Cisco Nexus 1000V Virtual Switch

Product Overview

The Cisco Nexus™ 1000V virtual machine access switch is an intelligent software switch implementation for VMware ESX environments. Running inside of the VMware ESX hypervisor, the Cisco Nexus 1000V supports Cisco® VN-Link server virtualization technology, providing

- Policy-based virtual machine (VM) connectivity
- Mobile VM security and network policy, and
- Non-disruptive operational model for your server virtualization, and networking teams.

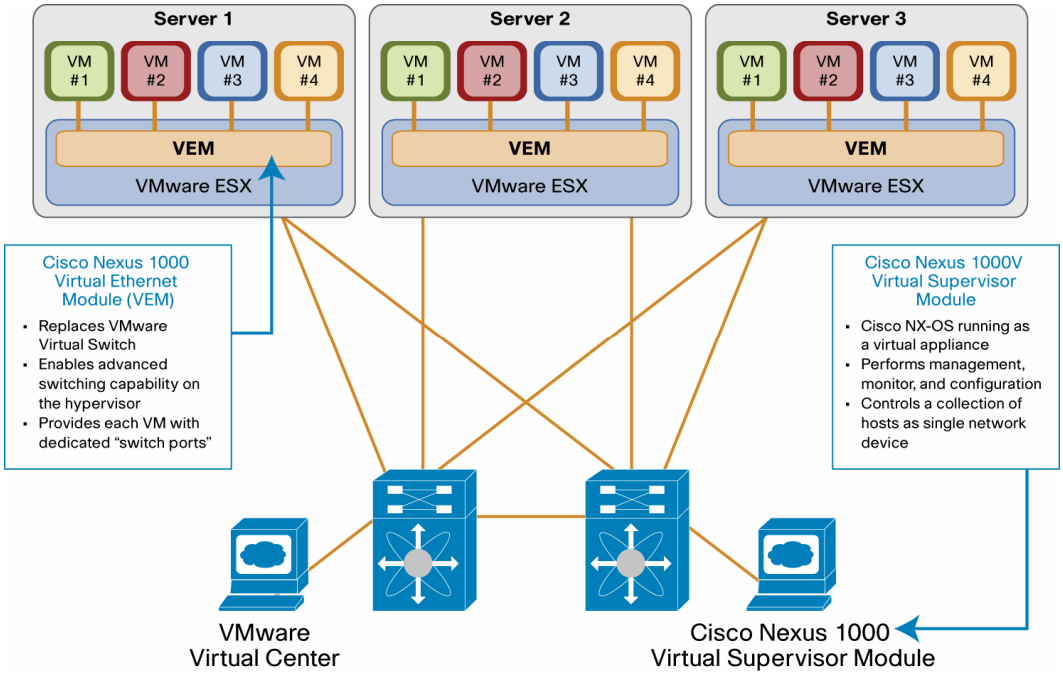
When server virtualization is deployed in the data center, virtual servers typically are not managed the same way as physical servers. Server virtualization is treated as a special deployment, leading to longer deployment time with a greater degree of coordination among server, network, storage, and security administrators. But with the Cisco Nexus 1000V you can have a consistent networking feature set and provisioning process all the way from the VM to the access, aggregation, and core switches. Your virtual servers can use the same network configuration, security policy, tools, and operational models as physical servers. Virtualization administrators can leverage predefined network policy that follows the nomadic VM and focus on virtual machine administration. This comprehensive set of capabilities helps you to deploy server virtualization faster and realize its benefits sooner.

Developed in close collaboration with VMware, the Cisco Nexus 1000V is fully integrated with VMware Virtual Infrastructure, including VMware Virtual Center, VMware ESX, and ESXi. You can use the Cisco Nexus 1000V to manage your VM connectivity with confidence in the integrity of the server virtualization infrastructure.

Product Architecture

The Cisco Nexus 1000V switch has two major components, the Virtual Ethernet Module (VEM) that executes inside the hypervisor and the external Virtual Supervisor Module (VSM) that manages the VEMs (Figure 1).

Figure 1. Cisco Nexus 1000V Architecture



Virtual Ethernet Module

The Cisco Nexus 1000V Virtual Ethernet Module executes as part of the VMware ESX or ESXi kernel and replaces the VMware Virtual Switch functionality. The VEM leverages the VMware vNetwork Distributed Switch API, which was developed jointly by Cisco and VMware, to provide advanced networking capability to virtual machines. This level of integration ensures that the Cisco Nexus 1000V is fully aware of all the server virtualization events, such as VMware VMotion and Distributed Resource Scheduler (DRS). The VEM takes configuration information from the Virtual Supervisor Module and performs advanced switching functions:

- Quality of service (QoS)
- Security: Private VLAN, access control lists, Cisco TrustSec architecture
- Monitoring: NetFlow, SPAN, ERSPAN

In the event of loss of communication with the Virtual Supervisor Module, the VEM has Nonstop Forwarding capability to continue to switch traffic based on last known configuration. In short, the VEM provides advanced switching with data-center reliability for the server virtualization environment.

