Overview

This chapter includes the following sections:

Information About Virtualization

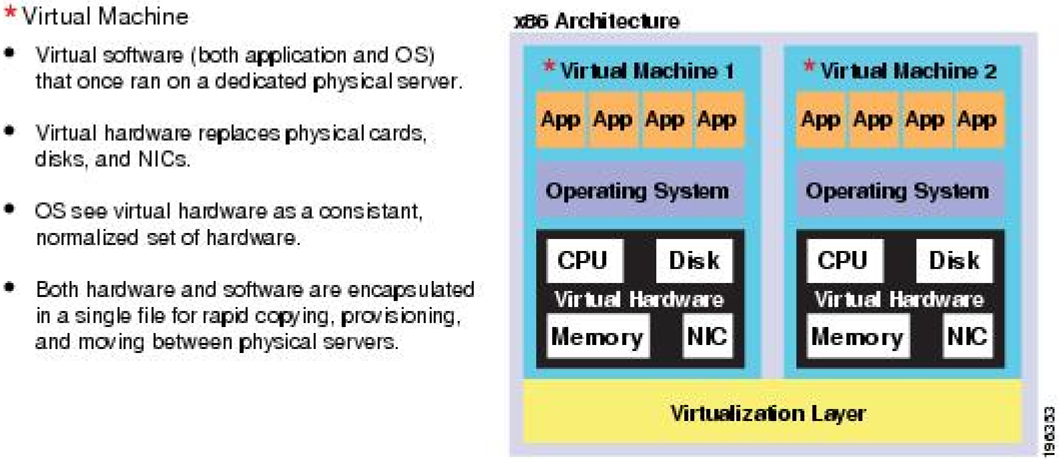
Virtualization allows multiple virtual machines to run in isolation, side by side on the same physical machine.

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 detects a consistent, normalized set of hardware regardless of the actual physical hardware components.

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

The following figure shows two virtual machines (VMs) side by side on a single host.

Figure 1: Two Virtual Machines Running on the Same Physical Machine


* Virtual Machine
• Virtual software (both application and OS) that once ran on a dedicated physical server.
• Virtual hardware replaces physical cards, disks, and NICs.
• OS see virtual hardware as a consistant, normalized set of hardware.
• Both hardware and software are encapsulated in a single file for rapid copying, provisioning, and moving between physical servers.
x86 Architecture
* Virtual Machine 1
App App App App
Operating System
CPU
Disk
Virtual Hardware
Memory
NIC
* Virtual Machine 2
App App App App
Operating System
CPU
Disk
Virtual Hardware
Memory
NIC
Virtualization Layer
196353

The following table lists the documents and videos that you need to use when performing a new installation or upgrade to Release 4.2(1)SV1(5.2).

Procedure	Document	Video
New Installation	Installing the Cisco Nexus 1000V	Cisco Nexus 1000V Release 4.2(1)SV1(5.1) Installation
Upgrading from Release 4.0(1)SV1(3) through Release 4.0(1)SV1(3d) to Release 4.2(1)SV1(5.2).	Upgrading from Releases 4.0(4)SV1(3, 3a, 3b, 3c, 3d) to Release 4.2(1)SV1(5.2)	Upgrading from Release 4.0(4)SV1(3, 3a, 3b) to Release 4.2(1)SV1(4)
Upgrading from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.2)	Upgrading from Releases 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), or 4.2(1)SV1(5.1) to Release 4.2(1)SV1(5.2)	Upgrading the Cisco Nexus 1000V VSMs from Release 4.2(1)SV1(4) to Release 4.2(1)SV1(4a)

Information About the Cisco Nexus 1000V

The Cisco Nexus 1000V is compatible with any upstream physical access layer switch that is Ethernet standard compliant, including the Catalyst 6500 series switch, Cisco Nexus switches, and switches from other network vendors. The Cisco Nexus 1000V is compatible with any server hardware listed in the VMware Hardware Compatibility List (HCL).

Cisco and VMware jointly designed APIs that produced the Cisco Nexus 1000V. The Cisco Nexus 1000V is a distributed virtual switch solution that is fully integrated within the VMware virtual infrastructure, including VMware vCenter for the virtualization administrator. This solution offloads the configuration of the virtual switch and port groups to the network administrator to enforce a consistent data center network policy.

