What's New in VMware vSphere 5.5 Networking

VMware vSphere 5.5

TECHNICAL MARKETING DOCUMENTATION

vmware®

Table of Contents

Introduction 3
VMware vSphere Distributed Switch Enhancements 3
Link Aggregation Control Protocol 4
Traffic Filtering 5
Quality of Service Tagging 6
Troubleshooting and Performance Enhancements 6
Enhanced Host-Level Packet-Capture Tool 6
40GB Network Adapter Support 6
Single-Root I/O Virtualization Enhancements 6
About the Author 7

Introduction

With the release of VMware vSphere® 5.5, VMware brings a number of enhancements to the networking capabilities in the vSphere platform. These enhancements enable users to manage their virtual networking infrastructure with greater efficiency and confidence. The following are the enhancements made in the vSphere 5.5 release:

- More hashing algorithms for link aggregation
- More link aggregation groups
- Traffic-filtering support
- Differentiated Service Code Point (DSCP) marking support
- Improved host-level packet-capture tool
- Improved single-root I/O virtualization (SR-IOV) support
- 40GB network adapter support

VMware vSphere Distributed Switch Enhancements

VMware vSphere® Distributed Switch™ is a centrally managed, data center–wide switch that provides advanced networking features on the vSphere platform. Having one virtual switch for the entire vSphere environment greatly simplifies management. vSphere 5.5 builds on the improvements made in the 5.1 release by enhancing the link aggregation control protocol (LACP) support and introducing traffic filtering and DSCP marking support.

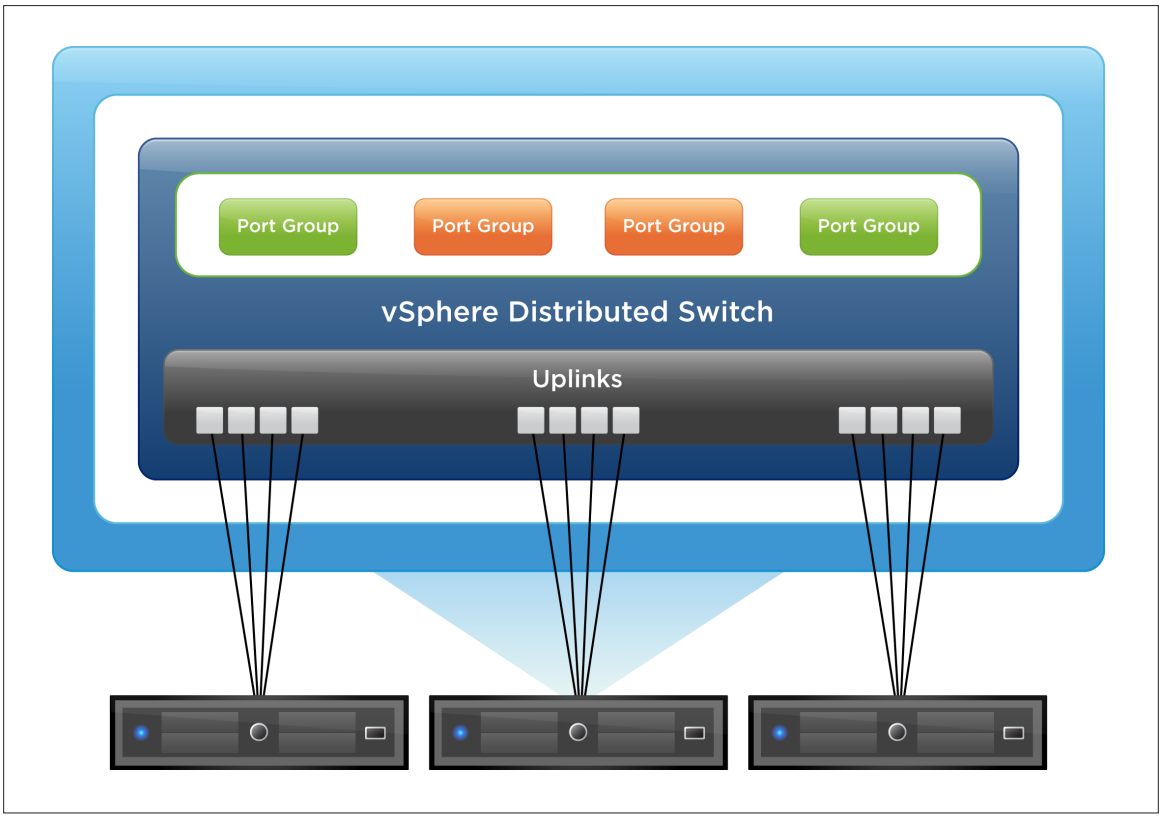

Figure 1. vSphere Distributed Switch

Link Aggregation Control Protocol

LACP is supported in vSphere 5.1. LACP is a standards-based method for controlling the bundling of several physical network links together to form a logical channel, for increased bandwidth and redundancy purposes.

