TECHNOLOGY BRIEF
Intel® Xeon® Processor E5-2600 Product Family
Intel® Ethernet Converged Network Adapter Family
VMware vSphere* 5.1

Simplified, High-Performance 10GbE Networks Based on a Single Virtual Distributed Switch, Managed by VMware vSphere* 5.1

New capabilities in VMware vSphere* provide manageability advantages that enhance the performance, simplicity, and flexibility advantages associated with large-scale 10 Gigabit Ethernet networks. By making it easier to configure and manage network bandwidth by traffic type, this approach avoids inefficiencies associated with static allocations patterned after older Gigabit Ethernet topologies.

1 Executive Summary

Early virtualization models used large numbers of Gigabit Ethernet (1GbE) connections, patterned after the older approaches previously used in non-virtualized networks. During the transition to 10 Gigabit Ethernet (10GbE), network architects attempted to continue that model by carving up 10GbE ports into multiple smaller ports to control bandwidth and allocate bandwidth to the different virtual infrastructure traffic types. That approach created limitations in terms of scalability and made the environment inflexible and overly complex. With the introduction of VMware vSphere* 5.1, dynamic management of the entire physical and virtual network infrastructure from a single pane of glass addresses those limitations, using VMware vCenter* Server (formerly VMware VirtualCenter*), which is part of vSphere.

The VMware vSphere environment implements new capabilities for virtual networking that take advantage of the virtualization features built into Intel® Ethernet Converged Network Adapters. This combination of technologies enables greater flexibility from the virtual networking environment, resulting in dynamic balancing of resources to optimize performance, while maintaining high availability (HA) and quality of service (QoS).

VMware vSphere 5.1 can support up to eight physical 10GbE ports, which helps to take advantage of the processing headroom of servers based on the Intel® Xeon® processor E5-2600 product family. As a capability of vSphere, those ports can provide up to four Fibre Channel over Ethernet (FCoE) adapters, eight iSCSI adapters, and four VMware vMotion* paths. Managing these types of large-scale resources in the VMware environment is dramatically simplified using features that are available only from vSphere Enterprise Plus, including the VMware vSphere Distributed Switch (VDS).

In prior versions of vSphere, the virtual network had to be configured using multiple VMware vSphere Standard Switches (VSSs, vSwitches), which involves far more complexity, making costly human error more likely. Moreover, the use of multiple VSSs involves the static allocation of bandwidth, which reduces flexibility and adds the risk that bandwidth will be misallocated, reducing network-resource utilization and negatively impacting performance. Using a single VDS dramatically simplifies implementation, while VMware vCenter Server dynamically monitors and manages physical and virtual bandwidth.

This paper describes the advantages of dynamically allocating virtualized network resources using VDSs and VMware vCenter Server. It provides guidance to network architects, CTOs, and other decision makers at medium-sized to large organizations in planning implementations of vSphere 5.1, with a focus on Intel® Xeon® processor-based servers and Intel Ethernet Converged Network Adapters. The paper's main sections are as follows:

- **Overview: Evolution of Virtual Switches to Enhance Efficiency and Performance** describes the transformations in the data center associated with the development of the VSS and the VDS.
- **Software Entities at the Heart of the Virtualized Network** discusses how software constructs such as virtual NICs, virtual switches, and port groups form the basis of virtual network architecture.
- **Superior Traffic Management with VDS-based Networking** describes the benefits of using the VDS as the basis for automated resource allocation to replace older methods based on static segmentation.
- **Management and Security for Virtual Networks and the Cloud** describes VMware tools built to provide distributed management and security functionality across virtualized networks and cloud infrastructures.

Table of Contents

2 Overview: Evolution of Virtual Switches to Enhance Efficiency and Performance

Large-scale virtualization involves the use of combinations of virtual and physical networking components. Therefore, virtual switches must provide similar capabilities to those of physical switches in areas such as HA, quality of service, and security. It must also perform that management at the data center level, rather than at the level of a single physical host or isolated segment of the virtual network. A single VMware VDS can handle interconnections among virtual machines (VMs) on as many as 500 physical hosts, and a single vCenter instance can include as many as 128 VDSs.

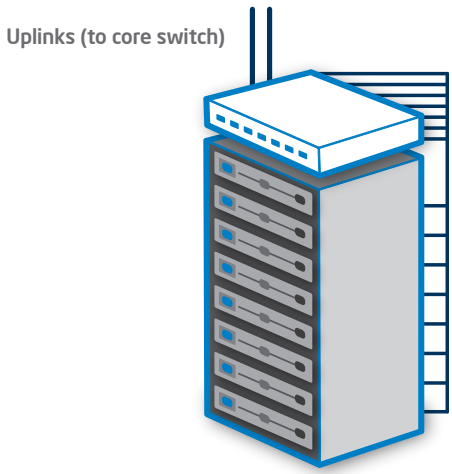
Simple server consolidation using virtualization replaces individual servers with VMs, many of which can reside together on a single host. Whereas networking among the non-virtualized servers was based on cables, switches, and other physical components, networking among the VMs requires the addition of virtualized, software-based components. The simplest form of virtual networking replaces the physical top-of-rack switch with a software-based virtual switch that runs on the physical host, as shown in Figure 1. A virtual switch works like a Layer 2 physical switch.

