Cisco Nexus 1000V Switch for KVM

Product Overview

Bring enterprise-class networking features to OpenStack cloud operating system environments.

The Cisco Nexus® 1000V Switch for the Ubuntu Kernel-based Virtual Machine (KVM) reduces the operating complexity associated with virtual machine networking. Together with the OpenStack cloud operating system, this switch helps you gain control of large pools of computing, storage, and networking resources.

The Cisco Nexus 1000V Switch provides a comprehensive and extensible architectural platform for virtual machine and cloud networking. This switch is designed to accelerate your server virtualization and multitenant cloud deployments in a secure and operationally transparent manner.

Operating as a distributed switching platform, the Cisco Nexus 1000V enhances the visibility and manageability of your virtual and cloud networking infrastructure. It supports multiple hypervisors and many networking services and is tightly integrated with multiple cloud management systems.

The Cisco Nexus 1000V Switch for KVM offers enterprise-class networking features to OpenStack cloud operating system environments, including:

- Advanced switching features such as access control lists (ACLs) and port-based access control lists (PACLS).
- Support for highly scalable, multitenant virtual networking through Virtual Extensible LAN (VXLAN).
- Manageability features such as Simple Network Management Protocol (SNMP), NETCONF, syslog, and advanced troubleshooting command-line interface (CLI) features.
- Strong north-bound management interfaces including OpenStack Neutron plug-in support and REST APIs.

Benefits

The Cisco Nexus 1000V Switch reduces the operational complexity associated with virtual machine networking and enables you to accomplish the following:

- **Easily deploy your Infrastructure-as-a-service (IaaS) networks**
  - As the industry's leading networking platform, the Cisco Nexus 1000V delivers performance, scalability, and stability with familiar manageability and control.
- **Preserve your existing investment in operation processes and management tools**
  - You can manage network policies across both physical and virtual environments using the same familiar interfaces with no additional overhead in retraining costs. You can also use your existing network monitoring, management, and troubleshooting tools to manage both environments.

- **Simplify virtual networking operations**
  - With greater visibility into traffic between virtual machines, these switches simplify your network troubleshooting and your network policy management.
  - REST APIs facilitate orchestration and management by providing access to numerous server configuration management tools.
- **Strengthen security**
  - By extending network policies and network visibility to the virtual machine level, virtualization-aware networking increases security.

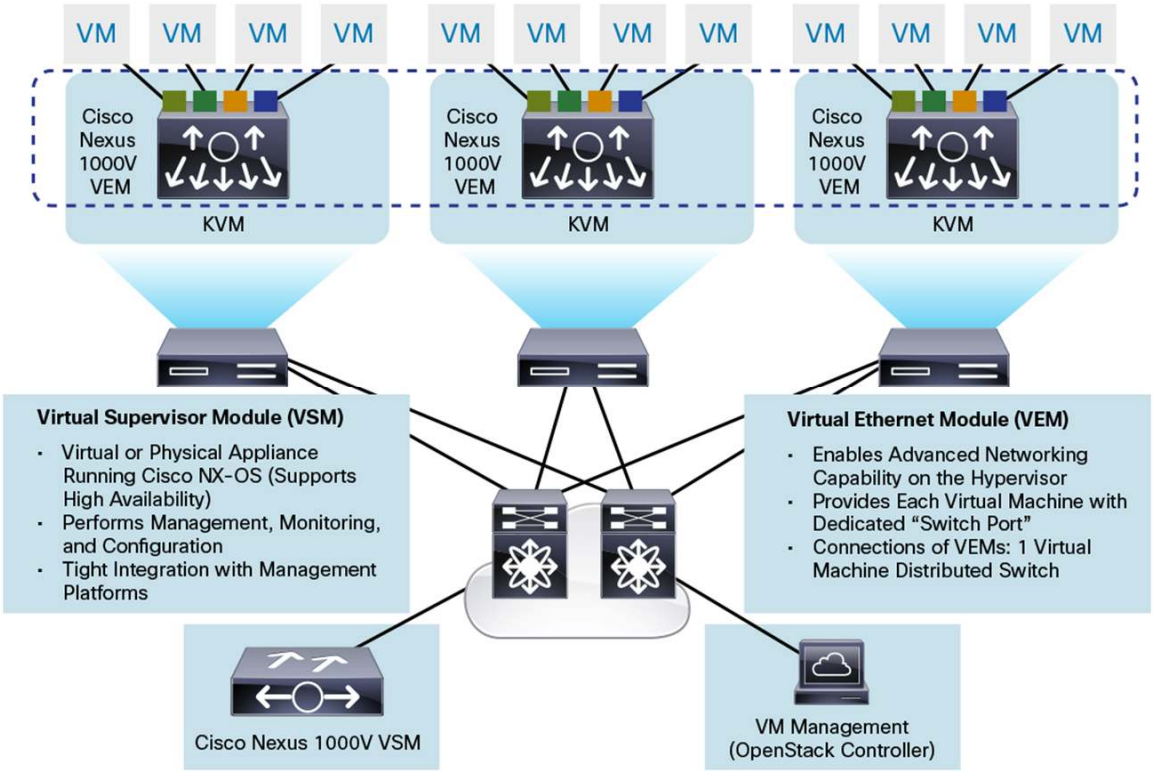
In addition to the virtual form factor, a physical form factor to host all virtual appliances relevant to the Cisco Nexus 1000V Switch is available: the Cisco Nexus 1100-S Virtual Services Appliance.

