Cisco Nexus 1000V Series Switches

Product Overview

Cisco Nexus® 1000V Series Switches are virtual machine access switches that are an intelligent software switch implementation for VMware vSphere environments running the Cisco® NX-OS operating system. Operating inside the VMware ESX hypervisor, the Cisco Nexus 1000V Series supports Cisco VN-Link server virtualization technology to provide:

- 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. With the Cisco Nexus 1000V Series, you can have a consistent networking feature set and provisioning process all the way from the VM access layer to the core of the data center network infrastructure. Virtual servers can now leverage the same network configuration, security policy, diagnostic tools, and operational models as their physical server counterparts attached to dedicated physical network ports. Virtualization administrators can access predefined network policy that follows mobile virtual machines to ensure proper connectivity saving valuable time to 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 Series is certified by VMware to be compatible with VMware vSphere, vCenter, ESX, and ESXi, and with many other VMware vSphere features. You can use the Cisco Nexus 1000V Series to manage your virtual machine connectivity with confidence in the integrity of the server virtualization infrastructure.

Product Architecture

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

Figure 1. Cisco Nexus 1000V Series Architecture
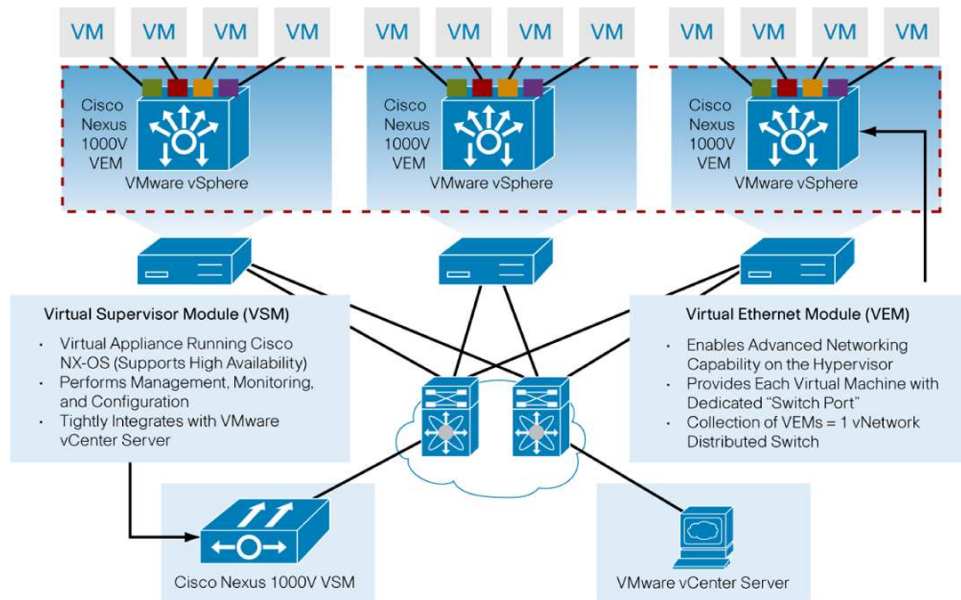
Virtual Ethernet Module

The Cisco Nexus 1000V Virtual Ethernet Module (VEM) 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 (vDS) 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 server virtualization events, such as VMware VMotion and Distributed Resource Scheduler (DRS). The VEM takes configuration information from the Virtual Supervisor Module and performs layer 2 switching and advanced networking functions:

- Port Channels
- Quality of service (QoS)
- Security: Private VLAN, access control lists, port security
- Monitoring: NetFlow, Switch Port Analyzer (SPAN), Encapsulated Remote 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 Series Virtual Supervisor Module (VSM) controls multiple VEMs as one logical modular switch. Instead of physical line card modules, the VSM supports multiple VEMs running in software inside of the physical servers. Configuration is performed through the VSM and is automatically propagated to the VEMs. Instead of configuring soft switches inside the hypervisor on a host- by- host basis, administrators can define configurations for immediate use on all VEMs being managed by the Virtual Supervisor Module from a single interface.