2.1 Managing Virtualized Traffic within a Single Host with VSSs

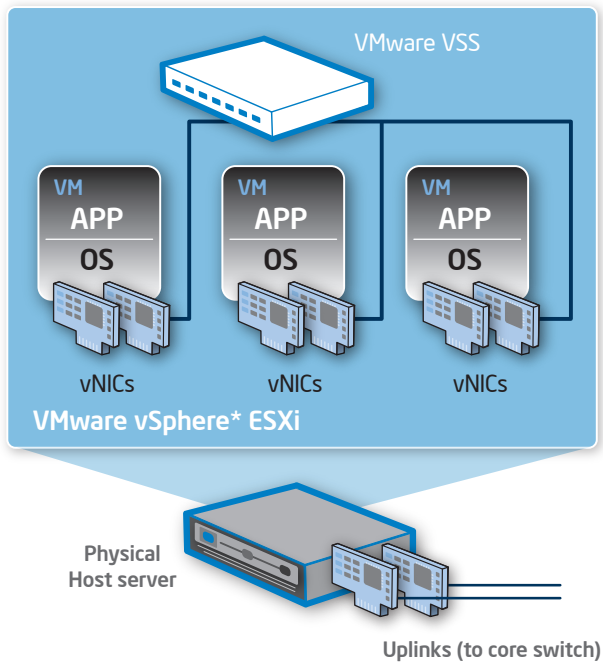
In the non-virtualized version of the model shown in Figure 1, dedicated servers were often used to host specific applications, for technical reasons such as using a specific OS, for business reasons such as isolating payroll information, or for legal reasons such as meeting regulatory requirements. LAN connections between individual servers and the top-of-rack switch were typically based on two 1GbE connections for redundancy. Particularly network-intensive workloads might be accommodated by additional 1GbE connections between the server and the switch. In either case, certain limitations arose.

- **Inflexible topologies**. Physical connections segmented network bandwidth into dedicated 1 Gb connections for different traffic types, which could not easily be changed, decreasing flexibility. To add bandwidth required physically connecting and configuring new connections at the server and the switch.
- **Inefficient designs**. Network architects were forced to assign extra bandwidth to servers by using link aggregation of multiple connections, to handle workload peaks leading to poor overall utilization of network resources.
- **Prevalent bottlenecks**. Even with link aggregation, connections were still limited to a maximum of 1 Gb per session and required additional switch configuration and coordination. Trying to provide enough bandwidth for peak times on each of these dedicated connections often put strain on budgets, because over-provisioning was necessary to avoid not having enough throughput available when it was needed.

In the virtualized server-consolidation scenario shown in Figure 1, a software-based virtual switch (such as the VMware VSS) is used to route traffic among the VMs, acting analogously to the top-of-rack switch in the non-virtualized case. In addition to handling network traffic within the host, a VSS can connect to external networks through the use of physical Ethernet network adapters. Moving the access layer from the physical- to software-based virtual entities allows the environment to more dynamically assign network resources as needed, addressing the limitations listed above by creating a more agile network in the presence of changing conditions.



Non-virtualized infrastructure:
Multiple servers are connedted to a top-of-rack physical switch



Virtualized server consolidation:
Each server is replaced by a VM, co-located on the virtualized host and networked using a software-based virtual switch

Figure 1. VMware vSphere Standard Switches (VSSs) connect multiple virtual machines (VMs) within the physical host, analogous to top-of-rack switches connecting multiple servers within a rack.

In the virtualized server-consolidation scenario, the physical host's network connections function as switch uplinks that carry traffic from a large number of VMs, in the same way that on the left side, the top-of-rack switch's uplinks carry traffic from a large number of physical servers. Therefore, the network connections on physical hosts should use the same type of configurations used on switch uplinks, such as using 10GbE connections, rather than the 1GbE connections used on the non-virtualized servers. This transition is described in greater detail in the Intel technology brief, "Virtual Switches Demand Rethinking Connectivity for Servers."[1]

A common approach in deploying new technologies is to use existing data center deployment models to ease the transition as new methods are developed and paradigm shifts in thinking are accepted. In some cases, new methods or products are created to help bridge the old models and new technologies. These bridging methods tend to lose favor quickly as new deployment models are proven and the earlier methods become regarded as more restrictive than useful. An example of a bridging method is to carve up a 10GbE port into multiple smaller ports that are a subset of the total 10 Gb potential bandwidth.

This deployment method could have helped organizations transition their multiple-port 1GbE hosts to 10GbE by not having to change their previous VSS configuration tools used in older version of VMware products. However, it limited the use of the enhancements and optimizations of the VDS made available in VMware vSphere 5.0. While the transition from 1GbE to 10GbE requires upgrading the physical switch and network adapters on the hosts, the transition from carved-up 10GbE ports to "big open pipes" to the server is primarily a software configuration change. In that sense, this transition is analogous to removing traffic cones that were temporarily used to direct traffic during road construction.

The recent advances in server performance and the convergence of network and storage networking provide further enhancements that benefit this "big open pipe" model, in terms of flexibility and performance. In conjunction with those advances, the QoS features in virtualization software such as vSphere and related network management tools continue to drive more sophisticated usage models, making it relatively straightforward to accommodate multiple traffic types on a single virtual switch while achieving line-rate throughput that rivals or even outperforms the earlier physical server deployment models.