Virtual Supervisor Module

The Cisco Nexus 1000V Virtual Supervisor Module controls multiple VEMs as one logical modular switch. Instead of physical line card modules, the Virtual Supervisor Module supports VEMs running in software inside servers. Configurations are performed through the Virtual Supervisor Module and automatically propagated to the VEMs. Instead of configuring soft switches inside the hypervisor on one host at a time, administrators can define configurations for immediate use on all VEMs being managed by the Virtual Supervisor Module.

By using the capabilities of Cisco NX-OS, the Cisco Nexus 1000V provides these benefits:

- **Flexibility and scalability:** Configuration of ports by category enables the solution to scale to a large number of ports. Common software can run all areas of the data center network, including LAN and storage area networks.
- **High availability:** Synchronized, redundant supervisors enable rapid, stateful failover.
- **Manageability:** Access the Cisco Nexus 1000V through the Cisco command-line interface (CLI), Simple Network Management Protocol (SNMP), and XML API.

Like the rest of the Cisco Nexus family, the Cisco Nexus 1000V can also be managed using the comprehensive tools of Cisco Data Center Network Manager. In addition, Cisco VFrame Data Center can control the Cisco Nexus 1000V for complete orchestration of the virtualized data center.

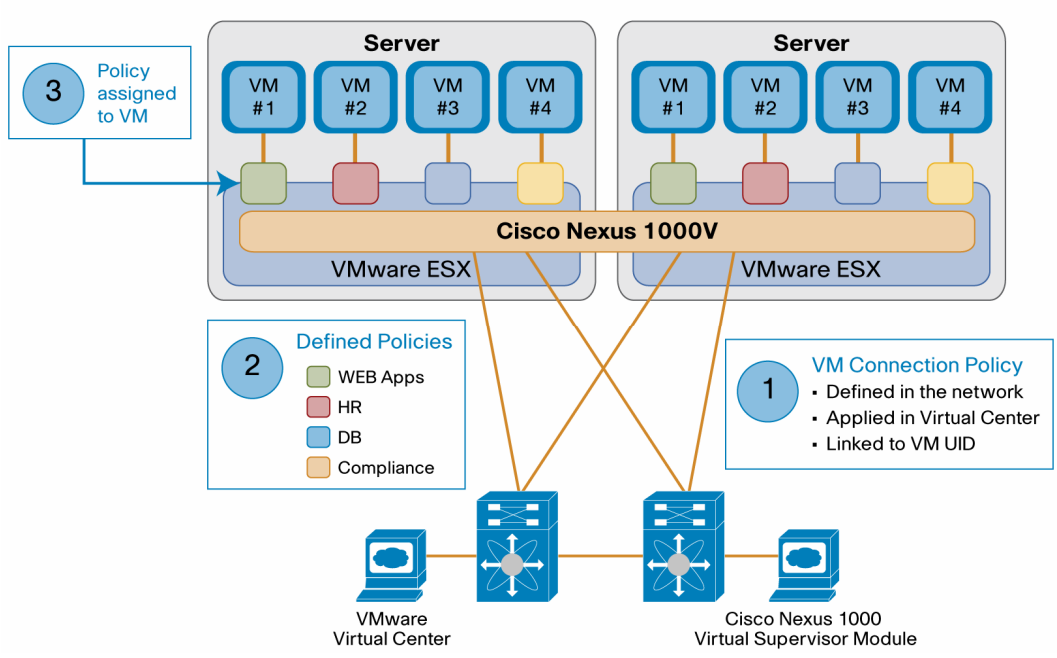
The Virtual Supervisor Module is also integrated with VMware Virtual Center so that the virtualization administrator can take advantage of the network configuration in the Cisco Nexus 1000V.

Features and Benefits

The Cisco Nexus 1000V gives you a common management model for both physical and virtual infrastructures through Cisco VN-Link technology that includes policy-based VM connectivity; mobility of VM security and network properties; and a non-disruptive operational model.

