Table of Contents

Table of Contents 1
Executive Summary 2
Current Server Virtualization Environments 3
- Hypervisors 3
- Virtual Switches 3

Leading Server Virtualization Vendors 5
- VMware™ 5
- Xen 5
- Microsoft 5
- KVM 5
- Oracle VM 5

VMready™ 6
How VMready Works 7
- Virtual Machine Identities 7
- Grouping 8
- Local VM Groups 8
- Distributed VM Groups 8
- NMotion™ 9

VMready Products 10
Conclusion 10

Executive Summary

Data centers are undergoing monumental paradigm shifts. Servers and more importantly the services they provide are expected to be available 24 hours a day, 7 days a week by design.

Enterprise data centers previously adapted to this change by following the rule that more is better and redundant configurations never hurt. However, as demand for greater processing continues to outstrip available floor space, rack space, power and air-conditioning, the market has turned to virtualization to efficiently use the resources available.

It has long been recognized that most systems spend their time in idle states. For any physical computing platform, the bulk of the processing resources are underutilized. Attempts to solve this inefficiency problem resulted in experiments with virtualization as far back as the 1960s. Mainframe processors were running multiple images of virtual machines which could be made active when resources were required and placed in the background when idle.

Virtualization technology has since been adapted to personal computer and server platforms. Multiple virtual machines (VMs) can be created in a single physical platform greatly increasing the efficiency of the data centers by enabling more work from less hardware.

As the workload on the physical servers increases VMs can be migrated to available servers to ensure that service level agreements and response times are met. When workloads decrease, the VMs can be migrated for consolidation to fewer servers and allow the unused servers to be powered down to save energy and cost.

Virtualization can also improve the availability of applications, because Virtual Machines can quickly be restarted on new hardware when physical servers fail. VMs can be simply migrated ahead of time when servers need to be shut down for service or upgrades.

To truly exploit the benefits of server virtualization, data centers need to enable the dynamic and automatic movement of Virtual Machines while protecting their security and maintaining accessibility.

Current networking switches are not aware of Virtual Machines and this creates security and availability issues for both server and network administrators as they try to fully exploit the value of virtualization and manage this new environment.

To further the virtualization evolution, network vendors need to provide products that:

- Are Virtual Machine aware
- Provide network configurations at a Virtual Port level, rather than just at the physical port
- Track the mobility of Virtual Machines across data centers and into the cloud
- Automatically reconfigure the network as Virtual Machines move

Today, BLADE Network Technologies (BLADE) offers these abilities. With VMready™, switches from BLADE can:

- Recognize individual virtual machines within physical servers
- Support all leading hypervisor vendors, such as: VMware, Microsoft, Citrix and Red Hat
- Assign unique operating, security and quality of service characteristics for each VM
- Fully integrate with hypervisor managers such as VMware's vCenter to enforce the same networking policy in physical switches and vSwitches
- Recognize when Virtual Machines are created and migrated
- Move the network policies in real-time to the new locations to ensure that Virtual Machines stay available and secure as they migrate

Current Server Virtualization Environments

Server virtualization refers to the process of dividing physical resources such as processors, memory, disks and network interface cards among “virtual machines” operating within the physical server.

Hypervisors

Virtual machines operate under the control of software commonly referred to as a ‘hypervisor,’ which provides a global mechanism for control and scheduling system resources. Hypervisors can run natively on the server hardware (bare-metal) or can be hosted within a conventional operating system. VMready can support Virtual Machines running on both hypervisor types.

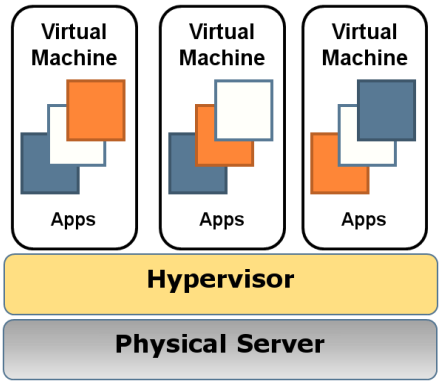

Figure 1: Type 1 Hypervisor

Virtual Switches

Virtual switches (vSwitch) are software network switches that provide the initial switching layer for Virtual machines. They forward packets from vNICs in the Virtual Machines to other VMs on the same physical server or into the physical network via uplink adapters. Some vSwitches provide Layer 3 as well as Layer 2 switching and can also assign network attributes for VMs such as VLANs and traffic shaping.