LACP dynamically negotiates link aggregation parameters such as hashing algorithms and number of uplinks across vSphere Distributed Switch and physical access layer switches. If link failures or cabling mistakes occur, LACP automatically renegotiates parameters across the two switches. This reduces the manual intervention required to debug cabling issues.

The following key enhancements are available in vSphere Distributed Switch with vSphere 5.5:

- **Comprehensive load-balancing algorithm support** – 22 new hashing algorithm options are available. For example, source and destination IP address and VLAN field can be used as the input for the hashing algorithm.
- **Support for multiple link aggregation groups (LAGs)** – 64 LAGs per host and 64 LAGs per VMware vSphere Distributed Switch are supported.
- **Configuration templates** – Because LACP configuration is applied per host, it can be time-consuming for large deployments. In this release, new workflows for configuring LACP across a large number of hosts are made available through templates.

Figure 2 shows a deployment in which a vSphere host has four uplinks, and those uplinks are connected to the two physical switches. LAGs are created by combining two uplinks on the physical and virtual switch. The LACP configuration on the vSphere host is performed on vSphere Distributed Switch and the port groups.

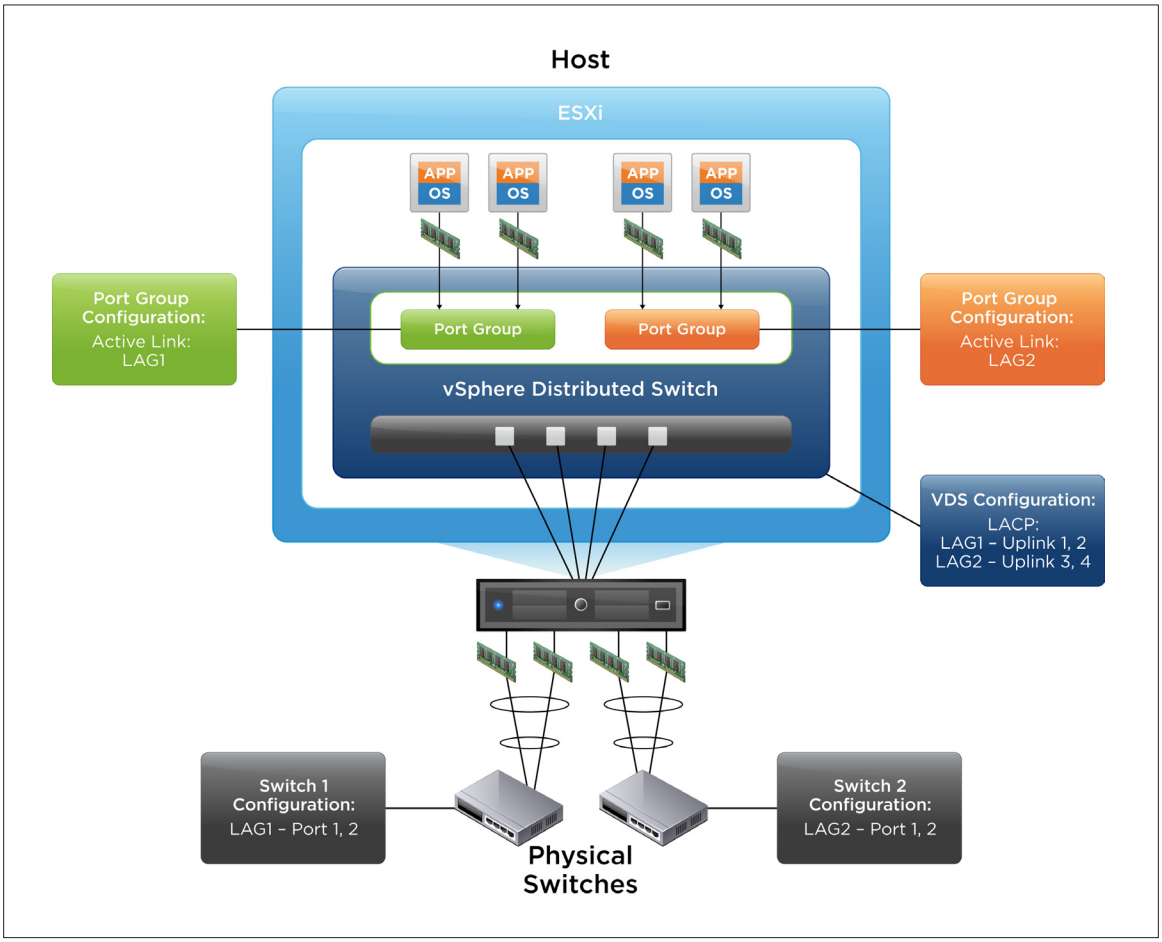

Figure 2. LACP Example: Two LAGs

First, the LAGs and the associated uplinks are configured on vSphere Distributed Switch. Then, the port groups are configured to use those LAGs. In this example, the green port group is configured with LAG1 and the yellow port group is configured with LAG2. All the traffic from virtual machines connected to the green port group follow the LAG1 path.

Traffic Filtering

Traffic filtering is the ability to filter packets based on the parameters of the packet header. This capability—also referred to as *access control lists* (ACLs)—is used to provide port-level security.

vSphere Distributed Switch supports packet classification, based on the following types of qualifiers:

- MAC source address and destination address qualifiers
- System traffic qualifiers: VMware vSphere vMotion®, vSphere management, vSphere Fault Tolerance, and so on
- IP qualifiers: Protocol type, IP source address, IP destination address, and port number

After the qualifier is selected and packets are classified, users have the option to either filter or tag those packets.

After the classified packets are selected for filtering, users have the option to filter ingress, egress, or traffic in both directions. As shown in Figure 3 the traffic-filtering configuration is at the port-group level.