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

- **Flexibility and Scalability:** Port Profiles, a new Cisco NX-OS feature, provides configuration of ports by category, enabling the solution to scale to a large number of ports. Common software can run all areas of the data center network, including the LAN and SAN.
- **High Availability:** Synchronized, redundant Virtual Supervisor Modules enable rapid, stateful failover and ensure an always available virtual machine network.

- **Manageability:** The Cisco Nexus 1000V Series can be accessed through the Cisco command-line interface (CLI), Simple Network Management Protocol (SNMP), XML API, and CiscoWorks LAN Management Solution (LMS).

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

Features and Benefits

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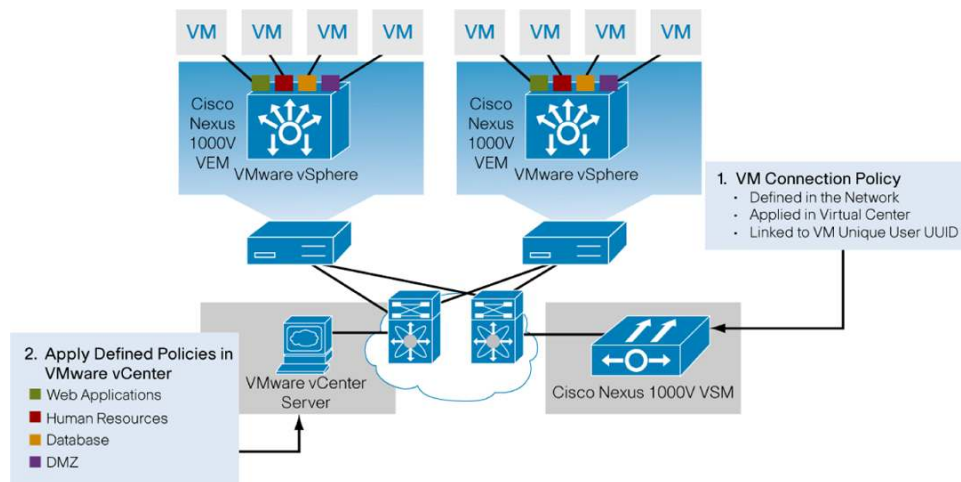
Mobility of VM Security and Network Properties: Network and security policies defined in the Port Profile follow the VM throughout its lifecycle whether it is being migrated from one server to another (Figure 3), suspended, hibernated, or restarted. In addition to migrating the policy, the Cisco Nexus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