Some virtualization vendors also provide distributed virtual switches that span several servers and act as one large vSwitch with consistent configurations.

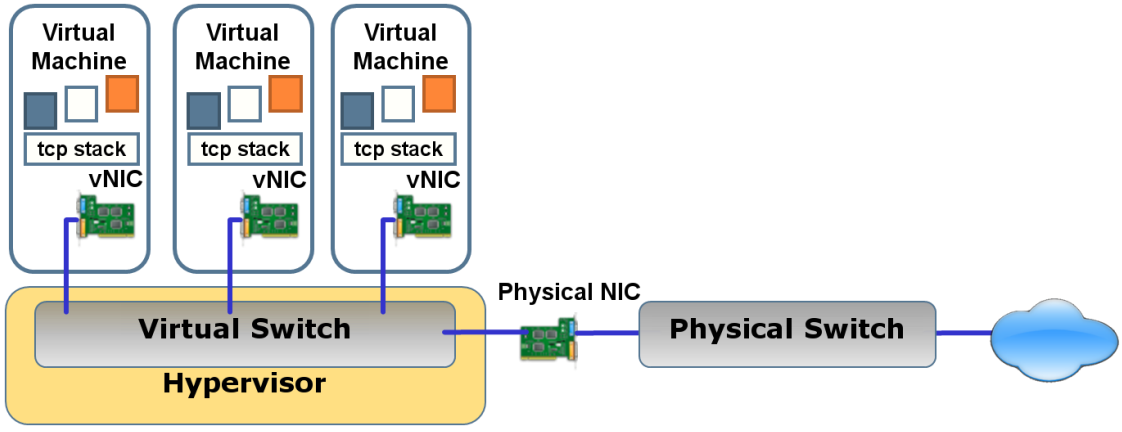

Figure 2: Virtual Switch

Virtual Machine Migration

Virtual machine migration refers to the mobility of VMs within the virtual environment. This can be in response to events or conditions based on sets of predefined criteria, such as:

- When a VM should move from one location to another in a scheduled fashion
- When a VM should be replicated (cloned) in another location in a scheduled fashion
- When a VM should be able to move from one location to another in an unscheduled fashion
- When a VM should be replicated (cloned) in another location in an unscheduled fashion

With the above set of policies, the server administrator is able to define a coherent set of rules that provide both the ability to adapt to changing workloads and to respond to and recover from catastrophic events in both virtual and physical environments.

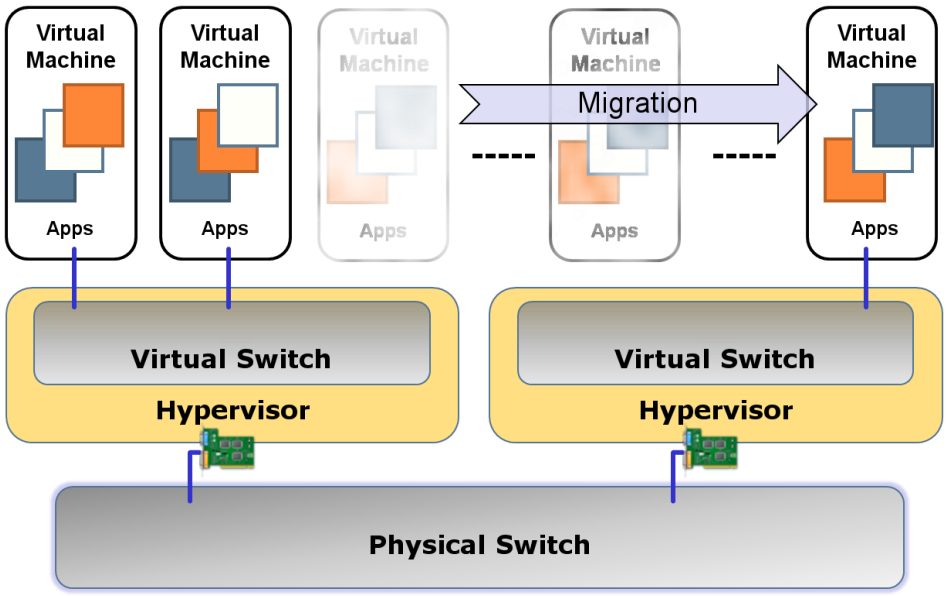

Figure 3: Virtual Machine Migration

For many services, changes in demand are generally regular and therefore predictable. Such expected changes can be anticipated and automated with a set of rules that allows the administrator to allocate demand to pools of available resources (such as CPU cycles, or memory) on platforms (servers) that have the lowest utilization.

