



Cisco Nexus 1000V Release Notes, Release 4.0(4)SV1(2)

Updated: June 23, 2011
OL-20454-01-G0

This document describes the features, limitations, and caveats for the Cisco Nexus 1000V Release 4.0(4)SV1(2) software. Use this document in combination with documents listed in the [“Related Documentation”](#) section on page 16.

Table 1 shows the online change history for this document.

Table 1

Part Number	Revision	Date	Description
OL-20454-01	A0	December 21, 2009	Created release notes for Release 4.0(4)SV1(2).
	B0	February 15, 2010	<ul style="list-style-type: none">Added a statement under Limitations and Restrictions about completing VMotion when using OVA VSM installation.Added open Caveat CSCtc28866.
	C0	February 18, 2010	Added resolved Caveat CSCtc34170.
	D0	March 08, 2010	Revised the restriction for using VMotion and DRS.
	E0	March 22, 2010	Added resolved Caveat CSCtf43373.
	F0	April 14, 2010	<ul style="list-style-type: none">Added VMware Lab Manager limitation.Added NetFlow limitation on port channels.Added ACL limitation on port channels.
	G0	August 23, 2010	Added open caveat CSCth99337.



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

Contents

This document includes the following information about the Cisco Nexus 1000V Release 4.0(4)SV1(2) software.

- [Introduction, page 2](#)
- [Software Compatibility, page 2](#)
- [New and Changed Information, page 2](#)
- [Limitations and Restrictions, page 7](#)
- [Caveats, page 14](#)
- [Related Documentation, page 16](#)

Introduction

The Cisco Nexus 1000V provides a distributed, layer 2 virtual switch that extends across many virtualized hosts. The Cisco Nexus 1000V manages a Datacenter defined by the vCenter Server. Each server in the Datacenter 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 running 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(2)*

New and Changed Information

This section provides the following information about this release:

- [Changed Software Features, page 2](#)
- [New Software Features, page 4](#)

Changed Software Features

The following software features are changed in this release:

- [Removal of the Capability Uplink Command, page 3](#)

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

- [Evaluation Licenses, page 3](#)
- [Interface Rate Statistics, page 3](#)
- [vPC-HM, page 3](#)

Removal of the Capability Uplink Command

The **capability uplink** command is removed from the port profile configuration in this release. A port profile used as an uplink is now designated as **type ethernet** instead.

When you upgrade the software, existing uplink port profiles are automatically changed to Ethernet type port profiles.

Evaluation Licenses

The Cisco Nexus 1000V software includes an evaluation license for 16 CPU sockets that are valid for a period of 60 days. The evaluation period starts when you install or upgrade the software. These evaluation licenses are only used if you do not have permanent licenses installed. When you install permanent licenses, the evaluation licenses are no longer used.

If you have evaluation licenses installed when you upgrade your software, they are invalidated.

If the 60 day evaluation period ends before you install permanent licenses, all VEMs become unlicensed.



Note

Service Disruption—When VEMs are unlicensed, the vEthernet interfaces on the VEMs are removed from service and the traffic flowing to them from virtual machines is dropped. This traffic flow is not resumed until you add a permanent license file with licenses for the VEMs.

For more information, see the *Cisco Nexus 1000V License Configuration Guide, Release 4.0(4)SV1(2)*.

Interface Rate Statistics

The following commands are changed to display 5 minute input and output packet or bit rate statistics for Ethernet and vEthernet interfaces.

- **show interface ethernet**
- **show interface vethernet**

For more information, see the *Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(2)*.

vPC-HM

Virtual port channel host mode (vPC-HM) is changed as follows:

- Member ports in a port channel can connect to more than two upstream switches.
- Ports can be grouped into 32 subgroups (0–31) for traffic separation.
- The following command is added to the CLI for creating subgroups:
 - **channel-group auto mode on [sub-group {cdp | manual}] [mac-pinning]**
- Static pinning is added. For more information, see the “[Static Pinning](#)” section on page 6.

