CHAPTER 1

Overview

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

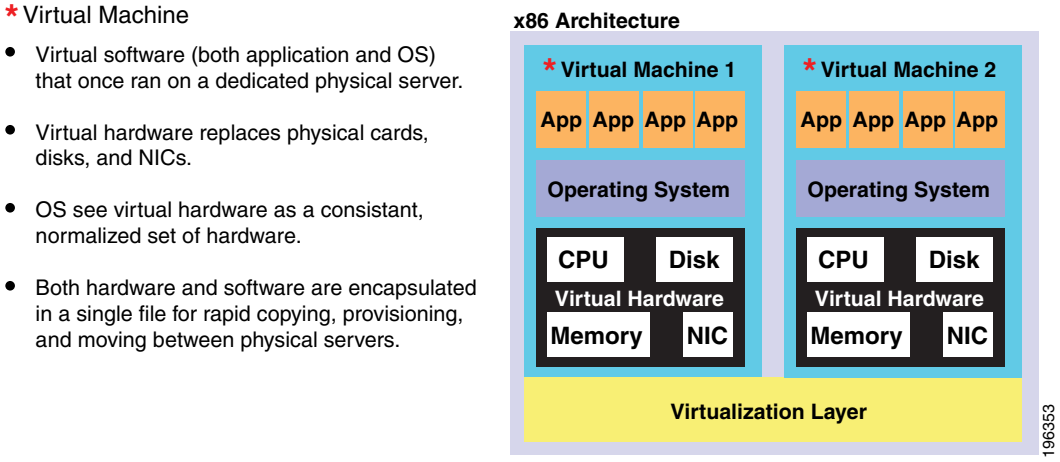
Information about Virtualization

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.

Figure 1-1 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:

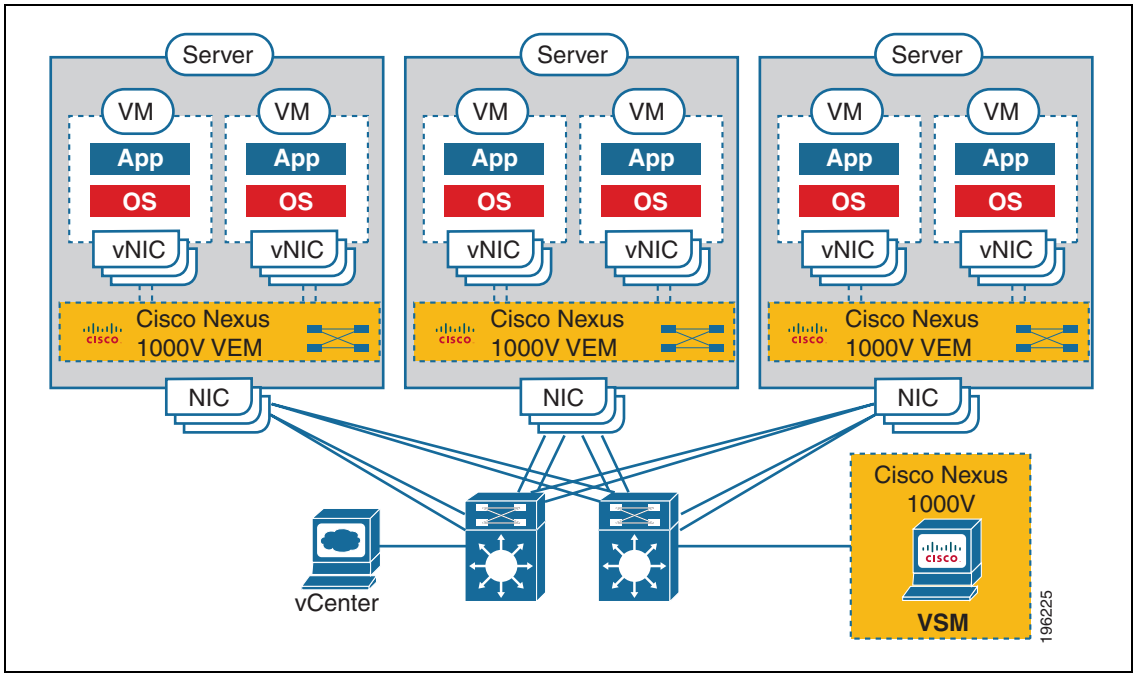
System Description

The Cisco Nexus 1000V is a virtual access software switch that works with VMware vSphere and has the following components:

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

Figure 1-2 shows the relationship between the Cisco Nexus 1000V components.