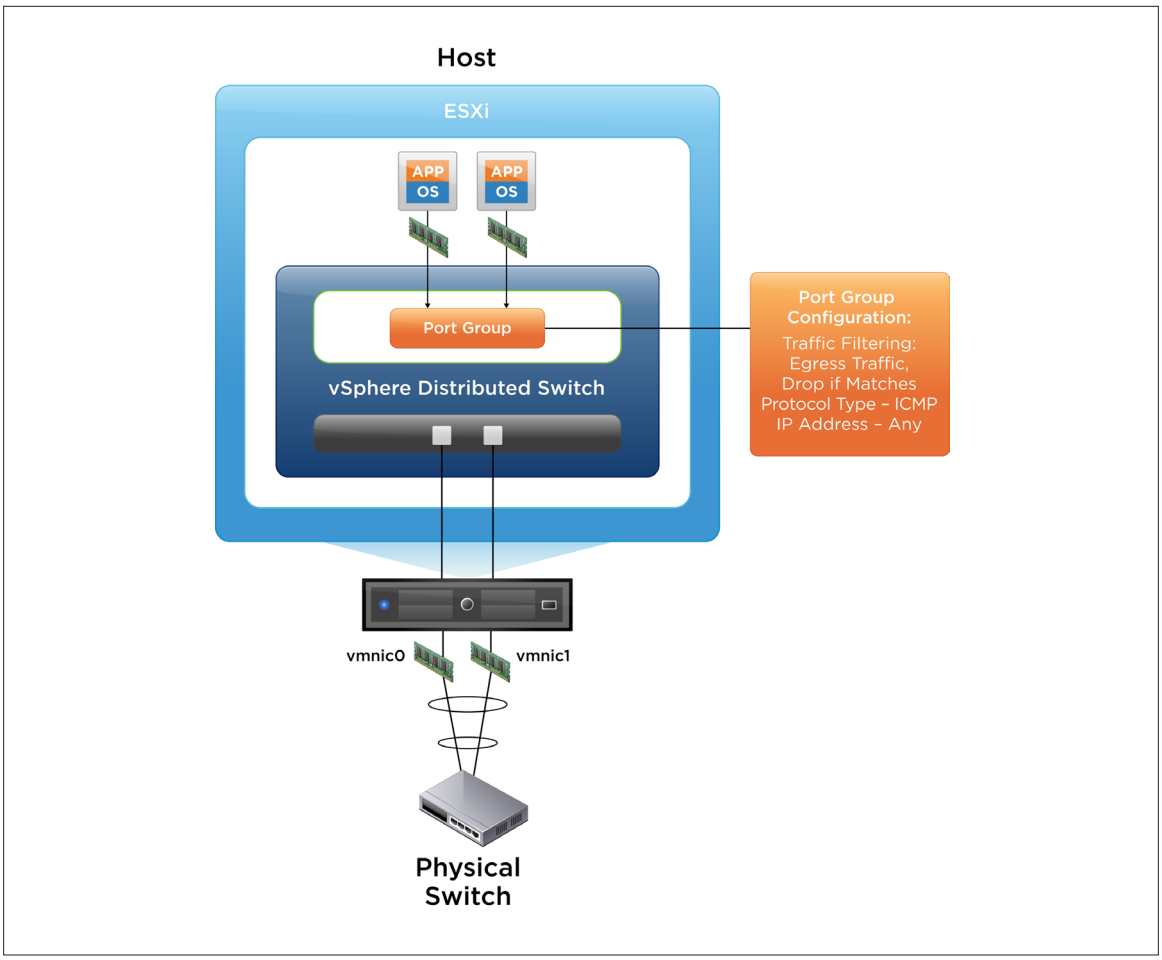

Figure 3. Traffic Filtering

Quality of Service Tagging

Two types of quality of service (QoS) marking or tagging common in networking are 802.1p Class of Service (CoS) applied on Ethernet (Layer 2) packets, and DSCP applied on IP packets. The physical network devices use these tags to identify important traffic types and provide QoS based on the value of the tag. Because business-critical and latency-sensitive applications are virtualized and run in parallel with other applications on a VMware ESXi™ host, it is important to enable the traffic management and tagging features on vSphere Distributed Switch.

The traffic management feature on vSphere Distributed Switch helps reserve bandwidth for important traffic types. The tagging feature enables the external physical network to detect the level of importance of each traffic type. It is a best practice to tag the traffic near the source to help achieve end-to-end QoS. In network congestion scenarios, the highly tagged traffic doesn't get dropped, which provides the traffic type with higher QoS.

VMware has supported 802.1p tagging on vSphere Distributed Switch since vSphere 5.1. The 802.1p tag is inserted in the Ethernet header before the packet is sent out on the physical network. In vSphere 5.5, the DSCP marking support enables users to insert tags in the IP header. IP header–level tagging helps in Layer 3 environments, where physical routers function better with an IP header tag than with an Ethernet header tag.

After the packets are classified based on the qualifiers described in the "Traffic Filtering" section, users can choose to perform Ethernet (Layer 2) or IP (Layer 3) header level marking. The markings are configured at the port group level.

Troubleshooting and Performance Enhancements

Troubleshooting any network issue requires various sets of tools. In a vSphere environment, vSphere Distributed Switch provides standard monitoring and troubleshooting tools, including NetFlow, Switched Port Analyzer (SPAN), Remote Switched Port Analyzer (RSPAN), and Encapsulated Remote Switched Port Analyzer (ERSPAN). In this release, an enhanced host-level packet capture tool is introduced.

Enhanced Host-Level Packet-Capture Tool

