Cisco Nexus 1000V Series Switch

Q. What is the Cisco Nexus® 1000V Switch?

A. The Cisco® Nexus 1000V provides virtual machine-level network visibility, isolation, and security for VMware server virtualization. The Cisco Nexus 1000V is a software switch that is embedded in the software kernel of VMware vSphere ESX to deliver virtual machine-aware network services.

It offers the following features:

- Policy-based virtual machine connectivity
- Mobile virtual machine security and network policy
- Nondisruptive operational model

It offers these benefits:

- Enables virtualization of 30 percent more servers
- Allows organizations to spend 30 percent less time on virtual networks
- Eliminates network hurdles to server virtualization

Q. Is there a free 60-day evaluation for the Cisco Nexus 1000V?

A. Yes. The evaluation and download are free and available now at http://www.cisco.com/go/1000veval. All you need is a Cisco.com login, which is free and takes two minutes to obtain (Figure 1).

Figure 1. Evaluate the Cisco Nexus 1000V Today

Q. Is the Cisco Nexus 1000V compatible with VMware products?

A. Yes. The Cisco Nexus 1000V is VMware Ready Certified and supports vSphere 4 Enterprise Plus, in both the embedded or “i” version (ESXi) and the classic version (ESX) of VMware vSphere. The virtual supervisor module can be deployed as a virtual machine on VMware ESX or ESXi 3.5U2 or later or ESX or ESXi 4.

The Cisco Nexus 1000V does not support earlier editions of VMware vSphere (such as the Enterprise or Advanced editions) because these do not have the vDS APIs that are necessary for Nexus 1000V to communicate with vCenter. Earlier versions of the VMware ESX product (for example, ESX 3.0 or 3.5) are also not supported for the same reason.

Q. What are the main VMware vSphere features supported by the Cisco Nexus 1000V?

A. VMware has certified the Cisco Nexus 1000V as VMware Ready Certified. The Cisco 1000V is compatible with the following features:

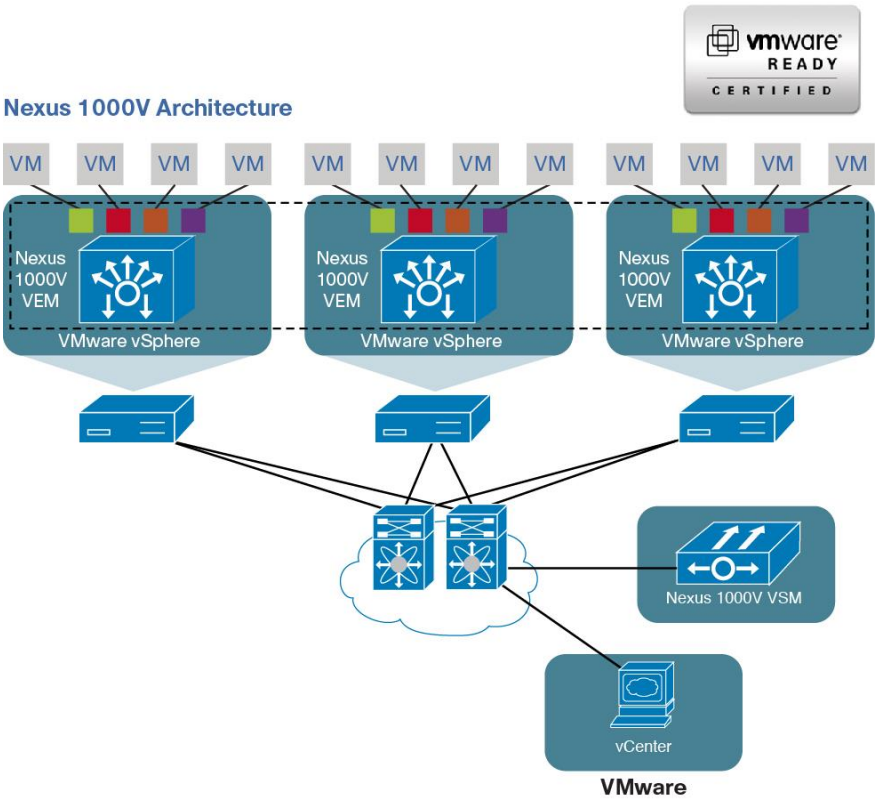
- VMware vMotion
- VMware Distributed Resource Scheduler (DRS)
- VMware High Availability (HA)
- VMware Storage vMotion
- VMware Fault Tolerance (FT)
- VMware Update Manager

Q. What are the components of the Cisco Nexus 1000V?

A. The Cisco Nexus 1000V consists of two components (Figure 2).

- The Cisco Nexus 1000V Series Virtual Supervisor Module (VSM) provides the management plane functions of the switch and is the component that runs Cisco NX-OS Software. The VSM is not in the forwarding path.
- The Cisco Nexus 1000V Series Virtual Ethernet Module (VEM) is a lightweight component that is installed on the hypervisor and provides the switching functions.

