listed in the "Available Documents" section.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

Internet Protocol (IP) addresses used in this document are for illustration only. Examples, command display output, and figures are for illustration only. If an actual IP address appears in this document, it is coincidental.

© 2010 Cisco Systems, Inc. All rights reserved.