Network Implications of Server Virtualization in the Data Center

Abstract

Server virtualization solutions such as VMware® Infrastructure are increasingly being deployed because of their effectiveness in addressing current challenges related to the cost and operation of the server environment in the data center. VMware addresses these challenges by running multiple virtual machines on a single physical server, thus increasing utilization and simplifying operations, which reduces both operating expenses (OpEx) and capital expenditures (CapEx). However, widespread deployment of virtual machines can stress data center infrastructure designed to support the traditional server model, where one application runs on one physical server. Cisco Catalyst® switches and Cisco® MDS 9000 family storage area network (SAN) switches address these new design requirements and support functions that deliver predictable application performance, security, segmentation, and availability for dense virtual machine environments.

Introduction

Server virtualization and the use of virtual machines is profoundly changing data center dynamics. Most organizations are struggling with the cost and complexity of hosting multiple physical servers in their data centers. The expansion of the data center, a result of both scale-out server architectures and traditional “one application, one server” sprawl, has created problems in housing, powering, and cooling large numbers of underutilized servers. In addition, IT organizations continue to deal with the traditional cost and operational challenges of matching server resources to organizational needs that seem fickle and ever changing.

Virtual machines can significantly mitigate many of these challenges by enabling multiple application and operating system environments to be hosted on a single physical server while maintaining complete isolation between the guest operating systems and their respective applications. Hence, server virtualization facilitates server consolidation by enabling organizations to exchange a number of underutilized servers for a single highly utilized server running multiple virtual machines.

By consolidating multiple physical servers, organizations can gain several benefits:

- Underutilized servers can be retired or redeployed.
- Rack space can be reclaimed.
- Power and cooling loads can be reduced.
- New virtual servers can be rapidly deployed.
- CapEx (higher utilization means fewer servers need to be purchased) and OpEx (few servers means a simpler environment and lower maintenance costs) can be reduced.

Because of these compelling financial and operational benefits, the vast majority of organizations are either piloting virtual machines or have production applications running in virtual machine environments. Because of the compelling value proposition of virtual machines, some organizations are now making virtual machines their default operating environment.

Effects on the Data Center

The adoption (or readoption) of data center virtualization in general, and virtual machine server technology in particular, has significant implications for data center networking and represents a change in data center architecture and design. Traditionally, data center networks were designed around three premises:

- A server has a single identity: one MAC address, one IP address, and one World Wide Name (WWN)
- Each application needs its own server.
- Segmentation required for regulatory, security, or political reasons is accomplished through physical separation: that is, dedicated hardware.

By design, virtualization, and the deployment of virtual machines, eschews these principles, because over time they have given rise to the complexity, cost, and flexibility challenges noted earlier. Virtual machines have the potential to address these challenges while maintaining the functional separation needed for sound business practices.

As organizations deploy IT strategies based on wide-scale server consolidation and virtualization, it is essential that they revisit both their data center network design and the capability of their underlying products to support that strategy. Today, organizations are typically consolidating servers on virtual machines at a ratio of from 4:1 (four virtual machines on one physical server) to 8:1. As organizations become more familiar with the technology and develop operational expertise, this ratio is expected to quickly grow to from 10:1 to 20:1. With the advent of multicore CPUs, virtual machine densities are expected to approach 50:1 within 2 years.

IT architects, planners, and operations need to understand how virtual machine deployment affects the Layer 2 and SAN fabrics in the data center. At current virtual machine density levels, many organizations may already be operating at nearly the maximum capacity afforded by their current data center architectures. As organizations strive to deliver higher virtual machine densities, steps must be taken ensure that the network and SAN fabrics support the top-level IT strategy. Minimally, organizations run the risk of not being able to fully realize their server virtualization vision; more important, organizations run the risk of compromising security, regulatory compliance, and application availability.

