Virtualization:

Benefits, Challenges and Solutions

By Dr. Jim Metzler

Sponsored by:

Produced by

Table of Contents

Executive Summary

While it is possible to virtualize almost any component of IT, this report will focus on three forms of virtualization: server virtualization, desktop virtualization and virtualized appliances. A key reason for this focus is that significant synergies exist between and amongst these forms of virtualization.

The majority of IT organizations have already implemented server virtualization and most intend to implement additional server virtualization during the next year. The primary factors driving the movement to deploy server virtualization are cost savings and the ability to dynamically provision and dynamically move VMs among physical servers.

There are, however, a number of significant challenges associated with server virtualization. Some of the challenges include:

Contentious Management of the vSwitch
Each virtualized server includes at least one software-based virtual switch (vSwitch). This adds yet another layer to the existing data center LAN architecture. It also creates organizational stress and leads to inconsistent policy implementation.

Breakdown of Network Design and Management Tools
The workload for the operational staff can spiral out of control due to the constant stream of configuration changes that must be made to the static date center network devices in order to support the dynamic provisioning and movement of VMs.

Limited VM-to-VM Traffic Visibility
The first generation of vSwitches doesn't have the same traffic monitoring features as does physical access switches. This limits the IT organization's ability to do security filtering, performance monitoring and troubleshooting within virtualized server domains.

Some of the emerging approaches to managing a virtualized environment include:

Dynamic Infrastructure Management
A dynamic virtualized environment can benefit greatly from a highly scalable and integrated DNS/DHCP/IPAM solution. Where DNS, DHCP and IPAM share an integrated database, this obviates the need to manually coordinate records in different locations.

Distributed Virtual Switching (DVS)
Most vSwitches include an integrated control and data plane. With DVS, the control and data planes are decoupled. This makes it easier to integrate the vSwitch's control plane with the control planes of other switches and with the virtual server management system.

Orchestration and Provisioning
Service orchestration is an operational technique that helps IT organizations to automate many of the manual tasks that are involved in provisioning and controlling the capacity of dynamic virtualized services.

Half of all IT organizations have already implemented at least some desktop virtualization and within a year roughly 75% of IT organizations will have implemented it. Desktop virtualization is driven by a combination of cost savings, increased ability to comply with myriad regulations and an improvement in data and application security. The two fundamental forms of desktop virtualization are:

- Server-side application/desktop virtualization
- Client-side application/desktop virtualization

With server-side virtualization, the client device plays the familiar role of a terminal accessing an application or desktop hosted on a central presentation server. There are two primary approaches to server-side application/desktop virtualization. They are:

- Server Based Computing (SBC)
- Virtual Desktop Infrastructure (VDI)

Client-side application virtualization is based on a model in which applications are streamed on-demand from central servers to client devices. On the client-side, streamed applications are isolated from the rest of the client system by an abstraction layer inserted between the application and the local operating system.

One of the primary challenges that are associated with implementing desktop virtualization is achieving an acceptable user experience for client-to-server connections over a WAN. For example, VDI requires at least 200 Kbps of bandwidth per simultaneous user and the minimum peak bandwidth required for a PCoIP[1] connection is one Mbps. In most cases, the successful deployment of desktop virtualization requires that WAN optimization techniques that focus on the particular characteristics of the traffic that are associated with desktop virtualization be widely deployed.

---

[1] PC-over-IP is a relatively recently developed display protocol from Teradici Corporation.

A *Virtual Appliance* is based on network appliance software running in a VM. Virtual appliances can include WOCs, ADCs, firewalls, and performance monitoring solutions among others. An important set of synergies exist between virtual servers, virtual desktops and virtual appliances such as a WOC or a performance monitoring solution. Perhaps the most important synergy is that virtual appliances are of particular interest to IT organizations in those instances in which server virtualization technology has already been disseminated to branch offices and has also been implemented in the data center.

