Virtual Networking Features of VMware vSphere Distributed Switch and Cisco Nexus 1000V Series Switches

This solution overview is a joint creation of Cisco and VMware®.

What You Will Learn

With the introduction of VMware ESX® many virtualization administrators are managing virtual switches inside the hypervisor. This document will help virtualization and network administrators understand the available virtual networking features.

This document includes improvements resulting from the VMware vSphere™ 5 and Cisco Nexus® 1000V Series Switches Version 1.4a updates.

Alternatives for Virtual Networking

With VMware virtual networking, VMware has a number of alternatives for virtual networking in vSphere 5. Table 1 summarizes and compares the features of these alternatives.

VMware vSphere Standard Switch

The VMware vSphere Standard Switch (VSS) is the base-level virtual networking alternative. It extends the familiar appearance, configuration, and capabilities of the standard virtual switch (vSwitch) in VMware vSphere 5.

VMware vSphere Distributed Switch

The VMware vSphere Distributed Switch (VDS) extends the feature set of the VMware Standard Switch, while simplifying network provisioning, monitoring, and management through an abstracted, single distributed switch representation of multiple VMware ESX and VMware ESXi™ Servers in a VMware data center. VMware vSphere 5 includes significant advances in virtual switching by providing monitoring, troubleshooting and enhanced NIOC features. VMware vSphere Distributed switch provides flexibility to the I/O resource allocation process by introducing User Defined network resource pools. These new features will help Network Administrators in managing and troubleshooting their virtual infrastructure using familiar tools as well as provide advanced capabilities to manage traffic granularly.

Cisco Nexus 1000V Series Switches

Cisco Nexus 1000V Series Switches are the result of a Cisco and VMware collaboration building on the VMware vNetwork third-party vSwitch API of VMware VDS and the industry-leading switching technology of the Cisco Nexus Family of switches. Featuring the Cisco® NX-OS Software data center operating system, the Cisco Nexus 1000V Series extends the virtual networking feature set to a level consistent with physical Cisco switches and brings advanced data center networking, security, and operating capabilities to the VMware vSphere environment. It provides end-to-end physical and virtual network provisioning, monitoring, and administration with virtual machine-level granularity using common and existing network tools and interfaces. The Cisco Nexus 1000V Series transparently integrates with VMware vCenter™ Server and VMware vCloud™ Director to provide a consistent virtual machine provisioning workflow while offering features well suited for data center-class applications, VMware View, and other mission-critical virtual machine deployments.

Table 1: Virtual Networking Feature Comparison

	VMWARE VSPHERE 5 STANDARD SWITCH (ENTERPRISE)	VMWARE VSPHERE 5 DISTRIBUTED SWITCH (ENTERPRISE PLUS)	CISCO NEXUS 1000V SERIES 1.4a
Switching Features			
Layer 2 forwarding	Yes	Yes	Yes
IEEE 802.1Q VLAN tagging	Yes	Yes	Yes
Multicast support (Internet Group Management Protocol [IGMP] Version 2 and Version 3)	Yes	Yes	Yes
IGMPv3 snooping	No	No	Yes
VMware vSphere vMotion® support	Yes	Yes	Yes
VMware vSphere Network vMotion®	No	Yes	Yes
Physical Switch Connectivity			
Virtual MAC Pinning	Yes	Yes	Yes
EtherChannel	Yes	Yes	Yes
Virtual Port Channels	No	No	Yes
Link Aggregation Control Protocol (LACP)	No	No	Yes
Load-balancing algorithms			
Load-based teaming	No	Yes	No
Source Virtual Port ID	Yes	Yes	Yes
Source MAC address	Yes	Yes	Yes
Advanced Load Balancing Options*	No	No	Yes
Traffic Management Features			
Small Computer System Interface over IP (iSCSI) Multipathing	Yes	Yes	Yes
Unknown Unicast Flooding Control	No	No	Yes
Quality-of-Service (QoS)			
Transmit-rate (from virtual machine) limiting	Yes	Yes	Yes
Receive-rate (to virtual machine) limiting	No	Yes	Yes
IEEE 802.1p Tagging	No	Yes	Yes
Differentiated Services Code Point (DSCP)	No	No	Yes
Type of service	No	No	Yes
Classification with Access Control List (Advanced Classification)**	No	No	Yes
Weighted Fair ClassBased Queuing	No	No	Yes

