Enabling VMware ESX Server VLAN Network Configurations

for the Dell PowerEdge 1855 Blade Server

When used in conjunction with virtual LAN (VLAN) technology, server virtualization software can help build virtual infrastructures to support the scalable enterprise. In particular, VMware® ESX Server™ software, modular Dell™ PowerEdge™ 1855 blade servers, and Dell PowerConnect™ 5316M switches can be used along with VLAN configurations to create complex network infrastructures in virtualized data centers.

BY BALASUBRAMANIAN CHANDRASEKARAN, KYON HOLMAN, CUONG T. NGUYEN, AND SCOTT STANFORD

Related Categories:

Blade servers

Data networking

Dell PowerEdge blade servers

Internetworking

Network fabric

Virtualization

VMware

Visit www.dell.com/powersolutions for the complete category index.

Virtualization allows for the creation of multiple virtual machines (VMs) that can run simultaneously on a single physical server. These VMs can communicate among each other and with other physical systems through virtual switches. Virtual switches are software entities that provide the functionality of a physical Ethernet switch. Coupled with virtual LAN (VLAN) technology, virtualization can be effectively used to set up complex network infrastructures for test, development, and production environments. For example, VLANs can provide traffic isolation channels and enhanced network security models for physical server hosts and the VMs running on them.

To show how VLANs can improve security and traffic isolation, engineers from the Dell PowerConnect Networking and Scalable Enterprise Development teams have developed best-practices methodologies for deploying VLANs and designed four network deployment models for VLAN architecture based on Dell PowerEdge 1855 servers, Dell PowerConnect 5316M switches, and VMware ESX Server 2.5 software. IT administrators and systems engineers can use these best practices and models to implement and support a secure, scalable virtualized network infrastructure.

Configuring the Dell PowerEdge 1855 for VMware ESX Server

VMware ESX Server software includes the VMotion™ feature, which allows for live migration of a VM from one physical server to another. VMotion copies the memory state of a VM from the source physical server to the destination server through the network fabric. The virtual disk is stored in a Fibre Channel storage device, which is shared between the two physical servers.

The Dell PowerEdge 1855 blade server can hold up to 10 server blades within its chassis, which is called the Dell Modular Server Enclosure. To enable VMotion in a blade environment using Fibre Channel storage area network (SAN) connectivity, a Fibre Channel daughtercard must be used in the server blade. Because the PCI daughtercard slot is used for Fibre Channel connectivity, this leaves room for only two network interface cards (NICs) per server blade. The two NICs are exposed to a server blade through the midplane interconnect. In an optimal ESX Server environment, four NICs are required: one for management, one for VMotion, and two teamed together for redundant connectivity for VMs. Management is enabled through the VMware service console, which is a Linux®-based environment running an Apache Web server. The configurations described in this article assume only two NICs are used for the VMware ESX Server environment.

The following sections describe the advantages of using VLAN configurations in combination with the Dell PowerConnect 5316M switch—which is the network I/O module in the Dell Modular Server Enclosure—to support an optimal VMware ESX Server environment that enables highly available and secure network traffic. Four configurations that leverage the Dell PowerEdge 1855 and PowerConnect 5316M switch infrastructure are provided as well instructions on how to set up the ESX Server environment and the advantages of each configuration.

Exploring key concepts and advantages of VLANs

Current-generation blade servers provide a unique challenge because of the limited network ports available when compared to non-blade servers. Each server blade in the PowerEdge 1855 comes with two embedded Gigabit Ethernet[1] NICs, which are referred to as NIC 0 and NIC 1. For VMware ESX Server 2.5.1 software, the NICs must be either dedicated to the VMware service console, dedicated to the VMs, or shared between the service console and the VMs. In a default installation, NIC 0 is dedicated to the service console and NIC 1 is dedicated to the VMs.

