Cisco Nexus1000V Release Notes, Release 4.0(4)SV1(1)

Updated: May 10, 2013
OL-19420-01

This document describes the features, caveats, and limitations for the Cisco Nexus 1000V Release 4.0(4)SV1(1) software. Use this document in combination with documents listed in the "Related Documentation" section on page 14.

Contents

This document includes the following information about Release 4.0(4)SV1(1) of the Cisco Nexus 1000V.

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 linecard 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

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

- Virtual Ethernet Module (VEM), which acts as a Line Card and runs in each virtualized server to handle packet forwarding and other localized functions, and is compatible with any upstream physical access layer switch that is Ethernet standard's compliant. This includes Catalyst and Nexus switches from Cisco as well as switches from other network vendors.

Software Compatibility

The servers running the Cisco Nexus 1000V VSM and VEM must be in the VMware Hardware Compatibility List (HCL) . This is a requirement for running the ESX 4.0 software, VMWare vSphere 4.0 Enterprise Plus.

Limitations and Restrictions

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	256	
Distributed Virtual Switches (DVS) per vCenter	12	
	Per DVS	**Per Host**
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	1024	128
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	1024	128
Port Security	1024	216
MultiCast Groups	512	64

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

VMware Lab Manager

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

Access Lists

ACLs have the following limitations and restrictions:

Limitations:

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

Restrictions:

- IP ACL rules for TCP and UDP traffic cannot use logical operator *neq* (not equal to) to filter traffic based on port numbers.
- IP ACL rules do not support the following:
  - established TCP connections filtering option
  - 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.
- Multicast traffic type is not supported. Cache entries are created for multicast packets but packet/byte count does not reflect replicated packets.

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(1)*.

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(1)*.

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 the CLI, see the *Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(1)*.

Layer 2 Switching

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

- Maximum Allowed VLANs and MAC Addresses per VLAN, page 6.

For detailed information about Layer 2, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(1)*.

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 Cisco Nexus 1000V MAC address table, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(1)*.

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(1)*.

Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) runs over the data link layer and is used by the Cisco Nexus 1000V to advertise information to all Cisco devices it attaches to, and, in turn, to discover and view information about those Cisco devices. CDP runs on all Cisco-manufactured equipment.

Cisco Discovery Protocol (CDP) has the following configuration guidelines and limitations:

- CDP can discover up to 256 neighbors per port if the port is connected to a hub with 256 connections.
- The CDP feature is enabled globally by default.
- If disabled globally on the Cisco Nexus 1000V, 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(1)*.

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

Caveats

The following are descriptions of the caveats in Cisco Nexus 1000V Release 4.0(4)SV1(1).

Bug ID	Caveat
CSCsq66077	**Headline**: Shutting an Ethernet interface in Cisco Nexus 1000V VSM is not reflected in the Cat6K. **Symptom**: After shutting down an Ethernet interface for an uplink port on the VSM, the physical network interface attached to it on the VEM and the switch port attached to the physical NIC do not shut down as expected. The output of the following command shows the interface as shut down: **show interface ethX/Y** The output of the following command shows that the NIC is up: **esxcfg-nics -l** **Conditions**: This happens on any ESX platform running Cisco NX-OS. **Workaround**: Use the **shutdown** command on the interface of the upstream switch. This brings down both the link on the upstream switch and the ESX physical NIC. **Further Problem Description**: The VEM sets the uplink port in the DOWN state, so that no traffic flows through that port. It is only the physical NIC attached to that DVS port which is not brought down.
CSCsw32257	**Headline**: Shutting down a VSM VEthernet interface is not reflected in the VM. **Symptom**: After you shut down a VEthernet port on the VSM, it does not appear to be down from the VM. **Conditions**: The VM Guest OS, connected to the Cisco Nexus 1000V through a vEthernet port, does not see a link going down. A **shutdown** command on the VSM VEthernet interface shuts down the interface and stops traffic forwarding. **Workaround**: You can use the GuestOS utilities to bring down the interface. In a Linux system, for example, use the **ifconfig down eth0** command. **Further Problem Description**:
CSCsw49458	**Headline**: A change to the speed or duplex settings on a physical NIC causes module flap. **Symptom**: The port bounces and the module flaps after changing speed or duplex settings on an Ethernet interface. **Conditions**: The speed and duplex settings on Ethernet interfaces do not work on an interface carrying system VLANs. **Workaround**: Avoid configuring speed or duplex settings in a VSM connected to an upstream switch. **Further Problem Description**: None.

