CHAPTER 1

Overview

This chapter provides an overview of the product, Cisco Nexus 1000V, and includes the following sections:

- Information about Virtualization, page 1-1
- Information About Cisco Nexus 1000V, page 1-2

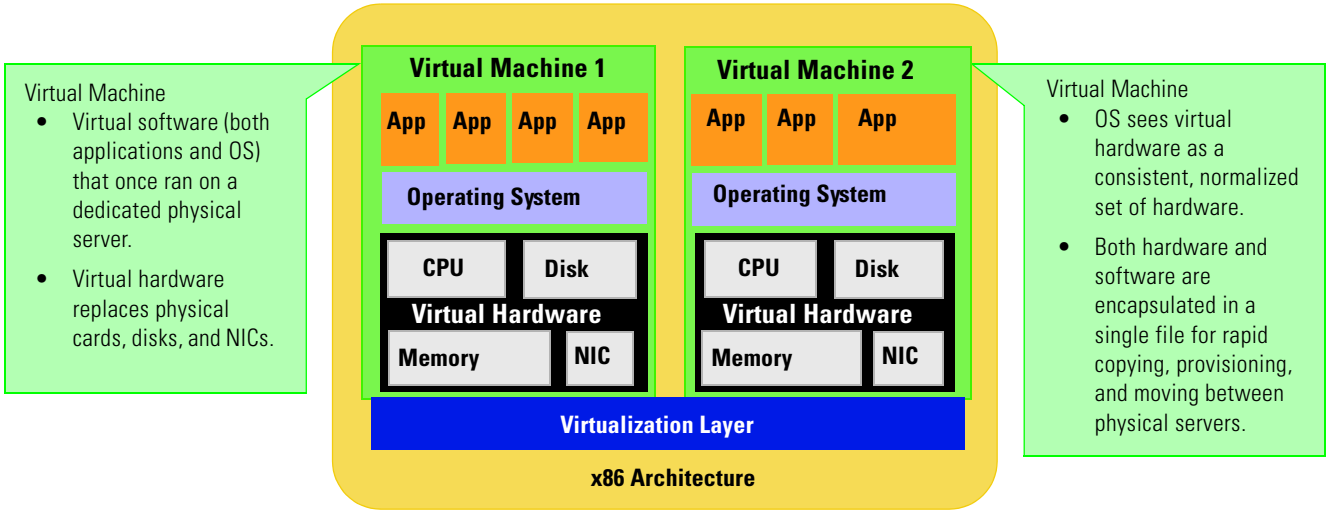
Information about Virtualization

Virtualization allows the creation of multiple virtual machines to run in isolation, side-by-side on the same physical machine.

Each virtual machine has its own set of virtual hardware (RAM, CPU, NIC) upon which an operating system and applications are loaded. The operating system sees a consistent, normalized set of hardware regardless of the actual physical hardware components.

Virtual machines are encapsulated into files, for rapid saving, copying and provisioning. Full systems (fully configured applications, operating systems, BIOS and virtual hardware) can be moved, within seconds, from one physical server to another for zero-downtime maintenance and continuous workload consolidation.

Two virtual machines running in isolation side-by-side on the same physical machine



Information About Cisco Nexus 1000V

This section includes the following topics:

- System Description, page 1-2
- Administrator Roles, page 1-4
- Contrasting the Cisco Nexus 1000V with a Physical Switch, page 1-5
- Implementation Considerations, page 1-5
- Configuring Cisco Nexus 1000V with CLI, page 1-5