In the branch office, a suitably placed virtualized server could potentially host a virtual WOC appliance as well as other virtual appliances. Alternatively, a router or a WOC that supports VMs could also serve as the infrastructure foundation of the branch office. Virtual appliances can therefore support branch office server consolidation strategies by enabling a single device to perform multiple functions typically performed by multiple physical devices.

A virtualized ADC makes it easy for an IT organization to package and deploy a complete application. One example of this packaging is the situation in which an entire application resides on VMs inside a physical server. The virtualized ADC that supports the application resides in the same physical server and it has been tuned for the particular application. This makes it easy to replicate or migrate that application as needed. In this case, a virtualized ADC also provides some organizational flexibility. For example, the ADC might be under the control of a central IT group or it might be under the control of the group that supports that particular application. The later is a possibility from an organizational perspective because any actions taken by the application group relative to the ADC will only impact their application.

One of the compelling advantages of a virtualized appliance is that the acquisition cost of a software-based appliance can be notably less than the cost of a hardware-based appliance with same functionality. In addition, a software-based solution can potentially leverage the functionality provided by the hypervisor management system to provide a highly available system without having to pay for a second appliance. Another advantage is that if virtualized appliances have been deployed, then it is notably easier than it is in a more traditional environment for various networking functions to be migrated along with VMs in order to replicate the VMs's networking environment in its new location.

A critical factor that must be considered when evaluating the deployment of virtual appliances in a dynamic, on-demand fashion is the degree of integration of the virtual appliance with the virtual server management system. Ideally this management system would recognize the virtual appliances as another type of VM and understand associations between appliance VM and application VMs in order to to allow a coordinated migration whenever this is desirable.

This report will only briefly mention the impact that virtualization has on networking. That topic will be covered in detail in a report to be published on or about October 1, 2010. That report is entitled *Cloud Networking*.

Introduction

In the current environment, almost every component of IT can be virtualized. This includes:

- Servers
- Desktops
- Applications
- Management probes
- I/O
- Wide Area Networks
- Local Area Networks
- Switches

- Routers
- Firewalls
- Storage
- Appliances such as WAN optimization controllers, application delivery controllers and firewalls

This report will focus primarily on three forms of virtualization: server virtualization, desktop virtualization and virtualized appliances. The benefits of server and desktop virtualization have been discussed in length in various trade publications. As a result, this report will not dwell on those topics, but will instead focus on defining the challenges associated with server and desktop virtualization as well as on the technologies, both existing and emerging, that enable IT organizations to respond to those challenges. Because the benefits of virtual appliances have not been discussed in length in the trade publications, this report will discuss those benefits. This report will also discuss the challenges associated with virtual appliances as well as the technologies, both existing and emerging, that enable IT organizations to respond to those challenges.

This report will only briefly mention the impact that virtualization has on networking. That topic will be covered in detail in a report to be published on or about October 1, 2010. That report is entitled *Cloud Networking*.
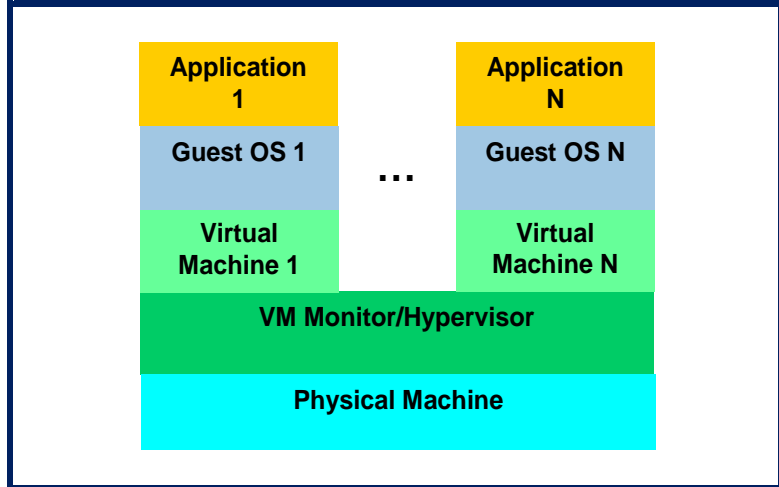
Server Virtualization