This remainder of this document discusses the architecture of the market-leading VMware ESX Server virtualization solution and how it affects the data center network. This document also discusses best-practice deployment guidelines that describe how Cisco data center switching platforms such as the Cisco Catalyst 6500 Series Switches, Cisco Catalyst 4948 Switch, and Cisco MDS 9000 family uniquely address the performance, security, and availability demands of dense virtual machine environments.

VMware ESX Primer

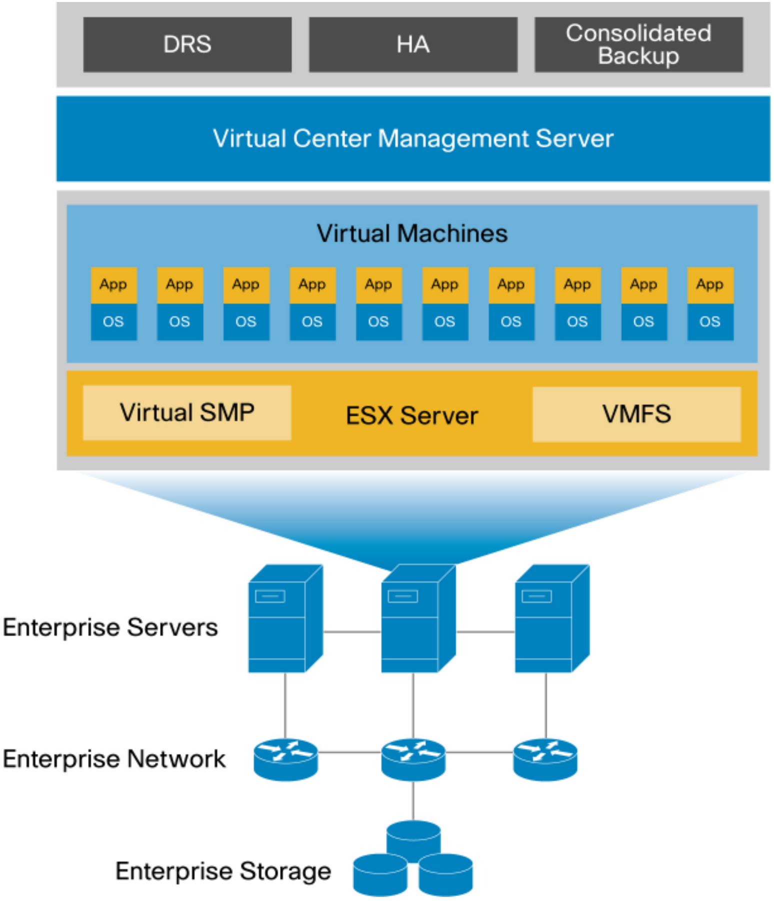
VMware ESX Server is a host operating system dedicated to the support of virtual servers or virtual machines. The ESX host system kernel (vmkernel) controls access to the physical resources of the server shared by the virtual machines. The ESX host system helps ensure that the following four primary hardware resources are available to guest virtual machines:

- Memory
- Processors
- Storage (local or remote)
- Network adapters

The ESX host virtualizes this physical hardware and presents it to the individual virtual machines and their associated operating system for use, a technique commonly referred to as full virtualization. A hypervisor achieves full virtualization by allowing virtual machines to be unaware and indifferent to the underlying physical hardware of the ESX Server platform. A standard virtual hardware is presented to all virtual machines. The vmkernel is a hypervisor whose primary function is to schedule and manage virtual machine access to the physical resources of the ESX server. This task is fundamental to the reliability and performance of the ESX virtualized machines. The ESX vmkernel creates this virtualization layer and provides the virtual machine containers where traditional operating systems such as Windows and Linux are installed.

VMware defines a virtual machine as a virtualized x86 PC environment on which a guest operating system and associated application software can run. This arrangement allows multiple virtual machines to operate concurrently on the same host machine, providing server consolidation benefits and optimization of server resources. CPU, disk, memory, and network connections (SAN and LAN) used by the virtual machine guest operating system are virtual devices (Figure 1).