Hypervisor-Independent Architecture

The Cisco Nexus 1000V Switch for KVM employs the same hypervisor-independent architecture used across other hypervisors (such as VMware vSphere and Microsoft Hyper-V), and has two components (Figure 1):

- The virtual Ethernet module (VEM) is deployed on each physical host managed by the Cisco Nexus 1000V as part of the KVM hypervisor.
- The virtual supervisor module (VSM) can be deployed as a virtual appliance on any KVM host or on the Cisco® Cloud Services appliance.

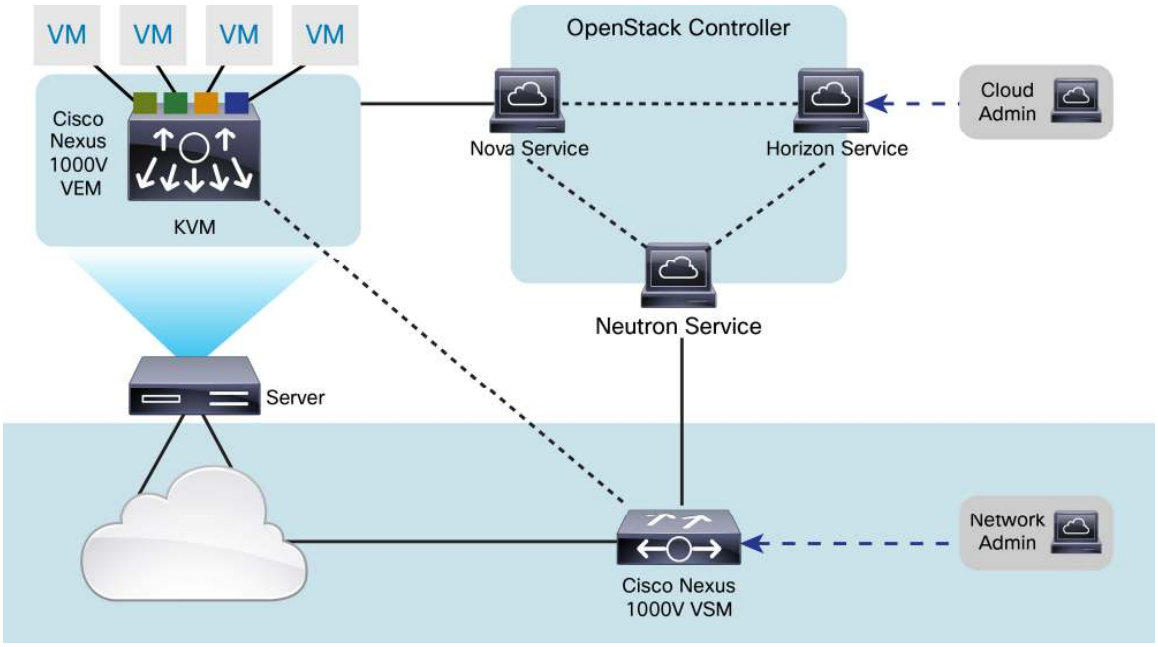
Figure 1. Cisco Nexus 1000V Architecture



Both of these components are tightly integrated with the OpenStack environment to provide operational simplicity:

- The VEM is a hypervisor-resident component and is tightly integrated with the KVM architecture.
- The VSM is integrated with OpenStack using the Neutron plug-in (Figure 2).

Figure 2. Cisco Nexus 1000V for KVM Integration with OpenStack



Features

High Availability

The Cisco Nexus 1000V Switch is designed to be resilient with high availability built into the system at multiple levels:

- Cisco NX-OS Software, the OS run by the VSM, is specifically designed for high availability at the network, system, and process levels. Critical processes run independently for ease of isolation, fault containment, and upgrades. Processes can restart independently in milliseconds without losing state information, affecting data forwarding, or affecting adjacent devices or services.
- VSMs are typically deployed in active-standby pairs for high availability. The state and configuration remain constantly synchronized between the two VSMs to provide stateful switchover if the active VSM fails.