One of the primary benefits of server virtualization is that it allows IT organizations to consolidate servers. As shown in **Figure 1**, after being virtualized a single physical server can support multiple virtual machines (VMs). This means that applications that would normally require a dedicated server can now share a single physical server. This result in a reduction in the number of servers in a data center which leads to significant savings in CapEx (i.e., costs of server hardware, SAN Host bus adapters,

and Ethernet NICs) and OpEx i.e., server management labor expense plus facility costs for power, cooling and floor space.

Initially the primary factor that drove the movement to deploy server virtualization was the cost savings discussed in the preceding paragraph. Today two other factors are also acting as significant drivers of that movement. Those factors are the ability to dynamically provision VMs and the ability to dynamically move VMs among physical servers, both within a given data center and between disparate data centers without service interruption[2].

Figure 1: Simplified View of Server Virtualization

Application 1	...	Application N
Guest OS 1		Guest OS N
Virtual Machine 1		Virtual Machine N
VM Monitor/Hypervisor		
Physical Machine		

As a result of being able to rapidly provision VMs, IT organizations can potentially respond to the business requirement for additional computing resources in a matter of seconds or minutes. The mobility of VMs means that many system administration tasks, including backup and restore, system upgrades, and hardware/software maintenance can be performed without impacting the availability of applications or services. Mobility can also be leveraged to ensure high application availability and workload balancing across a cluster of virtualized servers.

The Adoption of Server Virtualization

In early 2010, Ashton, Metzler & Associates (AM&A) administered a survey to the attendees of the Interop conference. Throughout this report, the IT professionals who responded to that survey will be referred to as The Survey Respondents.

The Survey Respondents were asked to indicate the percentage of their company's data center servers that have either already been virtualized or that they expected would be virtualized within the next year. Their responses are shown in **Table 1**.

The data in Table 1 shows the deep and ongoing interest that IT organizations have relative to deploying virtualized servers. In particular, the data in Table 1 indicates that the majority of IT organizations have already virtualized at least some of their data center servers. Two other observations that can be drawn from Table 1 are that within the next year:

---

[2] Within VMware, this capability is referred to as VMotion.

Table 1: Deployment of Virtualized Servers					
	None	**1% to 25%**	**26% to 50%**	**51% to 75%**	**76% to 100%**
Have already been virtualized	30%	34%	17%	11%	9%
Expect to be virtualized within a year	22%	25%	25%	16%	12%

- The number of IT organizations that have not implemented server virtualization will be cut by over twenty five percent.
- The number of IT organizations that have virtualized the majority of their servers will grow by forty percent.

As previously noted, two of the factors that are currently driving the movement to virtualize data center servers are the ability to dynamically provision VMs and the ability to dynamically move VMs among physical servers. As shown in **Table 2**, 46% of The Survey Respondents indicated that the dynamic provisioning of VMs will be of either significant or very significant importance to them by early 2011. This is a notable increase from the 29% of The Survey Respondents who indicated that this capability was currently either of significant or very significant importance to them.

The combination of the ease and speed with which VMs can be provisioned and migrated within and potentially among data centers has led many IT organizations to create initiatives to further leverage virtualization throughout their IT infrastructure. The goal of these initiatives is to have an infrastructure that has the ability to provide each application and network service with the required resources even as the demand for each service fluctuates dynamically. The ultimate in *elastic computing* (a.k.a., on-demand computing) is realized when the demand for infrastructure resources can be met with instant-on, real-time delivery of virtualized network services.

Table 2: Importance of Dynamically Provisioning VMs		
	Importance Currently	**Importance in a Year**
Very Significant Importance	13%	23%
Significant Importance	16%	23%
Moderate Importance	20%	24%
Slight Importance	25%	15%
No Importance	26%	14%

Challenges of Server Virtualization

One way to think about the current generation of virtualized data centers, and the related management challenges, draws on the concept of a fractal[3]. A fractal is a geometric object that is similar to itself on all scales. If you zoom in on a fractal object it will look similar or exactly like the original shape. This property is often referred to as self-similarity.