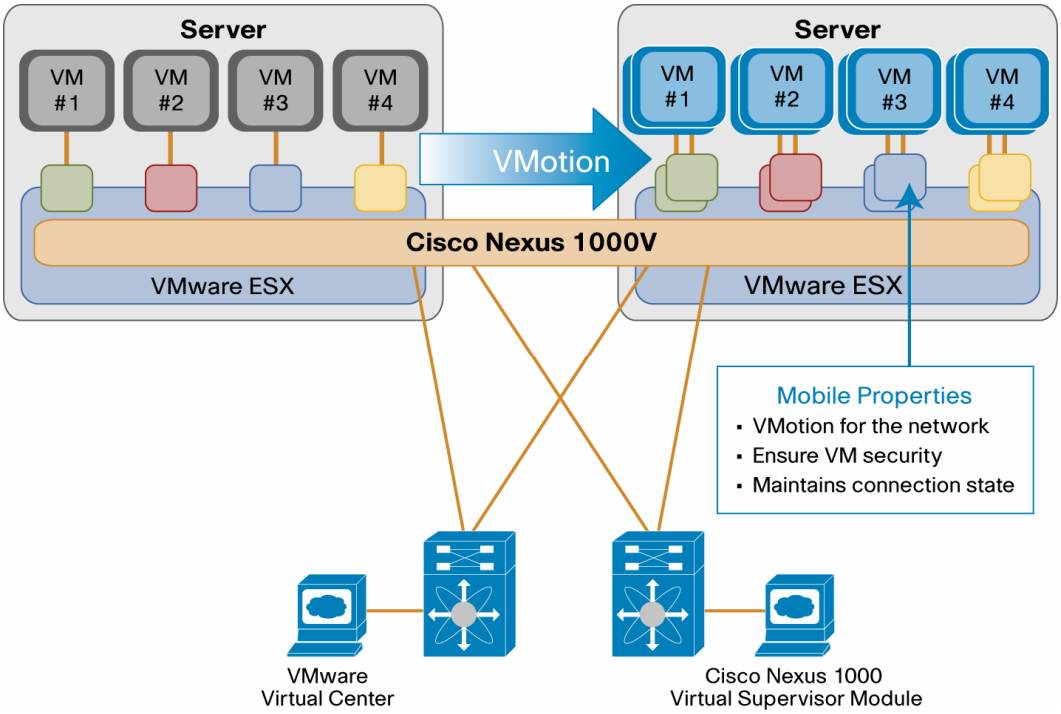
Policy-Based VM Connectivity: To complement the ease of creating and provisioning VMs, the Cisco Nexus 1000V includes the Port Profiles feature to address the dynamic nature of server virtualization from the network's perspective (Figure 2). Port Profiles enable you to define VM network policies for different types or classes of VMs, then apply them through VMware's Virtual Center GUI for transparent provisioning of network resources. Port Profiles are a scalable mechanism to configure networks with large numbers of VMs.

Figure 2. Policy-based VM Connectivity



Mobility of VM Security and Network Properties: Network and security policies defined in the Port Profile follow the VM throughout its lifecycle whether it is being migrated from one server to another (Figure 3), suspended, hibernated, or restarted. In addition to migrating the policy, the Cisco Nexus 1000V Virtual Supervisor Module also moves the VM's network state, such as the port counters. VMs participating in traffic monitoring activities, such as Cisco NetFlow or ERSPAN, can continue these activities uninterrupted by VMotion operations. When a Port Profile is updated, the Cisco Nexus 1000V automatically provides live updates to all the ports using that Port Profile. With the ability to migrate network and security policies through VMotion, regulatory compliance is much easier to enforce, because the security policy is defined in the same way as physical servers and constantly enforced by the Cisco Nexus 1000V.

Figure 3. Mobility of Network and Security Properties



Non-Disruptive Operational Model: Because of its close integration with VMware Virtual Center, the Cisco Nexus 1000V allows virtualization administrators to continue using VMware tools to provision VMs. At the same time, network administrators can provision and operate the VM network the same way they do the physical network using Cisco CLI, SNMP, and XML API along with tools such as ERSPAN and NetFlow. While both teams work independently, using familiar tools, the Cisco Nexus 1000V enforces consistent configuration and policy throughout the server virtualization environment. This level of integration lowers the cost of ownership while supporting various organizational boundaries among server, network, security, and storage teams.

Inside VMware Virtual Center, VMs are configured as before. Instead of having the network configuration being defined in Virtual Center, Port Profiles defined on the Cisco Nexus 1000V Supervisor are displayed inside Virtual Center as Port Groups. Virtualization administrators can take advantage of preconfigured Port Groups and focus on VM management, while network administrators can use Port Profiles to configure large number of ports. Together, both teams can deploy server virtualization more efficiently and with lower operational cost.

These and other features and benefits of the Cisco Nexus 1000V are summarized in Table 1.