To better utilize the network bandwidth and to provide redundancy, the NICs can be configured in one of the four configurations described in Figure 1: default, segregated traffic, dedicated VMotion network, and redundant. When added to an ESX Server environment, a VLAN can help improve traffic isolation and thereby the security of each of these configurations.[2] However, adding a VLAN may introduce some complexity to the initial setup stage. In addition, PowerEdge 1855 and ESX Server infrastructure maintenance tasks must be modified to include the additional VLAN layers. Still, these potential disadvantages are significantly offset by the benefits of increased security and traffic isolation, especially when VMotion or the service console shares a physical NIC with production VM traffic.

Additional important VLAN concepts include the following:

- Ethernet traffic sent on one VLAN will not be forwarded to another VLAN in a Layer 2 Ethernet switch. In addition, broadcast traffic will be sent only within the same VLAN.
- VLAN membership can be defined in the switch by associating specific network and virtual switch ports to a given VLAN. This means that only the ports associated with the VLAN may communicate with each other. Also, broadcast messages sent to any of these ports for a given VLAN can only be sent to other ports belonging to the same VLAN.
- A port may belong to different VLANs at the same time. In this case, the packet sent to the port must identify the VLAN to which it belongs. If the packet sent does not identify its VLAN, the switch will automatically associate the port to a default VLAN as configured in the port.
- VLAN configuration allows traffic to be groomed in the inbound direction and for nonconforming traffic to be automatically dropped.
- A VLAN does not necessarily guarantee quality of service (QoS). For example, if two VLANs share the same port, they will not split the network bandwidth between them. Thus, in heavily oversubscribed switch configurations, network traffic on one VLAN can potentially cause congestion of network traffic in the other VLAN.
- QoS parameters may be configured on the switch to select specific traffic types and provide priority to the traffic type (such as VM traffic versus VMotion traffic). The QoS setup is beyond the scope of this article.

If VLAN configurations are used, then once a particular configuration is selected, this same configuration choice must be applied to all the server blades in a chassis. As shown in Figure 1, for example, if the default configuration is selected (in which the service console uses NIC 0 and NIC 1 is reserved for the VMs and VMotion), then this configuration must also be used for all the other server blades. This restriction will simplify VLAN configuration in Ethernet switches. It is possible to circumvent this restriction, but the complexity of the configuration in that case is beyond the scope of this article.

Key points to consider for all four configurations shown in Figure 1 include:

- VMware management traffic from the service console is encrypted by default.
- VMotion traffic is not encrypted. To help ensure effective and secure VMotion events, best practices recommend configuring the VMotion NIC on a separate VLAN or using a separate physical NIC for VMotion.
- The service console does not generate only VMware management traffic. Systems management software suites, such as Dell OpenManage™ software, are also installed on the service console. In addition, baseboard management console (BMC) traffic, Simple Network Management Protocol (SNMP) traffic, and backup traffic use the same NIC as the service console.
- The three non-default configurations require sharing NIC 0 between the service console and the VMs, which requires administrators to perform additional steps during installation.

[1] This term does not connote an actual operating speed of 1 Gbps. For high-speed transmission, connection to a Gigabit Ethernet server and network infrastructure is required.

[2] For more information about the use of VLANs, see the *Dell PowerConnect 5316M Ethernet Switch Module User's Guide* at support.dell.com/support/edocs/network/PC5316M/en/UG/index.htm.

Configuration type	Use of NIC 0	Use of NIC 1	Fault tolerance for VMs	Installation type	Traffic isolation	VM performance	Security (VLAN)
Default	Service console	VMs and VMotion	No	Standard	Moderate	Acceptable if VMotion events are infrequent	**Moderate:** VMotion runs on a production network; adding a VLAN helps improve security and isolation of VMotion traffic
Segregated traffic	Service console and VMotion (shared)	VMs	No	Command-line post-installation steps	Good	Acceptable if management traffic is infrequent	**Good:** The service console runs on a private network; adding a VLAN helps improve isolation of traffic between VMotion and the service console
Dedicated VMotion network	Service console and VMs (shared)	VMotion	No	Command-line post-installation steps	Moderate	Acceptable if management traffic is infrequent and VMotion events are frequent	**Moderate:** The service console runs on a production network; adding a VLAN helps improve security and isolation of the service console traffic
Redundant NIC	NIC 0 shared between the service console and the VMs; NIC 0 and NIC 1 teamed and used by the VMs and VMotion		Yes	Command-line post-installation steps	Moderate and flexible	Acceptable if VMotion events are infrequent	**Poor:** VMotion and the service console run on a production network; adding VLAN helps improve security and isolation of the service console and VMotion traffic