Figure 2. Cisco Nexus 1000V Architecture



Q. What are the system requirements?

A. System requirements are as follows:

- Works with all switching architectures
- Cisco Nexus 1000V VSM
  - VMware vSphere Enterprise Plus Version 4.0 or later
  - Can be deployed as a virtual machine on VMware ESX 3.5 or 4
  - Hard disk: 3 GB
  - RAM: 2 GB
  - One virtual CPU at 1 GHz
- Cisco Nexus 1000V VEM
  - VMware vSphere Enterprise Plus version 4.0 or later
  - Hard disk space: 6.5 MB
  - RAM: 150 MB

Q. Is the Cisco Nexus 1000V a Layer 3 switch?

A. No. The Cisco Nexus 1000V is a Layer 2 switch with Layer 3 and 4 awareness to support features such as access control lists (ACLs), NetFlow, quality of service (QoS), and Internet Group Management Protocol (IGMP) snooping.

Q. Can I create a PortChannel to two separate physical switches?

A. Yes. Two options are available.

- If the upstream switches use Cisco Virtual PortChannel (vPC) technology (with Cisco Nexus 5000 or 7000 Series Switches) or Cisco Virtual Switching System (VSS) technology (with Cisco Catalyst® 6500 Series Switches), then just configure a standard PortChannel on the Cisco Nexus 1000V uplink ports.
- If the upstream switches do not use vPC or VSS, you can configure the Cisco Nexus 1000V with the vPC end host mode to connect to two separate physical switches.

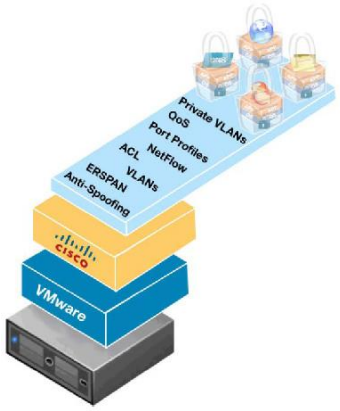
Q. Does the Cisco Nexus 1000V have the security capabilities of the VMware Standard vSwitch?

A. Yes, and more (Figure 3). Security features include protection against MAC address spoofing and flooding and switch forwarding database (FDB) attacks. In addition, the switch provides full ACL and private VLAN support and protection for virtual desktop infrastructure (VDI) deployments. Some of the main features are:

- VLANs
- Private VLANs
- Port mirroring (Switched Port Analyzer [SPAN] and Encapsulated Remote SPAN [ERSPAN])
- ACLs
- Anti-spoofing features
- QoS
- NetFlow Version 9
- Port profiles

- Dynamic Address Resolution Protocol (ARP) inspection
- Dynamic Host Configuration Protocol (DHCP) snooping
- IP source guard

Figure 3. Network Services Provided by the Cisco Nexus 1000V



Q. How does the Cisco Nexus 1000V support existing Cisco Catalyst switches and third-party switches?

A. The Cisco Nexus 1000V works transparently with any type of upstream switch because it uses standard Ethernet protocols to communicate with the upstream switches (including Cisco Discovery Protocol). Switches include both Cisco and third-party switches, including Cisco Catalyst and Cisco Nexus switching architectures.

Q. Should the distributed virtual switch (DVS) also manage the service console virtual network interface card (vNIC) or should the vNIC be on a traditional vSwitch?

A. The service console vNIC as well as the vMotion vNIC and Small Computer System Interface over IP (iSCSI) interfaces can reside on the Cisco Nexus 1000V DVS. Be sure to create the VLANs used by these interfaces as system VLANs.

Q. What MIBs must be included in network management software (such as OpenView Network Node Manager [NNM] for Simple Network Management Protocol [SNMP] monitoring)?

A. Nexus 1000V Data Sheet has complete set of supported MIBs.

Q. Can multiple NICs with the Cisco Nexus 1000V have different uplink profiles and carry different VLANs?

A. Yes.

Q. VMware vSphere currently supports the virtual guest tagging (VGT), virtual switch tagging (VST), and external switch tagging (EST) VLAN tagging modes. What modes does the Cisco Nexus 1000V support?