Figure 3.   Mobility of Network and Security Properties
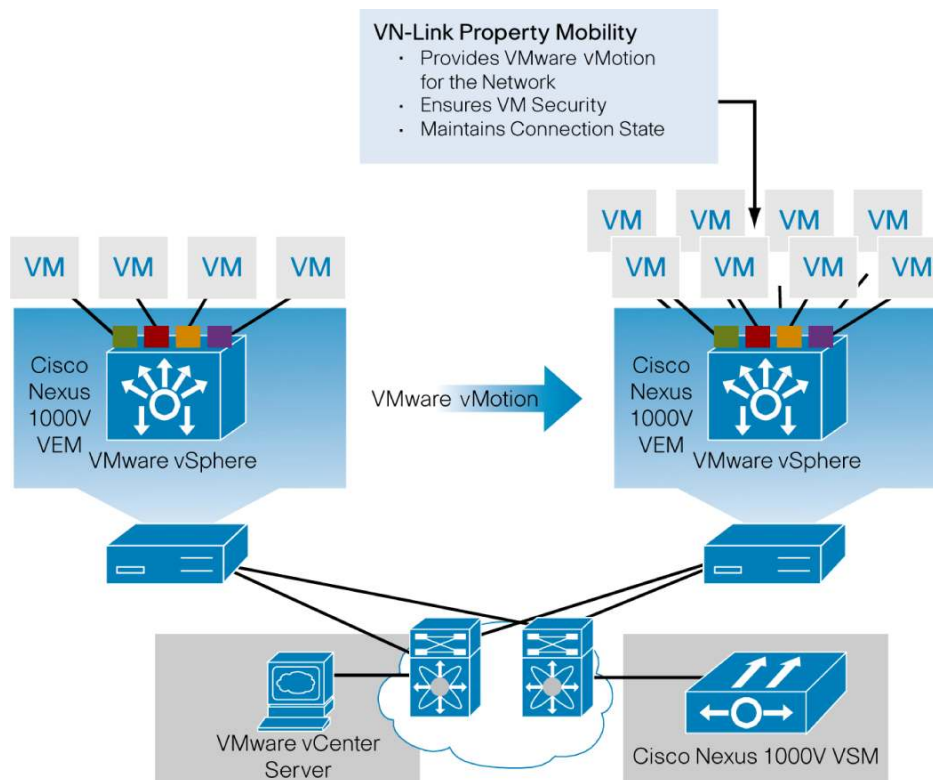
Non-Disruptive Operational Model: Because of its close integration with VMware vCenter Server, the Cisco Nexus 1000V allows virtualization administrators to continue using VMware tools to provision VMs. At the same time, network administrators can provision and operate the VM network the same way they do the physical network using Cisco CLI and SNMP along with tools such as ERSPAN and NetFlow (Figure 4). 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 vCenter Server, VMs are configured as before. Instead of defining network configuration in vCenter Server, Port Profiles defined on the Cisco Nexus 1000V Virtual Supervisor Module are displayed by vCenter 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 apply policy for a large number of ports at the same time. Together, both teams can deploy server virtualization more efficiently and with lower operational cost.

Figure 4. Nondisruptive Operational Model

Network Administrator View of Network Policy   Virtualization Administrator Applying Network Policy
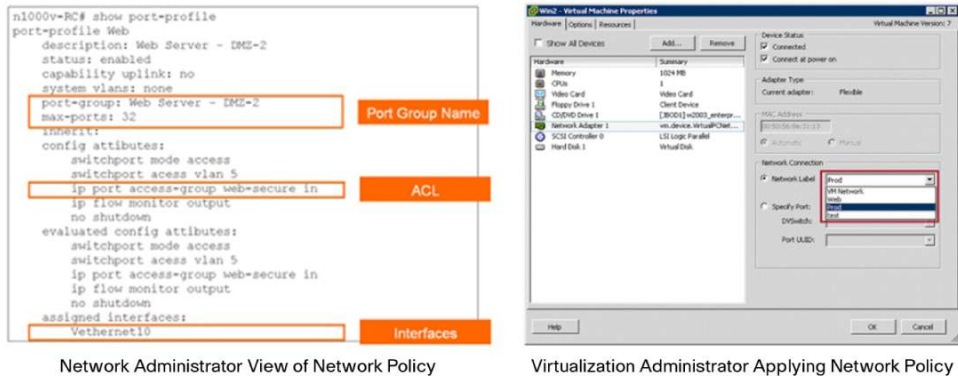
Enhanced Deployment Scenarios

Optimize Server Bandwidth for I/O-Intensive Applications

Today, network interface are often dedicated to a particular type of traffic, such as VMware Console or vMotion. With the Cisco Nexus 1000V, all the network interface cards (NICs) on the server can be treated as a single logical channel with QoS attached to each type of traffic. With VMware vSphere Version 4.1, the Cisco Nexus 1000V Series can even provide different service-level agreements (SLAs) for production virtual machines. Consequently, the bandwidth to the server can be more efficiently utilized with virtualization of network-intensive applications.

Secure Server and Desktop Virtualization

The number of virtual machines running on a server is increasing quickly, similar to the way that CPU performance follows Moore's Law. With a large population of virtual machines on a server, an infected VM can quickly spread a virus or malware to other virtual machines on the same server. VMware vMotion can then migrate an infected VM to another server, spreading the infestation. Consequently, virtual machines must have the same security policy as physical servers.