Bug ID	Caveat

CSCsx11210	**Headline**: Unable to add match criteria in a QoS class map after changing to **match-any**.
	Symptom: Adding match criteria does not work after changing a class map to match-any.
	Conditions: If you create a class map with **match-all packet length** as the only criteria, then changing the map to **match-any** prevents you from adding new match criteria.
	Example:
	`n1000v(config)# class-map c1`
	`n1000v(config-cmap-qos)# match packet length 1028`
	`n1000v(config-cmap-qos)# exit`
	`n1000v(config)# class-map match-any c1`
	`n1000v(config-cmap-qos)# match packet length 1038`
	`n1000v(config-cmap-qos)# show class-map c1`
	`Type qos class-maps`
	`====================`
	`class-map type qos match-any c1`
	`match packet length 1028`
	Workaround: Always verify a class map configuration using the **show class-map** command. If the map is not correct, delete the criteria using the **no match** command and then add it again.
	Example:
	`n1000v(config)# class-map match-any c1`
	`n1000v(config-cmap-qos)# no match packet length 1028`
	`n1000v(config-cmap-qos)# match packet length 1028, 1038`
	Further Problem Description: None.

CSCsx68200	**Headline**: Attempting to rename a port-group causes the port group to be deleted and a new port group to be created. **Symptom**: When you use the following command to rename a port group, the existing port group is deleted and a new port group is created with the new name. switch (config-port-prof)# **vmware port-group new-name** **Conditions**: Attempt to change the name of a port group. **Workaround**: None **Further Problem Description**: Deleting and creating a new port group may also cause the related NICs to be moved into the Quarantine port groups. **Example**: `2009 May 20 10:26:39 switch %VMS-3-DVPG_NICS_MOVED: '6' nics have been moved from port-group 'WebApp' to 'Unused_Or_Quarantine_Veth'` In this case, the NICs must again be re-associated with the port-group.

Bug ID	Caveat
CSCsy25906	**Headline**: Error logged after changing the system port profiles for VMNIC with control VLAN **Symptom**: If you change the system port profile for a physical adapter carrying the control VLAN, the following system logs are generated: ETH_PORT_CHANNEL-3-COMPAT_CHECK_FAILURE PORT_PROFILE_CHANGE_VERIFY_REQ_FAILURE **Conditions**: Port profiles sys1 and sys2 are configured as channel-group and have the control VLAN configured as part of the system VLANs. Two physical adapters are attached to port profile sys1. From the vSphere client, change the adapters from port profile sys1 to port profile sys2 in a single step. **Workaround**: Do not change the system port profile attached to a physical adapter in a single step. Instead, use the following procedure: 1. From the vSphere client, remove the adapters from the port profile sys1. 2. Click OK. 3. Add the adapters to port profile sys2. **Further Problem Description**: None
CSCsy88176	**Headline**: Inaccurate **show policy-map interface** output if there are numerous policy-maps **Symptom**: When displaying the statistics for multiple policy-maps, the results may not reflect accurate statistics. **Conditions**: Multiple large policies are configured on a single VEM, especially if they use complex match-any conditions. **Workaround**: Instead of displaying all policy maps at once, use the following command to display them one at a time: **show policy-map interface** *name* **Further Problem Description**: The syslog alerts you that too much data is being returned at one time.
CSCsz03271	**Headline**: The same ACL cannot be used multiple times in a QoS policy-map. **Symptom**: When an ACL policy is used more than once in a QoS policy-map, the system fails to apply it to an interface. **Conditions**: Using the same ACL multiple times in a single policy-map. **Workaround**: Do not use the same ACL in different class-maps that are referenced in a single QoS policy. Instead, create and reference a new ACL with same set of rules. **Further Problem Description**: None