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

New Software Features

The following software features are new in this release:

- [GUI Configuration Set Up, page 4](#)
- [Layer 3 Control, page 4](#)
- [Virtual Service Domain, page 5](#)
- [iSCSI Multipath, page 5](#)
- [XML API, page 5](#)
- [DHCP Snooping, page 6](#)
- [Dynamic ARP Inspection, page 6](#)
- [IP Source Guard, page 6](#)
- [MAC Pinning, page 6](#)
- [Static Pinning, page 6](#)
- [IPv6 Support, page 7](#)

GUI Configuration Set Up

A GUI is provided for initial configuration of the VSM after installing the software. The GUI streamlines your configuration of the following:

- Create the SVS connection between the VSM and vCenter, and the resulting connection to the DVS.
- Create the following VMware port groups:
 - Control port profile
 - Packet port profile
 - Management port profile
- Create the following VLANs:
 - Control VLAN
 - Packet VLAN
 - Management VLAN
- Enable SSH and configure an SSH connection.
- Create a Cisco Nexus 1000V plug-in and register it on the vCenter server.
- Power off and then restart the VSM.

Layer 3 Control

With Layer 3 control, a VSM can be Layer 3 accessible and control hosts that reside in a separate Layer 2 network. All hosts controlled by a VSM, however, must still reside in the same Layer 2 network. Since a VSM cannot control a host that is outside of the Layer 2 network it controls, the host on which it resides must be controlled by another VSM.

For more information about Layer 3 control, see the following documents:

- *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(2)*
- *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)*

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

Virtual Service Domain

Virtual service domains (VSDs) allow you to classify and separate traffic for network services.

Interfaces within a VSD are shielded by a service VM (SVM) that provides a specialized service like a firewall, deep packet inspection (application aware networking), or monitoring.

Each Service VM has three virtual interfaces:

Interface	Description
Management	A regular interface that manages the SVM Should have Layer 2 or Layer 3 connectivity, depending on its use.
Incoming	Guards the traffic coming into the VSD Any packet coming into the VSD must go through this interface.
Outgoing	Guards the traffic going out of the VSD. Any packet that originates in the VSD and goes out must go through the SVM and out through the outgoing interface.

There is no source MAC learning on these interfaces.

For more information about virtual service domains, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(2)*.

iSCSI Multipath

The iSCSI multipath feature sets up multiple routes between a server and its storage devices for maintaining a constant connection and balancing the traffic load. The multipathing software handles all input and output requests and passes them through on the best possible path.

For more information about the iSCSI Multipath feature, see the *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(2)*.

XML API

The Xtensible markup language (XML) application programming interface (API) lets you quickly develop client applications to manage and monitor the Cisco Nexus 1000V.

Client applications encode requests in XML API tags sent to the device over secure SSH connections.

For more information about the XML API, see the *Cisco Nexus 1000V XML API User Guide, Release 4.0(4)SV1(2)*

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

DHCP Snooping

DHCP snooping acts like a firewall between untrusted hosts and trusted DHCP servers and functions as follows:

- Validates DHCP messages received from untrusted sources and filters out invalid response messages from DHCP servers.
- Builds and maintains a database of information about untrusted hosts with leased IP addresses.
- Uses this database to validate subsequent requests from untrusted hosts.

Dynamic ARP inspection (DAI) and IP Source Guard also use information stored in the DHCP snooping database. For more information about DHCP snooping, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(2)*.

Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) validates ARP requests and responses and functions as follows:

- Intercepts all ARP requests and responses on untrusted ports.
- Verifies that a packet has a valid IP-to-MAC address binding before updating the ARP cache or forwarding the packet.
- Drops invalid ARP packets.

DAI determines the validity of an ARP packet using the DHCP snooping database.

For more information about DAI, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(2)*.

IP Source Guard

IP Source Guard filters traffic on interfaces and only permits traffic whose IP and MAC address matches that in the DHCP snooping database or static IP source entries that you configure.

MAC Pinning

If one or more upstream switches do not support port channels, you can use MAC pinning to assign each Ethernet port member to a particular port channel subgroup. There are a maximum of 32 subgroups, so a maximum of 32 Ethernet port members can be assigned.

For more information, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)*.

Static Pinning

You can use vPC-HM to configure a port channel subgroup so that traffic is forwarded only through its member ports by assigning (or pinning) one of the following to the subgroup:

- vEthernet interface
- Control VLAN
- Packet VLAN

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

For more information, see the following documents:

Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2).

Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(2).

IPv6 Support

Support for IPv6 is added for the following:

- mgmt0 interface
- SNMP
- Syslog

For more information, see the following document:

Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(2)

Limitations and Restrictions

- [Configuration Limits, page 8](#)
- [Vmotion of VSM, page 9](#)
- [VMware Lab Manager, page 9](#)
- [Virtual Service Domain, page 9](#)
- [Upgrade, page 10](#)
- [Access Lists, page 10](#)
- [Netflow, page 10](#)
- [Port Security, page 11](#)
- [Port Profile, page 11](#)
- [Telnet Enabled by Default, page 11](#)
- [SSH Support, page 11](#)
- [Cisco NX-OS Commands May Differ from Cisco IOS, page 12](#)
- [Layer 2 Switching, page 12](#)
- [Cisco Discovery Protocol, page 13](#)
- [DHCP Not Supported for the Management IP, page 13](#)
- [LACP, page 13](#)

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

Configuration Limits

Use the following configuration limits with 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 (VSD)	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
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.

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

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 installation, 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. There is no functional impact resulting from this limitation.

VMware Lab Manager

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

Virtual Service Domain

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, the following should be configured before assigning a service virtual machine (SVM) to a port profile on vCenter:
 - 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 service virtual machine (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.
- The control and packet VLANs must be removed 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(2)*.

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

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, it cannot be downgraded 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 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 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 VUM to the Internet, you may need to disable the proxy before starting a VUM upgrade of your VEMs. Because in 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(2)*.

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, limitation, and restrictions:

- L2 match fields are not supported.
- Netflow Sampler is not supported.
- Netflow Exporter format V9 is supported
- Netflow Exporter format V5 is not supported.

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

- Multicast traffic type is not supported. Cache entries are created for multicast packets but 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 configured using the CLI defines the number of entries and 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:

- The Port Security feature is enabled globally by default. The CLI command `feature/no feature port-security` is not supported.
- In response to a security violation, you can shut down the port
- 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 port profile. It is possible to apply a non-existent 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(2)*.

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(2)*.

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

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 Cisco IOS.

For information about CLI commands, see the *Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(2)*.

For information about the CLI command modes, see the *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(2)*

Layer 2 Switching

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

- [No Spanning Tree Protocol, page 12](#)
- [MAC Address Table, page 12](#)
- [Maximum Allowed VLANs and MAC Addresses per VLAN, page 12.](#)

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

No Spanning Tree Protocol

Its forwarding logic is designed to prevent network loops so the Cisco Nexus 1000V does not need to participate in Spanning Tree Protocol. Packets 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

The following are limitations and restrictions for the MAC address table:

- The forwarding table for each VLAN in a VEM can store up to 1024 MAC addresses.

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

Maximum Allowed VLANs and MAC Addresses per VLAN

The following are the allowable number of VLANs and MAC addresses per VLAN that can be configured:

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

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

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

Cisco Discovery Protocol

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 Cisco Discovery Protocol, see the *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(2)*.

DHCP Not Supported for the Management IP

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

LACP

Link Aggregation Control Protocol 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 switchports to bounce as per protocol before starting the port aggregation process.