Cisco Nexus 1000V Series includes the Cisco Integrated Security Features that are found on Cisco physical switches to prevent a variety of attack scenarios (Table 1). For example, a rogue virtual machine can spoof its MAC and IP addresses to appear to be an existing production VM, send a rogue Address Resolution Protocol (ARP) transaction mimicking the way that VMware vMotion announces the location of a migrated virtual machine, and divert traffic from the production virtual machine to the rogue virtual machine. With Cisco Integrated Security Features, this type of attack can easily be prevented with simple networking policy. Since server virtualization is being used for desktop and server workloads, it is critical that this type of security feature be deployed for the proper operation of a virtualized environment.

Table 1. Cisco Integrated Security Features

Feature	Capability	Prevents
Port Security	Restricts MAC addresses on a port	MAC address spoofing by rogue virtual machine
IP Source Guard	Maps IP address to MAC address	IP and MAC address spoofing
Dynamic ARP Inspection	Monitors virtual machine ARP transactions, which are also used for VMware vMotion	ARP cache poisoning on other virtual machines, hosts, and network devices
Dynamic Host Configuration Protocol (DHCP) Snooping	• Prevents DHCP client requests from reaching untrusted entities • Prevents untrusted entities from acting as DHCP server • Rate limits DHCP requests to prevent denial-of-service (DoS) attacks	• Rogue DHCP server • Denial of service to DHCP services

In addition to built-in security features, the Cisco Nexus 1000V Series enables Layer 4 through 7 services virtual machines to be specified as part of the virtual machine network policy. In particular, Virtual Service Domain (VSD) groups virtual machines, which may be on multiple servers, into zones and forces traffic traveling between zones

through a Layer 4 through 7 services virtual machine, such as a firewall, including VMware vShield Zones (Figure 5). This extensible capability makes the Cisco Nexus 1000V Series much easier to use with a variety of Layer 4 through 7 services.

Figure 5.   Virtual Service Domain
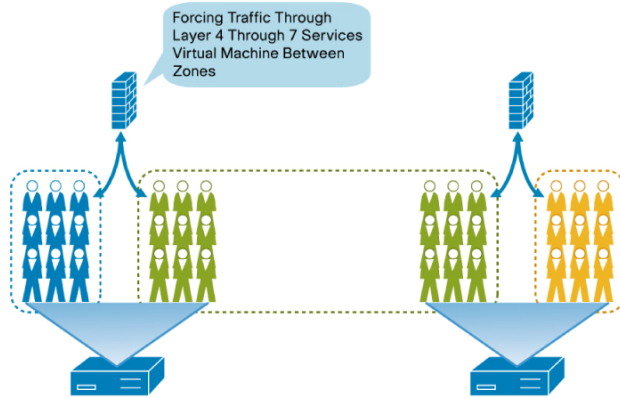
Virtualized Network Services with Cisco vPath

Although VSDs have the flexibility to provide network services through any Layer 4 through 7 virtual machine, they require a network service virtual machine on every host. In addition, the network service virtual machines are slower when compared to performance in the hypervisor kernel, as in the case of switching in the VEM.

Cisco addresses these concerns with the introduction of the Cisco vPath architecture where network service VM, called Virtual Service Node, provides the network service. Specifically, the Cisco vPath architecture provides:

- Intelligent Traffic Steering
  - Redirect traffic from server requesting network service to Virtual Service Node
  - Extend Port Profile to include network service profile
- Flexible Deployment:
  - Each Virtual Service Node can serve multiple physical servers
  - Virtual Service Node can be hosted on a separate or dedicated server
- Network service acceleration:
  - Network Service Decision Caching: Nexus 1000V remembers network service policy from prior traffic reducing traffic steering
  - Performance of virtual network services can be accelerated through enforcement in hypervisor kernel

In Figure 6, when VM 1 sends a packet to VM 2 requiring virtualized network services), the VEM forwards the request to a VSN, possibly on a different host. The VSN responds to the originating VEM with the suitable action: for example, sending or dropping packets in this flow. The original VEM caches and executes the decision that the VSN requested. For future packets from VM 1 to VM 2, the VEM can implement the virtualized network service without requests to the VSN. Hence, the VEM:

- Implements the virtualized network service decision
- Accelerates network service since it is running in the hypervisor kernel
- Scales network service since the VEM is on every hypervisor host

In addition, the VSN can be placed on any host, providing greater flexibility and separation of production work load and network services. In fact, the vPath architecture is designed to support a variety of network services.

