Cisco Nexus 1000V Series Switches

Product Overview

Cisco Nexus 1000V Series Switches are virtual machine access switches that are an intelligent software switch implementation based on IEEE 802.1Q standard for VMware vSphere environments running the Cisco® NX-OS Software 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 connectivity
- Mobile virtual machine security and network policy
- Non-disruptive operational model for server virtualization and networking teams
- VXLAN based overlays for physical topology independent L2 segments

With the Cisco Nexus 1000V Series, you can have a consistent networking feature set and provisioning process all the way from the virtual machine access layer to the core of the data center network infrastructure. Virtual servers can now use 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 pre-defined network policy that follows mobile virtual machines to help ensure proper connectivity, saving valuable time for virtual machine administration.

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 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.

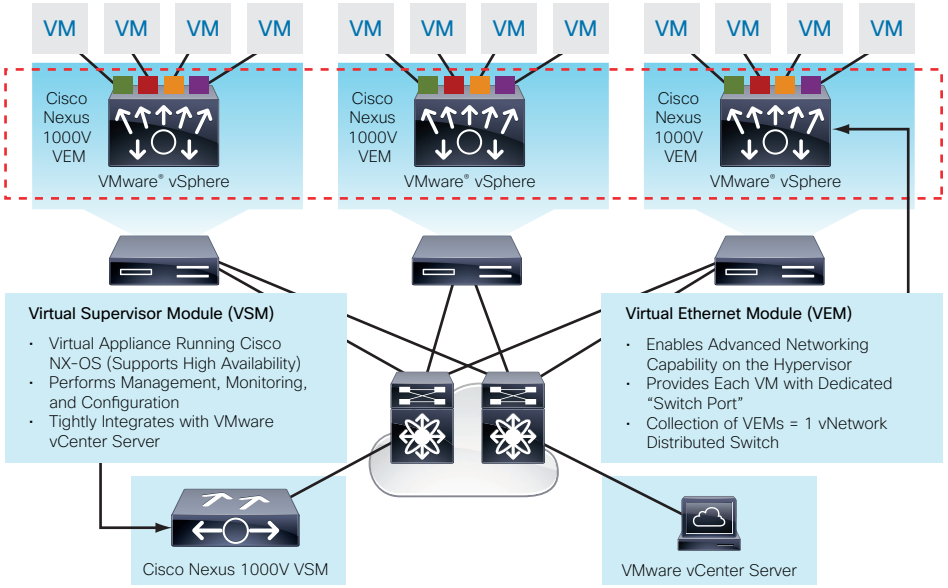
The Cisco Nexus 1000V Release 2.2 software onwards, is being offered in two editions:

- **Cisco Nexus 1000V Essential Edition:** This is available at no cost and provides most of the comprehensive Layer 2 networking features of the Cisco Nexus 1000V Series, including VXLAN, Cisco vPath for service insertion and chaining, and VMware vCloud Director integration.
- **Cisco Nexus 1000V Advanced Edition:** This version offers value-added security features such as Domain Host Control Protocol (DHCP) snooping, IP source guard, Dynamic Address Resolution Protocol (ARP) Inspection, and Cisco TrustSec® Secure Group Access (SGA) support, Unicast mode, no flood and learn and MAC (address distribution). The Cisco VSG zone-based virtual firewall is also included in the Advanced Edition.

Product Architecture

Cisco Nexus 1000V Series Switches have two major components: the Virtual Ethernet Module (VEM), which runs inside the hypervisor, and the external Virtual Supervisor Module (VSM), which manages the VEMs (Figure 1).

Figure 1. Cisco Nexus 1000V Series Architecture



Virtual Ethernet Module

The Cisco Nexus 1000V Series VEM runs as part of the VMware ESX or ESXi kernel and replaces the VMware virtual switch (vSwitch). This level of integration helps ensure that the Cisco Nexus 1000V Series is fully aware of all server virtualization events, such as VMware vMotion and Distributed Resource Scheduler (DRS). The VEM takes configuration information from the VSM and provides advanced networking functions: quality of service (QoS), security features, and monitoring features.

Virtual Supervisor Module

The Cisco Nexus 1000V Series VSM controls multiple VEMs as one logical modular switch. 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 VSM from a single interface.