The relevance of fractals is that the traditional data center is comprised of myriad physical devices including servers, LAN switches and firewalls. The virtualized data centers that most IT organizations are in the process of implementing are still comprised of physical servers, LAN switches and firewalls. In addition, these data centers house servers which have been virtualized and which are comprised of a wide range of functionality including virtual machines, a virtual LAN switch and in many cases virtual firewalls. Hence, if you take a broad overview of the data center you see certain key pieces of functionality. If you were to then zoom inside of a virtualized data center server you would see most, if not all of that same functionality. Hence, a virtualized data center can be thought of as a fractal data center.

Because of the fractal nature of a virtualized data center, many of the same management tasks that must be performed in the traditional server environment need to be both extended into the virtualized environment and also integrated with the existing workflow and management processes. One example of the need to extend functionality from the physical server environment into the virtual server environment is that IT organizations must be able to automatically discover both the physical and the virtual environment and have an integrated view of both environments. This view of the virtual and physical server resources must stay current as VMs move from one host to another, and the view must also be able to indicate the resources that are impacted in the case of fault or performance issues.

Some of the other specific challenges that server virtualization poses for the network infrastructure and network management include:

Contentious Management of the vSwitch

Each virtualized server includes at least one software-based virtual switch, and at least in the first generation of server virtualization, each of these switches had to be configured and managed manually as a separate entity. Another aspect of the management difficulty associated with server virtualization is that the server management team typically manages the new access layer that is comprised of virtual switches, while the rest of the data center network is the responsibility of the networking team. The combination of dual access layers (e.g., the new access layer

---

[3] http://www.pha.jhu.edu/~ldb/seminar/fractals.html

inside of the virtualized server and the traditional access layer in the data center network) and split responsibilities increases the complexity of the virtualized data center network and reduces the efficiency of management. These effects become dramatically more evident as the number of virtualized servers increases.

Breakdown of Network Design and Management Tools

As the virtual IT infrastructure becomes more dynamic in order to deliver on-demand application delivery, the traditional approach to network design and the associated labor-intensive management tools that are typically used to control and manage the IT infrastructure will not be able to keep pace with the frequent, dynamic changes that are required. For example, the traditional approach to data center network design is based on the concept of interconnecting and managing relatively static physical devices. This approach has two fundamental limitations when used to support virtualized servers. One limitation is that the workload for the operational support staff can spiral out of control due to the constant stream of configuration changes that are needed to support the dynamic provisioning and movement of VMs. The second limitation is that even if IT organizations had enough support staff to implement the necessary configuration changes, the time to support these changes is typically measured in days and weeks. In order to truly have a dynamic IT infrastructure, these changes must be made in the same amount of time that it takes to provision or move a VM; i.e., seconds or minutes.

Poor Management Scalability

The ease with which new VMs can be deployed has often led to VM proliferation, or VM sprawl. This introduces new management challenges relative to tracking VMs and their consumption of resources throughout their life cycle. In addition, the normal best practices for virtual server configuration call for creating separate VLANs for the different types of traffic to and from the VMs within the data center. While not all of these VLANs need to be routable, they all must be managed. The combined proliferation of virtualized servers, VMs, and VLANs places a significant strain on the manual processes traditionally used to manage servers and the supporting infrastructure. The problem of scalability places an emphasis on management tools that can provide some degree of integration by being able to manage homogenous, or even somewhat heterogeneous, collections of physical and virtual data center entities as a single system.

Multiple Hypervisors

As recently as 2009, VMware was the dominant hypervisor vendor. Today, VMware is still the most commonly used hypervisor. It is, however, becoming increasingly common to find IT organizations using other hypervisors, including Xen from Citrix, KVM (Kernel-based Virtual Machine) from Red Hat and Hyper-V from Microsoft.