A. The Cisco Nexus 1000V supports all the models supported by the VMware vSwitch.

Q. In a Cisco Nexus 1000V environment with a single VEM in each host, is VEM-level teaming supported?

A. In a third-party environment, teaming can be configured at the vSwitch level, and the configuration will be overruled by any teaming definitions at the port-group level. In a Cisco Nexus 1000V environment, teaming is configured only at the port-group level (using PortChannels). PortChannels apply only to physical-level NICs (that is, on a per-host basis), so VEM-level teaming is supported.

Q. The settings of the VMware VMkernel NIC and service console NIC were previously configured through the host or VMware vCenter. How are these system uplinks configured in a Cisco Nexus 1000V deployment?

A. Both methods are supported, but the VMware vCenter approach is optimized.

- Example of system uplinks: VMware VMkernel and vMotion, VMkernel and iSCSI, and VMware Service Console
- Example of VMware VMkernel NIC settings: IP address, gateway, speed, and mode

Q. What are the differences in Cisco Nexus 1000V configuration and functions for VMware ESX and ESXi?

A. The Cisco Nexus 1000V does not differentiate between VMware ESX and ESXi except in the installation of the binary packages, which is handled transparently.

Q. Does the Cisco Nexus 1000V support 64-bit hosts?

A. Yes. In fact, VMware vSphere supports only 64-bit hosts. VMware supports both 64- and 32-bit virtual machines on those hosts.

Q. Does the Cisco Nexus 1000V support Ethernet switching?

A. The Cisco Nexus 1000V supports high-density, high-performance Ethernet systems and provides the following Ethernet switching features:

- IEEE 802.1Q VLANs and trunks
- Private VLANs
- Cross-chassis private VLANs

Q. Does the Cisco Nexus 1000V support jumbo frames?

A. Yes. The Cisco Nexus 1000V supports jumbo frames up to 9000 bytes, as long as the NIC supports them.

Q. Does the Cisco Nexus 1000V support IGMP?

A. The Cisco Nexus 1000V supports IGMPv3 and performs replication locally in the host to optimize delivery of the multicast traffic only to the virtual machines that are part of the specific multicast group. IGMP support includes:

- IGMPv1, v2, and v3 router roles
- IGMPv2 host mode
- IGMP snooping
- Ethernet interfaces and PortChannels

Q. Does the Cisco Nexus 1000V support Link Aggregation Control Protocol (LACP)?

A. Yes. Both static and dynamic LACP are supported.

Q. Does the Cisco Nexus 1000V support NetFlow?

A. Yes. NetFlow Version 9 is supported.

Q. Does the Cisco Nexus 1000V support private VLAN promiscuous trunks?

A. Yes.

Q. Does the Cisco Nexus 1000V support QoS?

A. The Cisco Nexus 1000V supports classification, marking, rate limiting, and policing.

Q. Does the Cisco Nexus 1000V support SNMP?

A. Yes:

- SNMPv1, v2, and v3
- Enhanced SNMP MIB support

Q. What high-availability features are available on the Cisco Nexus 1000V?

A. The following high-availability features are supported:

- Nonstop forwarding (NSF): Forwarding continues despite communication disruption between the VSM and VEM.
- Stateful supervisor failover: Synchronized redundant supervisors are always ready for failover while maintaining consistent and reliable state information.
- Process survivability: Critical processes run independently for ease of isolation, fault containment, and upgrading. Processes can restart independently in milliseconds without losing state information, affecting data forwarding, or affecting adjacent devices or services.

Q. Does the Cisco Nexus 1000V support multiple VSMs for redundancy?

A. Yes. VSM redundancy is available. Up to two VSMs can be deployed in an active-standby configuration, using the same active-standby failover model that customers have today in the Cisco Nexus 7000 Series with redundant supervisors. Redundant VSMs do not require additional licenses.

Q. Is there a Layer 2 requirement for the high availability of active and standby VSMs?

A. Yes. The active and standby VSMs need to be Layer 2 adjacent.

Q. Can VSMs be part of a VMware vSphere high-availability cluster?

A. Yes.

Q. Will the VSM be supported in a high-availability configuration with its virtual machine disk format (VMDF) in a shared logical unit number (LUN)?

A. Yes.

Q. What happens if the VSM is down?

A. While the VSM is down, the VEMs continue to forward traffic using the last known configuration. Any new virtual machines that are started on those VEMs will not have connectivity because the VSM will not be available to set up the port configurations. When the virtual machine is migrated, the virtual Ethernet (vEth) ports will not be configured on the new host because the VSM is not there. However, Cisco plans to address this situation in the future. The NetFlow cache will be maintained in the VEM, and the Switched Port Analyzer (SPAN) will continue to work.