2.2 Managing Virtualized Traffic across Up to 500 Hosts with VDSs

In the virtualized server consolidation model using one or more VSSs on each host, as described above, multiple physical hosts (and the virtualized resources on them) are connected to the physical switches, but unlike the deployment illustrated in Figure 2 are made up of multiple network connections and VSSs. This deployment model constrains network performance and flexibility in similar fashion to the static assignment of network resources in the non-virtualized model. While the scope of the total workload per server is greater in the virtualized server consolidation model with VSSs compared to non-virtualized servers, the fundamental problem of balance between over-allocating and under-allocating network resources persists.

To address the limitations placed on virtual networks by the physical segmentation between hosts inherent to the VSS model described above, VMware vSphere Enterprise Plus provides the VDS, which creates a higher level of abstraction, with virtual interconnections among VMs that span across hosts, as shown in Figure 3. In its role as a single virtual switch across all associated hosts, the VDS functions as a network switch for internal and external network connectivity. The VDS handles network traffic at the multi-host level; it can route traffic internally between VMs or link to an external network by connecting to physical Ethernet network adapters.

A particular benefit of the VDS is that it allows VMs to maintain consistent network configuration as they migrate across multiple hosts in the vSphere environment.

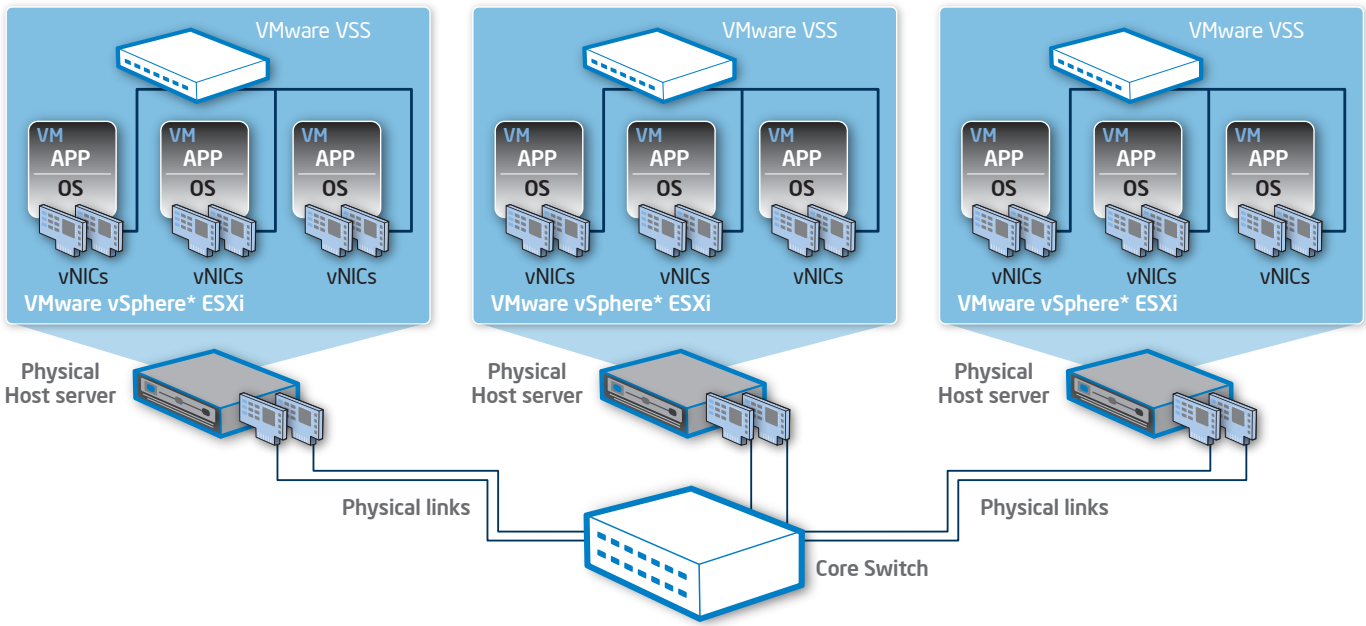


Figure 2. In a virtual network based on VMware vSphere Standard Switches (VSSs), the limitations of physical networking constrain the communication between virtual machines (VMs) on different hosts.