Figure 1. VMware ESX Architecture



Effect of Virtual Machines on the LAN

Beyond providing an emulated hardware platform for virtual machines, ESX Server offers connectivity to the external physical enterprise network and other virtual machines local to the host. The following ESX networking components provide this internal and external access:

- Physical network interface cards (PNICs)
- Virtual machine network interface cards (VMNICs)
- Virtual switches

The ESX host links local virtual machines to each other and to the external enterprise network through a software construct called a virtual switch (vswitch). The vswitch emulates a traditional physical Ethernet network switch to the extent that it forwards frames at the data link layer. ESX Server may contain multiple vswitches, each providing more than 1000 internal virtual ports for virtual machine use. Each VMNIC assigned to the vswitch uses one internal virtual port, which implies that a significant number of virtual machines can be used per virtual switch.

The virtual switch connects to the enterprise network through outbound VMNIC adapters. A maximum of eight Gigabit Ethernet ports or ten 10/100 Ethernet ports can be used by the virtual switch for external connectivity. The vswitch is capable of binding multiple VMNICs together, in a manner much like NIC teaming on a traditional server. This binding provides greater availability and bandwidth to the virtual machines using the vswitch. A public virtual switch employs outbound adapters, whereas a private vswitch does not, offering a completely virtualized network for virtual machines local to the ESX host. ESX internal networks are commonly referred to as VMnets.

Best-practice design, power and cooling load, and rack space typically limits server density within a data. Although blade servers tend to increase density within the data center, virtual machines have a far more profound effect as they can be created as required with little additional “cost”. A data center that hosts 2000 physical servers, could, as a result of implementing virtual machines at a 10:1 density, radically increase the demands on the network infrastructure. Mathematically, the worst-case load is 20,000 servers. In reality, the load would be less because some physical servers will be taken offline as part of consolidation, and not all applications can be moved to a virtual machine environment. On the other hand, the availability of virtual machines and available server cycles makes additional virtual machines more likely to be brought online. Regardless of the exact consolidation ratio, experience shows that the net server count increases. Additionally, because virtual machine creation is so easy, the rate of growth in the number of servers also increases in comparison to traditional models where procurement and provisioning requirements serve to limit the rate at which servers can be added to the data center.

Virtual machines increase the density of server identities, which places additional demands on the network fabric, especially when the dynamic creation and migration of virtual machines is considered. This stresses multiple network components in the following ways:

- Increased identity density: MAC and IP addresses and applications
- Increased control plane overhead because of increased service density
- Increased high-availability requirements because of increased risk exposure
- Increased services, such as firewalls and load balancers, which affects performance

The result is that both the growth and the rate of growth place stress on the data forwarding capacity of the network, including services modules, and also on the control-plane aspects of the network devices.

Fortunately, Cisco Catalyst switches support rich functions that enable very dense virtual machine environments to be successfully deployed.

Most switches can forward at line rate or near line rate on all ports, and forwarding performance generally is not a major concern. However, as the density of servers on a physical port increases through the implementation of virtual machines, the network’s original design parameters may become overwhelmed. Provisioning sufficient bandwidth to meet application service-level agreements (SLAs) is a primary consideration. Secondary factors such as network protocol and feature implementation, buffer architecture, and switch-control plane also are crucial.

For a simple example of these complex interactions, consider a subnet of 250 physical servers. With traditional server provisioning, this environment can be supported with very little challenge or complexity. However, if each server hosts four virtual machines, the low end of typical virtual machine density, 1,000 IP addresses are required, which may entail multiple IP subnet ranges on a single interface. If traffic flows between virtual machines on different IP subnets is required, the switch may need to support not just secondary addressing, but also hardware-assisted forwarding unless proxy Address Resolution Protocol (ARP) and subnet masks are widened on the hosts to facilitate direct communications.

