# CAE

# Nexus 1000V 1.4
# Command Enhancements White
# Paper

**TABLE OF CONTENTS**

# 1  Introduction

The Cisco Nexus 1000V, is a Cisco developed server virtualization switching architecture for VMware ESX environments.  The Nexus 1000V enables policy based virtual machine (VM) connectivity, mobility of security and network properties, and a non-disruptive operational model for both Server and Network administrators.

Offering a set of network features, management tools and diagnostic capabilities consistent with the customer's existing physical Cisco network infrastructure and enhanced for the virtual world, the Nexus 1000V allows customers to accelerate their adoption of VMs through the unification & simplification of the physical and virtual networks.  The Nexus 1000V also secures & simplifies the deployment & movement of VM's to increase service velocity while maintaining and enforcing security policy.

## 1.1  White Paper

The purpose of this white paper is to describe some of the new command enhancements to both the VSM and the VEM  in version 1.4

## 1.2  Assumptions

The assumptions of this white paper are that the reader has
- Installed VMware VC 4.0U1/U2 or VC 4.1
- Installed Cisco Nexus 1000V 1.4 on an ESX VM in HA mode
- At least 2 ESX 4.0U2/U1 or 4.1  boxes with VEM module already loaded
- Created a Nexus 1000V Distributed Virtual Switch (DVS) under vCenter
- Added the ESX boxes to the Nexus 1000V DVS

# 2  Enhancements (Minor Changes)

## 2.1  Feature Command

New in this release of the Nexus 1000V is that many features are now controlled from the feature command. Many features are now turned off by default and the user will have to enable them first with the "feature" command before they can be used.  Below is a list of the features that are now controlled

```
n1kv-bl(config)# feature ?
  dhcp                Enable/Disable DHCP Snooping
  http-server         Enable/Disable http-server
  lacp                Enable/Disable LACP
  netflow             Enable/Disable NetFlow
  port-profile-roles  Enable/Disable Port-profile Roles Feature
  private-vlan        Enable/Disable private-vlan
  ssh                 Enable/Disable ssh
  tacacs+             Enable/Disable tacacs+
  telnet              Enable/Disable telnet  tacacs+
```

```
n1kv-bl# show feature
Feature Name          Instance  State
--------------------  --------  --------
dhcp-snooping         1         disabled
http-server           1         enabled
lacp                  1         enabled
netflow               1         disabled
port-profile-roles    1         enabled
private-vlan          1         disabled
sshServer             1         enabled
tacacs                1         disabled
telnetServer          1         disabled
```

Note that the number of features from 1.4 beta to the FCS version has changed. Some experimental features like LISP and IP pooling were removed for 1.4 FCS.

## 2.2   vemcmd changes

The vemcmd command has also been expanded in this release. You can now query more of the Nexus 1000V configuration directly from the VEM. In addition you can now make minor VEM changes directly on the ESX host itself with vemcmd set.  Take a look at "vemcmd –help" to see all the available options now available with vemcmd.

## 2.3   ethanlyzer

Ethanlyzer has been added to the 1.4 code. It is now possible to analyze traffic without needing an external sniffer or debug plugin.

## 2.4   System VLAN checks

First in version 1.4 the number of supported port-profiles with "system vlan" set has changed from 16 to 32.

New in 1.4 is a change to port-profiles and how they behave when system vlans are set.

When a port-profile is setting "system vlan x" and vlan x is not explicitly allowed in allowed vlan list the command will fail. Below is an example.

```
n1kv-bl(config)# port-profile type eth system-vlan-test
n1kv-bl(config-port-prof)# switchport mode trunk
n1kv-bl(config-port-prof)# vmware port-group
n1kv-bl(config-port-prof)# no shut
n1kv-bl(config-port-prof)# system vlan 2,10
ERROR: Port mode is trunk and the list of configured trunk allowed vlans does not
include some or all of the system vlans being set.
```

Previous versions of the VSM will assume that the allowed vlan list is all when the switchport mode is set to trunk. In 1.4 release you need to explicitly set the systems vlans to be allowed for the command to succeed. Example below…

```
n1kv-bl(config)# port-profile type eth system-vlan-test
n1kv-bl(config-port-prof)# switchport mode trunk
n1kv-bl(config-port-prof)# switchport trunk allowed vlan all
n1kv-bl(config-port-prof)# vmware port-group
n1kv-bl(config-port-prof)# no shutdown
n1kv-bl(config-port-prof)# system vlan 2,10
```

Now you can see that the system vlan succeeds. Just an important note as the default behavior has changed.