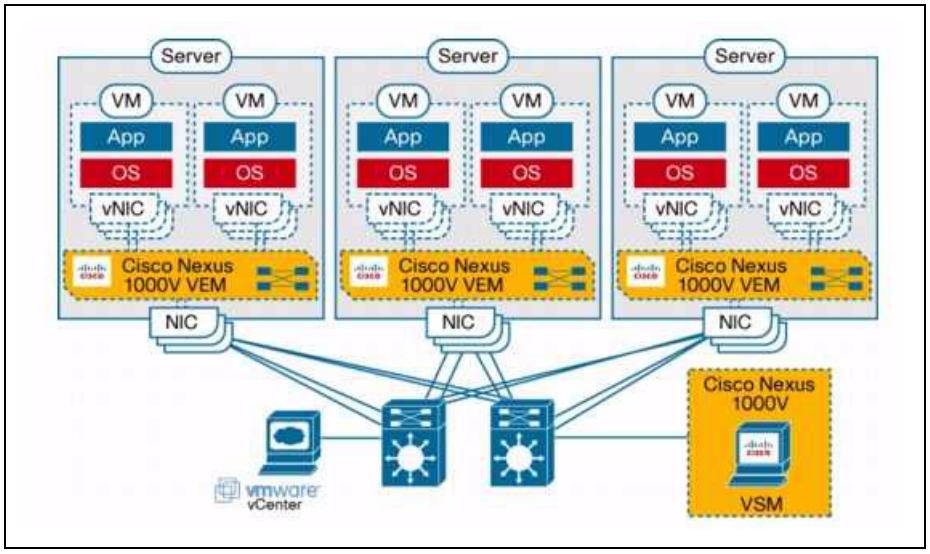
System Description

The Cisco Nexus 1000V is a virtual access software switch for vNetwork Distributed Switches that work with VMware vSphere 4.0. It has the following components:

- The Virtual Supervisor Module (VSM)— the control plane of the switch and a virtual machine that runs the NX-OS operating system.
- The Virtual Ethernet Module (VEM) —a virtual line card embedded in each VMware vSphere (ESX) host that is a part of the distributed switch. The VEM is partly inside the kernel of the hypervisor and partly in a user world process, called the VEM Agent.

Figure 1-1Cisco Nexus 1000V Distributed Virtual Switch, page 1-2shows the relationship between the Cisco Nexus 1000V components.

Figure 1-1 Cisco Nexus 1000V Distributed Virtual Switch



The VSM uses an external network fabric to communicate with the VEMs. The physical NICs on the VEM server are uplinks to the external fabric. VEMs switch traffic between the local virtual Ethernet ports connected to VM vNICs, but do not switch traffic to other VEMs. Instead, a source VEM switches

packets to uplinks that the external fabric then delivers to the target VEM. The VSM runs the control plane protocols and configures the state of each VEM, but it never takes part in the actual forwarding of packets.

A single VSM can control up to 64 VEMs.Cisco recommends that you install two VSMs in an active-standby configuration for high availability. With the 64 VEMs and the redundant supervisors, the Cisco Nexus 1000V can be viewed as a 66-slot modular switch.

The VSM(s) and the VEMs must be in the same Layer 2 network. The VMware vCenter server can be separated from the VSM(s) and the VEM by a Layer 3 router.

A single Cisco Nexus 1000V instance, including dual redundant VSMs and managed VEMs, forms a switch domain. Each Cisco Nexus 1000V domain within a VMware vCenter Server needs to be distinguished by a unique integer called the Domain Identifier.

Control and Packet VLANs

The Control VLAN and the Packet VLAN are used for communication between the VSM and the VEMs within a switch domain: .

- The Packet VLAN is used by protocols such as CDP, LACP, and IGMP.
- The Control VLAN is used for the following:
  - VSM configuration commands to each VEM, and their responses
  - VEM notifications to the VSM, for example a VEM notifies the VSM of the attachment or detachment of ports to the DVS
  - VEM NetFlow exports are sent to the VSM, where they are then forwarded to a NetFlow Collector.

Cisco recommends that the Control VLAN and Packet VLAN be separate VLANs; and that they also be on separate VLANs from those that carry data.

Caution If you are installing more than one VSM within the same VMware vCenter Server, Cisco recommends the use of distinct Control/Packet VLAN pairs for each domain. If you must use the same VLAN pair for multiple domains, you must ensure that their domain identifiers are different.

Port Profiles

A port profile is a set of interface configuration commands that can be dynamically applied to either the physical (uplink) or virtual interfaces. A port profile can define a set of attributes including the following:

- VLAN
- port channels
- private VLAN (PVLAN),
- ACL
- port security
- NetFlow
- rate limiting
- QoS marking

The network administrator defines port profiles in the VSM. When the VSM connects to vCenter Server, it creates a distributed virtual switch (DVS) and each port profile is published as a port group on the DVS. The server administrator can then apply those port groups to specific uplinks, VM vNICs, or management ports, such as virtual switch interfaces or VM kernel NICs.