One of the challenges associated with having multiple hypervisors is that each comes with their own management system. This means that IT organizations need to learn multiple management interfaces. Another challenge associated with having multiple hypervisors is that the management functionality provided by each hypervisor varies as does the degree to which each hypervisor management system is integrated with other management systems. As a result, the IT organization's ability to manage VMs and the associated data center infrastructure will vary based on which hypervisor supports which groups of VMs.

Limited VM-to-VM Traffic Visibility

Prior to server virtualization, IT organizations were able to leverage their data center LAN access and aggregation switches in order to monitor the traffic that flowed between servers. With traditional hardware switches, however, it is not generally possible to monitor traffic or to apply network security policy to the traffic that is switched between VMs on the same physical server by the first generation of hypervisor virtual switch (vSwitch). That follows because the first generation of virtual switches embedded within the hypervisor generally don't have the same extensive traffic monitoring features and port mirroring features as physical access switches. For example, while most embedded virtualization management tools can identify the total volume of traffic within the entire virtual environment, they cannot provide information on individual network services such as HTTP or FTP. This lack of management insight can dramatically limit the ability of the IT organization to be able to do granular security filtering and performance monitoring and/or troubleshooting within virtualized server domains.

Inconsistent Network Policy Enforcement

Traditional vSwitches can lack some of the advanced features that are required to provide the degree of traffic control and isolation required in the data center. This includes features such as private VLANs, quality of service (QoS), and extensive access control lists (ACLs). Even when vSwitches support some of these features, they often must be configured manually through the virtual server management application and may not be fully compatible with similar features offered by physical access switches. This situation results in difficulties in implementing consistent end-to-end network policies.

Complex Troubleshooting on a per-VM Basis

Most IT organizations have deployed a form of distributed computing often referred to as *n-tier applications*. The typical 4-tier application (Figure 2) is comprised of a Web browser, a Web server, an application server and a database server. Even in the traditional environment in which the servers that support the application are not virtualized, when the performance of the application degrades it is typically noticed first by the end user and not by the IT organization. In addition, when the IT organization is made aware of the fact that the performance of the application has degraded, it often takes a considerable amount of time to find the root cause of the degradation.

Figure 2: A 4-Tier Application

End Users — LAN — WAN — Web Servers — Application Servers — Database Servers
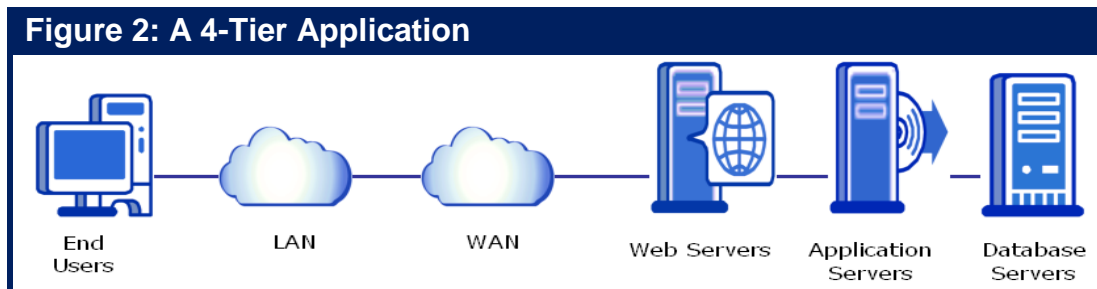
As previously noted, many of the same management tasks that must be performed in the traditional server environment need to be extended into the virtualized environment. Another example of this is that IT organizations must be able to troubleshoot on a per-VM basis.

To put the challenge of troubleshooting on a per-VM basis into perspective, consider a hypothetical 4-tier application that will be referred to as TheApp. For the sake of this example, assume that TheApp is implemented in a manner such that the web server, the application server and the database server are each running on VMs on separate servers, each of which have been virtualized using different hypervisors. It is notably more difficult to troubleshoot TheApp than it is to troubleshoot the traditional 4-tier application in part because each server has a different hypervisor management system and in part because of the lack of visibility into the inter-VM traffic on a given physical server.

