TANEJA GROUP
TECHNOLOGY ANALYSTS

T E C H N O L O G Y B R I E F

Switching on the Virtual World: The Role of Fabric-Driven Services for the Virtualized Environment

September 2008

THE NET NET

Virtualization in the data center is widely accepted and deployments are growing at a fast clip. The advantages of virtualizing servers, networks and storage are compelling: consolidating and utilizing resources, higher availability with redundant virtualized paths, and added flexibility to change the IT infrastructure are just a few of them.

However, there is a looming disparity between physical and virtual environments in terms of managing and securing data. This is because SAN management software depends on physical attributes of devices, but virtualization masks these very attributes. If management software cannot pierce through the virtualization veil to secure and manage data by application priority, then many of the virtualization initiatives in the data center will backfire. Server virtualization alone will be successful in the elementary terms of consolidating physical machines, but will threaten QoS, security, performance and troubleshooting in the entire virtual environment.

For the fabric to evolve to fully support virtualized storage in the data center fabric vendors must evolve their feature sets and operating systems to enable users to employ virtualization securely and economically to best serve business processes. This enables IT to place virtualization support services in the fabric in order to serve large virtual server and storage deployments. Smart vendors recognize this and are updating their offerings for the virtualized worlds.

Virtualizing the Data Center

Many data center managers and IT professionals still think of virtualization as consolidating servers. This is virtualization's original and still strongest usage, but virtualization is increasingly sophisticated in this area and is extending beyond the basics when it comes to networking and storage virtualization.

- **Server virtualization.** The key here is abstracting the physical server from the applications and their data. Server virtualization abstracts server resources from applications; applications share CPUs, memory, and network infrastructure as shared resource pools. Developed capabilities from virtual server vendors include the ability to share more computing resources and to dynamically migrate VMs.

- **Storage network virtualization.** Virtualizing the network enables IT to create multiple virtual fabric components from physical ones. Usages include assigning network resources to VMs using

virtual port technologies, and creating virtual SANs (VSANs) to aid in resource assignments and troubleshooting. Growing capabilities in this area enable IT to create multiple virtual ports from single physical HBAs.

- **Storage virtualization.** Virtualized storage enables application data to share pooled resources. Array-based storage pools as well as virtual SANs (VSANs) are well established technologies. However, the tools to efficiently integrate dense virtual server configurations with multiple zones of virtualized storage are new. These next-generation storage and network management capabilities are appearing to include new levels of resource management and security. This will give virtual storage networking the same advantages as physical SANs already enjoy.

The present reality is that virtualization tends to be segregated in discrete virtual networks within the data center. Tying VM migration and management to underlying storage threatens virtualization expansion, and confines virtualization to narrowly defined deployments.

Given the growing popularity of virtualizing servers, the present state of affairs will result in filling the data center with hard-to-manage discrete networks of virtualized servers and their storage. Even within a single virtualized network it will remain difficult to practice the storage management techniques common to physical networks: LUN masking, multiple zoning, thin provisioning and deduplication for example. An individual storage array will be capable of some of these operations, but array-based storage is specific to the VMs using that particular storage system. Even then the storage array cannot solve every problem, such as using a single zone within the virtual network – not because the SAN is incapable of multiple zones, but because single zoning is the only efficient method of keeping the logical storage pathway intact during VM migrations.

Next-Generation Virtualization

Forward looking fabric vendors are seeking to change this state of affairs by supporting server and storage virtualization in the fabric. In this scenario, storage utilization tools like thin provisioning and deduplication run from a virtualized fabric to support multiple virtual storage zones created from pooled storage. Based on automated policies, the fabric directs storage provisioning for non-disruptive hardware and virtual additions and removal, and fulfills application service levels.

The more successful these virtualization tools become the wider virtualization networks can safely expand. Eventually they can include large swaths of the data center, enabling administrators to offer integrated data center resources as a centralized application delivery framework. Let us look at a few of the most important drivers for this evolution.

Driver #1: Growing fabric scalability and performance. High performance fabric such as 8Gb Fibre Channel scales to support large, dense VM environments. However, there are limitations on the

number of Fibre Channel domain IDs when it comes to dense VM networks. Large virtual server deployments can require an unmanageable number of Fibre Channel domain IDs, which currently stand at 16 IDs per server. By deploying network components like intelligent HBAs to dynamically assign virtual port IDs to VMs, no such upper limit exists.