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, which includes policy-based virtual machine connectivity, mobility of virtual machine security and network properties, and a non-disruptive operational model.

Policy-Based Virtual Machine Connectivity

To facilitate easy creation and provisioning of virtual machines, the Cisco Nexus 1000V Series includes port profiles. Port profiles enable you to define virtual machine network policies for different types or classes of virtual machines and then apply the profiles through the VMware vCenter. Port profiles are a scalable mechanism for configuring networks with large numbers of virtual machines. When the Port Profiles include QoS and security policies, they formulate a complete service-level agreement (SLA) for the virtual machine's traffic.

Mobility of Virtual Machine Security and Network Properties

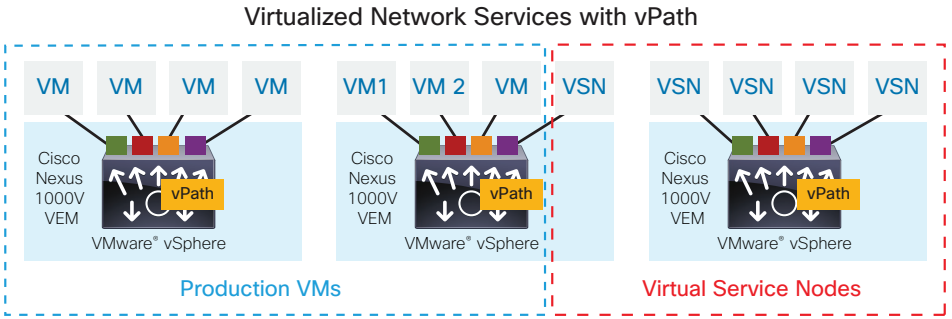
Network and security policies defined in the port profile follow the virtual machine throughout its lifecycle, whether it is being migrated from one server to another, suspended, hibernated, or restarted. In addition to migrating the policy, the Cisco Nexus 1000V Series VSM moves the virtual machine's network state. Virtual machines participating in traffic-monitoring activities can continue these activities uninterrupted by VMware vMotion operations. When a specific port profile is updated, the Cisco Nexus 1000V Series automatically provides live updates to all the virtual ports using that same port profile. The capability to migrate network and security policies through VMware vMotion makes regulatory compliance much easier to enforce with the Cisco Nexus 1000V Series because the security policy is defined in the same way as for physical servers and is constantly enforced by the switch.

Besides traditional switching capability, the Cisco Nexus 1000V Series offers the Cisco vPath architecture to support virtualized network services with:

- **Intelligent Traffic Steering:** This feature redirects packets in a network flow to a virtual service virtual machine called a Virtual Service Node (VSN), which can be on a different server. Thus, a VSN is not required on every server, providing flexible and consolidated deployment.
- **Performance Acceleration:** VEM caches the VSN's decision for a flow, implements the service in all subsequent packets of the flow, and accelerates virtualized network service in the hypervisor kernel.

Cisco Virtual Service Gateway (VSG) is the first VSN to leverage the Cisco vPath architecture and provides multi-tenant, scalable, security services for virtual machines on the Cisco Nexus 1000V Series Switches.

Figure 2. Cisco vPath Architecture



VXLAN support

Nexus 1000V offers support for VXLAN based overlay segments in addition to vlan based segments. Virtual eXtensible LAN (VXLAN) is an IETF proposed draft from Cisco and other industry vendors, to address new requirements for scalable LAN segmentation and stretching L2 segments across physical topologies for broader mobility. Virtual Extensible LAN (VXLAN), defines a 24-bit LAN segment identifier that provides segmentation at cloud scale. In addition, VXLAN provides an architecture that customers can use to expand their cloud deployments with repeatable pods in different Layer 2 domains. VXLAN can also enable migration of virtual machines between servers across Layer 3 networks.

Additional enhancements to VXLAN functionality

- **Multicast-less mode:** VXLAN functions on Cisco Nexus 1000V Series are enhanced to support a multicast-independent solution while preserving the flooding behavior. In this mode, the ingress node replicates the flooded frames instead of depending on the multicast configuration in the physical infrastructure. Each replicated frame is encapsulated in a IP-UDP packet and is sent as a unicast packet to the destination VTEP. The VSM helps identify all the network nodes currently active in a bridge domain.
- **Unicast Flood-less mode:** VXLAN uses traditional flood-and-learn behavior to learn the MAC addresses of the virtual machines. If the destination MAC address of a frame is unknown, the packet is flooded in the VXLAN segment. In the virtual environment, the VEM knows the MAC address when the virtual machine is attached to the network. This information can be used to learn the MAC address of all the devices in the segment. This capability can eliminate the need to flood to find the frames with unknown MAC addresses.