Figure 6.   Cisco vPath Architecture
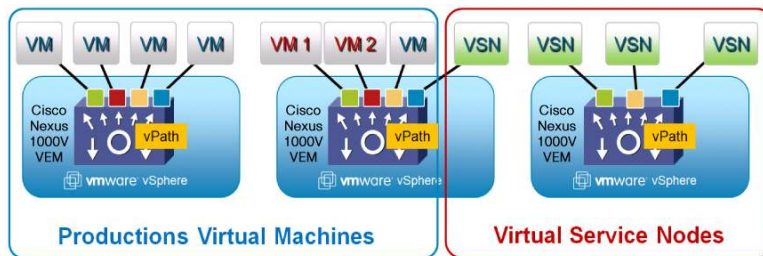
The first VSN to use vPath is the Cisco Virtual Security Gateway (VSG). The Cisco VSG enforces attribute-based security policies for single and multi-tenant environments. Because Cisco VSG is offered as a virtual appliance, customers can scale its deployment with the vPath architecture and by deploying more Cisco VSG appliances on demand.

Virtual Machine as Basic Building Block of the Data Center

With the Cisco Nexus 1000V Series, virtual machines are treated in the same way as physical servers in 1) security policy, 2) monitoring and troubleshooting, and 3) operational model between network and server administrators. Therefore, virtual machines can finally be true basic building blocks of the data center. These operational efficiencies lead to greater scaling of server virtualization deployments with lower operating costs.

Cisco NX-OS Software Overview

Cisco NX-OS Software is a data center-class operating system built with modularity, resiliency, and serviceability at its foundation. Based on the industry-proven Cisco MDS 9000 SAN-OS Software, Cisco NX-OS Software helps ensure continuous availability and sets the standard for mission-critical data center environments. The self-healing and highly modular design of Cisco NX-OS Software makes zero-impact operations a reality and enables exceptional operational flexibility. Focused on the requirements of the data center, Cisco NX-OS Software provides a robust and rich feature set that fulfills the Ethernet and storage networking requirements of present and future data centers. With a CLI like that of Cisco IOS® Software, Cisco NX-OS Software provides state-of-the-art implementations of relevant networking standards as well as a variety of true data center - class Cisco innovations.

Cisco NX-OS Software Features and Benefits

- **Software Compatibility:** Cisco NX-OS Software Release 4.0 interoperates with Cisco products running any variant of the Cisco IOS Software operating system. Cisco NX-OS Software Release 4.0 also interoperates with any networking OS that conforms to the networking standards listed as supported in this data sheet.

- **Common Software Throughout the Data Center:** Cisco NX-OS Software simplifies the data center operating environment and provides a unified OS designed to run all areas of the data center network, including the LAN, SAN, and Layer 4 through 7 network services.

- **Modular Software Design:** Cisco NX-OS Software modular processes are instantiated on demand, each in a separate protected memory space. Thus, processes are started and system resources allocated only when a feature is enabled. The modular processes are governed by a real-time preemptive scheduler that helps ensure the timely processing of critical functions.

- **In-Service Software Upgrade (ISSU):** The Cisco Nexus 1000V Series enables server and network administrators to transparently upgrade the VEM and VSM software, reducing downtime and allowing customers to integrate the newest features and functions with little or no negative effect on network operations. Network and server administrators can upgrade the VSM and VEM during different maintenance windows and continue operation of the Cisco Nexus 1000V Series.