Cisco Nexus 1000V and Its Components

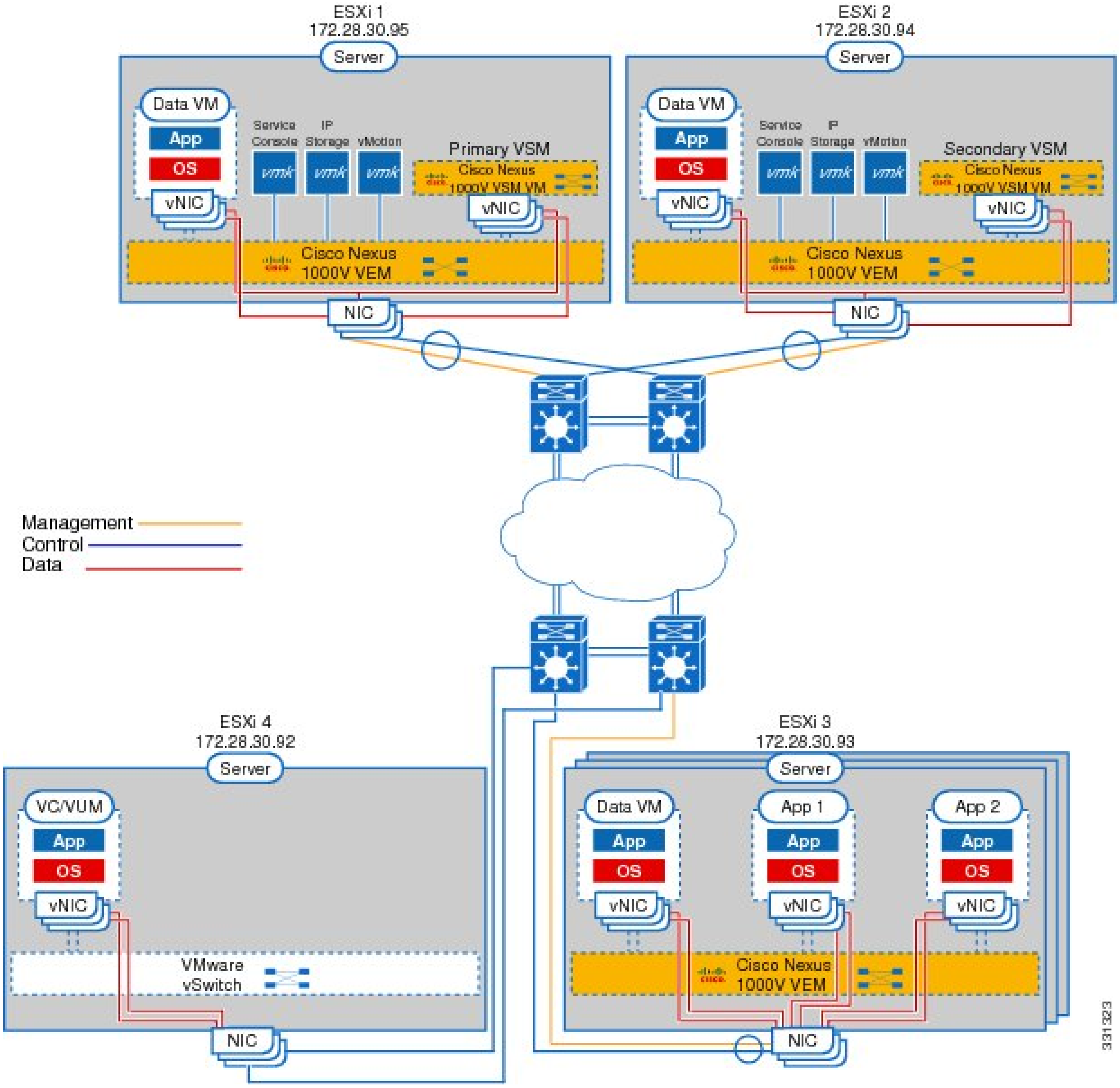
Note A list of terms used with the Cisco Nexus 1000V can be found in Glossary.

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

- Virtual Supervisor Module (VSM)—The control plane of the switch and a virtual machine that runs Cisco NX-OS.
- 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.

The following figure shows the relationship between the Cisco Nexus 1000V components.