Layer 2 Fabric Scalability and Integrity

Because consolidation and virtualization concentrates applications and their related business operations, they can significantly increase the business risk associated with a switch or data center domain failure. As noted earlier, migration to a dense virtual machine environment can stress a network in terms of both scale and volume of traffic. Thus, in dense virtual machine environments, the requirement to protect network switches from being overwhelmed by CPU-bound traffic, both legitimate and malicious, is a crucial design goal for maintaining application availability and deterministic performance.

In addition to a high-speed application-specific integrated circuit (ASIC) forwarding engine, all networking devices have a central CPU for processing control functions such as network control protocols (ARP, Spanning Tree Protocol, routing protocols, etc.), packets destined for the device (Simple Network Management Protocol [SNMP], Telnet, etc.), and nonhardware switchable packets such as those that have exceeded the maximum time to live (TTL) or those that have IP options set.

The increase in server density within a switched domain places stress not only on the forwarding and buffering performance of the switch, but also on the switch control plane. This additional stress is the result of the increased number of servers associated with the data center network and their increased volume of traffic.

As the density of servers increases, the number of MAC and IP addresses that need to be supported increases. If a data center network of 1000 servers is considered, this can easily mean 8000 to 10,000 MAC and IP addresses that need to be supported. Although from a forwarding perspective, this support can be achieved easily with modern data center switches, the volume of MAC addresses and control-plane-bound traffic can still be considerable.

Because virtual machines are highly mobile, the data center network mechanisms in place must support the mobility of associated Layer 2 services. The easiest way to do this is to limit virtual machine mobility to physical servers in the same VLAN. For most organizations, this is a reasonable and satisfactory approach to supporting VMotion while still maintaining the segmentation needed for regulatory compliance, security, etc.

From a design perspective, as VLANs are extended between switches within the data center network, Spanning Tree Protocol is required to help ensure that loops do not occur within the topology, and the switches must use MAC learning to determine where a particular MAC address is within the switched network. VMware ESX actively updates the Layer 2 forwarding databases of all switches on the LAN by sending Reverse ARP (RARP) whenever a VMotion event occurs. Under most circumstances, this self-learning behavior has a fairly low overhead. However, when a spanning-tree event occurs, self-learning can introduce unique challenges in the data center aggregation switches. When a topology change occurs within a spanning-tree-based network, the core MAC addresses are typically flushed to prevent stale forwarding information from causing traffic to not be routed. Although flushing resolves this problem, if the switch does not know through which port the destination MAC address is available, the switch will flood all traffic associated with that address until the destination-to-port association is relearned.

As most MAC-address-to-port associations are flushed during a spanning-tree event, the rate at which MAC addresses are relearned is a critical metric, especially in dense virtual machine environments. Because potentially high volumes of unicast traffic may be flooded, the effect on network links, buffers, vswitches, and application performance can be significant.

Because unknown destination unicast traffic is flooded on all forwarding links, the links may be overwhelmed and packets buffered at egress and ingress to the switch. To protect against control traffic being dropped, which would destabilize the network, Cisco Catalyst switches support dedicated network control packet buffers on a per-port basis. As the flooded unicast traffic is received at the virtual-machine-enabled servers, the vswitch needs to inspect traffic that in most cases will be dropped. This takes away from the applications both bandwidth and CPU cycles, which can cause unpredictable application response times and performance until the switch's MAC address table is repopulated.

Because practically, virtual machine mobility requires Layer 2 adjacency, the switch MAC address learning rate is a critical factor in dense virtual machine environments. For example, a data center module of 1000 servers with 8 virtual machines per server will have 8000 MAC addresses. If a LAN switch can learn only 1000 MAC addresses per second, then traffic may be flooded for up to 8 seconds until all MAC-to-port associations can be relearned.

Note: VMotion itself does not require Layer 2 adjacency. However, the virtual machine being migrated should be moved within the same VLAN, unless host routes are being generated to help ensure that user sessions are reestablished to the virtual machine.