VSM and VEM communication is built for reliability. In the event of loss of communication with the VSM, the VEMs can use nonstop forwarding (NSF) to continue to switch traffic according to the last-known configuration.

Enhanced Visibility with Cisco NX-OS

The Cisco Nexus 1000V Switch provides advanced Cisco NX-OS features including:

- Enhanced visibility and troubleshooting of virtual machine traffic through features such as Cisco NetFlow and packet statistics.
- Simplified virtual networking operations and manageability through a strong partner ecosystem and features including SNMP, NETCONF, and syslog.
- Advanced switching and security through features such as VXLANs and ACLs.

The switch uses the familiar Cisco NX-OS CLI to configure both physical and virtual environments:

- Manage network policies across Cisco Nexus 5000, 6000, and 7000 Series Switches as well as the Cisco Nexus 1000V.
- Use REST APIs to deliver better orchestration by creating your own scripts.
- Use existing networking monitoring tools to manage and troubleshoot both environments.

Product Specifications

Maximum Supported Configurations

- 64 hosts per VSM
- 4096 virtual Ethernet ports per vswitch, with 300 virtual Ethernet ports per physical host
- 2048 active VLANs
- 2048 active VXLANs
- 4000 port profiles
- 6 physical NICs per physical host
- 256 PortChannels per vswitch, with 4 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 ports
  - 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 PortChannel Host Mode (Static, MAC address pinning, MAC address pinning relative, manual and subgroup Cisco Discovery Protocol)
- Internet Group Management Protocol (IGMP) Snooping Versions 1, 2, and 3
- Jumbo-frame support; up to 9216 bytes

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
- 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

VXLAN

- Scalable network isolation
- Port statistics
- ACL (ingress only)
- NetFlow (ingress only)
- Multicast mode
- Unicast flooding and learn mode
- Multicast traffic

Management

- Management through Cisco NX-OS CLI, OpenStack's Horizon dashboard, and other configuration management tools
- Layer 3 connectivity between VSM and VEM, recommended through the management interface of the VSM
- Cisco NX-OS CLI console
- ISSU
- Cisco Discovery Protocol Versions 1 and 2
- SNMP (read) v1, v2, and v3
- SNMP ACL
- Enhanced SNMP MIB support
- SSH v2
- Telnet
- Authentication, authorization, and accounting (AAA)
- TACACS+
- RADIUS
- Syslog
- Ingress and egress packet counters per interface
- Network Time Protocol (NTP) RFC 1305
- REST API's (Create/Read/Update/Delete)

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
- Miscellaneous MIBs
  - CISCO-CDP-MIB
  - CISCO-LICENSE-MGR-MIB
  - CISCO-ENTITY-ASSET-MIB

Supported Standards

Table 1 presents IEEE compliance information, and Table 2 presents RFC compliance information.

Table 1. IEEE Compliance

Standard	Description
IEEE 802.1q	VLAN tagging
IEEE 802.3	Ethernet
IEEE 802.3ad	Link Aggregation Control Protocol (LACP)

Table 2. 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

Standard	Description
RFC 3376	IGMPv3 snooping

System Requirements

- Ubuntu 12.04 LTS
- Cisco Nexus 1000V VSM
  - VSM can be deployed as a virtual machine on Ubuntu 12.04
  - Hard disk: 3 GB
  - RAM: 4 GB
  - 2 virtual CPUs at 1.5 GHz
- Cisco Nexus 1000V VEM
  - Hard disk space: 6.5 MB
  - RAM: 150 MB
- Compatible with any upstream physical switches, including all Cisco Nexus and Cisco Catalyst® switches and Ethernet switches from other vendors
- VXLAN requires physical switches that support multicast (RFC 2236) for multicast mode

For More Information

- For more information about the Cisco Virtual Networking portfolio, visit http://www.cisco.com/go/1000v.
- For more information about the Cisco Nexus 1000V Switch for KVM, visit http://www.cisco.com/go/1000v/kvm.
- For more information about Cisco Nexus 1100 Series Cloud Services Platforms, visit http://www.cisco.com/go/1100.
- For more information about the Cisco Nexus 1000V community, visit http://communities.cisco.com/community/technology/datacenter/nexus1000v.
- For more information about Cisco NX-OS Software, visit http://www.cisco.com/go/nxos.

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 C78-730833-00 02/14