Figure 1. NIC and VLAN configurations for Dell PowerEdge 1855 blade servers

Using the default VLAN configuration

In the default configuration, NIC 0 is dedicated to the service console for management traffic and NIC 1 is used for VMotion and traffic. No special steps are required to enable this configuration—it is part of the default installation of VMware ESX Server. This configuration provides network isolation by separating the management network from the VM network.

A VLAN can help address the problem of securing VMotion traffic by creating a separate virtual network for VMotion. Figure 2 shows the default configuration with a VLAN enabled. ESX Server allows administrators to create virtual switches, which are connected to the VMs for networking and also can be configured for VMotion. These virtual switches support the VLAN.

Enabling the default configuration

The following steps can be used to secure VMotion traffic through VLANs:

1. **Set up virtual switches in the ESX Server software to provide VLAN tags for all VM traffic.** Administrators can define the same VLAN tag for all VMs to share or specify a VLAN tag for each VM or for any group of VMs. The decision for assigning specific VLAN tags to the VMs depends on whether the VMs need to communicate with each other. If only a few VMs need to communicate with each other, administrators should group those VMs together and configure the switch to tag all traffic from those VMs with the same VLAN ID. Allowing the switch to tag the traffic can help improve ESX Server performance by offloading VLAN tag and packet inspection and routing processing tasks to the Dell PowerConnect 5316M application-specific integrated circuit (ASIC).
2. **Set up a VLAN on the PowerConnect 5316M switch connected to NIC 1.** This switch is represented as "Switch 1" in Figure 2. All the internal ports connected to the server blades are configured with the VLAN for VMotion (shown as VLAN ID = A in the figure). The PowerConnect switch connected to the service console NIC ("NIC 0")—represented as "Switch 0" in Figure 2—is left unconfigured.
3. **Assign one external port on Switch 1 to be a member of VLAN A.** Administrators should make sure this external port's permanent VLAN ID (PVID) is set to 4095, which will cause all untagged traffic to be discarded. Alternatively, if the external system does not support VLANs, then untagged traffic could be allowed into this port and the switch could automatically tag the traffic for VMotion. This option is slightly less secure but easier to manage than the first option of discarding all untagged traffic. The external port should be used only for transmitting and receiving VMotion traffic. This configuration means that VMotion traffic coming from an external source to the server blade must go through this port.

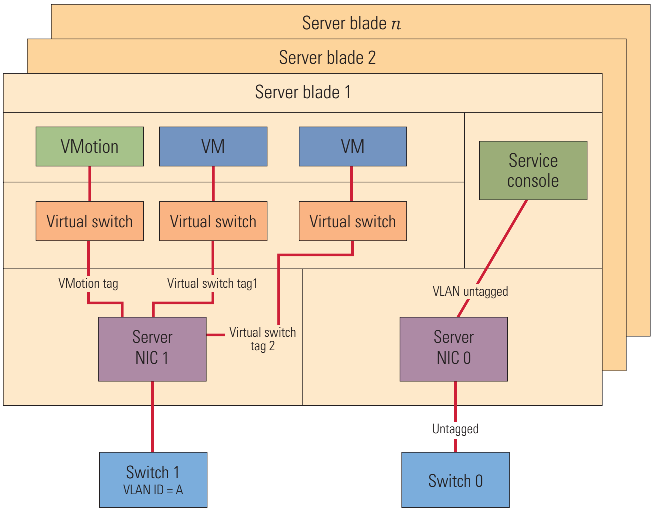

Figure 2. Default VLAN architecture using ESX Server virtual switches and physical Dell PowerConnect 5316M switches

4. **Configure the remaining external ports on Switch 1 to be specific members of the VM VLANs, if desired.** By assigning ports to specific VM VLANs, administrators can help isolate traffic from various VMs.

