Cisco Nexus 1000V Release Notes, Release 4.2(1)SV2(1.1a)

Last Updated: 2013-08-01
Release: NX-OS Release 4.2(1)SV2(1.1a)

This document describes the features, limitations, and bugs for the Cisco Nexus 1000V Release 4.2(1)SV2(1.1a) software. The following is the change history for this document.

Date	Description
2013-08-01	Updated the "LACP" section and added the "Upstream Switch Ports" section.
2013-01-30	Created release notes for Release 4.2(1)SV2(1.1a).

Contents

This document includes the following sections:

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

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 the Cisco Nexus 1000V and can be managed as if it were a line card in a physical Cisco switch.

The 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 with VMware

The servers that run the Cisco Nexus 1000 VSM and VEM must be in the VMware Hardware Compatibility list. This release of the Cisco Nexus 1000V supports vSphere 4.1.0, 5.0.0, and 5.1.0 release trains. For additional compatibility information, see the *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV2(1.1a)*.

Note All virtual machine network adapter types that VMware vSphere supports are supported with the Cisco Nexus 1000. Refer to the VMware documentation when choosing a network adapter. For more information, see the VMware Knowledge Base article #1001805.

Software Compatibility with Cisco Nexus 1000

This release supports hitless upgrades from Release 4.0(4)SV1(3a) and later releases. Upgrades are supported from 4.0(4)SV1(3) and earlier releases. For additional information, see the *Cisco Nexus 1000V Software Upgrade Guide, Release 4.2(1)SV1(5.1)*.

ISSU Upgrades

Performing an ISSU from Cisco Nexus 1000V Release 4.2(1)SV1(4a) or Release 4.2(1)SV1(4b) to Cisco Nexus 1000V Release 4.2(1)SV2(1.1a) using ISO files is not supported. You must use kickstart and system files to perform an ISSU upgrade to Cisco Nexus 1000V Release 4.2(1)SV2(1.1a).

New and Changed Information

No new features are added or changed for release 4.2(1)SV2(1.1a).

Limitations and Restrictions

This section lists the Cisco Nexus 1000V limitations and restrictions.

Configuration Limits

Table 1 lists the Cisco Nexus 1000V configuration limits.

Table 1 Configuration Limits for Cisco Nexus 1000V

Component	Supported Limits for a Single Cisco Nexus 1000V Deployment Spanning up to 2 Physical Data Centers	
Maximum modules	66	
Virtual Ethernet Module (VEM)	64	
Virtual Supervisor Module (VSM)	The VSMs can be placed in different physical data centers. **Note** The previous restrictions requiring the active-standby VSMs in a single physical data center no longer apply.	
Hosts	64	
Active VLANs or VXLANs across all VEMs	2048 (any combination of VLANs and VXLANs)	
MACs per VEM	32,000	
MACs per VLAN per VEM	4000	
vEthernet interfaces per port profile	1024	
PVLAN	512	
Distributed Virtual Switches (DVS) per vCenter with VMware vCloud Director (vCD)	32	
DVS per vCenter without vCD	32	
vCenter Server connections	1 per VSM HA pair **Note** Only one connection to the vCenter server is permitted at a time.	
Maximum latency between VSMs and VEMs	100 ms	
Component	**Per DVS**	**Per Host**
Virtual Service Domains (VSDs)	64	6
VSD interfaces	2048	216
vEthernet interfaces	2048	216
Port profiles	2048	—
System port profiles	32	32
Port channel	256	8
Physical trunks	512	—
Physical NICs	—	32
vEthernet trunks	256	8
ACL	128	16 **Note** This number can be exceeded if the VEM has available memory.

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

Component	Supported Limits for a Single Cisco Nexus 1000V Deployment Spanning up to 2 Physical Data Centers	
ACEs per ACL	128	128 **Note** This number can be exceeded if the VEM has available memory.
ACL instances	2048	256
NetFlow policies	32	8
NetFlow instances	256	32
SPAN/ERSPAN sessions	64	64
QoS policy map	128	128
QoS class map	1024	1024
QoS instances	2048	256
Port security	2048	216
Multicast groups	512	512

Single VMware Data Center Support

The Cisco Nexus 1000V can be connected to a single VMware vCenter Server data center object. Note that this virtual data center can span multiple physical data centers.

VMotion of VSM

VMotion of the VSM has the following limitations and restrictions:

- VMotion of a VSM is supported for both the active and standby VSM VMs. For high availability, we recommend that the active VSM and standby VSM reside on separate hosts.
- If you enable Distributed Resource Scheduler (DRS), 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 CD image is still mounted. To complete the VMotion, either click **Edit Settings** on the VM to disconnect the mounted CD image, or power off the VM. No functional impact results from this limitation.
- If you are adding one host in a DRS cluster that is using vSwitch to a VSM, you must move the remaining hosts in the DRS cluster to the VSM. Otherwise, the DRS logic does not work, the VMs that are deployed on the VEM could be moved to a host in the cluster that does not have a VEM, and the VMs lose network connectivity.