It is fairly common to see MAC learning rates in the range of 1000 to 2000 MAC addresses per second for software-based MAC-learning switches. This rate protects the CPU from being overwhelmed with MAC learning, thereby preventing the switch from processing other critical functions such as spanning tree. For access or edge switches, this behavior is usually not a concern if the number of attached MAC addresses is fairly low. For example, if a 48-port Ethernet switch has 40 Gigabit Ethernet attached hosts, each with 8 virtual machines, the switch will need to learn 320 MAC addresses; this is a manageably low number, and the behavior of modern Spanning Tree Protocol is very efficient in not flushing MAC address tables.

Exposure is greater with aggregation switches that have many thousands of MAC address associations or with dense end-of-row access switch deployments: that is, greater than 1000 MAC addresses. In these cases, software-based MAC address learning can cause unpredictable application performance.

The Cisco Catalyst 6500 Series Switches are unique with respect to MAC address learning in that they use specialized hardware to populate MAC address table entries and can learn MAC addresses at wire rate. For example, testing has shown that the Cisco Catalyst 6500 Series can learn 10,000 unique MAC-to-port associations in 4 microseconds. This behavior enables the Cisco Catalyst 6500 Series to minimize unicast flooding during spanning tree events, helping ensure predictable application performance and response times and offloading processing from the switch CPU to help ensure device and network stability.

Another consideration for dense networks is protection of the switch control plane. During normal network forwarding, a certain amount of traffic is handled by the switch CPU. These packets include ARP request and response handling, TTL-exceeded packets, and IP Multicast unicast reverse path forwarding (URPF) failure traffic. As the density of the virtual machine increases, so will the aggregate traffic load, which will cause more traffic to be sent to the switch CPU. Note that certain network worm behaviors may also inadvertently target the switch CPUs, thus denying service if the CPU is consumed handling the worm connections.

The Cisco Catalyst 6500 Series supports control-plane policing (CoPP) to help prevent systemic outages caused by network traffic from overwhelming the CPU, and it also maintains network stability by intelligently filtering traffic based on interest. CoPP works by filtering traffic that is bound for the switch CPU into traffic that is required for network stability, such as spanning-tree bridge protocol data units (BPDUs) and routing protocol updates, and traffic that is not interesting from a systems perspective, such as TTL-exceeded traffic and ping instructions. This traffic is then queued for the CPU in separate buffers that are rate limited according to importance. To protect systems availability, interesting traffic is buffered in a high-priority queue that the CPU checks more often than other queues. Although lower-priority packets may be dropped, this will not adversely affect network traffic as more packets will arrive and be processed eventually. If the traffic is malicious, it will have little effect on the switch’s operation, and other mechanisms such as Cisco IOS® NetFlow in conjunction with Arbor Peakflow can detect and proactively manage the attack.

Note: Cisco express forwarding protects against worms, such as Code Red, that can cause systemic outages that can affect switches that use flow-based cache forwarding. Because flow-based systems send the first packet of a flow to the switch CPU to build a hardware switched path for subsequent packets, the Code Red worm can overwhelm these systems by opening multiple sessions from and to random IP addresses; these sessions eventually overwhelm the switch CPU and cause systemic outages because network protocol functions, such as spanning tree, cannot be processed.

By using a combination of hardware-based MAC learning, intelligent control-plane policing, buffering, and powerful CPUs, the Cisco Catalyst 6500 Series can maintain application performance and availability of dense virtual machine environments, even under extreme network conditions. In addition, features such as Cisco express forwarding, quality-of-service (QoS) classification, marking and queuing, and Cisco IOS NetFlow provide tools that effectively identify the source of problems and protect against malicious events.

Broadcast Radiation

Broadcast radiation refers to the processing that is required every time a broadcast is received on a host. Although IP is very efficient from a broadcast perspective when compared to traditional protocols such as Novell Internetwork Packet Exchange (IPX) Service Advertising Protocol (SAP), virtual machines and the vswitch implementation require special consideration. Because the vswitch is software based, as broadcasts are received the vswitch must interrupt the server CPU to change contexts to enable the vswitch to process the packet. After the vswitch has determined that the packet is a broadcast, it copies the packet to all the VMNICs, which then pass the broadcast packet up the stack to process. This processing overhead can have a tangible effect on overall server performance if a single domain is hosting a large number of virtual machines.

