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

What You Will Learn

With the introduction of VMware ESX, many virtualization administrators are managing virtual switches inside the hypervisor. Since the virtual switches need to be configured consistently with the physical network, virtualization and network administrators have to work closely to help ensure proper virtual machine connectivity.

This document will help virtualization and network administrators understand the virtual networking features and capabilities introduced by VMware and Cisco in 2009.

Alternatives for Virtual Networking

With VMware vNetwork in 2009, VMware is introducing a number of alternatives for virtual networking with VMware Infrastructure (VI). Table 1 summarizes and compares the features of these alternatives.

VMware vNetwork Standard Switch

The VMware vNetwork Standard Switch is the base-level virtual networking alternative. It extends the familiar appearance, configuration, and capabilities of the standard virtual switch (vSwitch) in VMware ESX 3.5 to the new release in 2009.

VMware vNetwork Distributed Switch

The VMware vNetwork Distributed Switch (vDS) is new with the 2009 release of VI. The VMware 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 ESXi Servers in a VMware data center.

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 VI 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 to provide a consistent virtual machine provisioning workflow while

© 2009 Cisco | VMware. All rights reserved.

offering features well suited for data center–class applications, VMware View, and other mission-critical virtual machine deployments.

Table 1. Virtual Networking Feature Comparison

Feature	VMware ESX 3.5: Standard vSwitch	VMware vNetwork Standard Switch	VMware vNetwork Distributed Switch	Cisco Nexus 1000V Series
Switching Features				
Layer 2 forwarding	Yes	Yes	Yes	Yes
IEEE 802.1Q VLAN tagging	Yes	Yes	Yes	Yes
Multicast support (Internet Group Management Protocol [IGMP] v2 and v3)	Yes	Yes	Yes	Yes
IGMPv3 snooping	–	–	–	Yes
VMware VMotion support	Yes	Yes	Yes	Yes
Network VMware VMotion	–	–	Yes	Yes
Physical Switch Connectivity				
EtherChannel	Yes	Yes	Yes	Yes
Virtual PortChannels	–	–	–	Yes
Link Aggregation Control Protocol (LACP)	–	–	–	Yes
Load-balancing algorithms				
• Virtual port ID	Yes	Yes	Yes	Yes
• Source MAC address	Yes	Yes	Yes	Yes
• Source and destination IP	Yes	Yes	Yes	Yes
• Source and destination MAC addresses	–	–	–	Yes
• Source and destination port IP	–	–	–	Yes
• Additional hashing options	–	–	–	Yes
Traffic Management Features				
Transmit-rate (from virtual machine) limiting	Yes	Yes	Yes	Yes
Receive-rate (to virtual machine) limiting	–	–	Yes	Yes

© 2009 Cisco | VMware. All rights reserved.

Quality-of-service (QoS) marking				
• Differentiated Services Code Point (DSCP)	–	–	–	Yes
• Type of service	–	–	–	Yes
• Class of service	–	–	–	Yes
Security Features				
Port security	Yes	Yes	Yes	Yes
VMware VMsafe compatible	Yes	Yes	Yes	Yes
Private VLANs (PVLANs)	–	–	Yes	Yes
Local PVLAN enforcement	–	–	–	Yes
Access control lists (ACLs)	–	–	–	Yes
Dynamic Host Configuration Protocol (DHCP) snooping	–	–	–	Yes
IP source guard	–	–	–	Yes
Dynamic Address Resolution Protocol (ARP) Inspection (DAI)	–	–	–	Yes
Management Features				
VMware vCenter support	Yes	Yes	Yes	Yes
Third-party-accessible APIs	Yes	Yes	Yes	Yes
Network policy groups	Yes	Yes	Yes	Yes
Multitier policy groups	–	–	–	Yes
VMware port mirroring (promiscuous)	Yes	Yes	Yes	–
Switched Port Analyzer (SPAN)	–	–	–	Yes
Encapsulated Remote SPAN (ERSPAN)	–	–	–	Yes
NetFlow v5	Yes*	Yes*	Yes*	Yes
NetFlow v9	–	–	–	Yes
Simple Network Management Protocol (SNMP) v3 read and write	–	–	–	Yes
Cisco Discovery Protocol v1 and v2	Yes	Yes	Yes	Yes
Syslog	Yes**	Yes**	Yes**	Yes

© 2009 Cisco | VMware. All rights reserved.

Packet capture and analysis	–	–	–	Yes
RADIUS and TACACS+	–	–	–	Yes
Configuration and management console and interface	VI Client	VI Client	VI Client to VMware vCenter Server	VMware vCenter and Cisco CLI

* Experimental support provided.
** Virtual switch network syslog information is exported and included with VMware ESX Server events.

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 PortChannel 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.

Traffic Management 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.

© 2009 Cisco | VMware. All rights reserved.

Security Features

- **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 in addition to IP source guard, DAI, and DHCP snooping to help isolate malicious virtual machines.
- **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.

Management Features

- **Multitier policy groups:** The unique port profile capabilities of the Cisco Nexus 1000V Series allow network administrators to build multitier network policies, simplifying policy creation and enforcement.
- **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.”
- **Packet capture and analysis:** The Cisco Nexus 1000V Series enables true packet capture and analysis by supporting features such as SPAN and ERSPAN, which allow traffic to be copied to a local or 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 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.
- **Configuration and management console and interface:** Virtual networking with VMware vSwitches is configured through the VI Client interface. A VMware vCenter Server must be used when configuring and using the 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.

© 2009 Cisco | VMware. All rights reserved.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

VMware, Inc
3401 Hillview Ave
Palo Alto, CA 94304
USA
www.vmware.com
Tel: 1-877-486-9273 or 650-427-5000
Fax: 650-427-5001

Copyright © 2009. VMware, Inc. All rights reserved. Protected by one or more U.S. Patent Nos. 6,397,242, 6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,880,022, 6,944,699, 6,961,806, 6,961,941, 7,069,413, 7,082,598, 7,089,377, 7,111,086, 7,111,145, 7,117,481, 7,149, 843, 7,155,558, 7,222,221, 7,260,815, 7,260,820, 7,269,683, 7,275,136, 7,277,998,7,277,999, 7,278,030, 7,281,102, 7,290,253, 7,356,679 and patents pending.

Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

(0903R) C22-526262-00 03/09