For more information about VMotion of VSM, see the *Cisco Nexus 1000V Software Installation Guide, Release 4.2(1)SV1(5.1).*

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.
- The 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.

- 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 Profiles

Port profiles have the following restrictions or limitations:

- There is a limit of 255 characters in a **port-profile** command attribute.
- We recommend that you save the configuration across reboots, which shortens the VSM bringup time.
- We recommend that if you are altering or removing a port channel, you migrate the interfaces that inherit the port channel port profile to a port profile with the desired configuration. Do not edit the original port channel port profile directly.
- 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 information, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV2(1.1)*.

SSH Support

Only SSH version 2 (SSHv2) is supported.

For information, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV2(1.1)*.

Cisco NX-OS Commands Might Differ from Cisco IOS

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

For information, see the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV2(1.1)*.

Layer 2 Switching: 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.

For information about Layer 2 switching, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV2(1.1)*.

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 you disable CDP globally, CDP is also disabled for all interfaces.

For more information about CDP, see the *Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV2(1.1)*.

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.

The 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.

- If LACP offload is disabled, at least two ports must be configured as part of LACP channel.

Note This restriction does not apply if LACP offload is enabled. You can check the LACP offload status by using the **show lacp offload status** command.

- The upstream switch ports must be configured in **spanning-tree port type edge trunk** mode.

Upstream Switch Ports

All upstream switch ports must be configured in **spanning-tree port type edge trunk** mode.

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, the 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**

DNS Resolution

The Cisco Nexus Virtual Services Appliance (1000V) cannot resolve a domain name or hostname to an IP address.

Interfaces

When the maximum transmission unit (MTU) is configured on an operationally up interface, the interface goes down and comes back up.

Layer 3 VSG

When a VEM communicates with Cisco VSG in Layer 3 mode, an additional header with 94 bytes is added to the original packet. You must set the MTU to a minimum of 1594 bytes to accommodate this extra header for any network interface through which the traffic passes between the Cisco Nexus 1000V and the Cisco VSG. These interfaces can include the uplink port profile, the proxy ARP router, or a virtual switch.

VM Name Display Length Limitation

VM names for VMs on ESX 4.1 hosts that exceed 21 characters are not displayed correctly on the VSM. When you use a **show vservice** command that displays the port profile name—for example, the **show vservice port brief port-profile** *port-profile-name* command—only VMs with names that are 21 characters or less are displayed correctly. Longer VM names might be truncated or have extra characters appended. Depending on the network adapter, the name length limitation varies. For example:

- The E1000 or VMXNET 2 network adapters allow 26-character names. At 27 characters, the word ‘.eth’ is appended to the VM name. With each addition to the VM name, a character is truncated from the word ‘.eth’. After 31 characters, the VM name is truncated.
- The VMXNET 3 network adapters allow 21-character names. At 22 characters, the word ‘ethernet’ is appended to the VM name. With each addition to the VM name, a character is truncated from the word ‘ethernet’. After 30 characters, the VM name is truncated.

Note This is a display issue with ESX Release 4.1 only. Use VM names of 21 characters or less to avoid this issue.

ISSU Upgrades

Performing an ISSU from Cisco Nexus 1000V Release 4.2(1)SV1(4) or Release 4.2(1)SV1(4a) to Cisco Nexus 1000V Release 4.2(1)SV2(1.1a) using the ISO files is not supported. You must use the kickstart and the system files to perform an ISSU upgrade to Cisco Nexus 1000V Release 4.2(1)SV2(1.1a).

Copy Running-Config Startup-Config Command

When running the **copy running-config startup-config** command, do not press the PrtScn key. If you do, the command will abort.

Error Messages Appear During ESX 4.1.0 Server Bootup

Vssnet-load error messages can occur during a classic ESX 4.1.0 server bootup or restart when the VEM is already installed. The issue occurs while booting up because the path environment variable is not set up correctly, and the system is not able to identify the VMware command. After the system boots up, it is set up correctly and so is the ESX 4.10 system. There is no functional impact of the error messages and they can be ignored.

Dynamic Entries Are Not Deleted for a Linux VM

On a Linux VM that has multiple adapters, a DHCP release packet is sent from an incorrect interface (because of OS functionality) and the DHCP release packet is dropped. As a result, the binding entry is not deleted. This issue is a Linux issue where the packets from all interfaces go out of one interface (which is the default interface). To avoid this issue, put the interfaces in different subnets and make sure that the default gateways for each interface is set.