When a VM experiences very high workloads its performance can be negatively impacted unless it can be migrated to other available resources. For data centers to quickly migrate busy Virtual Machines requires that the network is configured correctly to avoid security or access issues.

Leading Server Virtualization Vendors

VMware™

VMware is the current market leader in server virtualization. Their flagship product, vSphere™, provides the infrastructure and management solutions for large enterprise level virtual environments. VMware was the first to offer migration technology (VMotion) to enable customers to quickly re-provision their data centers.

Xen

Xen is an open-source hypervisor that is available for Linux and Solaris operating systems. Citrix XenServer™ is a commercial and fully supported Xen hypervisor. Citrix also offers an accompanying suite of products for networking and management under the umbrella of Citrix Essentials which can manage both Xen and Microsoft's Hyper-V platforms.

Microsoft

Microsoft's Hyper-V™ (hypervisor) product runs on Windows 2008 Server™ and is provided with the server software. It supports Microsoft guest virtual machines and some non-Microsoft (Linux) guest operating systems. With Microsoft's backing, Hyper-V is gaining share in the server virtualization market.

KVM

Kernel-based Virtual Machine (KVM) is a hypervisor that is rapidly gaining interest. KVM has been part of the Linux kernel since 2.6.20 and provides native virtualization on Intel VT and AMD-V CPUs. Currently the management tools required for data center KVM deployments are still primitive, but they are evolving rapidly.

Oracle VM

Oracle VM is a Xen-based hypervisor that is fully supported by Oracle. Oracle will provide a single point of support for customers running Oracle Database and other Oracle certified applications on Oracle VM.

VMready™

BLADE Network Technologies has patented a unique solution to enable the network to be Virtual Machine aware. The approach extends the concept of virtualization into the network, allowing the configuration of network polices to a virtual port rather than just at the physical port.

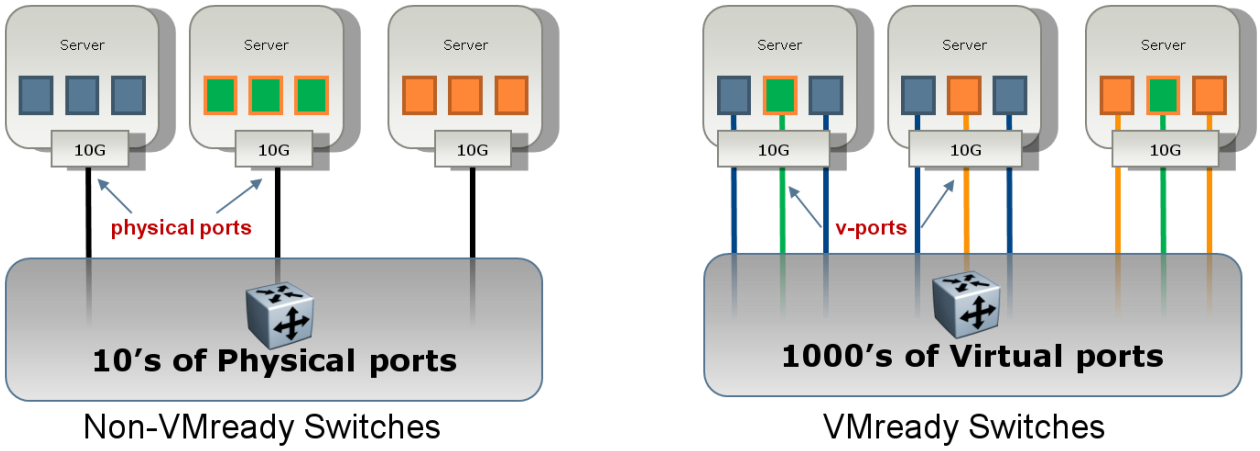

Figure 4: VMready vs. Non-VMready Switches

VMready is software that runs on the physical switch that provides:

- Thousands of virtual-ports per switch, with configurable parameters per virtual-port, including :
  - Access Control Lists (ACLs)
  - Quality of Service (QoS) attributes
  - VLAN membership
  - Traffic Shaping and monitoring

- Integration with VMware's vCenter to enable:
  - A single pane of management for both VMready switches and software vSwitches
  - Automatic discovery of VMs across the data center
  - Rich display of VM information such as IP addresses, VM name and ESX server location
  - Synchronization of each VM's network configurations between VMready and vCenter

- Tracking of VMs during migrations with automatic reconfiguration of network settings, to ensure :
  - Availability and security are maintained in real-time
  - Services levels are guaranteed

- VMready can scale across multiple switches allowing :
  - Virtual Machines to be protected as they migrate across the data center

- Support for all major hypervisors without modification including :
  - VMware; Hyper-V; Xen; KVM and Oracle VM
    - Works with both standard and distributed vSwitches

How VMready Works

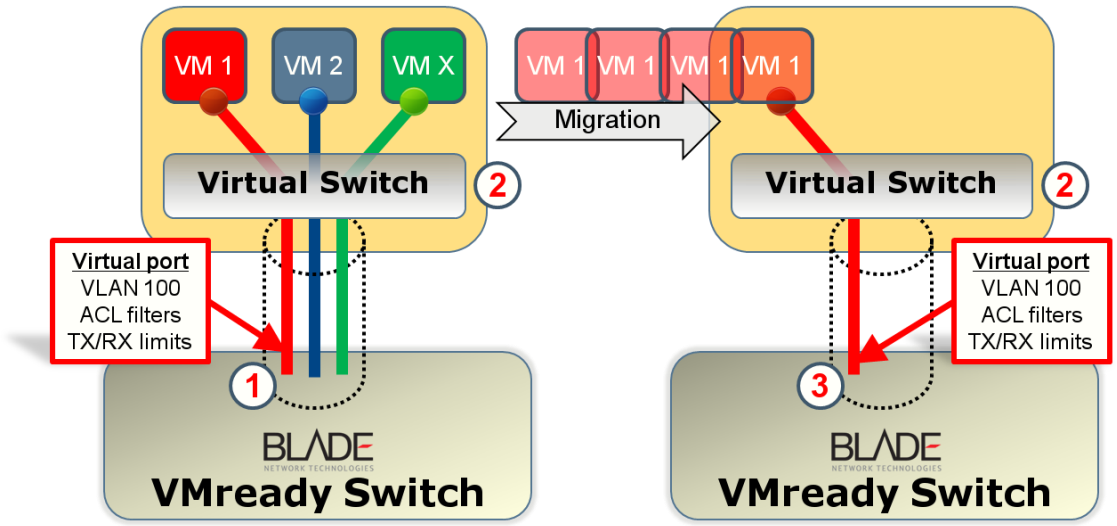

Figure 5: Virtual port connections between VMready and Virtual Machines

The above diagram shows Virtual ports between each Virtual Machine and VMready switches and how virtual ports move with a Virtual Machine under migration.

1. VMready automatically creates a unique virtual port for each VM when the VM first sends traffic or when pre-provisioned by an administrator. Each virtual port is uniquely indentified using open standards.

2. Each virtual port can be configured for networking parameters such as VLANs, ACLs, and QoS just like it was a physical port. The VMready configurations can be automatically exported to the hypervisor to configure the vSwitches and provide a single point of management.

3. VMready tracks Virtual Machines in real-time as they migrate and automatically moves the virtual port along with its network configurations to the new physical location. This ensures Virtual Machines are always correctly configured in the network no matter where they move.

VMready allows for a ‘define once, use many’ configuration that evolves as the server and network topologies evolve. Virtual machines are free to move as events require, retaining their configurations from origin to destination. Administrators no longer need to perform repetitive configurations or suffer the consequences of a missed configuration.

Virtual Machine Identities

The foundation of VMready is the ability to identify and then monitor virtual machines within the physical hosts attached to the switch. With an ability to identify each VM uniquely, VMready enables the administrator to apply the same philosophy to Virtual Machines as used with physical servers. VLAN and Quality of Service settings can be provisioned and Access Control List attributes can be set at a VM level with permit and deny actions based on Layer 2 to Layer 4 information.