Manual Network Reconfiguration to Support VM Migration

As previously discussed, many of the benefits of on-demand computing depend on the ability to migrate VMs among physical servers located in the same data center or in geographically separated data centers. The task of moving a VM is a relatively simple function of the virtual server management system. There can, however, be significant challenges in assuring that the VM's network configuration state (including QoS settings, ACLs, and firewall settings) is also transferred to the new location. In

the vast majority of instances today, making these modifications to complete the VM transfer involves the time-consuming manual configuration of multiple devices.

Regulatory compliance requirements can further complicate this task. For example, assume that the VM to be transferred is supporting an application that is subject to PCI compliance. Further assume that because the application is subject to PCI compliance that the IT organization has implemented logging and auditing functionality. In addition to the VM's network configuration state, this logging and auditing capability also has to be transferred to the new physical server.

Over-subscription of Server Resources

The RoI that is associated with server virtualization tends to increase as the number of VMs that are supported by physical server increases. However, the more VMs per server the higher the traffic load and the greater the number of CPU cycles that are required to move traffic through a software-based virtual switch. What this means is that in those instances in which a high percentage of the physical server's CPU cycles are required to support the applications that reside in the VMs, a high percentage of the physical server's CPU cycles are also required to switch the traffic between the VMs inside the physical server and between the VMs and the physical LAN switch to which the physical server is connected.

With a desire to cut cost and to reduce the need for new server acquisitions, there is the tendency for IT organizations to combine too many VMs onto a single physical server. The over subscription of VMs onto a physical server can result in performance problems due to factors such as limited CPU cycles or I/O bottlenecks. While these problems can occur in a traditional physical server, they are more likely to occur in a virtualized server due to consolidation of too many resources onto a single physical server.

Layer 2 Network Support for VM Migration

When VMs are migrated, the network has to accommodate the constraints imposed by the VM migration utility; e.g., VMotion. Typically the source and destination servers have to be on the same VM migration VLAN, the same VM management VLAN, and the same data VLAN. This allows the VM to retain its IP address, which helps to preserve user connectivity after the migration. When migrating VMs between disparate data centers, these constraints require that the data center LAN be extended across the physical locations or data centers without compromising the availability, resilience, and security of the VM in its new location. VM migration also requires the LAN extension service have considerable bandwidth and low latency. VMware's VMotion, for example, requires at least 622 Mbps of bandwidth and less

than 5 ms of round trip latency between source and destination servers over the extended LAN[4].

The speed of light in a combination of copper and fiber is roughly 120,000 miles per second. In 5 ms, light can travel about 600 miles. Since the 5 ms is round trip delay, that means that the data centers can be at most 300 miles apart. That 300 mile figure assumes that the WAN link is a perfectly straight line between the source and destination ESX servers and that the data that is being transmitted does not spend any time at all in a queue in a router or other device. Both of those assumptions are unlikely to be the case and hence the maximum distance between data centers is less than 300 miles.

Storage Support for Virtual Servers and VM Migration

The data storage location, including the boot device used by the virtual machine, must be accessible by both the source and destination physical servers at all times. If the servers are at two distinct locations and the data is replicated at the second site, then the two data sets must be identical. One approach is to extend the SAN to the two sites and maintain a single data source. Another approach is migrate the data space associated with a virtual machine to the secondary storage location. In each case it is necessary to coordinate the VM and storage migrations, which may be problematical without integration of the storage subsystems under the virtual server management system.

Meeting the Challenges of Server Virtualization

At the present time, there is no overarching solution for the comprehensive management of a computing environment composed of virtualized servers, storage, and networks. Vendors, however, are beginning to address the challenges previously described by enhancing the functionality of their products with virtualization features, automation, and support for some level of integration - primarily with the virtual server management system. IT organizations, however, need to avoid introducing a new suite of management tools every time they introduce a new technology such as virtualized servers. This approach is too expensive and creates additional management silos. To avoid the proliferation of management tools, IT organizations need to identify a core suite of tools that can evolve to span or eliminate the traditional boundaries between physical and virtual infrastructure elements.

