Cisco Nexus 1000V Release Notes, Release 4.2(1)SV1(5.2)

Release Date: March 11, 2014
Part Number: OL-27571-01
Current Release: NX-OS Release 4.2(1)SV1(5.2)

This document describes the features, limitations, and caveats for the Cisco Nexus 1000V Release 4.2(1)SV1(5.2) software. Use this document in combination with documents listed in the "Related Documentation" section on page 16. The following is the change history for this document.

Part Number	Revision	Date	Description
OL-27571-01	A0	August 21, 2012	Created release notes for Release 4.2(1)SV1(5.2).
	B0	September 11, 2012	Added new software feature information for Release 4.2(1)SV1(5.2).
	C0	September 26, 2012	Updated the configuration limits.
	D0	November 2, 2012	Added open caveat CSCud01427.
	E0	February 19, 2013	Added note for VSG solution not supporting VMware vSphere 5.1
	F0	June 6, 2013	Added resolved caveat CSCud38040
	G0	August 1, 2013	Updated the "LACP" section on page 9 and added the "Upstream Switch Ports" section on page 10.
	H0	March 11, 2014	Added a note for the change in the vn-service command to vservice command.

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

This section includes the following topics:

Software Compatibility with VMware

Note The Cisco VSG solution is not supported with VMware vSphere 5.1.

The servers that run the Cisco Nexus 1000V 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)SV1(5.2)*.

Note All virtual machine network adapter types that VMware vSphere supports are supported with the Cisco Nexus 1000V. 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 1000V

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(5.2)*.

New and Changed Information

This section provides the following information about Cisco Nexus 1000V Release 4.2(1)SV1(5.2):

Changed Software Features

The following software features were changed in Cisco Nexus 1000V Release 4.2(1)SV1(5.2):

Installer Enhancements

Starting with Cisco Nexus 1000V Release 4.2(1)SV1(5.1), the Cisco Nexus 1000V Installation Management Center is now a standalone Java application that can install the Cisco Nexus1000V VSM or VEM.

The Cisco Nexus 1000V Installation Management Center supports a single pane for invoking the Cisco Nexus1000V VSM installer and VEM installer.

For more information, see the *Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.2)*.

New Software Features

The following software features were added in Cisco Nexus 1000V Release 4.2(1)SV1(5.2):

Combined Upgrade

Starting with Cisco Nexus 1000V Release 4.2(1)SV1(5.1), combined upgrades are supported. A combined upgrade is a simultaneous upgrade of both the ESX and the VEM software versions in a host. You can perform the combined upgrading using VMware Update Manager (VUM) or manually.

Note Combined upgrades with VUM require vCenter Server 5.0 Update 1 or later releases.

Note The vn-service command is changed to the vservice command on the VSM port-profile in Nexus 1000V Release 4.2(1)SV1(5.2).

Release Support

This release supports VMware Release 5.1.

Limitations and Restrictions

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

Configuration Limits

Table 1 shows the Cisco Nexus 1000V configuration limits:

Table 1 Configuration Limits for Cisco Nexus 1000V

Component	Supported Limits for Cisco Nexus 1000V in the Same Datacenter		Supported Limits for Cisco Nexus 1000V Across Two Datacenters	
Maximum Modules	66		34	
Virtual Ethernet Module (VEM)	64		32	
Virtual Supervisor Module (VSM)	2 in an HA Pair (active-standby hosted in the same datacenter)		2 in an HA Pair (active-standby hosted in the same datacenter)	
Hosts	64		32	
Active VLANs or VXLANs across all VEMs	2048 (any combination of VLANs and VXLANs)		1024 (any combination of VLANs and VXLANs)	
MACs per VEM	32000		32000	
MACs per VLAN per VEM	4000		4000	
vEthernet interfaces per port profile	1024		1024	
PVLAN	512		128	
Distributed Virtual Switches (DVS) per vCenter with VMware vCloud Director (vCD)	12		12	
Distributed Virtual Switches (DVS) per vCenter without VMware vCloud Director (vCD)	32		32	
vCenter Server connections	1 per VSM HA Pair[1]		1 per VSM HA Pair[1]	
Maximum latency between VSMs and VEMs	5ms		5ms	
	Per DVS	**Per Host**	**Per DVS**	**Per Host**
Virtual Service Domains (VSDs)	64	6	32	3
VSD interfaces	2048	216	1024	108
vEthernet interfaces	2048	216	1024	108
Port profiles	2048	—	1024	—
System port profiles	32	32	16	16
Port channel	256	8	128	4
Physical trunks	512	—	256	—
Physical NICs	—	32	—	16
vEthernet trunks	256	8	128	4
ACL	128	16[2]	64	8[2]
ACEs per ACL	128	128[2]	64	64[2]
ACL instances	2048	256	1024	128
NetFlow policies	32	8	16	4
NetFlow instances	256	32	128	16
SPAN/ERSPAN sessions	64	64	32	32

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

Component	Supported Limits for Cisco Nexus 1000V in the Same Datacenter		Supported Limits for Cisco Nexus 1000V Across Two Datacenters	
QoS policy map	128	128	64	64
QoS class map	1024	1024	512	512
QoS instances	2048	256	1024	128
Port security	2048	216	1024	108
MultiCast groups	512	512	256	256

1. Only one connection to vCenter server is permitted at a time.
2. This number can be exceeded if VEM has available memory.

Single VMware Data Center Support

The Cisco Nexus 1000V can be connected to a single VMware vCenter Server datacenter object. Note that this virtual datacenter can span across 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 will shorten the VSM bringup time.

- We recommend that if you are altering or removing a port channel, you should migrate the interfaces that inherit the port channel port profile to a port profile with the desired configuration, rather than editing 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 more information about Telnet, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*.

SSH Support

Only SSH version 2 (SSHv2) is supported.

For more information, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*.

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 about CLI commands, see the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*.

Layer 2 Switching

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

- No Spanning Tree Protocol, page 9

For more information about Layer 2 switching, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(5.1)*.

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.

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)SV1(5.1)*.

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 is not applicable 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. For more information about this restriction, see Upstream Switch Ports, page 10.

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 1010 (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 properly 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 may cause the VM name to be truncated, or extra characters to be appended to the VM name. Depending on the network adapter, the name length limitation may vary. 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.

Workaround: 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)SV1(5.2) 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)SV1(5.2).

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.

Caveats

This section includes the following topics:

Open Caveats

The following are descriptions of the caveats in Cisco Nexus 1000V Release 4.2(1)SV1(5.2). The ID links you into the Cisco Bug Toolkit.

The caveats are listed in the following categories:

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

	ID	Open Caveat Headline
1.	CSCti39155	Need to send traffic from the destination VM to learn the vns-binding.
2.	CSCti85986	The Cisco Nexus 1000V cannot support more than 245 ports (physical and virtual) per VEM.
3.	CSCti98977	Not able to migrate VC/VSM and normal VM when adding host to DVS.
4.	CSCtj70071	SNMP V3 traps are not getting generated.