Q. In what cases will module 2 be used?

A. In a high-availability setup, the standby VSM will be module 2.

Q. What is a port profile?

A. A port profile is a container of network properties that can be saved and quickly applied to the various interfaces. A virtual machine inherits all the network properties of the port profile after VMware vMotion migration has occurred. Unlike with a smart-port macro, when you change a port profile, all the interfaces subscribed to that profile are instantly updated. Port profiles can inherit a configuration from another port profile; therefore, you can create a configuration hierarchy and easily and quickly apply configuration and policy changes.

Q. Is QoS implemented on each VEM or are there queues on the vEth interfaces?

A. The Cisco Nexus 1000V supports classification, marking (class of service [CoS] and Differentiated Services Code Point [DSCP]) and rate limiting. Queuing is not yet implemented. A QoS policy assigned to a port profile would allow classification and marking to occur and would apply rate limiting to the virtual machine vEth interface.

Q. What network properties are supported as policy definitions?

A. The following properties are supported as policy definitions:

- VLAN and private VLAN (PVLAN) settings
- ACLs, port security, and ACL redirection
- NetFlow collection
- Rate limiting
- QoS marking (CoS and DSCP)
- Remote port mirror (Encapsulated Remote SPAN [ERSPAN])

Q. Can port profiles (VLAN, virtual routing and forwarding [VRF], and firewall context) be modified in VMware vCenter?

A. No. Port profiles set in the network with Cisco Nexus 1000V will appear as VMware vCenter port groups. VMware vCenter will not be able to modify the policy settings.

Q. How are port profiles associated with port groups in VMware vCenter?

A. When the port profile is created on the VSM, the network administrator declares it as a VMware port profile. The VSM then pushes that port profile through an API to VMware vCenter. Within VMware vCenter, the port profile appears as a port group to the server administrator.

Q. How is a port profile applied to a virtual machine?

A. When a new port profile is configured on the VSM, it is pushed to VMware vCenter and appears as a port group. When the server administrator attaches a port group to a virtual machine using VMware vSphere, VMware vSphere notifies the VEM that it has to attach this vEth interface to this port profile. The VEM then updates the VSM, reporting that it has a new virtual machine using this port profile.

Q. Can a single port profile be applied to more than one port?

A. Yes. Unlike a physical port on a switch, which has a static configuration for each and every port, the port profile is a template that can be attached in a one-to-many relationship.

Q. Can a port profile be changed while it is in use?

A. Yes.

Q. Can a port profile be overridden?

A. Yes.

Q. When a port profile configuration is changed, does that change take effect immediately?

A. Yes.

Q. Can a port profile contain another port profile within its configuration?

A. Yes. Port profiles support the concept of inherency. This concept can be used, for example, to create base port profiles to define the VLAN and child port profiles to define different QoS levels within that same VLAN.

Q. Should multiple Cisco Nexus 1000V domains be created in large data centers and what criteria should be used to group them?

A. Domains can be based on physical points of delivery (PODs), business groups, security rules, compliance rules, failure domains, and other criteria according to the customer's business requirements. The number of domains that can be created depends on the number of servers. One VSM can support multiple VEMs across one or multiple clusters, within a single instance of vCenter. A VMware ESX or ESXi host can contain only one VEM and therefore can be managed by only one VSM pair (active-standby).

Q. What features should be configured using the port profile?

A. The port profile should include anything you can configure in a physical interface configuration such as VLANs, QoS policy, security policies, and administrative state.

Q. Does the Cisco Nexus 1000V support Cisco Discovery Protocol and in what modes?

A. Yes. Cisco Discovery Protocol is supported in both its modes: listen only and listen and advertise.

Q. Is the number of VLANs per virtual machine limited to the number of vNICs or pNICs?

A. No. Although the number of VLANs per virtual machine is not limited, VMware currently limits the number of vNICs per virtual machine to four. Thus, unless you are trunking multiple VLANs to each vNIC, you are limited to four VLANs per virtual machine.

Q. Will Cisco ship an IEEE 802.1Q driver for guest access?

A. No. The OS will provide this driver.

Q. The service console and virtual machines typically are connected to two different vSwitches. Can two Cisco Nexus 1000V instances be started?

A. The Cisco Nexus 1000V architecture, with a single VEM per host and advance networking capabilities, allows proper segmentation of VMware ESX functions while still providing a consistent management entity. Only one VEM instance is required per physical host.