	VMWARE VSPHERE 5 STANDARD SWITCH (ENTERPRISE)	VMWARE VSPHERE 5 DISTRIBUTED SWITCH (ENTERPRISE PLUS)	CISCO NEXUS 1000V SERIES 1.4a
Security Features			
Port security	Yes	Yes	Yes
Private VLANs (PVLANs)	No	Yes	Yes
Private VLAN with Promiscuous Trunks	No	No	Yes
Cross Host PVLAN Isolation	No	Yes***	Yes
Access control lists (ACLs)	No	No	Yes
DHCP Snooping - for virtual desktops	No	No	Yes
IP Source Guard - for virtual desktops	No	No	Yes
Dynamic Address Resolution Protocol (ARP) Inspection - for virtual desktops	No	No	Yes
Daily Management Features			
VMware vCenter™ support	Yes	Yes	Yes
Third-party-accessible APIs	Yes	Yes	Yes
Cisco Discovery Protocol v1 and v2	Yes	Yes	Yes
Link Layer Discovery Protocol (LLDP)	No	Yes	No
Network policy groups	Yes	Yes	Yes
Multi-tier policy groups	No	No	Yes
Physical and Virtual network consistency	No	No	Yes
RADIUS and TACACS+	No	No	Yes
IPv6 for Management	Yes	Yes	Yes
Console and interface	VMware vSphere Client	VMware vSphere Client	VMware vSphere Client and Cisco command-line interface (CLI)
Monitoring Features			
VMware port mirroring (promiscuous)	Yes	Yes	-
Cisco Switched Port Analyzer (SPAN)	No	Yes	Yes
Encapsulated Remote SPAN (ERSPAN)	No	No	Yes
Cisco NetFlow	No	Version 5	Version 9
Syslog	As VMware vCenter Server Events	As VMware vCenter Server Event	Yes
ACL Logging	No	No	Yes
Simple Network Management Protocol (SNMP) v3 read and write	No	No	Yes
SNMP Access Control List	No	No	Yes

	VMWARE VSPHERE 5 STANDARD SWITCH (ENTERPRISE)	VMWARE VSPHERE 5 DISTRIBUTED SWITCH (ENTERPRISE PLUS)	CISCO NEXUS 1000V SERIES 1.4a
Virtualized Network Services			
Virtual Service Domain	No	No	Yes
VMware VMSafe™ with Local Network Service Virtual Machine	Yes	Yes	Yes
Cisco vPath with Local and Remote Network Service Virtual Machine	No	No	Yes
Physical Appliance for Network Service Offload	No	No	Cisco Nexus 1010
Virtualized Network Services Options			
VMware vShield™ App	Yes	Yes	Yes
VMware vShield™ Edge	Yes	Yes	Yes
Cisco Virtual Security Gateway (VSG)	No	No	Yes
Cisco Network Analysis Module (NAM)	No	No	Yes
Solutions****			
Cisco Virtual Multi-Tenant Data Center Design Implementation Guide	N/A	N/A	Yes
Cisco Virtual Experience Infrastructure (VXI)	N/A	N/A	Yes
Virtual Workload Migration between Data Centers	N/A	N/A	Yes
Payment Card Industry (PCI) 2.0 Compliance Design Implementation Guide	N/A	N/A	Yes

* Advanced Load-Balancing Options: Destination MAC address; Source Layer 4 Port; VLAN ID; Source and Destination MAC Addresses; Source and Destination Layer 4 Port; Source IP Address and Source Layer 4 Port; Source IP Address and VLAN; Destination IP Address and Destination Layer 4 Port; Destination IP Address and VLAN; Source IP Address, Source Layer 4 Port, and VLAN; Destination IP address, Destination Layer 4 Port, and VLAN; Source and Destination IP Addresses and VLAN; Source and Destination of both IP Addresses and Layer 4 Ports; and Source and Destination of both IP Addresses and Layer 4 Ports plus VLAN.