- **VXLAN Trunk Mapping:** This feature enables the user to specify the IEEE 802.1q tag to VXLAN segment associations and attach them to the interface. The interface will be part of the mapped VXLAN segments, and any traffic to and from the VXLAN segment is mapped to the corresponding IEEE 802.1q tag.
- **Multiple MAC Mode:** With this feature, the VEM at the new location generates a special frame to refresh the Layer 2 table entries. This refresh helps ensure that Layer 2 table entries are relearned with the new location from subsequent frames. Until the MAC address is learned, other VEMs will flood the frames, including the new location.

VXLAN Gateway

The VXLAN gateway provides a mechanism for combining a traditional VLAN-based segment with a VXLAN segment to form a single broadcast domain. This mechanism enables the virtual machines in a VXLAN segment to communicate with physical servers, physical service nodes, and physical network nodes such as Layer 3 routes present on the VLAN segments.

The Cisco Nexus 1000V Series provides the VXLAN gateway as a service node running on the Cisco Nexus 1010, 1010-X, 1110-X, and 1110-S appliances. The service node is integrated with the Cisco Nexus 1000V Series Switch and appears as a module on the Cisco Nexus 1000V Series Switch with a common control and management plane. All the provisioning and management of the gateway function is performed on the VSM.

REST API

In the v2.1 release we introduced REST API's which are utilized by the VC Web Client to access N1Kv information such as virtual interfaces and port-profiles. In this release we are introducing dynamic in-field upgradability of these API's at the infrastructural level utilizing NXOS support for plugins. New CLI commands are available to manage the REST API plugin. This plugin is to be provided to the customer as a CCO or developer.cisco.com download.

Non-disruptive Operational Model

Because of its close integration with VMware vCenter, the Cisco Nexus 1000V Series allows virtualization administrators to continue using VMware tools to provision virtual machines. At the same time, network administrators can provision and operate the virtual machine network the same way they do the physical network. While both teams work independently, the Cisco Nexus 1000V Series enforces consistent configuration and policy throughout the server virtualization environment. This level of integration lowers the cost of ownership while supporting organizational boundaries among server, network, security, and storage teams.

Inside VMware vCenter, virtual machines are configured as before. For network configuration, port profiles defined on the Cisco Nexus 1000V Series VSM are displayed by VMware vCenter as port groups. Virtualization administrators can take advantage of preconfigured port groups and focus on virtual machine management, and 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 operating costs.

Enhanced Deployment Scenarios

- **Optimized server bandwidth for I/O-intensive applications:** Today, network interfaces are often dedicated to a particular type of traffic, such as VMware Console or vMotion. With the Cisco Nexus 1000V Series, all network interface cards (NICs) can be treated as a single logical channel with QoS attached to each type of traffic. Consequently, the bandwidth to the server can be more efficiently utilized, with network-intensive applica-tions virtualized.
- **Easier security audits with consistent security policy:** Security audits on virtual machines are usually more difficult to perform because virtual machines are secured differently than physical servers. As the Cisco Nexus 1000V Series provides persistent security policy to mobile virtual machines, security audits are similar to those for physical servers.
- **Virtual machine as basic building block of data center:** With the Cisco Nexus 1000V Series, virtual machines are treated the same way as physical servers in security policy, monitoring and troubleshooting, and the operational model between network and server administrators, enabling virtual machines to be true basic building blocks of the data center. These operational efficiencies lead to greater scaling of server virtualization deployments with lower operating expenses.

VMware Product Compatibility

The Cisco Nexus 1000V Series is compatible with VMware vSphere as a VMware vNetwork Distributed Switch (vDS) with support for VMware ESX and ESXi hypervisors and integration with VMware vCenter Server. Cisco Nexus 1000V Series Switches are compatible with the various VMware vSphere features.

For More Information

For more information, visit:

- http://www.cisco.com/go/vn-link
- http://www.cisco.com/go/nexus1000v

C45-492852-04 06/13