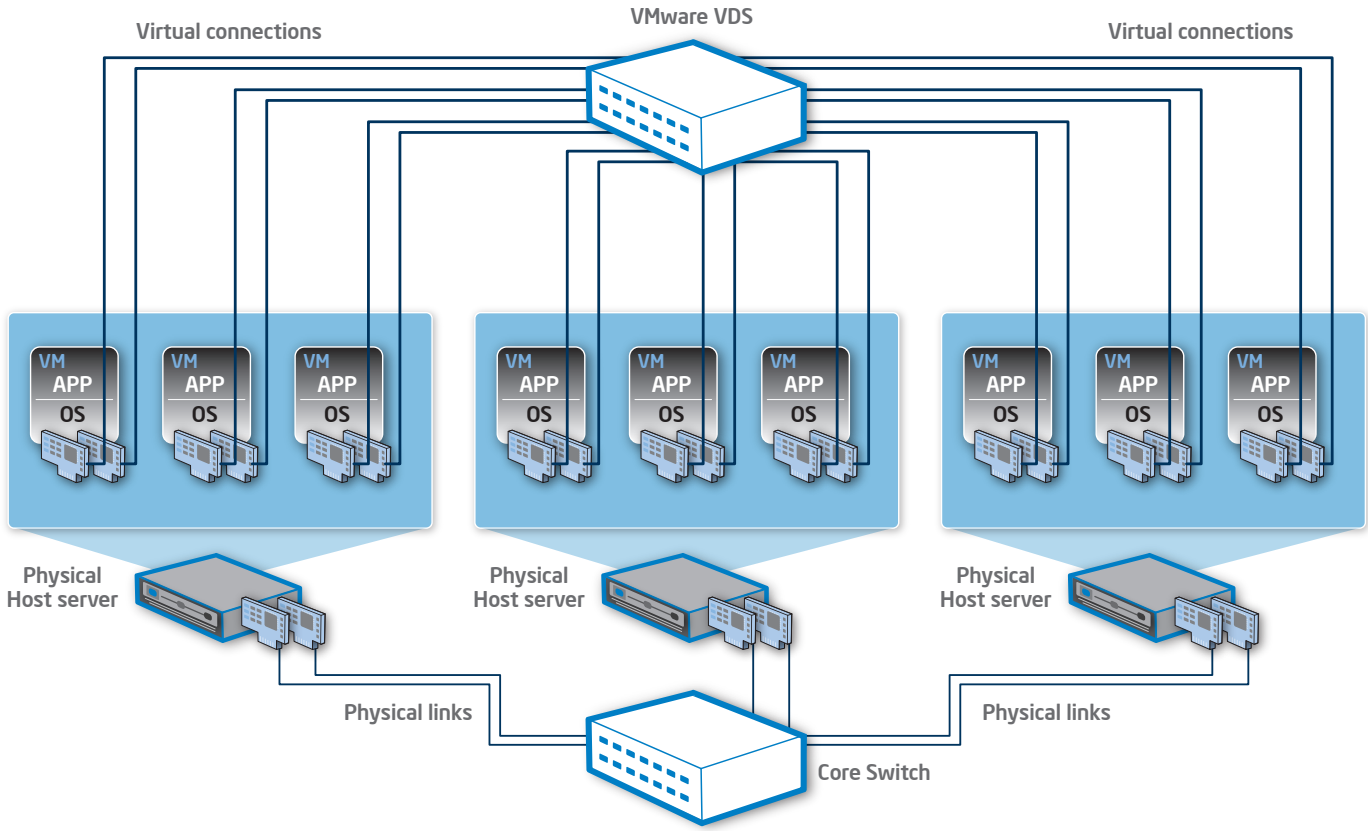


Figure 3. A VMware vSphere distributed switch (VDS) links virtual machine (VMs) on as many as 500 different hosts within the VMware vSphere* environment using virtual connections.

3 Multiple Approaches to Virtualized I/O Resource Sharing

The computing industry continues to develop technologies and approaches to enhance performance, maximize server consolidation, and work toward allowing virtualization of all workload types. A key requirement for expanded virtualization is the effective allocation and sharing of I/O resources; three primary models have emerged for doing so.

- **Software-based sharing** typically emulates physical I/O resources using software, translating requests so the software representation looks to the guest as if it were the actual physical resource. This approach requires the processor to handle the network traffic routing and management, with the possible result of increasing latency, reducing bandwidth, and limiting VM performance and scalability.
- **Hardware-assisted sharing** allows the hypervisor to offload part of the traffic-management function to the network controller, reducing the burden on the virtual switch. In this approach, VMware NetQueue*—enabled by Virtual Machine Device Queues (VMDq), a component of Intel® Virtualization Technology for Connectivity—can significantly enhance the performance of the virtual switch, in terms of reducing latency and increasing throughput. Benefits and limitations of hardware-assisted sharing include the following:

  - **Benefits**. Managing virtual environments with vSphere is well supported under this model, with near-native throughput across multiple 10GbE connections. VMDq functionality is exposed to the VMware software using an API that gives vSphere robust control over when to offload a specific process to the network controller and when to handle it in software.
  - **Limitations**. Because VMDq uses a software-based network path through the hypervisor, it may not be appropriate for some workloads that require particularly low latency and high throughput, especially with small packet sizes. Examples include databases, back-end virtual desktop infrastructure, firewalls, and load balancers.

- **Hypervisor-bypass hardware offload** using VMware DirectPath* I/O allows a VM to be directly assigned to a dedicated network port, bypassing the virtual switch completely. Using the PCI-SIG Single-Root I/O Virtualization (SR-IOV) specification—newly supported in vSphere 5.1—now allows a single network port to look like multiple entities known as "virtual functions" (VFs), each of which appears as a separate adapter that can be directly assigned to the VMs. This new capability greatly increases the usefulness of direct assignment by allowing multiple VMs to bypass the hypervisor using a single port. Careful consideration must always be given whenever hardware offloads are under consideration, because they often also bypass many valuable features to achieve their performance benefits. Here are some of the benefits and limitations that need to be considered:
  - **Benefits**. SR-IOV can significantly reduce latency and increase throughout beyond what is possible using hardware-assisted sharing with VMDq. Those enhancements make it possible to virtualize workloads where it would otherwise not be feasible.
  - **Limitations**. SR-IOV uses virtual functions that appear to the hypervisor as unique PCIe* devices (rather than network uplinks), so the virtual switch cannot dynamically allocate shared resources. Further, SR-IOV must be enabled or not enabled at the level of a whole physical port, disallowing the hypervisor and other tools from controlling resources on that entire port. See the VMware vSphere 5.1 Network Configuration documentation for a list of further limitations.