	ID	Open Caveat Headline
5.	CSCtn62514	LACP offload configuration is not persisting in stateless mode.
6.	CSCtq04886	Eth_port_sec crash occurs during migration in VC with interface override in VSM.
7.	CSCtq92519	CDP does not work for certain NIC cards without VLAN 1 allowed.
8.	CSCtr34519	Continuous SNMP polling causes high CPU usage.
9.	CSCtr36181	Integrate Apache with netstack.
10.	CSCtr55311	Legacy LACP takes 30 minutes to come up after a link flap.
11.	CSCts24105	The **load-interval counter** command configuration is not working.
12.	CSCts50066	Post module flap violated port is secured and the secured port is violated.
13.	CSCtt07479	A port profile configured with the **port-binding static auto** command reserves more than the default ports.
14.	CSCtt17073	A port profile via VCD fails when done immediately after a switchover.
15.	CSCtt24735	Editing a port profile fails with the error message “ERROR: unknown error.”
16.	CSCtt40944	In a PVLAN, all mappings are removed when a single mapping is removed.
17.	CSCtu10144	A virtual Ethernet interface as trunk has pinning issue in MN ESX hosts.
18.	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.
19.	CSCtw93579	Active VSMs CPU utilization is more than 50% when there are 512 groups.
20.	CSCtw96064	The **show tech-support dvs** command does not have output related to DHCP snooping.
21.	CSCtx06864	A native VLAN configured on the interface port channel is not programmed on the VEM.
22.	CSCtx30435	After upgrading the VEM to Cisco NX-OS Release 4.2(1)SV1(5.1), two Cisco VIBs are installed.
23.	CSCty59712	If you add a primary PVLAN as the SPAN/ERSPAN source, its promiscuous trunk members are not added to the SPAN session.
24.	CSCty64522	The VEM agent continues running after entering the **vem-remove -d** command.
25.	CSCua00940	PPM does not perform configuration checks when you configure a PVLAN in an offline port-profile mode.
26.	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).

	ID	Open Caveat Headline
27.	CSCua06287	Incorrect mapping for ethernet port profile with PVLAN configuration is displayed in the running configuration.
28.	CSCua11227	Cannot copy the running configuration from the TFTP server to the current running configuration.
29.	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.
30.	CSCua12592	Password validity is not checked when installing a VSM using an OVA installation.
31.	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.
32.	CSCua59482	Traffic is being redirected to the incorrect VSG.
33.	CSCtz90492	Cannot install later versions of VIB files using the VEM installer without vCenter Update Manager (VUM).

Quality of Service

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

Features

	ID	Open Caveat Headline
1.	CSCtk65252	PSEC with multiple MAC addresses and PVLAN not supported.
2.	CSCtl04632	Port migration with switchover causing ports to go to “No port-profile.”
3.	CSCtq89961	Snooping does not get applied on sec VLANs if executed in different order
4.	CSCtr06833	Split brain causes pending ACL/QoS transactions into err-disabled.
5.	CSCtr09746	Interface configuration fails when veths are nonparticipating due to unreachable module.

VMware

	ID	Open Caveat Headline
1.	CSCti34737	Removing host with Intel Oplin from DVS causes all ports to reset.
2.	CSCtk02322	After an ESX host exception, the port group configuration on PNIC is changed.
3.	CSCtk07337	Fully qualified domain name/user with port-profile visibility fails.
4.	CSCtk10837	Port-profile visibility feature is not able to update permissions.
5.	CSCtk53802	Improper sync with vCenter when port-profile names have special characters.
6.	CSCts80394	A VEM upgrade fails when the scratch space is a network file system.
7.	CSCtt00444	After unregistering Cisco Nexus 1000V on Vshield, the alert timer runs.
8.	CSCty78076	VEM upgrade error occurs when using VMware Update Manager.
9.	CSCtz90492	The Cisco Nexus 1000V Installation Management Center is not supported in VMware ESX 5.1 hosts.
10.	CSCua30356	An existing vAPP cannot be powered down, and a new vAPP cannot be deployed.
11.	CSCua40492	When the VEM is disconnected from the VSM (headless mode), the maximum number of vEthernet interfaces limit cannot be connected.
12.	CSCua48997	When VIBs are removed from ESX 4.1 hosts in maintenance mode, the hosts return to maintenance mode after reboot.
13.	CSCua78262	The incorrect release description name and release note URL is displayed with the ESX/ESXi 4.1.0 offline bundle.

Cisco Virtual Security Gateway

	ID	Open Caveat Headline
1.	CSCud01427	The VSM/VEM licensing for Cisco VSG enters an unlicensed mode after you upgrade from Cisco Nexus 1000V Series switch Release 4.2(1) SV1(5.1) or Release 4.2(1) SV1(5.1a) to Release 4.2(1) SV1(5.2).