Figure 2: Cisco Nexus 1000V Installation Diagram for Layer 3



Information About the Virtual Supervisor Module

The VSM is a virtual appliance that can be installed in either a standalone or active/standby HA pair. The VSM, with the VEMs that is controls, performs the following functions for the Cisco Nexus 1000V system:

- Configuration
- Management

- Monitoring
- Diagnostics
- Integration with VMware vCenter Server

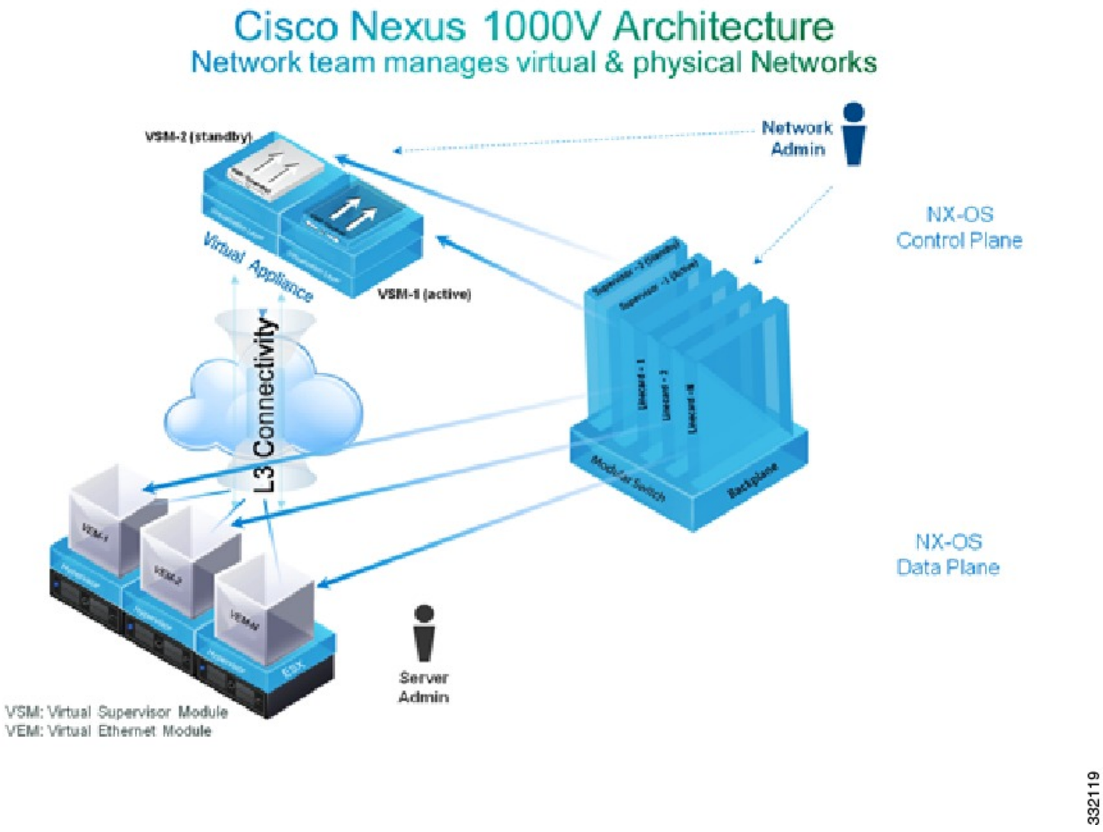
A single VSM can manage up to 64 VEMs.

Note We recommend an active/standby HA pair configuration.

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 delivers to the target VEM. The VSM runs the control plane protocols and configures the state of each VEM, but it never actually forwards packets.

A single VSM can control up to 64 VEMs. We recommend 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 1000V can be viewed as a 66-slot modular switch. See the following figure.

Figure 3: Cisco Nexus 1000V Architecture



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 must be distinguished by a unique integer called the domain identifier.

Information About the Virtual Ethernet Module

Each hypervisor is embedded with one VEM, which is a lightweight software component that replaces the virtual switch by performing the following functions:

- Advanced networking and security
- Switching between directly attached virtual machines
- Uplinking to the rest of the network

Note Only one version of VEM can be installed on an ESX/ESXi host at any given time.

In the Cisco Nexus 1000V, traffic is switched between virtual machines locally at each VEM instance. Each VEM also interconnects the local virtual machine with the rest of the network through the upstream access-layer network switch (blade, top-of-rack, end-of-row, and so forth). The VSM runs the control plane protocols and configures the state of each VEM accordingly, but it never forwards packets.