Q. When Cisco Nexus 1000V starts, does it reserve CPU space and memory? If traffic is heavy, will VMware vSphere prioritize Cisco Nexus 1000V over virtual machines?

A. No. There is no explicit reservation, but the scheduler is designed not to be starved or to overuse CPU or memory.

Q. What port security features are supported?

A. Port security, IP source guard, dynamic ARP inspection, DHCP snooping, ACLs, and private VLANs are supported. Nexus 1000V also supports Cisco vPath, which enables virtualized network services, such as the Cisco Virtual Security Gateway.

Q. Can a single policy define different levels of bandwidth for traffic that remains inside the Cisco Nexus 1000V in contrast to traffic that is destined for an external address?

A. You can implement policy that is enforced only on the pNIC so that the policy is enforced only for packets leaving that physical host. Weighted Fair Queuing can be used to help ensure minimum bandwidth across a port channel for different classes of traffic.

Q. Will the profile configurations be maintained in a host profile on VMware vSphere?

A. The Cisco Nexus 1000V will automatically push profiles down to new machines that are added to the switch. Cisco is exploring ways to better integrate with host profiles, and a solution will be available in the near future.

Q. Is creating a port profile on the Cisco Nexus 1000V and making it available within VMware vCenter equivalent to leaving a physical network interface open and enabled on a switch?

A. Yes and no: yes in the sense that after the port profile is created, a virtual machine can use it and connect to a vEth interface; and no in the sense that the interface will be constrained by whatever policy you have defined and will not be just an open port. You can, if you want, define a port profile without the **no shutdown** command. This command will force the network administrator to enter no shut in the CLI when the connection is created. One reason that server administrators like virtual connection is that they do not have to wait for the network administrator.

Q. What are the VMware vMotion configuration guidelines?

A. Follow these guidelines for VMware vMotion configuration.

- When moving a virtual machine with VMware vMotion, the vNICs of the virtual machine need to have the same policies configured on the source and destination hosts as on the switches on these hosts.
- Thus for VMware vMotion movement of a virtual machine, the source and destination hosts need to have the same switch type (Cisco Nexus 1000V or VMware DVS).
- You cannot use VMware vMotion to move a virtual machine when it is connected to a Cisco Nexus 1000V Switch on the source host to a VMware DVS on the target host, or the opposite.
- A single host can have one instance of Cisco Nexus 1000V and one or more instances of VMware DVS (just like multiple vSwitches on a single host today).
- When a host has Cisco Nexus 1000V and VMware DVS running on it, they are mutually exclusive: one does not talk to the other (and the same is true with multiple instances of VMware DVS running on that host).
- When a host has more than one switch instance, a single pNIC cannot be shared between the switch instances. However, a virtual machine can have one vNIC connected to one switch (for instance, Cisco Nexus 1000V) and another vNIC connected to another switch (for example, VMware DVS). If such a virtual machine migrates from this host to another, a similar configuration needs to exist on the target host (with both Cisco Nexus 1000V and VMware DVS present).
- All hosts in the cluster need to have the same type of switch present (for example, Cisco Nexus 1000V).
- All hosts in the cluster need to be part of the same Cisco Nexus 1000V instance. For example, if you have two Cisco Nexus 1000V instances (Cisco Nexus 1000V-A and Cisco Nexus 1000V-B), you cannot use VMware vMotion to move a virtual machine from a VEM (or host) on Cisco Nexus 1000V-A to a VEM (or host) on Cisco Nexus 1000V-B.
- A single Cisco Nexus 1000V VSM instance (for example, Cisco Nexus 1000V-A) can support multiple clusters across multiple VEMs.

Q. How does VMware vMotion work for a virtual machine that has vNICs connected to a Cisco Nexus 1000V DVS as well as vNICs connected to a VMware vSwitch?

A. Assuming that the VMware vSwitch and Cisco Nexus 1000V are both available on the source and destination hosts, the migration process will be transparent.

Q. How does VMware Storage vMotion work in a Cisco Nexus 1000V environment?

A. VMware Storage vMotion works as usual in a Cisco Nexus 1000V environment. If the back-end storage is accessed from the Cisco Nexus 1000V, VMware Storage vMotion will function as expected.

Q. Do the upstream physical switches have to be Layer 2 adjacent when virtual machines are moved from one host server to another using VMware vMotion?

A. Yes. The hardware switches provide VLAN and Layer 2 connectivity to the Cisco Nexus 1000V and the virtual machines running on the servers. If the physical access switches do not have access to the same Layer 2 domains, the virtual machine's connectivity will be disrupted during a VMware vMotion movement.