Virtual Machines can be configured in VMready using an intuitive Web GUI, command line interfaces (CLI) or via external management tools such as BLADEHarmony Manager™.

Grouping

VMready provides a simple and intuitive way to group similar Virtual Machines together and assign the same networking policies to all members of the groups to ensure consistent allocation of resources and security measures to meet service-level goals. Members of the group retain the group attributes wherever they are located within the virtual environment.

Grouping significantly simplifies the administration tasks when managing large numbers of Virtual Machines, as new VMs are simply added to existing groups.

In BLADEOS 6.1 & 6.3, VMready supports two types of groups:

- Local VM groups maintain VM configurations locally on the VMready switch
- Distributed VM groups are synchronized with VMware's vCenter and enhanced migration support

Local VM Groups

Local VM group configurations are maintained on the switch and do not directly synchronize with hypervisors. Local VM groups may include elements such as local switch ports and VMs that are connected to one of the switch ports or are pre-provisioned on the switch.

Local VM groups support migration. As VMs move to different hypervisors connected to the switch, the configuration of their group identity and features moves with them.

Distributed VM Groups

VMready creates profiles containing network configurations such as VLAN, traffic shaping and ACLs for distributed VM Groups. VMready then automatically synchronizes the profiles to VMware's vCenter to create Port Groups with the same network configurations on all required vSwitches. Consistent network policies are simply enforced regardless of the Virtual Machine's location.

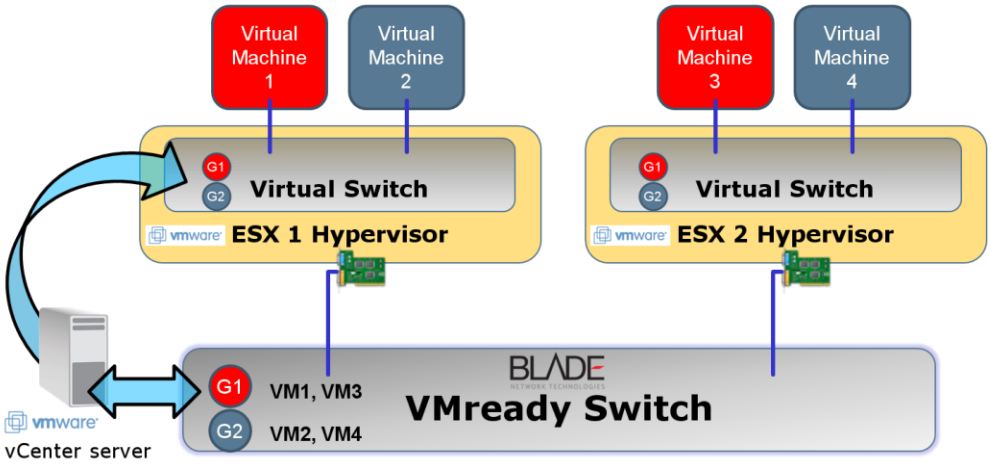

Figure 6: Distributed VM Groups

In BLADEOS 6.1 & 6.3, VMready is integrated with VMware's vCenter to provide a seamless infrastructure. The networking settings configured with VMready on the physical switch can be exported to vCenter to create new port groups on the vSwitches with the correct configuration.
VMready applies the VM networking settings to both physical VMready switches and the vSwitches residing within the ESX hypervisors, via VMware open APIs. Once configured, VMready policies follow the VMs regardless of their location.

VMready provides users with a single pane of network management for Virtual Machines. As new Virtual Machines are added to a distributed group or a group configuration is changed VMready automatically updates VMware's vCenter to distribute the changes to all associated hypervisor vSwitches. This integration simplifies administrative tasks and reduces the chance of configuration error.

NMotion™

A unique feature of VMready is NMotion which has the ability to detect VM migrations as they occur.

Without VMready, deterministic movement of VMs is manageable only if the number of permutations is small. Manually duplicating configurations on switch ports for numerous virtual machines is very labor-intensive and the risk of error is high.