Bug ID	Caveat
CSCsz15398	**Headline**: Performance impact when AIPC link goes down and comes back up **Symptom**: Ports go into the errDisabled state and **EthPM timeout** system messages are generated after the control traffic link goes down and comes back up. **Conditions**: A large number of interfaces (greater than 256 interfaces spread across 8 VEMs) are configured with ACL or QoS policies. **Workaround**: View module states using the **show module** command. Once all modules in the system are active, do one of the following: • If the number of errDisabled interfaces is limited, enter the following command sequence: – switch (config-if)# **shutdown** – switch (config-if)# **no shutdown** • If there is a particular VEM (or a few VEMs) that have interfaces in the errDisabled state, force a module removal and re-insert (one by one for all affected modules). This can be done by shutting the port on the upstream switch that connects to the VEM uplink for 10 seconds. • If there is no difference between the switch running-configuration and startup-configuration, you can reload the VSM using the **reload** command. **Further Problem Description**: None
CSCsz21291	**Headline**: Port security configured in the port profile is pushing stale data (sw port-sec maximum *number*). **Symptom**: The maximum secure MAC address count configured through the port profile is not applied to a vEthernet interface. **Conditions**: One of the following is true for the vEthernet interface: • It is not up. • It does not have port security enabled. **Workaround**: Re-configure the maximum secure address count when the interface is up and port security is enabled on the interface. **Further Problem Description**: None
CSCsz21693	**Headline**: Reload of iVISOR host removes the VIB package. **Symptom**: Rebooting an ESXi host causes it to not show up in the VSM. **Conditions**: This occurs if you load the N1KV VEM code onto the host before adding the host to vSphere Server. **Workaround**: Do one of the following: • Add the ESXi host to vSphere before installing Cisco Nexus 1000V VEM software. • Reboot the host after installing Cisco Nexus 1000V VEM software but before adding the host to vSphere. **Further Problem Description**: None

Bug ID	Caveat

CSCsz24042	**Headline**: Static MAC entries for VMs are not updated upon VLAN change
	
	Symptom: A private VLAN host virtual interface changed to a regular interface keeps the static MAC address in the running configuration.
	
	Conditions: You configure a virtual interface as a private VLAN host and then change it to a regular interface.
	
	Example:
	`switch# conf t`
	`switch (config)# port-profile pvlan153`
	`n1000v(config-port-prof)# vmware port-group`
	`n1000v(config-port-prof)# switchport mode private-vlan host`
	`n1000v(config-port-prof)# switchport private-vlan host-association 156 153`
	`n1000v(config-port-prof)# no shutdown`
	`n1000v(config-port-prof)# state enabled`
	
	`switch# conf t`
	`switch (config)# port-profile pvlan153`
	`n1000v(config-port-prof)# switchport mode access`
	
	Workaround: When you change an interface from a private VLAN host interface to a regular interface, you must manually remove the static MAC from the configuration.
	
	Example:
	`switch# conf t`
	`switch (config)# no mac address-table static 0050.5692.1b66 vlan 156 interface Vethernet1`
	
	Further Problem Description: None

CSCsz38042	**Headline**: **show vlan private-vlan** does not show promiscuous trunk information
	
	Symptom: The **show vlan private-vlan** command output does not show private-vlan promiscuous trunk port information.
	
	Conditions: The **show vlan private-vlan** command output does not list the interfaces associated with the private VLAN if it is configured as private VLAN promiscuous trunk port.
	
	Workaround: Use **show interface switchport** or **show running-config**,
	
	Further Problem Description: If the interface is configured as a private VLAN host port and private VLAN promiscuous access port, the **show vlan private-vlan** command output shows the secondary VLAN, the primary VLAN and interfaces associated with those private VLANs.
	