In the Cisco Nexus 1000V, the module slots are for the primary module 1 and secondary module 2. Either module can act as active or standby. The first server or host is automatically assigned to Module 3. The Network Interface Card (NIC) ports are 3/1 and 3/2 (vmnic0 and vmnic1 on the ESX/ESXi host). The ports to which the virtual NIC interfaces connect are virtual ports on the Cisco Nexus 1000V where they are assigned a global number.

Information About 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
- Private VLAN (PVLAN)
- Virtual Extensible LAN (VXLAN)
- Access Control List (ACL)
- Quality of Service (QoS)
- Catalyst Integrated Security Features (CISF)
- Virtual Service Domain (VSD)
- Port channel
- Port security
- Link Aggregation Control Protocol (LACP)
- LACP Offload

- NetFlow
- Virtual Router Redundancy Protocol (VRRP)
- Unknown Unicast Flood Blocking (UUFB)

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*.

Information About 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 is responsible for the installation, upgrade, or deletion of a VEM.

The following table compares the roles of the network administrator and server administrator.

Network Administrator	Server Administrator
• Creates, configures, and manages virtual switches (VMware 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).

Differences Between the Cisco Nexus 1000V and 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. Because the Cisco Nexus 1000V lacks this backplane, a VEM cannot directly forward packets to another VEM. Instead, it has to forward the packet using an uplink to the external fabric, which then switches it to the destination.
- No Spanning Tree Protocol—The Cisco Nexus 1000V does not run STP because STP deactivates 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.

Layer 3 and Layer 2 Control Modes

VSM to VEM Communication

The VSM and the VEM can communicate over a Layer 2 network or a Layer 3 network. These configurations are respectively referred to as Layer 2 or Layer 3 control mode.

Layer 3 Control Mode

The VEMs can be in a different subnet than the VSM and also from each other in the Layer 3 control mode. Active and standby VSM control ports should be Layer 2 adjacent. These ports are used to communicate the HA protocol between the active and standby VSMs.

Each VEM needs a designated VMkernel NIC interface that is attached to the VEM that communicates with the VSM. This interface, which is called the L3 Control vmknic, must have a system port profile applied to it (see the Information About System Port Profiles, on page 10 and Information About System VLANs, on page 10), so the VEM can enable it before contacting the VSM.

For more information on the Layer 3 control mode, see the "Configuring the Domain" chapter in the *Cisco Nexus 1000V System Management Configuration Guide*.

Layer 2 Control Mode

The VSM and VEM are in the same subnet in the Layer 2 control mode.

For more information on Layer 2 control mode, see Configuring Layer 2 Connectivity and Migrating from Layer 2 to Layer 3.

Management, Control, and Packet VLANs

Information About the Control VLAN

The control VLAN is used for communication between the VSM and the VEMs within a switch domain. The control interface is the first interface on the VSM and is labeled “Network Adapter 1” in the virtual machine network properties.

- 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 Distributed Virtual Switch (DVS).
    - VEM NetFlow exports that are sent to the VSM, where they are forwarded to a NetFlow Collector.
    - VSM active to standby synchronization for high availability.

Management VLANs

A management VLAN, which is used for system login and configuration, corresponds to the mgmt0 interface. The mgmt0 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 in Layer 2 mode. In (default) Layer 3 mode, when the (default) mgmt0 interface is used for Layer 3 connectivity on the VSM, the management interface communicates with the VEMs and the VMware vCenter Server.

The management interface is the second interface on the VSM and is labeled “Network Adapter 2” in the virtual machine network properties.

Information About the Packet VLAN

Note The packet VLAN is not a component of the Layer 3 control mode.

The packet VLAN is also used for communication between the VSM and the VEMs within a switch domain.

The packet interface is the third interface on the VSM and is labeled “Network Adapter 3” in the virtual machine network properties.

The packet VLAN is used to tunnel network protocol packets between the VSM and the VEMs such as the Cisco Discovery Protocol (CDP), Link Aggregation Control Protocol (LACP), and Internet Group Management Protocol (IGMP).

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

For more information about VLANs, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide*.

System Port Profiles and System VLANs

Information About System Port Profiles

System port profiles can establish and protect ports and VLANs that need to be configured before the VEM contacts the VSM.

When a server administrator adds a host to the DVS, its VEM must be able to contact the VSM. Because 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. The port profile becomes a system port profile and is included in the Cisco Nexus 1000V opaque data. Interfaces using the system port profile, which 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. 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 you do not configure the relevant VLANs as system VLANs.