- **Quick Development of Enhancements and Problem Fixes:** The modularity of Cisco NX-OS Software allows new features, enhancements, and problem fixes to be integrated into the software quickly. Thus, modular fixes can be developed, tested, and delivered in a short time span.
- **SNMP and XML API:** Cisco NX-OS complies with SNMPv1, v2, and v3. A rich collection of MIBs is supported. Cisco NX-OS also has a rich, documented XML API, enabling integration with third-party management tools.
- **Role-Based Access Control (RBAC):** With RBAC, Cisco NX-OS enables administrators to limit access to switch operations by assigning roles to users. Administrators can customize and restrict access to the users who require it.

Product Specifications

VMware Product Compatibility

The Cisco Nexus 1000V Series is VMware Ready Certified to be compatible with VMware vSphere as a vNetwork Distributed Switch with support for VMware ESX and ESXi hypervisors and integration with VMware vCenter Server.

VMware vSphere Feature Compatibility

The Cisco Nexus 1000V Series is supported with the following VMware vSphere features:

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

Maximum Supported Configurations

- 64 VMware ESX or ESXi hosts per VSM
- 2048 virtual Ethernet ports per VMware vDS, with 216 virtual Ethernet ports per physical host
- 512 active VLANs
- 32 physical NICs per physical host
- 256 PortChannels per VMware vDS, with 8 PortChannels per physical host

Layer 2 Features

- Layer 2 switch ports and VLAN trunks

- IEEE 802.1Q VLAN encapsulation

- Link Aggregation Control Protocol (LACP): IEEE 802.3ad

- Advanced PortChannel hashing based on Layer 2, 3, and 4 information

  ◦ Source MAC address (default)

  ◦ Virtual port ID

  ◦ Destination IP address and Layer 4 port

  ◦ Destination IP address, Layer 4 port, and VLAN

  ◦ Destination IP address and VLAN

  ◦ Destination MAC address

  ◦ Destination Layer 4 port

  ◦ Source and destination IP addresses and Layer 4 port

  ◦ Source and destination IP addresses, Layer 4 port, and VLAN

  ◦ Source and destination IP addresses and VLAN

  ◦ Source and destination MAC addresses

  ◦ Source and destination Layer 4 port

  ◦ Source IP address and Layer 4 port

  ◦ Source IP address, Layer 4 port, and VLAN

  ◦ Source IP address and VLAN

  ◦ Source MAC address

  ◦ Source Layer 4 port

  ◦ VLAN only

- Virtual Port Channel Host Mode

- Private VLANs with Promiscuous, Isolated, and Community ports

- Private VLAN on trunks

- Internet Group Management Protocol (IGMP) Snooping Versions 1, 2, and 3

- Jumbo-frame support; up to 9216 bytes

- Integrated loop prevention with Bridge Protocol Data Unit (BDPU) filter without running Spanning Tree Protocol

QoS Including Virtual Machine Granularity

- Classification

  ◦ Access group (ACL)

  ◦ IEEE 802.1p CoS

  ◦ IP Type of Service: IP precedence or DSCP (RFC 2474)

  ◦ User Datagram Protocol (UDP) ports

  ◦ Packet length

- Marking

  ◦ Two Rate Three Color Marker (RFC 2698)

  ◦ IEEE 802.1p CoS marking

  ◦ IP Type of Service: IP precedence or DSCP (RFC 2474)

- Traffic policing (transmit- and receive-rate limiting)

- Weighted Fair Queuing (only on VMware vSphere 4.1 or later versions)

- Modular QoS CLI (MQC) compliance

Security

- Ingress and egress ACLs on Ethernet and virtual Ethernet ports

- Standard and extended Layer 2 ACLs:

  ◦ MAC address and IPv4

  ◦ Source MAC address

  ◦ Destination MAC address

  ◦ Ethertype

  ◦ VLAN

  ◦ Class of service (CoS)

- Standard and extended Layer 3 and 4 ACLs:

  ◦ Source IP

  ◦ Destination IP

  ◦ DSCP

  ◦ Precedence

  ◦ Protocol (TCP, UDP, Internet Control Message Protocol [ICMP], and IGMP)

  ◦ Source port

  ◦ Destination port

  ◦ TCP flags

  ◦ ICMP and IGMP types

  ◦ ICMP code

- Port-based ACLs (PACLs)

- Named ACLs

- ACL statistics

- Cisco Integrated Security Features

  ◦ Port security

  ◦ IP Source Guard

  ◦ Dynamic ARP Inspection

  ◦ DHCP Snooping

- Virtual Service Domain for Layer 4 through 7 services virtual machine

High Availability

- **Stateful Supervisor Failover:** Synchronized redundant supervisors are always ready for failover while maintaining a consistent and reliable state.

