Cisco Virtual Networking Solution for OpenStack

Product Overview

Extend enterprise-class networking features to OpenStack cloud environments.

A reliable virtual network infrastructure that provides a scalable, secure environment is critical when you are building your OpenStack cloud. A solution that is easy to deploy, operate, and maintain is also very important for any successful OpenStack project.

The Cisco® Virtual Networking Solution for OpenStack addresses these challenges by bringing an enterprise-class Cisco NX-OS Software architecture to the OpenStack environment. It offers:

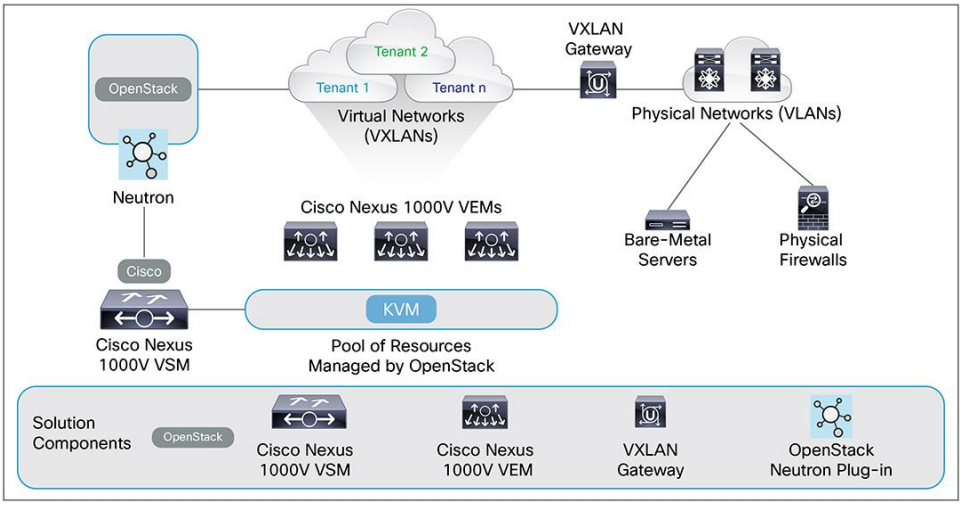
- Reduced operational risk through a reliable virtual networking infrastructure
- Simplified operational model through tight integration with OpenStack services
- Operational flexibility with a scalable switching and extensible services architecture

It brings the same robust architecture associated with traditional Cisco physical modular switches and with other virtualization environments (for example, VMware vSphere and Microsoft Hyper-V) to OpenStack deployments.

The solution has the following main components (Figure 1):

- The Cisco Nexus® 1000V Virtual Ethernet Module (VEM) is a software component that is deployed on each Kernel-based Virtual Machine (KVM) host. Each virtual machine on the host is connected to the VEM through virtual Ethernet (vEth) ports.
- The Cisco Nexus 1000V Virtual Supervisor Module (VSM) is the management component that controls multiple VEMs and helps in the definition of virtual machine-focused network policies. It is deployed either as a virtual appliance on any KVM host or on the Cisco Cloud Services Platform appliance.
- The Cisco Virtual Extensible LAN (VXLAN) Gateway is a gateway appliance to facilitate communication between a virtual machine located on a VXLAN with other entities (bare-metal servers, physical firewalls etc.) that are connected to traditional VLANs. It can be deployed as a virtual appliance on any KVM host.
- The OpenStack Neutron plug-in is used for communication between the VSM and OpenStack Neutron service and is deployed as part of the OpenStack Neutron service.
- The OpenStack Horizon Router tab is used for operational simplicity and is deployed as part of the OpenStack Horizon service.

Figure 1. Cisco Virtual Networking Solution for OpenStack



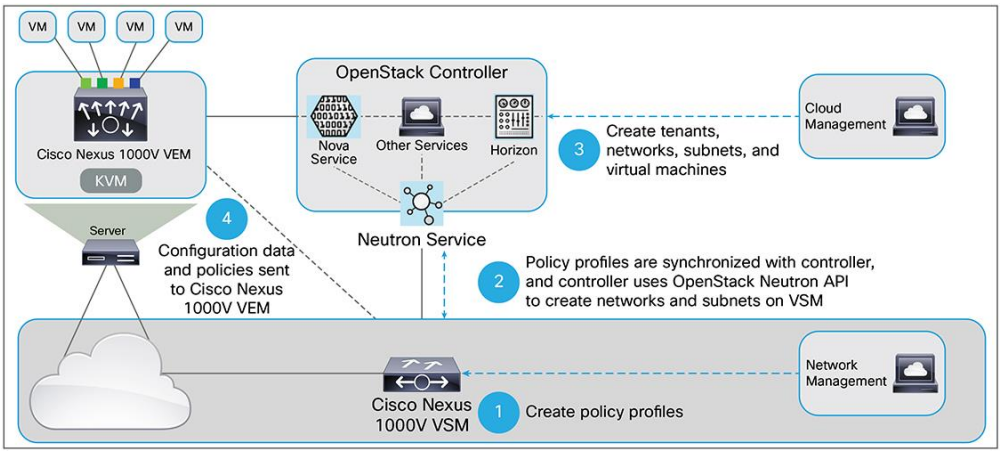
Each of these components is tightly integrated with the OpenStack environment:

- The VEM is a hypervisor-resident component and is tightly integrated with the KVM architecture.
- The VSM is integrated with OpenStack using the OpenStack Neutron plug-in.
- The OpenStack Neutron API has been extended to include two additional user-defined resources:
  - Network profiles are logical groupings of network segments.
  - Policy profiles group port policy information, including security, monitoring, and quality-of-service (QoS) policies.

Figure 2 shows the operational workflow in an OpenStack environment:

1. Proactively define the policy profiles on the VSM using the Cisco NX-OS command-line interface (CLI) or the Representational State Transfer (REST) API.The policies defined on the VSM are automatically propagated to the OpenStack Neutron service.
2. Proactively define the network profiles using the OpenStack Neutron CLI or API.
3. When a virtual machine is created, assign the right network and policy profiles according to the requirements.
4. The VSM propagates the right policy information to the VEM that hosts the virtual machine. Any virtual machine live-migration event triggers an update of the policy information on the target VEM.

Figure 2. Cisco Virtual Networking Solution for OpenStack Operational Workflow



Benefits

The Cisco Virtual Networking Solution for OpenStack offers the following benefits to customers:

- Reduced operational risk through:
  - Reliable, advanced Cisco NX-OS feature set
  - Well-tested, well-deployed architecture across a variety of hypervisors and use cases
  - Cisco service and support
- Simplified operational model through:
  - Tight integration with OpenStack
  - Tighter integration with the OpenStack deployment tools (for example, Juju Charms)
  - Capability to use existing tools to manage both physical and virtual networks
- Operational flexibility through:
  - Scalable switching architecture with support for VXLAN
  - Extensible services architecture through Cisco vPath
  - Strong management partner ecosystem

Main Features

Table 1 summarizes the features offered by the Cisco Virtual Networking Solution for OpenStack.

Table 1. Main Features

Feature	Description
Switching	Layer 2 switching, IEEE 802.1Q VLAN tagging, Link Aggregation Control Protocol (LACP), PortChannel, virtual PortChannel (vPC) host mode, Internet Group Management Protocol (IGMP) Versions 1, 2, and 3 (v1, v2, and v3) snooping, and jumbo-frame support
Security	Access control lists (ACLs; Layers 2 through 4 with redirect), port ACLs (PACLs), named ACLs, ACL statistics, RADIUS, and TACACS+
VXLAN	Unicast and multicast modes, port statistics, ACLs, Cisco NetFlow, and VXLAN-to-VLAN gateway
Provisioning	Integration with OpenStack Neutron APIs and OpenStack Horizon dashboard, virtual machine policy provisioning through port profiles, and capability to create service-level agreement (SLA)-based network profiles

Feature	Description
Visibility	Cisco NetFlow, port statistics, and virtual machine-level interface statistics
Manageability	Cisco NX-OS CLI, Simple Network Management Protocol (SNMP) (v1, v2, and v3), Cisco Discovery Protocol, syslog, Network Time Protocol (NTP), Cisco In Service Software Upgrade (ISSU), Secure Shell SSH v2, Telnet, REST APIs, and centralized management through VSM

High Availability

The Cisco Virtual Networking Solution for OpenStack 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 Manageability with Cisco NX-OS

The Cisco Virtual Networking Solution for OpenStack provides advanced Cisco NX-OS features, including:

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

Because this solution uses the same northbound interfaces as the Cisco Nexus physical switches, your existing network monitoring and management tools can be used across physical and virtual environments. The solution also provides a strong set of REST APIs that can be used to automate your operations.