Both 10 Gigabit Intel Ethernet Converged Network Adapters and vSphere 5.1 support network resource sharing with both VMDq and SR-IOV. Since the VMware VDS can dynamically allocate resources with VMDq but not SR-IOV, it is the recommended default choice for network I/O resource sharing. At the same time, VMware DirectPath with SR-IOV enables virtualization of workloads that could not otherwise be virtualized, making it a valuable special-case technology where it is needed.

4 Software Entities at the Heart of the Virtualized Network

vSphere supports a set of virtual networking elements that provide capabilities for networking VMs in the data center similar to how physical machines are networked in a physical environment. Because these elements are abstracted away from the physical plane, they tend to decouple workloads from specific physical resources, providing for dynamic assignment of those resources. The resulting increased efficiency is at the heart of resource elasticity in the data center, as well as for the cloud.

This section introduces key software entities in vSphere networking, including a description, where appropriate, of how they differ between environments based on VSSs and those based on VDSs.

4.1 Virtual Network Interface Cards (Virtual NICs)

Each VM has one or more virtual NICs. The guest OS and application programs communicate with virtual NICs through either a commonly available device driver or a VMware device driver optimized for the virtual environment. In either case, communication by the guest OS occurs just as it would with a physical device. Outside the VM, the virtual NIC has its own MAC address and one or more IP addresses. It responds to the standard Ethernet protocol just as a physical NIC would, and from the perspective of an outside agent, communicating with a virtual NIC is identical to communicating with a physical one. Network redundancy for these virtual NICs typically is provided for at the port group level on the virtual switch, but since SR-IOV bypasses the virtual switch, redundancy is configured in the guest. This is accomplished by using teaming software in the guest OS between two VFs from two different physical ports.

4.2 Port Groups and Distributed Port Groups

Port groups in a VSS specify port configuration for each member virtual port. A VM (using its virtual NIC) connects to the virtual ports that are part of the given port group. VMs that connect to the same port group belong to the same network inside the virtual environment, allowing them to exchange data. Administrators can configure port groups to enforce policies that provide enhanced security, network segmentation, better performance, HA, and traffic management.

The corresponding entity on a VDS is the distributed port group, which spans multiple hosts and defines how connections are made through the VDS to the network. Each VDS supports up to 10,000 static port groups. Configuration settings such as Virtual LAN (VLAN) IDs, traffic shaping parameters, teaming and load balancing configuration, and port security are configured through distributed port groups, ensuring configuration consistency for VMs and virtual ports necessary for such functions as live migration using vMotion. The port group construct provides the flexibility and agility that is the foundation for a software-defined network. For more information on VDSs, refer to the VMware vSphere Distributed Switch Best Practices.

4.3 VLANs and Private VLANs

A VLAN enables a software-defined means of logically segmenting a network, similar to using different network cables to attach to a physical switch. That is, VMs or physical hosts assigned to separate VLANs can use shared network connections and other resources while being restricted from communicating with one another. Typically each VLAN is assigned a separate IP subnet on the overall network. Much as with separate physical LANs, passing traffic between VLANs must be accomplished through a routing device.

VDSs also provide the capability to use private VLANs, which extend VLAN technology by providing the ability to restrict communication between VMs on the same VLAN. This capability can simplify network designs by reducing the number of VLANs (and therefore subnets) that are required to segment or isolate traffic. For more information regarding security-related use of VLANs, refer to the "vSphere 5.0 Security Hardening Guide."

Another aspect of VLANs is a Virtual eXtensible Local Area Network (VXLAN), which is used to address the need for overlay networks within virtualized data centers accommodating multiple tenants. The scheme and the related protocols can be used in cloud service provider and enterprise data center networks. This technology runs over the existing networking infrastructure and provides a means to "stretch" a Layer 2 network. In short, VXLAN is a Layer 2 overlay scheme over a Layer 3 network. This feature is part of the VMware vCloud Director product, which extends vSphere deployments into the cloud.

5 Superior Traffic Management with VDS-based Networking

The use of VDSs enables the virtual network to be treated as a single aggregated resource, as opposed to the management of resources at only the per-host level with VSSs. Many of the concepts associated with configuring VSSs also apply to configuring VDSs.

On one side of the VSS are one or more port groups that connect to VMs, as shown in Figure 4. On the other side are virtual uplink connections to physical Ethernet server adapters that allow the VMs to connect to the physical environment. A virtual switch can connect its uplinks to more than one physical Ethernet adapter to enable NIC teaming. With NIC teaming, two or more physical adapters can be used to share the traffic load or failover capabilities if a physical adapter fails or a network outage occurs.