- **Nonstop Forwarding:** Continued forwarding despite loss of communication between the VSM and VEM.

- **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.

Management

- VSM installation wizard for virtualization and network administrators
  - Installs VSM on its own VEM
  - Creates physical NIC Port Profiles
  - Configures VSM high availability
  - Configures VSM-to-VEM communication options
- Layer 2 and 3 connectivity between VSM and VEM
- Cisco NX-OS Software CLI console
- ISSU
- SPAN: Local port mirroring of physical interface, PortChannel, VLAN, and Port Profile
- Enhanced Remote SPAN (ERSPAN) Type III: Remote port mirroring
- NetFlow Version 9 with NetFlow Data Export (NDE)
- Cisco Discovery Protocol Versions 1 and 2
- SNMP (read) v1, v2, and v3
- XML API support
- Enhanced SNMP MIB support
- SSH v2
- Telnet
- Authentication, authorization, and accounting (AAA)
- TACACS+
- RADIUS
- Syslog
  - Includes VMware vMotion events
- Role based access control (RBAC)
- Ingress and egress packet counters per interface
- Network Time Protocol (NTP) RFC 1305
- Domain Name Services (DNS) for management interfaces
- CiscoWorks LMS v3.1, v3.0.1, and v2.6 with Service Pack 1 (SP1)

SNMP MIBs

- Generic MIBs
  - CISCO-TC
  - SNMPv2-MIB
  - SNMP-COMMUNITY-MIB
  - SNMP-FRAMEWORK-MIB
  - SNMP-NOTIFICATION-MIB
  - SNMP-TARGET-MIB
- Configuration MIBs
  - ENTITY-MIB
  - IF-MIB
  - CISCO-ENTITY-EXT-MIB
  - CISCO-ENTITY-FRU-CONTROL-MIB
  - CISCO-FLASH-MIB
  - CISCO-IMAGE-MIB
  - CISCO-CONFIG-COPY-MIB
  - CISCO-ENTITY-VENDORTYPE-OID-MIB
  - ETHERLIKE-MIB
  - CISCO-LAG-MIB
  - MIB-II
- Monitoring MIBs
  - NOTIFICATION-LOG-MIB
  - CISCO-PROCESS-MIB
  - CISCO-VIRTUAL-NIC-MIB
- Security MIBs
  - CISCO-AAA-SERVER-MIB
  - CISCO-COMMON-MGMT-MIB
  - CISCO-PRIVATE-VLAN-MIB
- Miscellaneous MIBs
  - CISCO-CDP-MIB
  - CISCO-LICENSE-MGR-MIB
  - CISCO-ENTITY-ASSET-MIB

Supported Standards

Table 2 presents IEEE compliance information, and Table 3 presents RFC compliance information.

Table 2.   IEEE Compliance

Standard	Description
IEEE 802.1p	CoS tagging for Ethernet frames
IEEE 802.1Q	VLAN tagging
IEEE 802.3	Ethernet
IEEE 802.3ad	Link Aggregation Control Protocol (LACP)

Table 3.   RFC Compliance

Standard	Description
IP Services	
RFC 768	User Data Protocol (UDP)
RFC 791	IP
RFC 792	Internet Control Message Protocol (ICMP)
RFC 793	TCP
RFC 826	Address Resolution Protocol (ARP)
RFC 854	Telnet
RFC 894	IP over Ethernet
RFC 1305	Network Time Protocol Version 3
RFC 1492	TACACS+
RFC 1591	Domain Name System (DNS) Client
RFC 2068	HTTP server
RFC 2138	RADIUS authentication
RFC 2139	RADIUS accounting
IP Multicast	
RFC 1112	IGMPv1 snooping
RFC 2236	IGMPv2 snooping
RFC 3376	IGMPv3 snooping
Quality of Service	
RFC 2474	DSCP marking
RFC 2698	Two Rate Three Color Marker