Scalable Networking with Support for VXLAN

VXLAN is a network virtualization technology that addresses the scalability requirements associated with large cloud deployments, for which the traditional network isolation mechanisms like VLANs may not work. VXLAN meets these challenges with a MAC in User Datagram Protocol (MAC-in-UDP) encapsulation technique and a 24-bit segment identifier in the form of a VXLAN ID. This larger VXLAN ID allows the infrastructure to scale up to 16 million logical networks. In addition, the UDP encapsulation allows each LAN segment to be extended across an IP network.

The standard VXLAN technology uses IP multicast to send broadcast, multicast, and unknown unicast flood frames. This approach may not work in some customer environments that don't want to deploy IP multicast.

The Cisco Virtual Networking Solution for OpenStack supports the standard VXLAN technology as well as an enhanced VXLAN mode that doesn't require IP multicast.

Product Specifications

Maximum Supported Configurations

- 128 hosts per VSM
- 8000 vEth ports per virtual switch (vswitch), with 300 vEth ports per physical host
- 4000 active VLANs
- 4000 active VXLANs
- 4000 port profiles
- 2000 network profiles
- 32 physical network interface cards (NICs) per physical host
- 1000 PortChannels per vswitch, with 4 PortChannels per physical host

Layer 2 Features

- Layer 2 switch ports and VLAN trunks
- IEEE 802.1q VLAN encapsulation
- 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
- vPC host mode (static, MAC address pinning, MAC address pinning relative, manual, and subgroup Cisco Discovery Protocol)
- IGMP v1, v2, and v3 snooping
- Jumbo-frame support: up to 9216 bytes

Security

- Ingress and egress ACLs on Ethernet and vEth 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
    - Differentiated Services Code Point (DSCP)
    - Precedence
    - Protocol (TCP, UDP, Internet Control Message Protocol [ICMP], and IGMP)
    - Source port
    - Destination port
    - TCP flags
    - ICMP and IGMP types
    - ICMP code
- PACLs
- Named ACLs
- ACL statistics

VXLAN

- Scalable network isolation
- Port statistics
- ACL
- Cisco NetFlow
- Multicast mode
- Unicast flooding and learn mode
- Multicast traffic

Management

- Management through Cisco NX-OS CLI, OpenStack 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 v1 and v2
- 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
- NTP RFC 1305
- REST APIs (create, read, update, and 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 2 presents IEEE compliance information, and Table 3 presents RFC compliance information.

Table 2. IEEE Compliance

Standard	Description
IEEE 802.1q	VLAN tagging
IEEE 802.3	Ethernet
IEEE 802.3ad	LACP

Table 3. RFC Compliance

Standard	Description
IP Services	
RFC 768	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	NTP v3
RFC 1492	TACACS+
RFC 1591	Domain Name System (DNS) client
RFC 2068	HTTP server
RFC 2138	RADIUS authentication
RFC 2139	RADIUS accounting

Standard	Description
IP Multicast	
RFC 1112	IGMP v1 snooping
RFC 2236	IGMP v2 snooping
RFC 3376	IGMP v3 snooping

System Requirements

- Ubuntu 14.04 Long-Term Support (LTS)
- Cisco Nexus 1000V VSM
  - VSM can be deployed as a virtual machine on Ubuntu 14.04
  - 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
- Cisco VXLAN Gateway
  - Hard disk: 10 GB
  - RAM: 2 GB
- Compatible with any upstream physical switches, including all Cisco Nexus and Cisco Catalyst® switches and Ethernet switches from other vendors

Essential and Advanced Editions

The Cisco Virtual Networking Solution for OpenStack is offered in two editions:

- Essential Edition: Provides all the basic Layer 2 networking features and is available at no cost for up to 20 physical hosts
- Advanced Edition: Includes the Cisco VXLAN Gateway in addition to the base functions of the Essential Edition

Table 4 summarizes the differences in the features of the Essential and Advanced Editions.

Table 4. Feature Comparison

Feature Description	Essential (Free)	Advanced
Number of CPUs	Limited to 20 hosts	Unlimited
Switching: VLANs, ACLs, LACP, and multicast	Yes	Yes
Monitoring: Cisco NetFlow	Yes	Yes
Management: SNMP and NETCONF	Yes	Yes
Cisco VXLAN Gateway		Yes

Licensing Information

The Cisco Nexus 1000V Switch is licensed based on the number of physical CPUs on the server on which the VEM is running. And these licenses support multiple hypervisors in that the same license can be used under different hypervisors. Please contact your local Cisco representative for any additional information. .

Cisco Services

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 Switch. 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 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/c/en/us/products/switches/nexus-1000v-kvm/index.html.
- 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 C78-730833-03 08/14