Q. Does the Cisco Nexus 1000V place any limitations on VMware vMotion?

A. No. The Cisco Nexus 1000V is bounded by the same limitations as VMware vSphere. There are known methods to increase the number of concurrent VMware vMotion migrations within VMware vSphere, and this tweak is supported by Cisco Nexus 1000V.

Q. When VMware vMotion migration occurs, does the port profile follow the virtual machine?

A. Yes. Not only does the port profile move, but the vEth interface itself moves, thus maintaining the port configuration and state, including NetFlow, port statistics, and any SPAN and ERSPAN sessions.

Q. Is port security supported in VMware vMotion scenarios?

A. Yes. Port security is supported across VMware vMotion. Port security is part of the port profile for a given virtual machine, and during a VMware vMotion process, the policy travels along from one physical server to another.

Q. Does the Cisco Nexus 1000V have any additional VMware vMotion requirements compared to a standard vSwitch?

A. No. The same requirements exist for VMware vMotion and Storage vMotion.

Q. Are evaluation licenses available for the Cisco Nexus 1000V?

A. Yes. A free 60-day evaluation license for 16 CPU sockets is available by default.

Q. Does the Cisco Nexus 1000V require a 64-bit virtual machine?

A. Yes. The Cisco Nexus 1000V requires a 64-bit virtual machine. When building the virtual machine, choose Linux Other 64-bit.

Q. What is the Cisco Nexus 1000V Installer application?

A. The Cisco Nexus 1000V Installer application helps complete the Cisco Nexus 1000V initial VSM configuration through a wizard-style user interface. In this installer, the VSM's connectivity option (either Layer 2 or Layer 3), management IP address, gateway, subnet mask, administrative password, and port groups will be configured. Additionally, the installer application will create a connection to VMware vCenter Server after registering the VSM's extension key.

Q. How can I access the Cisco Nexus 1000V Installer application?

A. The Cisco Nexus 1000V Installer application runs as a Java applet on the VSM's web server. After you deploy the Cisco Nexus 1000V open virtual appliance (OVA) image and choose the Installer deployment option, you can access the application through a browser at the management IP address allocated during installation. Note that the management port group, management IP address, gateway, and subnet mask must be correctly set during OVA deployment to allow the VSM's web server to remain accessible.

Q. Do I need to deploy the OVA image before using the installer application?

A. Yes. The Cisco Nexus 1000V OVA image must be deployed and set up with the installer deployment option to allow use of the installer application.

Q. Does the installer application set the control and packet VLANs in the upstream switch?

A. No. All VLAN configurations in the upstream switch must be set through normal means. The installer application manages only port group assignment and creation using these VLANs.

Q. Does the installer application create the DVS?

A. Yes, the Installer Application will use the provided information to create a DVS that will boot when the VSM is started.

Q. Does the installer application also install the VEM?

A. No. Currently the installer application only configures the VSM. VEMs can be installed either by using VMware Update Manager or through a manual installation.

Q. Can I manually configure the VSM and skip the installer application?

A. Yes. When deploying the Cisco Nexus 1000V OVA image, choose the Manual deployment option when prompted to configure the VSM manually.

Q. What kind of virtual connection credentials do I need to use the installer application?

A. To run the installer application, you need to have virtual connection credentials allowing you to edit the virtual machine host's network configurations as well as virtual machine administrative privileges (allowing you to power the virtual machine on and off and reconfigure the virtual machine).

Q. Will the installer application restart my VSM virtual machine?

A. Yes. To complete specific operations, the installer application will need to restart the VSM virtual machine twice during the configuration process.

Q. Can I name the new port group I chose to create through the installer application?

A. No. Currently, default names are given to any new port groups created through the installer application. These port groups are named Control-auto, Management-auto, and Packet-auto for the control, management, and packet port groups, respectively.

Q. Can I make changes to the information I entered in the installer application prior to clicking finish?

A. Yes. The installer application will make no changes to your virtual connection or virtual machine until you click Finish. Changes can be made by going back through the wizard and modifying the entered values.

Q. Can I use the installer application to configure port groups over multiple vSwitches?

A. No. Currently, the Cisco Nexus 1000V Installer application supports configuration of only the control, management, and packet port groups on a common vSwitch.

Q. I'm not using VMware Update Manager. Where can I find the VEM binary (VIB) file to use with esx4update?

A. The VIB files can be found on the Cisco.com website. A valid Cisco.com user ID is required to download the software. Registration is free. Go to: http://www.cisco.com/pcgi-bin/swsrch/SWSearch_results.cgi/SWSearch.txt?searchPhrase=nexus+1000v&isChild=false&file_delimiter=contains.