Information About System VLANs

A system VLAN must be defined in both the Ethernet and vEthernet port profiles to automatically enable a specific virtual interface to forward traffic outside the ESX host. If the system VLAN is configured only on the port profile for the virtual interface, the traffic will not be forwarded outside the host. Conversely, if the system VLAN is configured only on the Ethernet port profile, the VMware VMkernel interface that needs that VLAN 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 Secure Shell (SSH) or Telnet connections.
- VLAN used for remote storage access (iSCSI or NFS).

Caution You must use system VLANs sparingly and only as described in the section. Only 32 system port profiles are supported.

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 action prevents 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 and a regular VLAN on another port in the same ESX host.

To delete a system VLAN, see the *Cisco Nexus 1000V Port Profile Configuration Guide*.

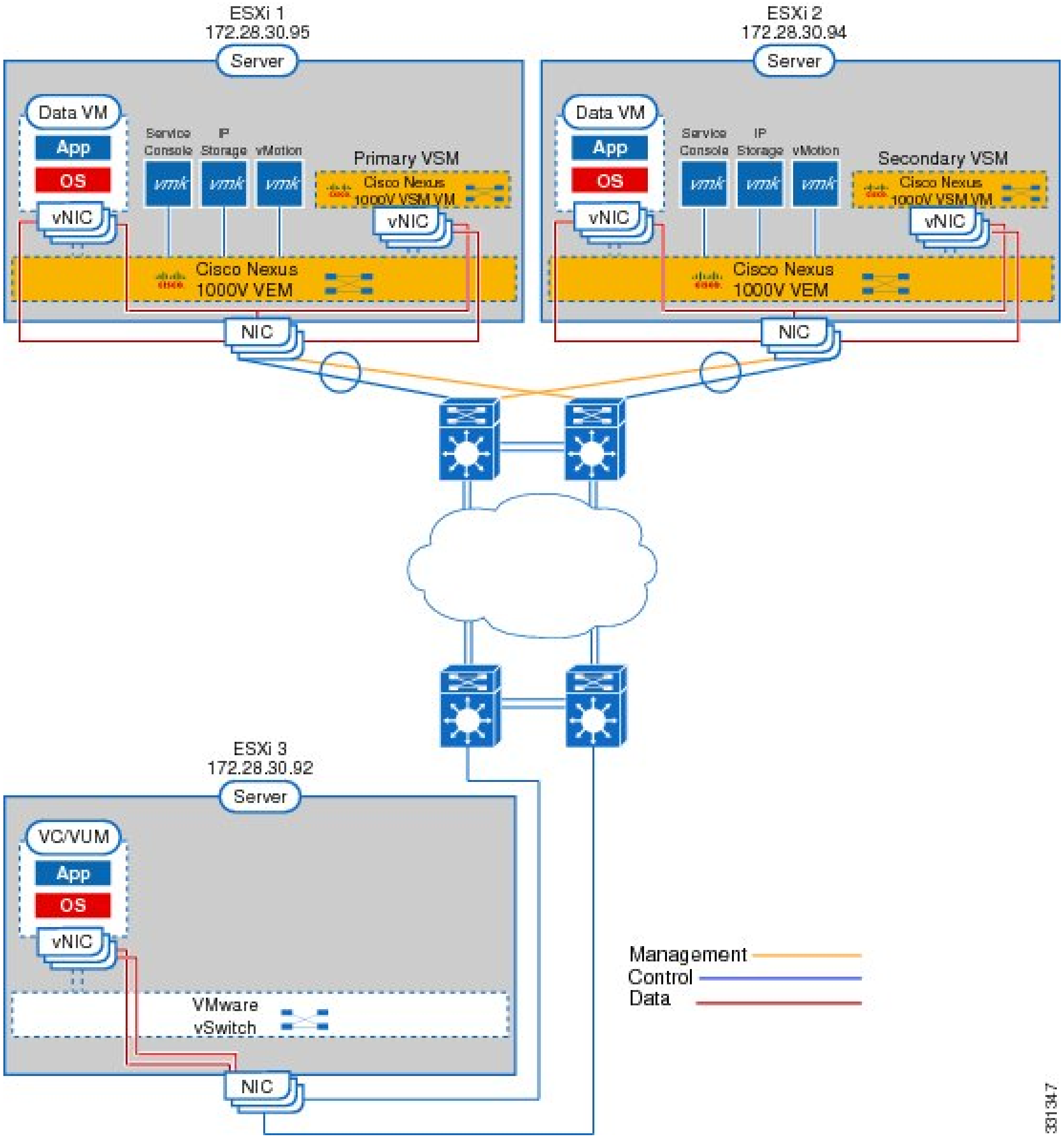
Recommended Topologies

Layer 3 Topology

The Cisco Nexus 1000V software installation installs the VSM software required to create the VSM VM.