The remainder of this section of the report will describe some the key developments that can help IT departments meet the challenges of virtualization.

---

[4] http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9402/white_paper_c11-591960.pdf

Dynamic Infrastructure Management

A dynamic virtualized environment can benefit greatly from a highly scalable and integrated DNS/DHCP/IPAM solution, which is also well integrated with the virtual server management system. Where DNS/DHCP/IPAM share a common database, the integration obviates the need to coordinate records in different locations and allows these core services to accommodate any different addressing and naming requirements of physical and virtual servers. Potential advantages of this approach include the automated generation of IP addresses for newly created VMs, the automated allocation of subnets for new VLANs, and the population of an IP address database with detailed information about the current location and security profiles of VMs. The integration of infrastructure utilities with the virtual server management system can also facilitate automated changes to the DHCP and DNS databases.

Virtualized Performance and Fault Management

Another example of a management capability in the traditional physical environment that is important to implement in a virtual environment is adaptive performance thresholding. This capability identifies systemic deviations from normal as well as time over threshold violations, and can automatically update thresholds based on changes to historic levels of utilization. That same capability is needed in a virtualized environment so that IT organizations can monitor the performance of individual VMs.

Virtual switches currently being introduced into the market can export traffic flow data to external collectors in order to provide some visibility into the network flows between and among the VMs in the same physical machine. Performance management products are currently beginning to leverage this capability by collecting and analysing intra-VM traffic data. Another approach to monitoring and troubleshooting intra-VM traffic is to deploy a virtual performance management appliance or probe within the virtualized server[5]. This approach has the advantage of potentially extending the fault and performance management solution from the physical network into the virtual network by capturing VM traffic at the packet level, as well as the flow level.

While changes in the virtual topology can be gleaned from flow analysis, a third approach to managing a virtualised server is to access the data in the virtual server management system. Gathering data from this source can also provide access to additional performance information for specific VMs, such as CPU utilization and memory utilization.

---

[5] This will be discussed in the section on virtual appliances.

Distributed Virtual Switching (DVS)

As noted earlier, with server virtualization each physical server comes with a virtual switching capability that allows connectivity among VMs on the same physical platform. The first generation virtual switch includes a data plane implemented in software, as well as an integral control plane with fairly limited functionality. With DVS, the control and data planes of the embedded virtual switch are decoupled. This allows the data planes of multiple virtual switches to be controlled by an external centralized management system that implements the control plane functionality. Decoupling the data plane from the control plane makes it easier to tightly integrate the virtual switch control plane with the control planes of physical access and/or aggregation switches and/or the virtual server management system.

DVS will be discussed in greater detail in the forthcoming report entitled *Cloud Networking.*

Edge Virtual Bridges (EVBs)

Edge Virtual Bridges constitute an alternative to virtualization of the edge of the network via DVS and virtual appliances. With EVB, the hypervisor is relieved from all switching functions, which are now all performed by the physical access and aggregation network. The IEEE 802.1 Work Group is creating a standard called Edge Virtual Bridging. The EVB standards work is based on a technology known as Virtual Ethernet Port Aggregator (VEPA). Using VEPA, all traffic from VMs is forwarded to the adjacent physical access switch and directed back to the same physical server if the destination VM is co-resident on the same server.

EVBs will be discussed in greater detail in *Cloud Networking.* Single Root I/O Virtualization (SR-IOV) will also be discussed in that report. SR-IOV will enable hardware NICs to support software-based virtual switch functionality.