System Requirements

- VMware vSphere Enterprise Plus Version 4.0 or later
- Cisco Nexus 1000V VSM:
  - VSM can be deployed as a virtual machine on VMware ESX or ESXi 3.5U2 or higher or ESX or ESXi 4.0
  - Hard disk: 3 GB
  - RAM: 2 GB
  - 1 virtual CPU at 1.5 GHz
- Cisco Nexus 1000V VEM
  - VMware ESX or ESXi 4.0
  - Hard disk space: 6.5 MB
  - RAM: 150 MB
- Number of VLANs for Layer 2 connectivity between VSM and VEM: 1
- Server on VMware Hardware Compatibility List (http://www.vmware.com/go/hcl)
- Compatible with any upstream physical switches, including all Cisco Nexus and Cisco Catalyst® switches as well as Ethernet switches from other vendors

Licensing and Ordering Information

The Cisco Nexus 1000V Series is licensed based on the number of physical CPUs on the server on which the VEM is running. Table 4 presents ordering formation for the Cisco Nexus 1000V Series.

Table 4.   Cisco Nexus 1000V Series Ordering Information

Part Number	Description
N1K-VSMK9-404S12=	Nexus 1000V VSM on Physical Media
N1K-VLCPU-01=	Nexus 1000V Paper CPU License Qty 1-Pack
N1K-VLCPU-04=	Nexus 1000V Paper CPU License Qty 4-Pack
N1K-VLCPU-16=	Nexus 1000V Paper CPU License Qty 16-Pack
N1K-VLCPU-32=	Nexus 1000V Paper CPU License Qty 32-Pack
L-N1K-VLCPU-01=	Nexus 1000V eDelivery CPU License Qty 1-Pack
L-N1K-VLCPU-04=	Nexus 1000V eDelivery CPU License Qty 4-Pack
L-N1K-VLCPU-16=	Nexus 1000V eDelivery CPU License Qty 16-Pack
L-N1K-VLCPU-32=	Nexus 1000V eDelivery CPU License Qty 32-Pack

Warranty

The Cisco Nexus 1000V Series has a 90-day limited software warranty. For more information about the Cisco Nexus 1000V Series warranty, see http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html.

Service and Support

Cisco Software Application Support plus Upgrades (SASU) is a comprehensive support service that helps you maintain and enhance the availability, security, and performance of your business-critical applications. Cisco SASU includes the following resources:

- Software updates and upgrades: The Cisco SASU service provides timely, uninterrupted access to software updates and upgrades to help you keep existing systems stable and network release levels current. Update releases, including major upgrade releases that may include significant architectural changes and new

capabilities for your licensed feature set, are available by software download from Cisco.com or by CD-ROM shipment.

- Cisco Technical Assistance Center (TAC): Cisco TAC engineers provide accurate, rapid diagnosis and resolution of software application problems to help you reduce outages and performance degradation. These specialized software application experts are trained to support the Cisco Nexus 1000V Series. Their expertise is available to you 24 hours a day, 365 days a year, by telephone, fax, email, or the Internet.

- Online support: Cisco SASU provides access to a wide range of online tools and communities to help you resolve problems quickly, support business continuity, and improve competitiveness.

For More Information

- For more information about the Cisco Nexus 1000V Series, visit http://www.cisco.com/go/nexus1000v

- For a free evaluation version of the Cisco Nexus 1000V Series, visit http://www.cisco.com/go/1000veval

- For more information about Cisco Virtual Security Gateway, visit http://www.cisco.com/go/vsg

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

- For more information about VMware vSphere, visit http://www.vmware.com/go/vsphere

- For more information about how Cisco and VMware are working together, visit http://www.vmware.com/cisco

Printed in USA

C78-492971-08   09/10