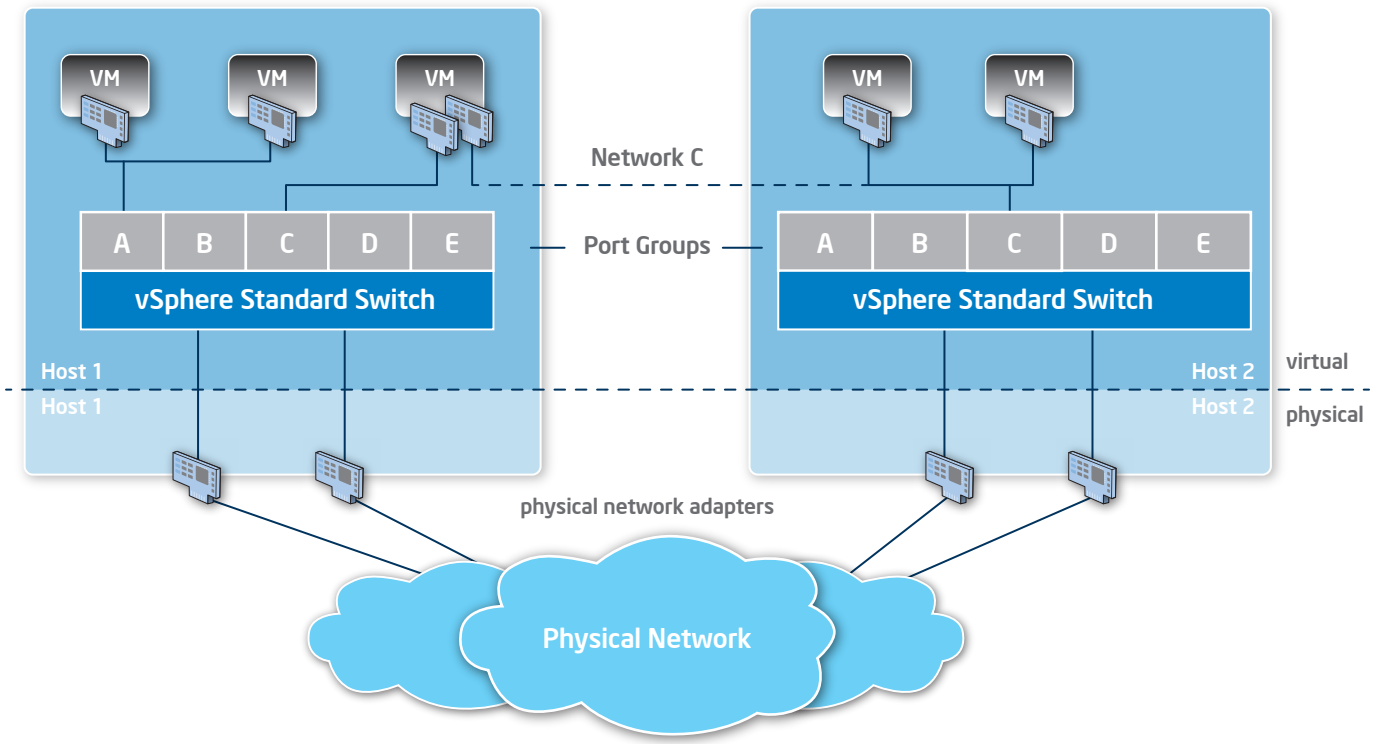


Figure 4. Virtual networking with VMware vSphere Standard Switches (VSSs): Both the virtual switch and port groups are specific to a single physical host.

Each port group is assigned a network label, which is specified when attaching a virtual NIC to a port group. All port groups in a data center that are able to pass data to one another are assigned the same network label, which allows functions such as vMotion or access to IP storage to occur within a port group, but not between multiple port groups. Port labels therefore enable interoperation while also enabling data isolation as needed.

The distributed port groups that VDSs use are similar in principle to the port groups used by VSSs, as shown in Figure 5. Distributed port groups aggregate multiple ports across physical hosts under a common configuration and provide a stable anchor point for VMs connecting to labeled networks.

The VMware virtual switching layer provides a set of features similar to those of traditional physical switches, including VLANs, traffic shaping, and monitoring. Traffic shaping is useful to limit the traffic to or from a VM (or a group of VMs), to prioritize a VM or other traffic in an oversubscribed network. Policies are defined by three characteristics: average bandwidth, peak bandwidth, and burst size.

The scope of traffic-shaping policies that can be configured in distributed port groups is a key area where the VDS improves on the corresponding capabilities for port groups with the VSS. Whereas the VSS supported policies for egress (VM to network) traffic shaping only, the VDS adds support for ingress (network to VM) traffic-shaping policies as well.

Network resource pools are used to configure the priority that different network traffic types are given on a VDS, by setting the physical adapter shares and limits parameters:

- **Physical adapter shares parameter** assigned to a network resource pool determines the share of the total available bandwidth guaranteed to the traffic associated with that network resource pool.
- **The limit parameter** of a network resource pool is the upper limit of bandwidth that the network resource pool can use.