If you are patching devices manually, new VMware kernel modules usually require a VEM patch. These patches are available for download from VMware at https://www.vmware.com/mysupport/download/. Choose VEM in the pull-down menu.

Q. If I am using VMware Update Manager, do I need to manually install the VEM package?

A. No. VMware Update Manager will install the correct version of Cisco Nexus 1000V on your host, including matching the correct version of VMware ESX or ESXi 4.0.0 that you are running.

Q. Are code versions backward compatible with each other?

A. Yes. Users can upgrade their VSMs and retain the existing configuration.

Q. Can a VSM control a set of VEMs of varying versions?

A. Yes, but any new features introduced in the newer versions will be available only to VEMs running that newer version of code.

Q. What is the feature level and how and when can I change it?

A. The feature level is the version number that defines which features can be enabled in the switch. By default, after a switch has been upgraded, the feature level will remain at the version number in effect before the upgrade. The feature level can be updated only after all the connected VEMs have been upgraded.

Q. Is the feature level automatically updated after an upgrade?

A. No. You must upgrade the feature level using the system **update vem** feature-level command.

Q. Is the feature level persistent across VSM reloads?

A. Yes.

Q. Can I downgrade only the VEM code?

A. No. VEM software downgrades are not supported in this release.

Q. Is ISSU supported for the Cisco Nexus 1000V?

A. Yes. ISSU is available as of the 4.0(4)SV1(4) release.

Q. How do I remove a VSM from VMware vCenter?

A. A VSM can be removed from VMware vCenter only using the **no vmware dvs** command under the svs connection. You cannot remove the DVS from within VMware vCenter.

If you remove or destroy the VSM without entering the command, the old Cisco Nexus 1000V will remain in VMware vCenter until you perform the steps described next. You will need to reconnect the existing VSM or create a new VSM with the same extension key to VMware vCenter to remove it.

1. Create a new VSM from either the ISO or OVF image.
2. Find the extension key linked to the old DVS and configure it on the new VSM. To find the extension key, follow the information in this link: http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0/troubleshooting/configuration/guide/trouble_3install.html#wp1206322.
3. Set the extension key on the new VSM with the following command: **n1000V(config)# vmware vc extension-key [key]**
4. Unregister the related extension key in VMware vCenter with the instructions in the following link: http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0/troubleshooting/configuration/guide/trouble_3install.html#wp1196708.
5. Open a browser, browse to the VSM, and download the extension.xml file. Make sure you refresh the browser page to get the current extension key.

6. Register the new extension.xml file in VMware vCenter.
7. Verify that the switch name of the VSM is the same as the name of the DVS you are trying to delete.
8. Create the svs connection to connect to the same data center.
9. Connect the VSM to VMware vCenter with **connect** under the svs connection.
10. After the VSM connects to VMware vCenter, delete the DVS using the **no vmware dvs** command under the svs connection.

Q. What is the virtual service domain (VSD)?

A. The VSD is a logical domain that groups a set of ports on a single host. Any typical VSD configuration contains service virtual machine (SVM) ports and VSD member ports. Any traffic destined to these member ports will be processed by SVMs. Similarly, any traffic that is sourced by these member ports will be processed by SVMs before being forwarded to the original destination.

SVM ports consist of inside ports, outside ports, and management ports:

- Inside port: Any traffic that is destined to a particular VSD will be redirected to the SVM through the inside port. After the traffic is processed by the SVM, the traffic will be forwarded to the VSD through the outside port. If the SVM is VMware vShield, this port is same as the protected-mode (P0) port of the VMware vShield instance.
- Outside port: Any traffic that originates from a particular VSD will redirected if it reaches the SVM through the outside port. After the traffic is processed by the SVM, the traffic will be forwarded to destinations through the outside port. If the SVM is VMware vShield, this port is same as the unprotected-mode (U0) port of the VMware vShield instance.
- Management port: This port is used by the SVM instance to talk to the SVM manager, which controls multiple SVMs across the cluster or data center.

Member ports are group of ports. Any traffic destined to or sourced from these ports is serviced by the SVM.

Q. What is the SVM?

A. A service virtual machine, or SVM, is any virtual machine that provides functions such as firewalls and monitoring capabilities. It should have separate ports for incoming and outgoing traffic. An SVM should have its own instance on each host on which the packets need to be serviced. Cisco Nexus1000V fully supports VMware vShield as an SVM.