Note: This overhead effect is not a limitation of the vswitch implementation. It is a result of the software-based nature of the vswitch embedded in the ESX hypervisor.

Operational Management

A primary consideration in a dense server environment is operational management of the infrastructure. The interaction of the vswitch and the network needs to be considered. The vswitch is managed independently of the network, which creates two management domains, network and server, that need to be concurrently managed to provide consistent application availability and performance.

Because VMotion excels at providing a dynamic and fluid environment, the capability to quickly identify problems is imperative. In addition to features such as comprehensive SNMP statistics collection and CiscoView Mini-Remote Monitoring (Mini-RMON),Cisco Catalyst switches support a number of unique features and tools that facilitate the diagnosis and resolution of problems. Of particular value is Layer 2 trace, which provides the capability to trace the path between any two MAC addresses within the data center. Because of the highly mobile nature of virtual machines, this feature can significantly reduce the time to resolution for a particular problem.

Deployment Scenarios

There are a number of general deployment scenarios for virtual machines. A common approach is to place many servers in a single VLAN to facilitate easy migration of virtual machines between physical servers using VMotion. However, because the physical servers are hosting multiple virtual servers, concerns such as broadcast radiation, size of the spanning-tree domain, IP address allocation, and security need to be considered.

The vswitch also supports traffic segmentation based on VLAN association. If VLANs are used to reduce broadcast radiation, virtual machine mobility will be limited to the physical servers that have an association with the VLAN with which the virtual machine is associated. Although this limitation is relatively easy to mitigate by using a trunk to extend VLANs from the network switch to the physical server, this approach can lead to problems with broadcast radiation.

The deployment of virtual machines in either model needs to be carefully considered. The network and server operations teams must meet the discuss the goals of the virtual machine implementation and how best to achieve those goals based on an understanding of the virtual machines in this environment.

Effect of Virtual Machines on the SAN

Virtual machines generally work well in a data center environment, and organizations commonly use both virtual machines and SAN as part of their data center architectures. As long as some modest requirements are met, integrating VMware ESX into a SAN environment is not a problem. Storage administrators should be aware, however, that the mobility and server virtualization offered by virtual machine techniques have ramifications for SAN access.

For storage access, the virtual machine does not support a virtual Fibre Channel switch but uses an N-port interface virtualization (NPIV) interface to present multiple virtual host bust adapters (HBAs) to the SAN. If separation between SAN environments is required for scalability, security, and compliance purposes, achieving this goal can be problematic if the SAN fabric cannot maintain separation between SAN environments. For instance, if three physical servers supporting the human resources, sales, and engineering departments are virtualized and consolidated onto a single physical server, a mechanism must exist to segment traffic between the different virtual machines and their distinct user communities. A similar consideration must be made in the case virtual machine migration, where VMotion is used to move a virtual machine between physical servers.

To maintain separation between the different SAN environments, a number of options may be considered. Deploying multiple HBAs, one associated with each SAN, often seems the simplest approach. Although this approach can be straightforward to implement, it can quickly get expensive. Buying multiple HBAs is an expensive proposition by itself, and the additional HBAs often require upgrading to a larger server chassis to house them, which also consumes additional rack space, which may be counter to organizational goals and which is not feasible for organizations standardizing on one-rack-unit (1RU) servers or blade servers.

The multiple-HBA approach is also relatively inflexible. For instance, adding a new virtual machine, which requires a connection to another SAN, involves adding hardware to the server, if space is available. Moving a virtual machine from one physical server to another presents similar hurdles.