** Classification with ACL: Class of Service, IP Precedence, Packet Length, Real Time Protocol (RTP), QoS Groups, 2-Rate, and 3 Color Policing.

*** VMware VDS Cross Host PVLAN Isolation requires upstream physical switch PVLAN support.

**** The solution category shows the validated and tested solutions provided by Cisco that includes VMware ESX®, VMware ESXi™ platform and various Cisco components. VMware along with various other partners have built various solutions and you can find those solution guides on VMware and Partner websites. However, there are no validated design guides focused on usage of vSphere standard and distributed switch.

Features

This section provides additional information about some of the features and capabilities listed in Table 1.

Switching Features

- **Multicast:** Both vSwitch alternatives support multicast traffic and multicast group membership through IGMP. The Cisco and VMware switches differ slightly in implementation. The VMware vSwitches learn multicast membership through a nonflooding registration process, and the Cisco Nexus 1000V Series uses IGMP snooping in a similar fashion on a physical switch.
- **Network VMware VMotion:** The network policy associated with a VMware VDS port is transferred with the virtual machine when it is migrated to another host using VMware VMotion. In addition, the Cisco Nexus 1000V Series Switch maintains the network state of management and troubleshooting data associated with a virtual machine's network interface. This feature provides a consistent view of a network interface regardless of the virtual machine's location.

Physical Switch Connectivity

- **EtherChannel:** EtherChannel and Port Channel are commonly used terms for IEEE 802.3ad and 802.1AX link aggregation. The VMware vSwitches use and require a static configuration on the adjacent physical switch without LACP negotiation, whereas the Cisco Nexus 1000V Series EtherChannels are fully negotiable through LACP. The Cisco Nexus 1000V Series additionally supports virtual PortChannels, which enables fine-grained traffic load balancing across multiple physical switches using a single PortChannel. This approach greatly simplifies network configuration and enhances the availability of network connectivity and therefore increases virtual machine uptime for EtherChannel configurations.

Load-Balancing Algorithms

- **Source Virtual Port ID:** There are many ways to distribute traffic within an EtherChannel or LACP. Virtual Port ID is just one of many techniques listed here. Cisco offers 17 advanced ways to load-balance traffic consistent with physical network load-balancing techniques.
- **Load Base Teaming:** VMware vSphere Distributed Switch provides this unique load balancing algorithm that takes physical port bandwidth utilization into account while distributing traffic across multiple active ports. This algorithm works on both Rx and Tx direction.

Traffic Management Features

- **iSCSI Multipathing:** iSCSI traffic uses multiple paths through the network.
- **Unknown Unicast Flooding Control:** This feature reduces unicast flooding and server CPU workload.

QoS Features

- **Transmit-rate (from virtual machine) limiting:** Transmit-rate limiting enables traffic from the virtual machine to the network to be rate limited.
- **Receive-rate (to virtual machine) limiting:** Receive-rate limiting enables traffic to the virtual machine from the network to be rate limited.
- **IEEE 802.1p Tagging:** Layer 2 QoS marking of the traffic is performed.

- **DSCP:** Layer 3 Differentiated Services QoS marking is performed.
- **Classification with ACL (Advanced Classification):** Cisco offers eight separate ways to classify, mark, and police traffic.

Security Features

- **Local PVLAN Enforcement:** This feature allows you to secure your virtual infrastructure with the PVLAN feature without configuring PVLAN on your physical network switch.
- **Port security:** Port security with VMware switches is a MAC address control feature governing the use of promiscuous mode, MAC address changes by a virtual machine, and forced transmits from a virtual machine. The Cisco Nexus 1000V Series supports MAC address-based port security and configurable Access Control Lists (ACLs).
- **PVLANs:** PVLANs are a new feature available with the VMware VDS and the Cisco Nexus 1000V Series. PVLANs provide a simple mechanism for isolating virtual machines in the same VLAN from each other. The VMware VDS implements PVLAN enforcement at the destination host. The Cisco Nexus 1000V Series supports a highly efficient enforcement mechanism that filters packets at the source rather than at the destination, helping ensure that no unwanted traffic traverses the physical network and so increasing the network bandwidth available to other virtual machines. Hence, the Cisco Nexus 1000V Series can implement PVLAN among multiple hosts without upstream switch support.
- **DHCP Snooping, IP Source Guard, and Dynamic ARP Inspection:** These three features secure virtual desktop deployments by securing the Layer 2 domain. These features prevent rogue DHCP servers and man-in-the-middle attacks by inspecting IP and ARP packets to confirm that they match the DHCP snooping table. For virtual desktop deployment, these features enable virtual desktops to have the same networking security posture as physical desktops.