Resolved Caveats

The following are descriptions of caveats that were resolved in Cisco Nexus 1000V Release 4.2(1)SV1(5.2). The ID links you into the Cisco Bug Toolkit.

	ID	Resolved Caveat Headline
1.	CSCtq34432	The **service-policy** command leaks to **veth-no service-policy** command with the wrong policy name.
2.	CSCtq34977	Interface in “NoPortProfile” state on mode changes from LACP to MAC pinning.
3.	CSCtw50899	Nsmgr pss state and port profiles state after the **write erase** command.
4.	CSCtw56889	Cisco Nexus 1000V does not recompute the UDP checksum when option 82 is inserted.
5.	CSCtw69713	A module does not come up if the lowest numbered vmnic on Cisco Nexus 1000V is down.
6.	CSCtw72196	Queues are not created when adding a class map in a policy map that has no cl.
7.	CSCtx02138	ERSPAN supports an MTU larger than 1500 bytes.
8.	CSCtx03892	A migration to Cisco Nexus 1000V multicast with 224.0.0.1 address stopped working.
9.	CSCtx32992	Multicast drops count as vEth output drops.
10.	CSCtx39449	Module flaps and disconnection of svs connection observed.
11.	CSCtx41516	Disable the **snmp trap link-status** command on a vEthernet interface.
12.	CSCtz12186	The **show http-server** command does not show the status of http and https.
13.	CSCtz57199	N1K portchannel loadbalance is not consistent on VEM.
14.	CSCua92452	A VMware critical failure is seen when unloading VEM modules during VEM Upgrade with VEM having L3 vmknic Control Interface with QoS and ACL configurations.
15.	CSCud38040	VEM upgrade from Release 4.2(1)SV1(5.1), 4.2(1)SV1(5.1a) to any higher release fails on ESXi 5.0-U2 and later.

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

Related Documentation

This section lists the documents used with the Cisco Nexus 1000V and available on 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 4.2(1)SV1(5.1)

Cisco Nexus 1000V Release Notes, Release 4.2(1)SV1(5.2)

Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(5.2)

Cisco Nexus 1010 Management Software Release Notes, Release 4.2(1)SP1(4a)

Install and Upgrade

Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.2)

Cisco Nexus 1010 Virtual Services Appliance Hardware Installation Guide

Cisco Nexus 1010 Software Installation and Upgrade Guide, Release 4.2(1)SP1(4a)

Configuration Guides

Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V Network Segmentation Manager Configuration Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.2(1)SV1(5.2)

Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V VXLAN Configuration Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1010 Software Configuration Guide, Release 4.2(1)SP1(4)

Programming Guide

Cisco Nexus 1000V XML API User Guide, Release 4.2(1)SV1(5.1)

Reference Guides

Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V MIB Quick Reference

Cisco Nexus 1010 Command Reference, Release 4.2(1)SP1(4)

Troubleshooting and Alerts

Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V Password Recovery Guide

Cisco NX-OS System Messages Reference

Virtual Security Gateway Documentation

Cisco Virtual Security Gateway for Nexus 1000V Series Switch

Virtual Network Management Center

Cisco Virtual Network Management Center

Virtual Wide Area Application Services (vWAAS)

Cisco Virtual Wide Area Application Services (vWAAS)

Network Analysis Module Documentation

Cisco Prime Network Analysis Module Software Documentation Guide, 5.1

Cisco Prime Network Analysis Module (NAM) for Nexus 1010 Installation and Configuration Guide, 5.1

Cisco Prime Network Analysis Module Command Reference Guide 5.1

Cisco Prime Network Analysis Module Software 5.1 Release Notes

Cisco Prime Network Analysis Module Software 5.1 User Guide

Obtaining Documentation and Submitting a Service Request

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

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.