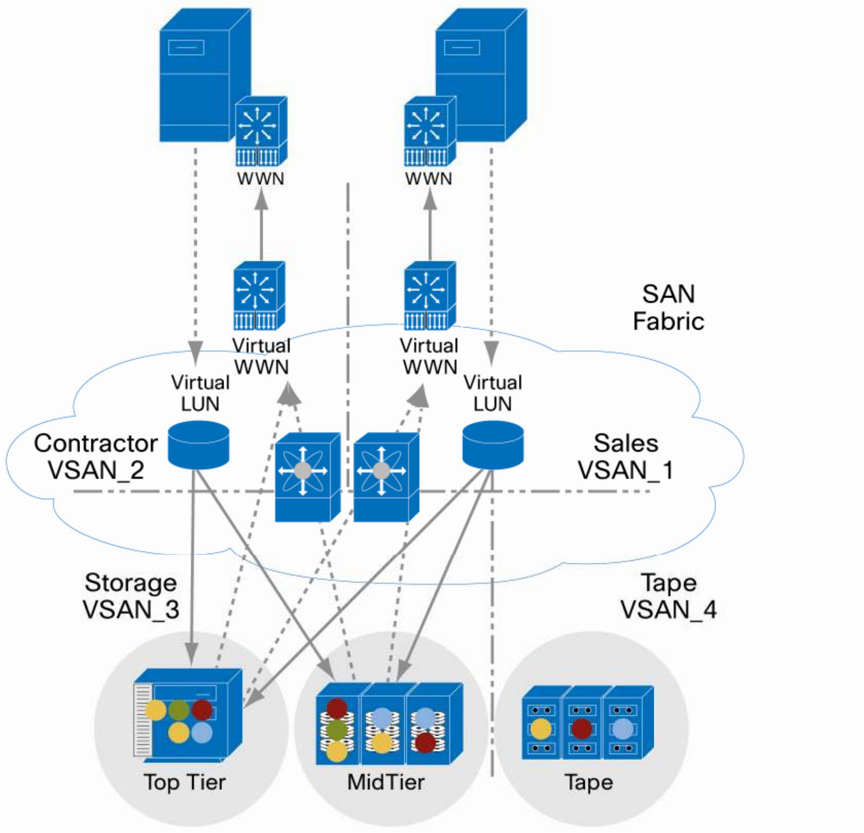
An alternative approach is possible if the server has the latest HBA hardware that supports VSAN trunking. In this case, the virtual machine virtual HBAs may be mapped to the appropriate VSAN to provide segmentation. By default, VMware allows each virtual machine to present a virtual HBA to the SAN using an NPIV connection. Assuming appropriate hardware support, this connection is relatively simple to achieve, but may require the three SAN networks in the earlier example to be consolidated into one large SAN. However, this approach is often not a viable course of action because of SAN design constraints, regulatory compliance, or political concerns.

The Cisco MDS 9000 family offers specific technologies that can address these challenges. VSANs allow a single physical SAN fabric to be segmented into multiple logical SANs, addressing the design, compliance, and political concerns related to SAN fabric consolidation and virtualization. Inter-VSAN Routing (IVR) is a routing protocol that allows transmission of data between VSANs without having to mesh the fabrics. For the case of HBAs that do not support SAN trunking, the Cisco MDS 9000 family supports mapping of WWNs to specific VSANs.

Using IVR, the servers in a virtual VMotion domain can be mapped to their own VSAN. That VSAN enables virtual machine migration between servers within that VMotion domain without loss of SAN connectivity. The VSAN can then be enabled to route traffic to the human resources, sales, and engineering department VSANs, with IVR using predefined rules that enable only specific virtual HBAs to access specific VSANs. By using IVR and logical-unit-number (LUN) zoning in the

VMotion domain VSAN, secure and scalable segmentation of storage resources can be maintained (Figure 2).

Figure 2. Segmentation using VSAN



Best-Practice Network Design Recommendations

As when deploying any network, the goals of the network design must be thoroughly reviewed in terms of performance, scalability, security, and availability. Although very dense server environments can be built using relatively small numbers of physical servers, this is not always the wisest course of action. For instance, factors such as business risk associated with a failure and growth of the business over the next 3 to 5 years should also be considered in planning and design discussions.