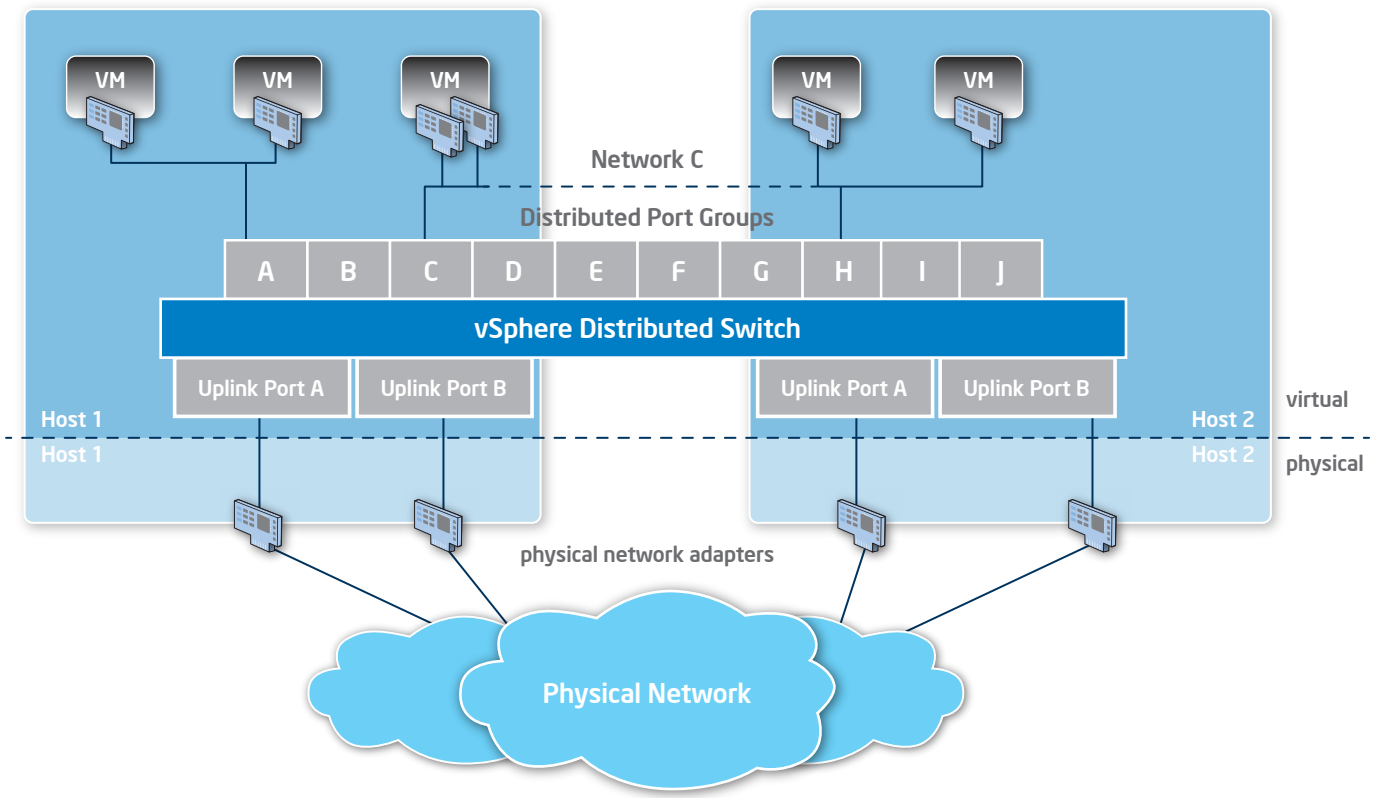


Figure 5. Virtual networking with a VMware vSphere distributed switch (VDS): Both the virtual switch and distributed port groups span multiple physical hosts.

5.1 Network Resource Management

When network resource management is enabled, VDS traffic is divided into the network resource pools shown in Table 1.

Network I/O Control – Quality-of-Service Traffic Types	
▪ VMware vMotion* traffic	▪ Virtual machine traffic
▪ Management traffic	▪ User-defined network resource pools
▪ NFS traffic	▪ VMware vSphere* replication traffic
▪ iSCSI traffic	▪ Fault-tolerant traffic

Note: The iSCSI traffic resource pool shares do not apply to iSCSI traffic on a dependent hardware iSCSI adapter.

The VDS (but not the VSS) supports vSphere Network I/O Control (NetIOC), which provides for the use of limits and shares parameters to control the allocation of shared physical network resources that are contended for by multiple traffic types on the same network pipe. NetIOC is a powerful feature that can make vSphere deployments even more suitable for I/O-consolidated data centers. The following best practices can help optimize the use of this feature:

- **Best practice 1: For bandwidth allocation, use shares instead of limits**, since the former has greater flexibility for unused capacity redistribution. Partitioning the available network bandwidth among different types of network traffic flows using limits has shortcomings. In other words, limits impose hard limits on the amount of the bandwidth usage by a traffic flow even when there is network bandwidth available.
- **Best practice 2: Consider imposing limits on a given resource pool** when you are concerned about physical switch or physical network capacity. Limiting the bandwidth usage of specific resource pools at the VMware ESX* host level can help prevent the possibility of jeopardizing performance for other flows going through the same points of contention.
- **Best practice 3: Set the corresponding resource-pool shares to the predefined default shares value for VMware FT**, because fault tolerance is a latency-sensitive traffic flow.
- **Best practice 4: Use Load-Based Teaming (LBT) as your VDS teaming policy while using NetIOC**, in order to maximize the networking capacity utilization.
- **Best practice 5: Use the DV Port Group and Traffic Shaper features offered by the VDS to maximum effect when configuring the VDS**. Configure each of the traffic flow types with a dedicated DV Port Group. Use DV Port Groups as a means to apply configuration policies to different traffic flow types, and more important, to provide additional Rx bandwidth controls through the use of Traffic Shaper. For instance, you might want to enable Traffic Shaper for the egress traffic on the DV Port Group used for vMotion. This can help in situations when multiple vMotion migrations initiated on different vSphere hosts converge to the same destination vSphere server.

5.2 Network Path Redundancy

Providing network path redundancy between cluster nodes is important, especially for vSphere HA reliability. A single management network constitutes a single point of failure and can result in failovers even though only the network has failed. Possible failures include NIC failures, network cable failures, network cable removal, and switch resets. Network architects must consider these possible sources of failure between hosts and try to minimize them, typically by providing network redundancy.

Network redundancy can be implemented at the NIC level with NIC teaming or at the management network level. In most implementations, NIC teaming provides sufficient redundancy; management network redundancy is a valuable option in cases where additional redundancy is desirable. Best practices call for configuring the fewest possible hardware segments between the servers in a cluster, to limit single points of failure and packet delays caused by excessive numbers of hops.