A change to a VSM port profile is propagated to all ports associated with the port profile. The network administrator uses the Cisco NX-OS CLI to change a specific interface configuration from the port profile configuration applied to it. For example, a specific uplink can be shut down or a specific virtual port can have ERSPAN applied to it, without affecting other interfaces using the same port profile.

For more information about port profiles, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(1)*.

System Port Profile and System VLAN

When a server administrator adds a host to the DVS, the VEM in that host needs to be able to configure the VSM. Since the ports and VLANs for this communication are not yet in place, System Port Profiles and System VLANs are configured to meet this need. VSM sends minimal early configuration to the vCenter Server, which then propagates it to the VEM when the host is added to the DVS.

A system port profile is designed to establish and protect vCenter Server connectivity. It can carry the following VLANs:

- System VLANs or VNICs used when bringing up the ports before communication is established between the VSM and VEM.
- The uplink that carries the control VLAN
- Management uplink(s) used for VMWare vCenter Server connectivity or SSH or Telnet connections. There can be more than one management port or VLAN, for example, one dedicated for vCenter Server connectivity, one for SSH, one for SNMP, a switch interface, and so forth.
- VMware kernel NIC for accessing VMFS storage over iSCSI or NFS.

Administrator Roles

The Nexus 1000V enables the network and server administrators to collaboratively manage the switch. The network administrator is responsible for the VSM, including its creation, configuration and maintenance. The server administrator manages the hosts and the VMs, including the connection of specific VM ports and host uplinks to specific port groups, which are published in the vCenter Server by the network administrator. The VEMs are part of the network administrator's domain, but the server administrator has a say in the installation, upgrade, or deletion of a VEM.

The following table describes the administrator roles.

Table 1-1 Administrator Roles

Network Administrator	Server Administrator
• Creates, configures, and manages vswitches. • Creates, configures, and manages port profiles, including the following: – security – port channels – QOS policies	• Assigns the following to port groups: – VNICs – vmkernel interfaces – service console interfaces • Assigns physical NICs (also called PNICs) to vswitches on each host.

Contrasting the Cisco Nexus 1000V with a Physical Switch

The following are the differences between the Cisco Nexus 1000V and a physical switch:

- **Joint management by network and server administrators**
- **External fabric**
  The supervisor(s) and line cards in a physical switch have a shared internal fabric over which they communicate. The Cisco Nexus 1000V uses the external fabric.
- **No switch backplane**
  Line cards in a physical switch can forward traffic to each other on the switch's backplane. Since the Nexus 1000V lacks such a backplane, a VEM cannot directly forward packets to another VEM. Instead, it has to forward the packet via some uplink to the external fabric, which then switches it to the destination.
- **No Spanning Tree Protocol**
  The Nexus 1000V does not run STP because it will deactivate all but one uplink to an upstream switch, preventing full utilization of uplink bandwidth. Instead, each VEM is designed to prevent loops in the network topology.
- **Port channels only for uplinks**
  The uplinks in a host can be bundled in a port channel for load balancing and high availability. The virtual ports cannot be bundled into a port channel, since there is no reason to.

Implementation Considerations

The following are things to consider when implementing Cisco Nexus 1000V:

- Vmotion of the VSM VM is not supported. In particular, DRS should not be enabled for the VSM VM. Vmotion and DRS are supported for other VMs connected to the Cisco Nexus 1000V.
- VMware Fault Tolerance is not supported for the VSM VM. It is supported for other VMs connected to Cisco Nexus 1000V.
- The snapshot of the VSM VM will not contain the configuration changes made since the snapshot was taken. So, restoring the VSM VM from a snapshot may require some care.
- The server administrator should not assign more than one uplink on the same VLAN without port channels. In other words, it is not supported to assign more than one uplink on the same host to a profile without port channels or port profiles that share one or more VLANs.

Software Compatibility

Cisco Nexus 1000V VSM can be implemented as a virtual machine in the following VMware environments:

- VMware ESX/i 3.5U2 or higher
- ESX/i 4.0. (requires Enterprise Plus edition of vSphere 4)

Configuring Cisco Nexus 1000V with CLI

Cisco Nexus 1000V is configured using a command line interface (CLI) from any of the following:

- an SSH session (SSH provides a secure connection.)

- a Telnet Session
- a service console for the VM running the VSM

For information about the CLI, see the "Understanding the CLI" section on page 2-1.