This will enable large virtual environments to take advantage of higher performance and bandwidth without suffering from domain ID limitations. (Or for that matter, single zoning to support VM migrations. Virtual port IDs enable administrators to retain the virtual ID even when moving the VM to a different zone.)

Driver #2: Protecting Quality of Service (QoS). New developments are providing new levels of granular management and troubleshooting for virtualized environments. Given the difficulty in performing granular levels of monitoring and trending over the virtualized network, it is very difficult to meaningfully assign performance and capacity monitoring by application. When each application runs on its own VM and that VM can be individually monitored, then IT will be able to fully protect services levels in even large virtualized environments.

And by adding granular, policy-driven provisioning IT can further optimize application service levels on VMs. The larger the virtual environment grows the trickier it becomes to provision for potentially hundreds of applications. By automatically setting QoS levels and policies in the virtualized storage pool, it becomes much easier to provision space for application-specific VM data.

Driver #3: Improved security. Security for the enterprise data center requires protecting data from accidental or malicious loss or damage, but not at the cost of lowered performance or scalability. Appliance-based security measures work for compact physical networks but can grow to unmanageable levels in large virtual deployments. Fabric-based encryption to protect data at rest and during VM migrations will safely expand data integrity on virtual networks. For example, wire-speed encryption built into a virtual network will secure fast-moving data during physical or virtual VM migrations.

These drivers are moving the data center towards a widespread virtual network. Physically the data center will not be drastically different. Fibre Channel will coexist along with Ethernet as it does now (although FCoE/CEE will enable convergence), there will be multiple servers and heterogeneous storage resources. The challenge will be to knit these disparate resources into a single virtual network, capable of dynamically assigning and configuring computing resources to fit applications amid the changing needs of business.

This will lead to high utilization rates for storage, seamless VM migrations and application changes, and high rates of encryption and role-based security. Management burdens will ease across the data center as automation and a single

interface enables IT to successfully manage highly virtualized data center network.

Energy efficiency will improve as well since consolidated servers and storage require less power, cooling and floor space. And in time this architecture may even make it possible to smoothly replicate VM data to secondary sites. In this model, whole server racks share computing components like centralized RAM while storage pools seamlessly replicate to remote secondary sites.

Virtualization Support in the Fabric

The trend towards data center virtualization is undeniably attractive, but how do you get there from here? We believe that by adding advanced virtualization support to the fabric, IT can achieve the highest levels of virtualization throughout the data center. Major fabric vendors already support both Fibre Channel and Ethernet and are vendor-neutral when it comes to supporting servers and storage. This neutrality makes the fabric the obvious place to provide the widest set of services for virtual servers and storage.

At the very least the fabric vendor must support VMware ESX Server, Microsoft Virtual Server and Citrix Xen. The fabric vendor must also be neutral to storage devices, either providing extended storage virtualization or fully integrating with the array controllers to provide virtual storage networking for a dense VM network. The fabric provides the physical and virtualized switches, ports and HBAs that allow mature support tools to run on virtual environments. The fabric can also extend the existing advantages of VSANs to a wider virtual deployment. This extends SAN storage capacity, protection and management to the entire virtual network while still protecting individual application and/or workgroup sectors.

We will look now at a few representative technologies for the highly virtualized data center. All of these technologies are available now.

Virtualization Technology: NPIV

NPIV is a vendor-neutral technology for creating virtual port IDs for virtualized Fibre Channel storage networks. (Emulex and QLogic provide HBAs with NPIV to Cisco and Brocade.) Used by both Cisco and Brocade, NPIV eases the stranglehold that Fibre Channel Host Bus Adapters (HBAs) have on Worldwide Port Names (WWPNs). NPIV enables IT to assign WWPNs to virtual HBAs, which in turn enables storage software to monitor, report and provision separately for VMs and not just the physical server on which they reside. This means that the tried and true methods of LUN masking and zoning now also apply to virtualized servers as well as physical, thus centralizing and simplifying server administration.

NPIV also aids in VMware VM migration, which is frequently a sticking point in expanding storage pools across physical storage systems. The migration itself using VMotion is not particularly difficult, but moving the underlying storage is. In response to the difficulty, VMware administrators usually create a single zone where every disk is exposed to a VMware ESX server. Admittedly this eases migration

problems since the migrated VM retains access to its data, but it does not make for good security or multiple zoning.