Q. What should I check before powering on the VMware vShield SVM instance?

A. Make sure that management, inside, and outside virtual machine network interface cards (VMNICs) on VMware vShield instances are configured with appropriate port profiles. Powering on a VMware vShield instance without attaching the correct port profile may result in flooding in the network. Any change in the port profile binding on a VMware vShield instance requires you to power off the instance.

Q. How are VMware vShield zones configured on the Cisco Nexus 1000V?

A. Every VMware vShield instance has three ports: a management port, an inside port, and an outside port.

1. Define the port profile with the service port capability inside: for example, Inside_Profile.
2. Define the port profile with the service port capability outside: for example, Outside_Profile.
3. The first VMNIC of the VMware vShield instance is always used to talk to the VMware vShield Manager (it should be Layer 3 connected: that is, the VMware vShield Manager and VMware vShield instance management port should have IP addresses). This VMNIC can be in the vSwitch or on the Cisco Nexus 1000V DVS. If it is on Cisco Nexus 1000V DVS, make sure that the correct profile is appended to the VMNIC that provides the connectivity to the VMware vShield Manager. For more information about configuring VMware vShield Manager and the VMware vShield management port, consult the VMware vShield documentation.
4. The second VMNIC must always be bound to the inside port: that is, attach Inside_Profile to this VMNIC.
5. The third VMNIC must always be bound to the outside port; attach Outside_Profile to this VMNIC.
6. Power on the VMware vShield instance of the host.
7. Tag all the member port profiles with the appropriate VSD through configuration commands.

Q. What is the significance of “default-action <drop| forward>” in the SVM port profile?

A. When the SVM of the VSD cannot be reached, the Cisco Nexus 1000V takes this attribute configuration into consideration and either forwards or drops the traffic that is destined to or sourced from members of the VSD.

Q. Can the member interface belong to multiple VSDs at the same time?

A. No. Any member interface can belong to only one VSD at a time.

Q. How many VMware vShield instances per host are supported?

A. Eight VMware vShield instances are supported per host. Every VMware vShield instance’s inside and outside port on the host should have a unique port profile bound to it. After the packet enters the host, it can be serviced by up to two VMware vShield instances.

Q. Which traffic is not serviced by a VMware vShield instance?

A. Any CPU-bound traffic such as Cisco Discovery Protocol, Link Aggregation Control Protocol (LACP), and Internet Group Management Protocol (IGMP) control packets is not serviced (filtered) by VMware vShield instance intra-VSD traffic: that is, any traffic between ports that are in the same VSD within a host will not be serviced by the VMware vShield instance.

Q. Is VMware vMotion migration of VMware vShield supported?

A. VMware vMotion migration of a VMware vShield instance is not supported because the VMware vShield instance is host based and needs to be installed on every host that must be processed by VMware vShield. However, the application virtual machines that are serviced by the VMware vShield instance can be migrated with VMware vMotion. If the VEM that is hosting the migrated virtual machine does not have a VMware vShield instance, it will drop the packets to and from this virtual machine after being migrated.

Q. Are features such as ACLs, ERSPAN, QoS, PortSec, DHCP, and PVLAN supported on SVM ports?

A. SVM ports are treated like standard promiscuous ports, so feature configuration is not recommended on SVM ports. However, all feature configurations are supported on member ports of VSD. For detailed Information about VMware vShield, see http://www.vmware.com/support/pubs/vsz_pubs.html.

Q. What is Cisco vPath and how does it relate to the Cisco Nexus 1000V?

A. Cisco vPath provides unified network services support in a virtualized environment. Specifically, vPath offers the following in the VEM:

- Intelligent traffic steering
- Flow classification and subsequent redirection to the designated virtual network service virtual machine or virtual service node (VSN)
- Network service acceleration, providing faster network services with flow-based decision caching in the VEM
- Scaling of network services because the VEM is on every hypervisor

Cisco Virtual Security Gateway (VSG) is the first product to use the Cisco vPath architecture.

Q. What is VXLAN and how does it relate to the Cisco Nexus 1000V?

A. Cloud-based computing requires support for large numbers of customers and applications and therefore demands even more scalable networks. In particular, each tenant, and each application within each tenant, requires its own network that is logically isolated from other networks. Because of this increased need for logical networks, Cisco introduced Virtual Extensible Local Area Network (VXLAN) in the Cisco Nexus 1000V Series, providing support for cloud networking. For more information, please visit the Cisco Nexus 1000V Series Switches Data Sheet.

Q. Is Cisco Nexus 1000V integrated with VMware vCloud Director?

A. Yes, the Cisco Nexus 1000V with VXLAN is fully integrated with VMware vCloud Director.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C67-556624-02 01/12