Daily Management Features

- **Multi-tier policy groups:** The unique port profile capabilities of the Cisco Nexus 1000V Series allow network administrators to build multi-tier network policies, simplifying policy creation and enforcement.
- **Console and Interface:** Virtual networking with VMware vSwitches is configured through the VMware vSphere Client interface. A VMware vCenter Server must be used when configuring and using VMware VDS. The Cisco Nexus 1000V Series uses a combination of the Cisco command-line interface (CLI) to allow the network administrator to configure network policy and VMware vCenter Server to preserve the virtual machine provisioning workflow.

Monitoring Features

- **VMware port mirroring (promiscuous):** The VMware vSwitch can send traffic for one VLAN or all VLANs to a virtual machine on a promiscuous virtual network interface card (vNIC) port configured with traffic monitoring or “sniffing.”
- **Cisco Switched Port Analyzer (SPAN) and Encapsulated Remoted SPAN (ERSPAN):** The VMware VDS and Cisco Nexus 1000V Series enable true packet capture and analysis by supporting features such as Cisco SPAN. In addition, the Cisco Nexus 1000V Series provides ERSPAN, which allow traffic to be copied to a remote destination, enabling thorough network troubleshooting and reducing time to resolution for virtual network problems.

- **Syslog:** VMware ESX Servers can export syslog information for the entire server. This process requires filtering and analysis to extract the VMware vSwitch events. The Cisco Nexus 1000V Series can export extensive network-specific events to appropriate syslog servers, potentially eliminating error reports unrelated to network issues. This feature enables the network administrator to quickly diagnose any potential problems.

- **Cisco NetFlow:** The VMware VDS supports Cisco NetFlow version 5 while Cisco Nexus 1000V provides support for NetFlow version 9. The NetFlow capability on virtual switches help in monitoring virtual infrastructure flows that are not visible to physical switch infrastructure. Version 9 provides more flexibility and adjusts the amount of information sent to NetFlow collector.

Virtualized Network Services

- **Virtual Service Domain:** This feature provides a way to define a logical group of virtual machines protected by a virtual appliance. All traffic entering or leaving the group will be sent to that particular virtual appliance.

- **Cisco vPath with Local and Remote Service virtual machine:** The service virtual machine can be on the same server as the production virtual machine or on a remote server.

- **Physical Appliance for Network Service Offload:** The Service virtual machine can be hosted on the Cisco Nexus 1010 for the network service team to manage and offload.

Virtualized Network Services Options

- **Cisco Network Analysis Module (NAM):** This module uses Cisco NetFlow and ERSPAN from the Cisco Nexus 1000V Series Switch and other sources for a holistic network view of data center.

Solutions

- **Cisco Virtual Multi-Tenant Data Center Design Guide:** Cisco has fully tested and documented infrastructure as a service (IaaS).
  - http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VMDC/2.0/introduction/vmdcIntro.html

- **Cisco Virtual Experience Infrastructure (VXI):** Using VMware vSphere and View and the Cisco Nexus 1000V Series, Cisco has a fully tested reference design for virtual desktop deployments.
  - http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VXI/configuration/VXI_Config_Guide.pdf

- **Virtual Workload Migration between Data Centers:** A Cisco Validated Design is available for VMware vMotion migration between data centers.
  - EMC: http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DCI/4.0/EMC/dciEmc.html
  - NetApp: http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DCI/4.0/Netapp/dciNetapp.html

- **Payment Card Industry 2.0 Compliance Design Implementation Guide:** This guide provides an in-depth roadmap for retail organizations to achieve PCI compliance, including virtual workloads with the Cisco Nexus 1000V Series.
  - http://www.cisco.com/en/US/docs/solutions/Verticals/PCI_Retail/PCI_Retail_DIG.html

C22-526262-02 09/11