Note: For VMotion to function properly, the switch names should be identical across all blade servers.

For the three non-default VLAN configurations, the following sections provide a general overview of the advantages provided by each configuration. For detailed setup and configuration steps for these VLAN configurations, see the supplemental online section of this article at www.dell.com/powersolutions.

Implementing a segregated traffic configuration

In the segregated traffic configuration, the service console resides on a private network. Adding VLANs can help improve isolation of VMotion traffic and service console traffic. This configuration can help prevent a loss of management capabilities for the ESX Server host and provide a moderate level of virtual and physical switch port isolation for VMs that reside on VMotion-enabled ESX Server hosts running on a PowerEdge 1855 blade server.

Implementing a dedicated VMotion network configuration

In contrast to the segregated traffic configuration, the service console resides on a production network in the dedicated VMotion network configuration. Adding VLANs can help improve security by isolating service console traffic while also supporting an dedicated VMotion environment. For deployments of ESX Server 2.x software on PowerEdge 1855 blade servers, which require a high degree of management and VMotion security and isolation, this configuration provides systems engineers and VMware administrators with options to enable a granular level of logical and physical distinction between management and VM-related traffic.

Implementing a redundant NIC configuration

Building upon the segregated traffic and dedicated VMotion network configurations, the redundant NIC configuration provides an infrastructure for production environments that require even higher levels of network redundancy that achievable with the other VLAN configurations. Because the VMotion and service console networks reside on a production network in this configuration, adding VLANs can help improve security and isolation of service console and VMotion traffic. This configuration is well suited for environments that require high availability at the VM and physical network infrastructure layers.

Enabling fault tolerance using PowerConnect 5316M switch modules

To enable NIC failover when using PowerConnect 5316M switches in the redundant NIC configuration, administrators can select the advanced configuration in the Options tab of the ESX Server Management User Interface and change the `Net.ZeroSpeedLinkDown` parameter value to 1.

Examining the impact of VMotion events on VM production traffic

In some of the configurations described in this article, particularly the default configuration, VMotion traffic shares a NIC with VM production traffic. To learn more about the impact of VMotion events on VM production traffic when network resources are shared, see the Dell white paper "VMware VMotion Performance on the Dell PowerEdge 1855 Blade Server" in the Dell/VMware Resource Center at www.dell.com/vmware.

Following Dell best practices in virtual infrastructures

The Dell best practices and deployment models introduced in this article are designed to help enterprise IT organizations determine the appropriate network configurations and requirements for VMware ESX Server 2.x environments on Dell PowerEdge 1855 blade servers. The four VLAN configurations presented in this article can be implemented to meet various VM, VMotion, and service console management scenarios. Systems engineers, enterprise architects, and VMware administrators can employ these best practices and deployment models as resources and guides to help them build a scalable, flexible virtual network infrastructure.

Balasubramanian Chandrasekaran is a systems engineer in the Scalable Enterprise Computing Lab at Dell. His research interests include virtualization of data centers, high-speed interconnects, and high-performance computing. Balasubramanian has an M.S. in Computer Science from The Ohio State University.

Kyon Holman is a lead software engineer on the tape storage team in the Dell Enterprise Product Group. He has a B.S. in Computer Science from the University of Michigan at Ann Arbor and an M.S. in Software Engineering from The University of Texas at Austin, and he is pursuing an Executive M.B.A. from The University of Texas at Austin.

Cuong T. Nguyen is a systems engineer on the Dell PowerConnect Ethernet switch team. His expertise is in network management systems, and he has more than 15 years of networking and telecommunications industry experience. Cuong has a B.S. in Computer Information Science from the University of California at Irvine.

Scott Stanford is a systems engineer in the Scalable Enterprise Computing team within the Dell Solutions Engineering Group. His current focus is on performance characterization and sizing for virtualized solutions. He has a B.S. from Texas A&M University and an M.S. in Community and Regional Planning from The University of Texas at Austin, and he is pursuing an M.S. in Computer Information Systems at St. Edward's University.