NPIV can preserve the VM's virtual port ID during and after the migration, which ties its storage to its new virtual location. No manual reconfiguration or pointing are necessary, as the method preserves not only the location of the data but also its LUN and zoning configuration. Since the names are no longer tied to physical HBAs, physical adapters can be swapped out without having to reconfigure the virtual SAN. Emulex LightPulse and QLogic SANblade virtual HBAs extend fabric virtualization by using NPIV to decouple virtual servers from the physical server port ID.

Virtualization Technology: VMs

Virtual machines are at the heart of the virtualized network. The primary goal of the virtualization services is the ability to make the VM and its logical storage act, to all intents and purposes, as a physical server and storage. Only this enables the virtual network to not only host applications, but also to receive the same level of data protection and performance monitoring as physical networks already receive.

Several crucial elements of SAN best practices are already in place, such as LUN masking and mapping. Logical Unit Number (LUN) masking guards the VMs against server data grabs, making a VM's data invisible to other VMs. LUN mapping tracks LUNs between the physical and logical storage locations, allowing administrators to assign a virtual network to a storage array.

NPIV in particular is increasing the level of per-VM control available to VM administrators. VMs were previously limited to a single Worldwide Port Name per physical port, meaning that server and storage management tools could not report on specific VMs, but could only aggregate results from the same physical port. Now NPIV-enabled virtual HBAs assign WWPNs at a much more granular level. NPIV allows administrators to track statistics like traffic, packet sizes, and error rates at the VM level. When matched with a performance management application, this enables administrators to run meaningful performance monitoring, trending, and planning at a granular VM level.

Virtualization Technology: VSANs

Virtual SAN (VSAN) technology partitions SANs into logical virtual SANs, each in its own protected zone with dedicated storage services and management. By segregating server-based storage into its own protected and easily manageable space, administrators maintain a dynamic logical storage pool while maintaining security and fault isolation levels.

VSAN is a proven technology standard, but its usefulness was limited when it came to VMs. If a VM was pointed to a single VSAN there was not an issue, but if the VM needed to share data across multiple VSANs then the entire SAN had to be exposed to the VM. In combination with NPIV, F-Port trunking enables administrators to virtually route VMs on the same physical server to multiple VSANs without having to expose the entire

storage network. (Fault isolation and security still operate at the VM level.) F-port trunking allows different workgroups to operate VMs on the same physical server and HBA while accessing dedicated VSANs. With NPIV, administrators can zone VSANs to support multiple VM access, or to restrict storage to a specific VM.

Virtualization Technology: Unified I/O

Unified I/O is typified by highly virtualized fabric. In this architecture, servers dispense with the traditional 1:1 server/interconnects ratio in favor of sharing pools of networking resources. Unified I/O typically virtualizes Ethernet NICs for the data network and Fibre Channel HBAs for the SAN. Other virtualized interconnects are common such as cluster configurations and InfiniBand.

Since servers can sport three to seven I/O interfaces, virtualizing them makes for a highly optimized and simplified network architecture. Consolidating network components also decreases rack space and computing equipment; avoiding data center build-out and high power and cooling costs. Upcoming standards like FCoE will enable an even higher degree of I/O virtualization. Converged network adapters (CNAs) will replace separate HBAs and NICs to carry Ethernet LAN and Fibre Channel SAN traffic.

Virtualization Technology: Virtual Blade Switches

Virtual blade switches combine multiple physical switches into a single logical switch. This aggregates the power of the physical switches into much deeper bandwidth for servers and their applications. It also relieves network traffic as blade servers within the same rack do not have to pass inter-rack traffic through multiple physical switches. The virtual switch also offers active/active configuration to blade servers by aggregating two switches per server, and can also aggregate multiple NICs per server. This increases bandwidth in dense blade server farms.

Technologies like F-port trunking and NPIV operate in virtualized blade environments as well. For example, Cisco's N-port virtualization (NPV) technology, in concert with NPIV, presents a blade switch as an HBA to the SAN fabric. This effectively makes the switch a powerful aggregate HBA that smoothly interconnects to large multi-vendor SAN deployments. The blade switch/HBA uses the F-port to connect to servers and the N-port proxy to connect to both physical SANs and VSANs.