The following figure shows an example of redundant VSM VMs, where the software for the primary VSM is installed on ESXi 1, and the software for the secondary VSM is installed on ESXi 2 for Layer 3 connectivity.

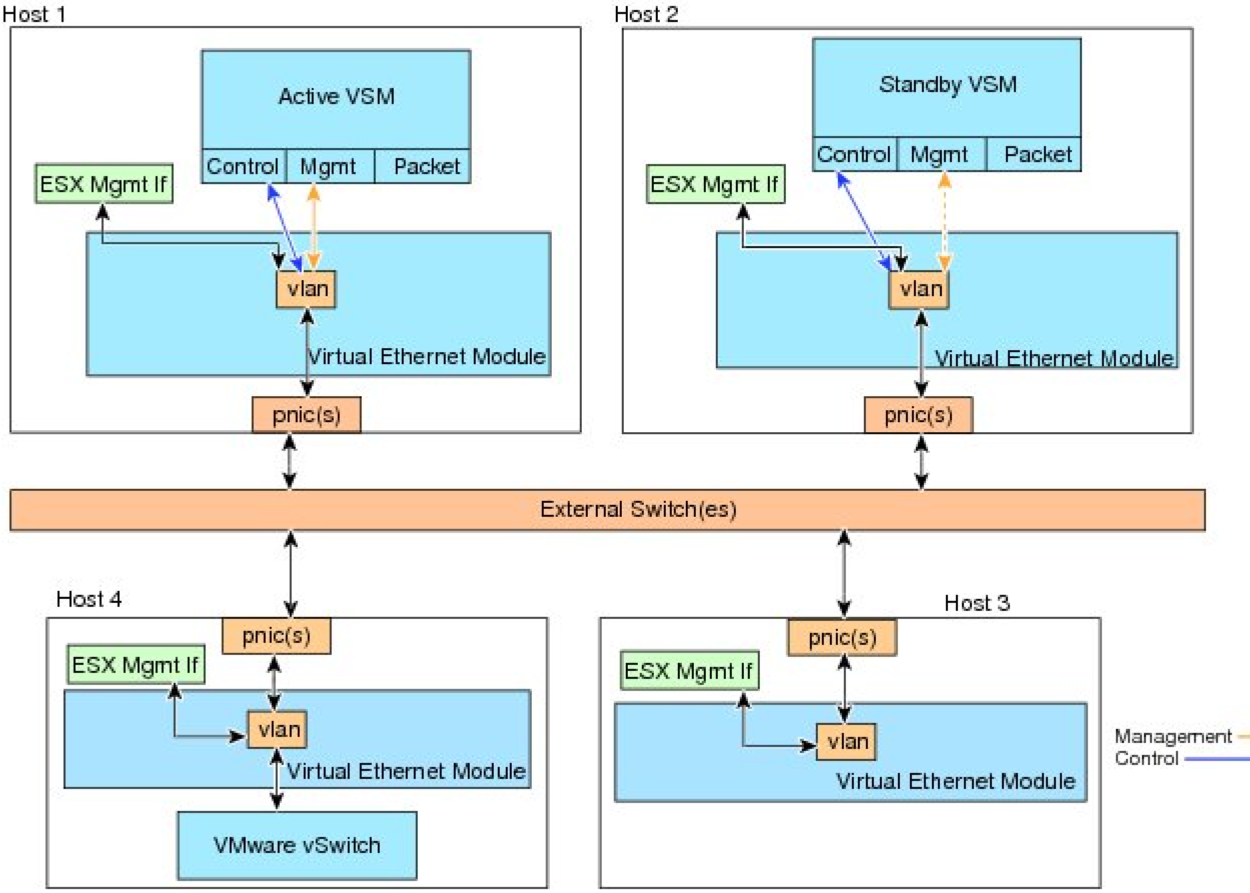
Figure 4: Cisco Nexus 1000V Installation Diagram for Layer 3



Control and Management on the Same VLAN Topology

The following figure shows a VSM and VEM that run on the same host in Layer 3 mode with the management and control interfaces on the same VLAN.