Source Filter TX VLANs Are Missing After the VSM Restarts

When a SPAN (erspan-source) session is created and the source interface is configured as a port channel and PVLAN Promiscuous access is programmed, the filter RX is not configured and the configured programmed filter TX is not persistent on VSM reload.

To work around this issue, configure all the primary and secondary VLANs as filter VLANs while using the port channel with PVLAN Promiscuous access as the source interface.

Default SSH Inactive Session Timeout

The default SSH inactive session timeout is 30 minutes, but the timeout setting is disabled by default, so the connection remains active. Use the **exec-timeout** command to explicitly configure the inactive session timeout limit.

Queueing Policy Cannot Be Changed in Flexible Upgrade Setup

Queuing is valid starting from Cisco NX-OS Release 4.2(1)SV1(51). Any queueing configuration that exists on the VSM in an earlier release will stop working. All port profiles that have a queueing configuration cannot be used. If a port is down, it should be moved to a profile without QoS queueing.

Clear QoS Statistics Fails on the VSM

When a policy map of type “queuing” has a class map of type “match-any” without any match criteria, and is applied on an interface, a resource pool is not created for that specific class ID. As a result, the collection of statistics fails and no data is sent back to the VSM. To work around this issue, add a match criteria on the empty class map.

Bugs

This section includes the following topics:

Open Bugs

The following are descriptions of the bugs in Cisco Nexus 1000V Release 4.2(1)SV2(1.1a). The ID links you to the Cisco Search Tool.

Platform, Infrastructure, Ports, Port Channel, and Port Profiles

ID	Headline
CSCti39155	Need to send traffic from the destination VM to learn the vns-binding.
CSCti85986	The Cisco Nexus 1000 cannot support more than 245 ports (physical and virtual) per VEM.
CSCti98977	Not able to migrate VC/VSM and normal VM when adding host to DVS.
CSCtj70071	SNMP V3 traps are not getting generated.
CSCtn62514	LACP offload configuration is not persisting in stateless mode.
CSCtq04886	Eth_port_sec crash occurs during migration in VC with interface override in VSM.
CSCtq92519	CDP does not work for certain NIC cards without VLAN 1 allowed.
CSCtr34519	Continuous SNMP polling causes high CPU usage.
CSCtr36181	Integrate Apache with netstack.

ID	Headline
CSCtr55311	Legacy LACP takes 30 minutes to come up after a link flap.
CSCts24105	The **load-interval counter** command configuration is not working.
CSCts50066	Post module flap violated port is secured and the secured port is violated.
CSCtt07479	A port profile configured with the **port-binding static auto** command reserves more than the default ports.
CSCtt17073	A port profile via VCD fails when done immediately after a switchover.
CSCtt24735	Editing a port profile fails with the error message “ERROR: unknown error.”
CSCtz04587	Reloading the VSM takes 12 minutes for modules to come online and vEthernet interfaces to come up
CSCtu10144	A virtual Ethernet interface as trunk has pinning issue in MN ESX hosts.
CSCtu17512	The Cisco Nexus 1000V to vShield Manager connection is down after release of VCD, DB, VSM. **Note** Only applicable with VMware vCloud Director 1.5.1 and vShield Manager 5.0.1.
CSCtw93579	Active VSMs CPU utilization is more than 50% when there are 512 groups.
CSCtw96064	The **show tech-support dvs** command does not have output related to DHCP snooping.
CSCtx06864	A native VLAN configured on the interface port channel is not programmed on the VEM.
CSCtx30435	After upgrading the VEM to Cisco NX-OS Release 4.2(1)SV1(5.1), two Cisco VIBs are installed.
CSCty59712	If you add a primary PVLAN as the SPAN/ERSPAN source, its promiscuous trunk members are not added to the SPAN session.
CSCua00940	PPM does not perform configuration checks when you configure a PVLAN in an offline port-profile mode.
CSCua02145	“SYSMGR_EXITCODE_FAILURE_NOCALLHOME” error message received while upgrading with ISO images from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.2).
CSCua06287	Incorrect mapping for ethernet port profile with PVLAN configuration is displayed in the running configuration.
CSCua11227	Cannot copy the running configuration from the TFTP server to the current running configuration.
CSCua12342	A Link Aggregation Control Protocol (LACP) port channel member port goes to the suspended state when the port is newly added to the LACP port channel, or the port is removed and re-added to the LACP port channel.
CSCua12592	Password validity is not checked when installing a VSM using an OVA installation.
CSCua16092	If you add a PVLAN promiscuous trunk port channel or Ethernet interface as the SPAN/ERSPAN source, some of the VLANs allowed on the port might not be spanned.