Non-deterministic movement of VMs occurs in response to unpredictable or unanticipated conditions within the physical or virtual hosts attached to the switch. To provision for all possibilities requires the configuration of all combinations on all network ports. If a configuration is missed, then a VM migration event can result in a service outage or a potential security breach.

VMready is able to solve management issues for both deterministic and non-deterministic movement through the implementation of NMotion (Network motion), which manages the distribution of network policies in real-time when VMs migrate. NMotion can identify and then track virtual machines as they move, guaranteeing that the underlying services not only remain available, but also retain their network characteristics of ACLs, QoS and VLAN membership.

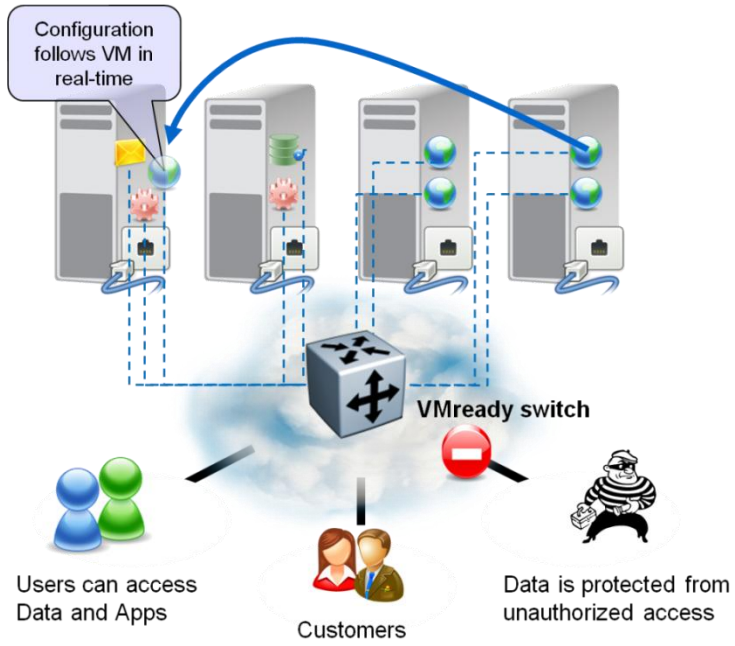

Figure 7: NMotion

VMready through NMotion migrates the network policies associated with a VM from origin port to destination port.

VMready Products

VMready is currently available on the following platforms:

- BLADE RackSwitch
  - RackSwitch G8124 24-port, 10G SFP+, low latency
  - RackSwitch G8000 48-port, 1/10G
- IBM BladeCenter
  - BNT Virtual Fabric 10G Switch Module
  - BNT 1/10G Uplink Ethernet Switch Module
- HP BladeSystem
  - HP 1:10G Ethernet BL-c Switch

Conclusion

Virtualization has the promise to make significant contributions to data center and cloud computing for the foreseeable future. It provides the ability to create multiple compute environments in a single bare-metal host, minimizing idle processor cycles and maximizing the return per physical server. New Virtual Machines can be quickly added to the environment so that revenue opportunities are quickly realized.

Virtualization also increases the availability of services by providing a mechanism for fast and reliable transition of services from a failing host machine.

However, the increase in flexibility resulting from virtualization comes at a price. As the probability of a VM appearing on any given network interface increases, so does the number of configurations to ensure maximum availability and security of the service delivered by that VM. The exposure to service outage or high security threat due to a missing or incorrect attribute assignment is directly proportional to the complexity of the virtual topology.

VMready is the only solution that maximizes the benefits of virtualization in the server environment while eliminating the exposure to error that exists in traditional networking environments. VMready can learn and adapt to the virtual implementation on the attached physical hosts. It can assign network policies on a VM level to guarantee the allocation of networking resources. And VMready can monitor and detect events in the virtual environment so that network policies remain associated with their virtual machines no matter where they reside.

Unlike competing solutions, VMready works with open standards and with all hypervisor vendors to enable customer choice, the freedom to used mixed vendor solutions and to transition between hypervisor vendor solutions all while maintaining consistent network configurations.

BLADE's VMready provides the simplicity, flexibility and power to manage the network in your dynamic virtual data center is a key element of BLADE's Unified FabricArchitecture™ (UFA), which provides a faster, virtual and proven data center networking platform.

MKT100604