- **Network redundancy using NIC teaming**. Using a team of two NICs connected to separate physical switches improves the reliability of a management network. Because servers connected through two NICs (and through separate switches) have two independent paths for sending and receiving heartbeats, the cluster is more resilient. To configure a NIC team for the management network, configure the vNICs in vSwitch configuration for Active or Standby configuration.

- **Enabling or disabling LACP on an uplink port group**. Link Aggregation Control Protocol (LACP) on a vSphere distributed switch provides a method to control the bundling of several physical ports together to form a single logical channel. LACP on a vSphere distributed switch allows network devices to negotiate automatic bundling of links by sending LACP packets to a peer. LACP sends frames down all links that have the protocol enabled. If it finds a device on the other end of the link that is also LACP enabled, it independently sends frames along the same links, enabling the two units to mutually detect multiple links and then combine them into a single logical link. Note that the preferred method used to provide redundancy for iSCSI traffic is to use multiple paths (MPIO), which is not supported on LACP-enabled uplinks. Likewise, FCoE connections also need special configurations if LACP is used. See the VMware vSphere 5.1 Storage Configuration documentation for more details.

6 Management and Security for Virtual Networks and the Cloud

Software tools from VMware are vital to the transition in mindset away from physical segmenting and static bandwidth allocation, to distributed switching and dynamic bandwidth re-allocation. Utilizing automated resource management in both the data center and the cloud lets the network tune resource usage as needed, in real time, with security deeply intertwined with the architecture's approach to administration. Key management tools that are either incorporated into vSphere or designed explicitly for ease of integration with it are described below.

6.1 Network Management: VMware vCenter Server

As the central management console for the vSphere environment, VMware vCenter Server provides both operational control and proactive management of all virtual and physical resources, including VMs, physical hosts, and virtual switches. VMware vCenter Server automates the robust dynamic network-resource allocation described in this paper, eliminating the guesswork and inefficiency associated with static assignments of bandwidth.

6.2 Health Check

VMware vSphere 5.1 Health Check helps identify configuration errors in distributed switches, including mismatched VLAN trunks between a distributed switch and physical switch; mismatched Maximum Transmission Unit (MTU) settings between physical network adapters, distributed switches, and physical switch ports; and mismatched virtual teaming policies for the physical switch port channel settings. Health Check monitors the following:

- **VLAN**. Checks whether the physical access switch port VLAN trunk configuration matches the distributed switch distributed port group VLAN range setting.
- **MTU.** Checks whether the physical access switch port MTU jumbo frame settings per VLAN matches the distributed switch MTU setting.
- **Teaming policies**. Checks whether the physical access switch ports' EtherChannel setting matches the distributed switch distributed port group IPHash teaming policy settings.

6.3 Network Rollback and Recovery

vSphere network rollback can help prevent accidental misconfiguration of management networking and loss of connectivity to the host by rolling back to a previous valid configuration. In vSphere 5.1, rollback is enabled by default. However, you can enable or disable rollbacks at the vCenter Server level. Several networking events can trigger a rollback, including the following:

- **Host networking rollbacks** occur when an invalid change is made to the host networking configuration. Every network change that disconnects a host also triggers a rollback.
- **Distributed switch rollbacks** occur when invalid updates are made to distributed switch-related objects, such as distributed switches, distributed port groups, or distributed ports.

If an invalid configuration for any of the changes occurs, one or more hosts will be disconnected from the vCenter server. The recovery option in vSphere 5.1 allows administrators to connect directly to a host and fix distributed switch properties or other networking misconfigurations using the DCUI. The rollback and recovery features provide the required reliability to the vSphere Distributed Switch to avoid management network configuration issues.

The ESXi core dump client, Dump Collector, sends VMkernel core contents to a network server when the system encounters a critical failure.

ESXi 5.1 Dump Collector supports both vSphere standard and distributed switches, as well as Cisco Nexus* 1000 series switches. Dump Collector can mark 802.1pq tags on dump packets when configured to do so. Dump Collector can also use any available uplink when the port group the collector is configured on is connected to a team.

7 Conclusion

Using the capabilities of vSphere 5.1 Enterprise Plus and related tools, network architects can enable dynamic allocation of network resources, providing excellent support for enterprise requirements in the areas of performance, HA, and QoS. The VDS extends management of virtualized resources using VMware vCenter Server to include VMs on many physical hosts in a single pool. That dynamic resource management at the data center level represents a significant advance over static bandwidth allocation between hosts, an obsolete holdover from pre-virtualization networking with 1GbE.

The hypervisor assist provide by VMDq is the network-resource sharing technology of choice for most virtualized workloads. It provides the virtualization software the ability to control dynamic resource allocation, as well as security and management functionality that enable robust virtual networking. SR-IOV extends the scope of virtualization to include workloads that require ultra-low latency and high throughput, especially with small packet sizes. That added flexibility enables a virtualized environment that primarily uses VMDq but which also uses SR-IOV for select special cases. The combination delivers optimal results for the broadest range of network applications, managed by vSphere's advanced tools and capabilities.

For more information on optimizing virtualized networks with VMware and Intel technologies, visit

www.vmwareintelalliance.com

Solution provided by:

vmware® | intel®

[1] www.intel.com/content/dam/www/public/us/en/documents/white-papers/virtualization-ethernet-adapters-rethinking-server-connectivity-brief.pdf.

1112/BJ/MESH/PDF 327784-001US

intel®