Virtualization Technology: Switches

Cisco's MDS 9000 series is the workhorse switch and director class that implements networked storage virtualization in Fibre Channel environments. Along with MDS Fibre Channel Storage Services Module and virtualization software, the 9000 series supports physical and virtual SAN deployments. Cisco MDS offers other virtualization and network support technologies as well for provisioning, traffic management and security. For example, Cisco VFrame Data Center integrates with MDS to accomplish resource provisioning for large virtual networks, while NPV and technologies like FlexAttach ease the

virtualization and administration of dense blade networks.

Cisco also offers a backbone switch platform that dynamically expands virtual services across the data center. Cisco Nexus 7000 supports 10Gb-and-up Ethernet and will support the FCoE standard for Fibre Channel traffic over Ethernet. The operating system NX-OS centralizes virtualization management in the switch by combining Layer 2 switching, Layer 3 routing protocols, and virtualization into a single control interface.

Brocade DCX Backbone also puts virtualization management and support into the switch. DCX supports multiple protocols including 8Gb Fibre Channel, FCoE and advanced Ethernet, and several others. Brocade includes a range of virtual SAN support technologies.

Benefits of Next-Generation Virtualization

This ability to expand virtualization from specific and limited virtual networks to the entire data center has dramatic advantages for the enterprise.

1. **Lower TCO through more efficient resource usage.** Fewer physical servers, network components and storage cuts down the number of physical resources required in the data center. In turn this frees up data center space, improves energy efficiency, and centralizes backup and data protection resources. Fibre Channel and NPIV can lower TCO even further by enabling a single physical HBA to provide multiple virtual IDs to VMs. By creating multiple virtual paths from a single physical one, IT can offload network processing onto virtual ports while preserving centralized management and control. This results in significant cost savings.

2. **Supports large virtual networks without sacrificing control.** Virtualized port technology adjusts to server changes without requiring manual reconfiguration, including server swaps and new deployments. Server utilization increases by virtualizing single physical servers to host multiple applications, and fabric virtualization preserves QoS by allocating each VM its own logical HBA port. This lets IT easily create multiple paths to prioritize traffic according to application priority.

3. **Improved migration experience.** Due to the common 30-month hardware depreciation schedule, storage is periodically refreshed. If the data center can access petabyte-sized virtualized storage from pooled storage devices, then even large physical device migrations will have minimal impact. Logical port IDs will allow migrated VMs to automatically retain paths to their storage, and data on a depreciated storage device can be painlessly migrated to another physical location within the logical storage pool.

4. **Extends full SAN benefits to virtual networks.** Data management and utilization capabilities that are now at the storage array level can run from the fabric level on logical storage pools. Thanks to

virtual port IDs, IT can migrate data transparently, can switch storage subsystems in and out, and can build new virtual SANs easily and flexibly. Storage throughout the data center could finally be provided as a flexible service, and not as a set of discrete storage subsystems.

Taneja Group Opinion

In terms of the highly virtualized data center, we are not there yet. Physical layer management tools are continually developing, but support for dense virtual networks lags far behind. Certainly individual virtualization technologies have existed for some time for servers, networks and storage. VMware and Citrix Xen are increasingly mature technologies, as are NPIV and array-based storage pooling. However, the ability to provide high levels of availability, utilization and data protection to the virtual environment is presently relegated to virtual networks with relatively simple configurations.

We believe that is changing in the face of business needs. Changing business requirements often translate to changes in applications and the need for highly flexible computing. Budgetary constraints both for computing and human resources demand high utilization rates and simplified management, while fast-growing data needs high performance and flexible storage that can dynamically respond to changing priorities.

Next-generation virtualization services built on present-day technologies are centered in the fabric. This enables IT to create and support the virtualized infrastructure as an available, flexible, and secure computing entity throughout the data center. In combination with rising levels of Fibre Channel and Ethernet performance and bandwidth, this achievement will allow the enterprise to safely integrate their vast computing resources into a highly flexible, scalable and logical framework.

Forward looking networking vendors are in the forefront of this evolution. Virtualizing all layers of the data center – servers, network and storage – enables the business to deliver application services through a powerful and flexible computing infrastructure. Success in this area will turn the data center from a collection of discrete virtual networks into a holistic infrastructure, where both physical and virtual environments smoothly support business needs.