Table 1. Cisco Nexus 1000V Features and Benefits

Feature	Benefit
Cisco VN-Link	
Policy-based VM connectivity	• Persistent network and security policy throughout VM lifecycle • Define policy for a port category rather than one port at a time • Manage large numbers of servers by defining policy through single management point
Mobile VM security and network policy	• Consistent network and security configuration during live VM migration • Easier security compliance as security policy follows VMs • Troubleshoot VM network even with live VM migration events
Non-disruptive operational model	• Operate virtual and physical servers identically • Operational consistency among administration teams • Improved collaboration while maintaining autonomy of different teams
Integration with VMware Virtual Infrastructure	
Compatible with VMware ESX and ESXi	• Choice of hypervisors • Compatible with future VMware versions through VMware vNetwork Distributed Switch API
Virtual Center integration	• Retain existing VM operational models • Offload network configuration to network administrators
Cisco NX-OS	
Availability	
Nonstop Forwarding	Continued forwarding despite communication disruption between Virtual Supervisor Module and VEM
Stateful Supervisor Failover	Synchronized redundant supervisors are always ready for failover while maintaining consistent and reliable state.
Minimally disruptive upgrade for Virtual Ethernet and Supervisor Modules	Easy software upgrades
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 impacting adjacent devices or services.
Flexibility and scalability	
Software compatibility	Interoperates with any standards based networking device including Cisco Catalyst and Nexus Switching Families.
Common software throughout data center	Designed to run all areas of the data center network including the Local and Storage Area Networks
Modular software design	Processes are instantiated on demand in separate memory spaces so that system resources are allocated only when a feature is enabled. Modular processes are governed by a real-time preemptive scheduler for timely processing of critical functions.
Manageability	
Programmatic XML API	Based on the NETCONF industry standard, the Cisco NX-OS XML interface provides a consistent API for devices, enabling rapid development of tools to enhance the network.
SNMP	Cisco NX-OS is SNMP version 1, version 2, and version 3 compliant. A large set of MIBs is supported.
Configuration verification with rollback	System operators can verify a configuration's consistency and resource availability before applying it, allowing devices to be preconfigured and the verified configuration applied at a later time. Configurations can be rolled back to previous ones as needed.
Role-based access control (RBAC)	Administrators can customize and limit access to switch operations by assigning roles to users.
Cisco Data Center Network Manager (DCNM)	Management solution for the Cisco NX-OS product family dedicated to data center network operations for high uptime and reliability, improving business continuity.

• Cisco Discovery Protocol Versions 1 and 2 • Link Level Discovery Protocol (LLDP) • Network Time Protocol • Ping • SSH v2 • Telnet • Cisco VFrame Data Center (future)	Full management features in line with physical network infrastructure
Serviceability	
Switched Port Analyzer (SPAN) and Encapsulated Remote Switched Port Analyzer (ERSPAN)	Administrators can analyze traffic between ports by nonintrusively directing session traffic to an analyzer.
Embedded packet analyzer	Packet analyzer, based on the Wireshark open-source network protocol analyzer, is built in for monitoring and troubleshooting VM traffic.
Cisco Embedded Event Manager (EEM)	Powerful device and system management technology uses network intelligence intrinsic to the Cisco software, enabling managers to customize behavior based on network events as they happen.
Cisco NetFlow	Supports version 5 and version 9 exports.
Switching Features	
• Layer 2 switching with Layer 3 aware features • Virtual Ethernet Interfaces for VM • Physical Server NICs enabled as switch uplinks • IEEE 802.1Q VLAN encapsulation • 128 active VLANs • IEEE 802.3ad (LACP) • IGMP Snooping • Traffic marking (CoS, DSCP) • Traffic policing • Jumbo Frame Support, 64-9216 bytes • BDPU Filter	Providing VMs robust switching features consistent with the physical network
Security Features	
• Private VLAN on access and trunk ports with Promiscuous, Isolated, and Community ports • L2 and L3 Access Control Lists • Port security	• Advanced security features allow for granular control of traffic flow and prevention of malware attacks • Consistent security policy for physical and virtual infrastructures
• TACACS and Radius	Authentication, admission, and access
• Cisco TrustSec (future)	Comprehensive network based security policy

System Specification

- Cisco Nexus 1000V Virtual Supervisor Module: Virtual appliance in VMDK or ISO image, supports up to 64 VMware ESX or ESXi
- Supports planned future version of VMware Virtual Infrastructure

For More Information

For additional information about the Cisco Nexus 1000V, visit http://www.cisco.com/go/datacenter.

For additional information about Cisco NX-OS, visit http://www.cisco.com/go/nxos.

For more information about Cisco Data Center Network Manager, visit http://www.cisco.com/go/dcnm.

For more information about Cisco VFrame Data Center, visit http://www.cisco.com/go/vframe.

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 C78-492971-00 09/08