	Example:
	`switch# show vlan private-vlan`
	`Primary  Secondary  Type              Ports`
	`-------  ---------  ---------------  ----------------------------------------! 152`
	`157        community         Eth3/4`
	`152      158        isolated          Eth3/4`
	`156      153        community         Eth3/4`
	`156      154        community         Eth3/4`
	`156      155        isolated          Eth3/4`

Bug ID	Caveat
CSCsz48343	**Headline**: Link up message while powering up VM (vnic not up) **Symptom**: As a guest operating system is booting, the vEthernet interface shows as link up for a few seconds, then down, and then it finally remains up. **Conditions**: Powering up guest operating system. **Workaround**: Use a flexible adapter and install VMware tools. **Further Problem Description**: If the adapter type is flexible and you have VMware tools installed the Cisco Nexus 1000V VSM indicates the link for a vEthernet interface is up during the virtual machine boot.
CSCsz63126	**Headline**: No switchport mode trunk - change modes to access and not to default **Symptom**: After configuring the switchport mode on an Ethernet interface, the **no switchport mode command** leaves the switchport mode access config setting on the interface, overriding the policy inherited by the port-profile. There is no way to remove it. **Conditions**: Configuring the switchport mode on an Ethernet interface. **Workaround**: If the switchport mode setting has not been saved in the startup-config yet, the VSM can be reloaded to remove the setting. If it has been saved in the startup-config, there is no way to remove it. **Further Problem Description**: None
CSCsz99235	**Headline**: Installing a permanent license file does not add new licenses to the license pool. **Symptom**: After installing a new license file on the VSM, the count of licenses is not increased to show that new licenses were added. **Conditions**: Adding a permanent license file without removing an evaluation license file. **Workaround**: Before installing a new license file, you must first transfer the evaluation licenses from the VEMs back to the VSM license pool and then uninstall the evaluation license from the VSM. **Further Problem Description**: None
CSCta05268	**Headline**: Modules do not come up for a VSM with a VEM port channel running in vPC-HM. **Symptom**: The output of the **show l2 <***control VLAN number***>** command shows *dynamic* for the VM Eth0 MAC. **Conditions**: After the VSM connects to the VEM, for example, when the VSM is reloaded. **Workaround**: Migrate the VSM VM to a vSwitch or another host without vPC-HM. **Further Problem Description**: When a VSM and VEM reconnect, the L2 table entries and port channel are deleted and the physical links carry the same VLANs. This causes broadcast packets from the VSM to go out through one upstream switch and come back through another. Therefore, the Eth0 MAC of the VSM VM is learned on a physical interface and the module never comes up.

Bug ID	Caveat
CSCte28866	**Headline**: Configuring a Cisco Nexus 1000V with the **vlan dot1Q tag native** command does not result in the desired behavior. **Symptom**: The traffic on the native VLAN is not tagged when sent across a trunk. **Conditions**: Configuring a Cisco Nexus 1000V with the **vlan dot1Q tag native** command. **Workaround:** There is currently no workaround. Disabling the native VLAN tagging on the upstream network infrastructure could alleviate the need to use the **vlan dot1Q tag native** command on the Cisco Nexus 1000V.

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

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

General Information

Cisco Nexus 1000V Release Notes, Release 4.0(4)SV1(1)

Cisco Nexus 1000V and VMware Compatibility Information, Release 4.0(4)SV1(1)

Install and Upgrade

Cisco Nexus 1000V Software Installation Guide, Release 4.0(4)SV1(1)

Cisco Nexus 1000V Virtual Ethernet Module Software Installation Guide, Release 4.0(4)SV1(1)

Configuration Guides

Cisco Nexus 1000V License Configuration Guide, Release 4.0(4)SV1(1)

Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(1)

Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(1)

Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(1)

Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(1)

Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.0(4)SV1(1)

Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(1)

Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(1)

Cisco Nexus 1000V High Availability and Redundancy Reference, Release 4.0(4)SV1(1)

Reference Guides

Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(1)

Cisco Nexus 1000V MIB Quick Reference

Troubleshooting and Alerts

Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(1)

Cisco Nexus 1000V Password Recovery Guide

Cisco NX-OS System Messages Reference

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