When considering virtual machine deployments, the overall density of the servers, both real and virtual, should be considered in terms of existing best-practice network design. Most networks are constructed to accommodate about 250 hosts per subnet, with 2000 hosts in total connected to a single domain.

To maintain IP subnet simplicity, if a density of 8:1 is anticipated, then 32 physical servers per VLAN can be supported without secondary IP subnets (32 x 8 = 256). If virtual machines need to be migrated within the same VLAN, VMotion should be configured to move machines within only that domain. This movement, in turn, may require the set up of server pools aligned to lines of business or other groupings dictated by security or regulatory requirements. This scenario is an example of consolidating with virtual machines, while still leaving “room” on the servers to provide flexibility.

If an organization needs to maintain separation between applications using VLANs, extending VLANs to physical servers using trunks can open the way to broadcast radiation, which can affect server performance. However, if the number of virtual machines and the number of VLANs is limited to three or four VLANs (vswitches), a reasonable degree of flexibility can be achieved. However, the load on the server should be monitored to help ensure that acceptable application performance is maintained.

The effect on the SAN should also be considered. If physical servers are connected to a SAN for storage access, three potential solutions can be applied depending on technology adoption and segmentation requirements:

- If the physical servers can be grouped by business unit or function, such as sales, human resources, and engineering departments, and the virtual machines are aligned to those servers by business unit, then the servers can be attached to their respective SANs using the default NPIV interface. This approach will maintain SAN separation and is the easiest model to manage and troubleshoot.
- If virtual machines from different business units need to be hosted on the same physical servers, then two options can be considered: use an HBA that supports VSAN trunking or create server-side VSANs that can be routed, using inter-VSAN routing, to the sales, human resources, and engineering department SANs.

The first option requires relatively new hardware that supports E-port trunking, which may not be feasible. The second option, using IVR on the Cisco MDS 9000 family SAN director switches, enables existing hardware to be used to gain the flexibility offered by virtual machines while maintaining the separation, security, and scalability of a discrete SAN.

Another factor to consider is how many total servers will be hosted within a domain. If there are 1000 servers with 8:1 virtual machine density, the result is 8000 virtual servers and associated IP and MAC addresses, which is a very dense server environment. Although a Cisco Catalyst data center module can easily support such an environment, risk and performance must be considered.

Also, if IP Multicast–based applications are to be hosted on virtual machine–enabled servers, note that the ESX vswitch implementation does not support Internet Group Management Protocol (IGMP) snooping. If high volumes of IP Multicast traffic will be received or transmitted, it is important to determine the impact to application performance on other virtual machines hosted on the same server. To prevent virtual machines from inadvertently joining high-volume IP Multicast streams, either disable IP Multicast routing on the virtual machine–facing VLANs or implement IGMP group filters.

Note: This configuration requires an understanding of the applications' requirements as applications may rely on low-volume IP Multicast exchange for normal operation.

Conclusion

Virtual machine environments place unique demands on network infrastructure. Although virtual machines can simplify the physical server infrastructure, they can add complexity to the LAN and SAN fabrics within the data center. The effect on the LAN and SAN in terms of resources consumed is amplified because each virtual machine is identified by a unique MAC, IP, and WWN address.

Cisco Catalyst switches support functions that delivers predictable application performance, security, and availability for dense virtual machine environments, as well as tools that simplify management and operation of the virtual machine environment.

In the SAN environment, the Cisco MDS 9000 family provides technologies such as VSANs and IVR to enable integration of the SAN fabric and virtual machine environments in a way that preserves the functional objectives of the virtual machine strategy while maintaining the segmentation necessary for proper information security and regulatory compliance.

For More Information

- http://www.cisco.com/go/dcswitching
- http://www.cisco.com/go/storage
- http://www.vmware.com/resources

Americas Headquarters
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

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C11-407964-00 07/07