Figure 1-2 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.

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.

Management, Control, and Packet VLANs

The Management VLAN is used for system login, configuration. and corresponds to the mgmt0 interface. The management interface appears as the mgmt0 port on a Cisco switch, and is assigned an IP address. Although the management interface is not used to exchange data between the VSM and VEM, it is used to establish and maintain the connection between the VSM and VMware vCenter Server.

The management interface is always the second interface on the VSM and is usually labeled **Network Adapter 2** in the virtual machine network properties.

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

- 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.
  - VSM active to standby synchronization for high availability.

You can use the same VLAN for control, packet, and management, but if needed for flexibility, you can use separate VLANs. Make sure that the network segment has adequate bandwidth and latency.

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 specifies a set of attributes that can include 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 4.2(1)SV1(4)*.

System Port Profiles and System VLANs

System port profiles are designed to establish and protect ports and VLANs which need to be configured before the VEM contacts the VSM.

When a server administrator first adds a host to the DVS, its VEM must be able to contact the VSM. Since the ports and VLANs used for this communication are not yet in place, the VSM sends a minimal configuration, including system port profiles and system VLANs, to the vCenter Server, which then propagates it to the VEM.

When configuring a system port profile, you assign VLANs and designate them as system VLANs. In doing so, the port profile becomes a system port profile and included in the Cisco Nexus 1000V opaque data. Interfaces using the system port profile, and that are members of one of the defined system VLANs, are automatically enabled and forwarding traffic when the VMware ESX starts, even if the VEM does not have communication with the VSM. By doing so, the critical host functions are enabled even if the VMware ESX host starts and cannot communicate with the VSM.

Caution VMkernel connectivity can be lost if the relevant VLANs are not configured as system VLANs.

A system VLAN must be defined in both the Ethernet and vEth port profiles to automatically enable a specific virtual interface to forward traffic on a physical interface. If the system VLAN is configured only on the Ethernet port profile, the VMware VMkernel interface that inherits this port profile is not enabled by default and does not forward traffic.

The following ports must use system VLANs:

- Control and packet VLANs in the uplinks that communicate with the VSM.
- Management VLAN in the uplinks and port profiles (that is, the Ethernet and vEthernet ports) and VMware kernel NICs used for VMware vCenter server connectivity or SSH or Telnet connections.
- Storage VLAN used by the VSM for VM file system access in the uplinks and VMware kernel NICs used for iSCSI or network file systems.

Note System VLANs must be used sparingly and only as described here.

After a system port profile has been applied to one or more ports, you can add more system VLANs, but you can only delete a system VLAN after removing the port profile from service. This is to prevent accidentally deleting a critical VLAN, such as a host management VLAN, or a VSM storage VLAN.

Note One VLAN can be a system VLAN on one port but a regular VLAN on another in the same ESX host.

To delete a system VLAN, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4)*.

Administrator Roles

The Cisco Nexus 1000V enables network and server administrators to collaborate in managing 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).

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 a VSM is supported for both the active and standby VSM VMs. For high availability, it is recommended that the active VSM and standby VSM reside on separate hosts. To achieve this, and prevent a host failure resulting in the loss of both the active and standby VSM, it is recommended that distributed resource scheduling (DRS) be disabled for both the active and standby VSMs.

  If you do not disable DRS, then 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 Fault Tolerance is not supported for the VSM VM. It is supported for other VMs connected to Cisco Nexus 1000V.
- Using a VSM VM snapshot is not recommended. VSM VM snapshots do not contain unsaved configuration changes.
- The server administrator should not assign more than one uplink on the same VLAN without port channels. Assigning more than one uplink on the same host is not supported for the following:
  - A profile without port channels.
  - 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 and 4.1. (requires Enterprise Plus license edition of vSphere 4)

For detailed information, see the *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(4)* document.

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 6-1.