Without spanning-tree portfast on upstream switch ports, it takes ~30 seconds to recover these ports on the upstream switch, and since they 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
```

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

Caveats

This section includes the following topics:

- [Open Caveats, page 14](#)
- [Resolved Caveats, page 15](#)

Open Caveats

The following is a list of open caveats in Cisco Nexus 1000V Release 4.0(4)SV1(2). The Bug ID links you into the Cisco Bug Toolkit.

Bug ID	Caveat Headline
CSCsq66077	Shutting an Ethernet interface in Cisco Nexus 1000V VSM is not reflected in the Cat6K.
CSCsw32257	Shutting down a VSM vEthernet interface is not reflected in the VM.
CSCsw49458	A change to the speed or duplex settings on a physical NIC causes module flap.
CSCsx11210	Unable to add match criteria in a QoS class map after changing to match-any .
CSCsy88176	Inaccurate show policy-map interface output if there are numerous policy-maps
CSCsz21693	Reload of iVISOR host removes the VIB package.
CSCsz48343	Link up message while powering up VM (vnic not up)
CSCta03484	Loss of connectivity to vSphere when cloning multiple VMs.
CSCta09184	The show policy-map and show class-map commands are not compatible with XML API.
CSCta29037	The vihostupdate command prevents the installation of multiple bundles.
CSCta97063	VUM cannot be configured to use the proxy for VMware patch URLs instead of the proxy for VSM.
CSCtb29215	The control 0 interface is not shown in the IFMIB.
CSCtb64596	XML API output is invalid for IGMP snooping show commands.
CSCtc05201	A network failure during a VUM upgrade causes the upgrade to fail.
CSCtc18601	Atomic change of a physical NIC portgroup results in module removal.
CSCtc29089	VUM does not work over IPv6.
CSCtc54895	VSD ports are untrusted in VSM.
CSCtc66615	Reapplying host profile causes loss of uplink.

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

Bug ID	Caveat Headline
CSCtc86474	Attempt to configure SGID on an Ethernet interface range results in an internal error.
CSCtd05737	The forwarding IP address at the end of a copy command is disregarded by the software.
CSCtd27624	LACP channel not forming after reload. The configuration has native vlan.
CSCtd30975	Default DHCP configurations should not be pushed to VSD and VSM control ports.
CSCtd31838	When copying or deleting a file from a server to the standby VSM, a false error is generated.
CSCtd71556	Control VLAN on VSD Service VM, Link flap/VSM reload, VSD loops packets.
CSCtd72257	Following switchover, removing a VSD from an APC port channel interface does not work.
CSCtd73576	IGMP snooping report-suppression is not working correctly.
CSCte28866	Configuring a Cisco Nexus 1000V with the vlan dot1Q tag native command does not result in the desired behavior.
CSCth99337	Host disconnect or PSOD on removal of KL.next beta host from DVS.

Resolved Caveats

The following is a list of caveats that were resolved in Cisco Nexus 1000V Release 4.0(4)SV1(2). The Bug ID links you into the Cisco Bug Toolkit.

Bug ID	Caveat Headline
CSCsx68200	Renaming a port-group causes the port group to be deleted and a new port group to be created.
CSCsy25906	Error logged after changing the system port profiles for VMNIC with control VLAN
CSCsz15398	Performance impact when AIPC link goes down and comes back up
CSCsz21291	Port security configured in the port profile is pushing stale data (sw port-sec maximum <i>number</i>).
CSCsz24042	Static MAC entries for VMs are not updated upon VLAN change
CSCsz38042	show vlan private-vlan does not show promiscuous trunk information
CSCsz63126	No switchport mode trunk - change modes to access and not to default
CSCsz99235	Installing a permanent license file does not add new licenses to the license pool.
CSCta05268	Modules do not come up for a VSM with a VEM port channel running in vPC-HM.
CSCtc34170	The vemcmd show card command displays the incorrect number of processors, processor core, processor sockets, and physical memory.

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

Bug ID**Caveat Headline**

CSCtf43373

There are intermittent connectivity issues when one of the switches goes down and comes back up.

Related Documentation

Cisco Nexus 1000V includes the following documents available on Cisco.com:

General Information

Cisco Nexus 1000V Release Notes, Release 4.0(4)SV1(2)

Cisco Nexus 1000V Compatibility Information, Release 4.0(4)SV1(2)

Install and Upgrade

Cisco Nexus 1000V Software Installation Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V Virtual Ethernet Module Software Installation Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V Software Upgrade Guide, Release 4.0(4)SV1(2)

Configuration Guides

Cisco Nexus 1000V License Configuration Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V XML API User Guide, Release 4.0(4)SV1(2)

Programming Guide

Cisco Nexus 1000V XML API User Guide, Release 4.0(4)SV1(2)

Reference Guides

Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(2)

Cisco Nexus 1000V MIB Quick Reference

Troubleshooting and Alerts

Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V Password Recovery Guide

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

Cisco NX-OS System Messages Reference

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” 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 and phone numbers that are used in the examples, command display output, and figures within this document are for illustration only. If an actual IP address or phone number appears in this document, it is coincidental.

© 2010 Cisco Systems, Inc. All rights reserved.

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