The packet capture tool is equivalent to the command-line tcpdump tool available on the Linux platform.

The following are some of the key capabilities of the packet capture tool:

- Available as part of the vSphere platform and can be accessed through the vSphere host command prompt
- Can capture traffic on the vSphere standard switch and vSphere Distributed Switch
- Captures packets at the following levels:
  - Uplink
  - Virtual switch port – virtual network adapter
- Can capture dropped packets
- Can trace the path of a packet with time stamp details

40GB Network Adapter Support

Support for 40GB network adapters on the vSphere platform enables users to take advantage of higher bandwidth pipes to the servers. In this release, the functionality is delivered via Mellanox ConnextX-3 VPI adapters configured in Ethernet mode.

Single-Root I/O Virtualization Enhancements

SR-IOV is a standard that enables one PCI Express (PCIe) adapter to be presented as multiple, separate logical devices to virtual machines. In this release, the workflow of configuring the SR-IOV–enabled physical network adapters is simplified. Also, a new capability is introduced that enables users to communicate the port group properties defined on the vSphere standard switch or vSphere Distributed Switch to the virtual functions.

The new control path through the vSphere standard switch and vSphere Distributed Switch communicates the port group specific properties to the virtual functions. For example, if promiscuous mode is enabled in a port group that configuration is then passed to virtual functions, and the virtual machines connected to the port group receives traffic from other virtual machines.

About the Author

Mike Brown is a senior technical marketing manager in the Cloud Infrastructure Technical Marketing Group at VMware. Mike's focus is VMware® vCenter™ availability and scalability, resource management, and the enablement of vSphere Enterprise Plus Edition™ features. He has multiple industry certifications, including VMware Certified Design Expert (VCDX).

Follow Mike's blogs at http://blogs.vmware.com/vsphere.

Follow Mike on Twitter: @vMikeBrown.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2014 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: VMW-TWP-WHATS-NEW-IN-vSPHERE-5-5-NETWORKING-USLET-101
03/14