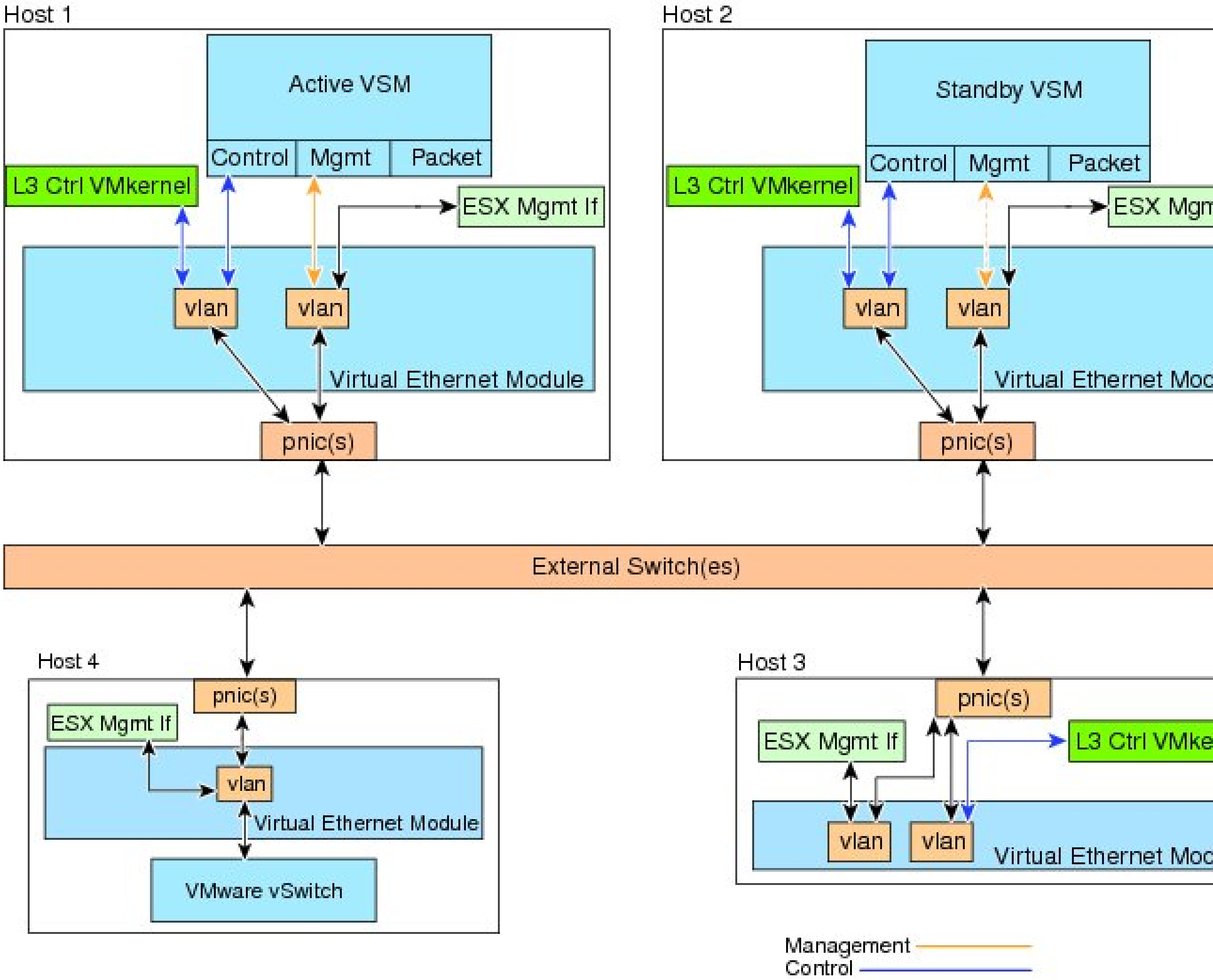
Figure 5: Control and Management on Same VLAN



Control and Management on Separate VLANs Topology

The following figure shows a VSM and VEM that run on the same host in Layer 3 mode with the management and control interfaces on different VLANs.

Figure 6: Control and Management on Separate VLAN



VMware Interaction

You can use a Cisco Nexus 1000V VSM as a virtual machine in ESX/ESXi 4.1 or later releases. (requires Enterprise Plus license edition of vSphere 4).

For more information, see the *Cisco Nexus 1000V and VMware Compatibility Information*.