ID	Headline
CSCua30287	An error occurs while trying to override the PVLAN mapping in the child port profile.
CSCua59482	Traffic is being redirected to the incorrect VSG.
CSCua73549	Modules are not reattached after a VMKnic MAC address change in Layer 3 mode.
CSCub23161	VCD does not display relevant error descriptions for error codes.
CSCub25986	NSM should fix the Cisco Nexus 1000V feature limitation issue.
CSCub33444	Powering up a single VM configures all vApp networks.
CSCub69289	Veths mapped to the port profiles are not counted in the **show resource-availability monitor** command.
CSCub79332	The server IP address becomes 0.0.0.0 for a MN stateless host.
CSCub90212	SPAN sources are deleted on the VEM output while adding the source interfaces. Duplicated by CSCtz82836.
CSCuc58678	The installer displays an error when a host with multiple VMKnics in the same VLAN is migrated.
CSCuc49513	The **show processes cpu history** command output has the graphing backwards.
CSCuc63801	Traffic loss occurs after the VSM reloads if PSEC is restricted and the DSM bit is set.

Quality of Service

ID	Headline
CSCtl00949	Configuring child with **no service policy** command is causing inherit to fail.
CSCtq34938	Applying policy fails sharing ACL between two class-maps of same policy.
CSCtu36119	QoS marking limitation in VCD environment.

Features

ID	Headline
CSCtk65252	PSEC with multiple MAC addresses and PVLAN not supported.
CSCtl04632	Port migration with switchover causing ports to go to “No port-profile.”
CSCtq89961	Snooping does not get applied on sec VLANs if executed in different order
CSCtr06833	Split brain causes pending ACL/QoS transactions into err-disabled.

ID	Headline
CSCtr09746	Interface configuration fails when veths are nonparticipating due to unreachable module.
CSCub44964	A RADIUS AAA error occurs when feature CTS is enabled and there is a switchover.
CSCue22423	Zombie (defunct) httpd processes are created after disabling or enabling http feature.

VMware

ID	Headline
CSCti34737	Removing host with Intel Oplin from DVS causes all ports to reset.
CSCtk02322	After an ESX host exception, the port group configuration on PNIC is changed.
CSCtk07337	Fully qualified domain name/user with port-profile visibility fails.
CSCtk10837	Port-profile visibility feature is not able to update permissions.
CSCtk53802	Improper sync with vCenter when port-profile names have special characters.
CSCts80394	A VEM upgrade fails when the scratch space is a network file system.
CSCtt00444	After unregistering Cisco Nexus 1000V on Vshield, the alert timer runs.
CSCty78076	VEM upgrade error occurs when using VMware Update Manager.
CSCua30356	An existing vAPP cannot be powered down, and a new vAPP cannot be deployed.
CSCua40492	When the VEM is disconnected from the VSM (headless mode), the maximum number of vEthernet interfaces limit cannot be connected.
CSCua48997	When VIBs are removed from ESX 4.1 hosts in maintenance mode, the hosts return to maintenance mode after reboot.
CSCua78262	The incorrect release description name and release note URL is displayed with the ESX/ESXi 4.1.0 offline bundle.
CSCub56123	Wrong message for VC user id and Password.
CSCub90212	Span sources gets deleted on VEM output while adding source intfs.
CSCuc71793	Ports go to error disabled state during ACL or QoS Commit Errors.
CSCuc75398	App fail power on with insufficient resource error.
CSCuc80063	IGMP process failing to read PVLAN association.

vPath

ID	Headline
CSCud81685	SP-id resolves to 0 when you upgrade ISSU without PA.

Resolved Bugs

The following are descriptions of bugs that are resolved in Cisco Nexus 1000V Release 4.2(1)SV2(1.1a). The ID links you to the Cisco Bug Search Tool.

ID	Headline
CSCuc66508	The VSG gets into unlicensed mode after 1.5.2 to 2.1.1 ISSU upgrade.
CSCud18794	PSOD encountered on ESXi host.
CSCud39246	VEM upgrade fails on ESXi4.1 hosts.
CSCuc75033	VM packet loss after VMotion when Qos applied.
CSCud01515	When VSG has no license, Nexus 1000 fails to open or close.
CSCud33791	Duplicate IP event in W2K8 VMs in vPath on flap of Network Adapter.

MIB Support

The Cisco Management Information Base (MIB) list includes Cisco proprietary MIBs and many other Internet Engineering Task Force (IETF) standard MIBs. These standard MIBs are defined in Requests for Comments (RFCs). To find specific MIB information, you must examine the Cisco proprietary MIB structure and related IETF-standard MIBs supported by the Cisco Nexus 1000V Series switch.

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

ftp://ftp.cisco.com/pub/mibs/supportlists/nexus1000v/Nexus1000VMIBSupportList.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.