Orchestration and Provisioning

Service orchestration is an operational technique that helps IT organizations automate many of the manual tasks that are involved in provisioning and controlling the capacity of dynamic virtualized services. By automatically coordinating provisioning and resource reuse across servers, storage, and networks, service orchestration can help IT organizations streamline operational workloads and overcome technology and organizational silos and boundaries. Orchestration engines use business policies to define a virtual service and to translate that service into the required physical and virtual resources that are needed for deployment. The orchestration engine then disseminates the needed configuration commands to the appropriate devices across the network in order to initiate the requested service. The orchestration engine can automatically initiate the creation of the required virtual machines while simultaneously deploying the network access and security models

across all of the required infrastructure components. This includes routers, switches, security devices, and core infrastructure services. The entire process can allow setup and deployment of network routes, VPNs, VLANs, ACLs, security certificates, firewall rules and DNS entries without any time consuming manual entries via device-specific management systems or CLIs.

Orchestration engines are generally limited in the range of devices with which they can interface due to differences in device and/or vendor management interfaces. Therefore, orchestration solutions mirror to some extent the constraints of virtual data center solutions that result from vendor partnerships among manufacturers of virtual server software, networks, and networked storage. The initial focus of such partnerships has been on promulgating validated network designs and architectures rather than on fully integrated or automated management. The next logical step for such partnerships is to include orchestration capabilities.

Orchestration solutions would benefit greatly from the emergence of an open standard for the exchange of information among the full range of devices that may be used to construct a dynamic virtual data center. In the Cloud Computing arena there are a number of standards under development, including the Open Cloud Computing Interface (OCCI) from the Open Grid Forum. These standards activities may also provide value within the enterprise virtual data center, since the stated scope of the specification is to encompass "all high level functionality required for the life-cycle management of virtual machines (or workloads) running on virtualization technologies (or containers) supporting service elasticity".

IF-MAP is another emerging standard proposed by the Trusted Computing Group and implemented by a number of companies in the security and network industries. It is a publish/subscribe protocol that allows hosts to lookup meta-data and to subscribe to service or host-specific event notifications. IF-MAP can enable auto-discovery and self-assembly (or re-assembly) of the network architecture. As such, IF-MAP has the potential to support automation and dynamic orchestration of not only security systems but also other elements of the virtual data center. For example, IF-MAP could facilitate automation of the processes associated with virtual machine provisioning and deployment by publishing all of the necessary policy and state information to an IF-MAP database that is accessible by all other elements of the extended data center.

Virtual firewall appliances can also help IT organizations respond to the challenges that are associated with server virtualization. These will be discussed in the subsequent section of this report that is entitled *Virtual Appliances*.

Desktop[6] Virtualization

The challenge of managing applications and desktop environments across the enterprise is becoming considerably more formidable as the range of applications that support employee productivity and business operations continues to grow. IT organizations are often stretched to the limit performing routine operational tasks such as:

- Deploying applications and application upgrades
- Provisioning new desktop systems
- Installing patches to keep desktop machines and applications up-to-date
- Securing systems and data from intrusions
- Providing help desk support
- Maintaining control of the PC environment to ensure demonstrable compliance with regulatory mandates

The challenge of managing applications is exacerbated in part by the increasing percentage of the employee population that is located in a branch office, a home office or is mobile. The growing number of remote and mobile workers presents IT organizations with the challenge of being able to centrally manage each of the tasks listed above without deploying an inordinate number of management tools. Remote locations differ from central facilities in that they often require more stringent security measures due to a lack of physical security and the frequent presence of guests, business partners and other visitors.

Desktop virtualization centralizes the management of complete desktops or individual desktop applications. Centralization simplifies management operations and allows a single maintenance operation to span a large number of virtualized desktops. There are a number of different approaches to desktop virtualization, but they all are share the concept that the desktop or application is virtualized in the sense that it appears to be installed on the client device when that is not actually the case.

The two fundamental forms of desktop virtualization are:

- Server-side application/desktop virtualization
- Client-side application/desktop virtualization

With server-side virtualization, the client device plays the familiar role of a terminal accessing an application or desktop hosted on a central presentation server. There are two primary approaches to server-side application/desktop virtualization. They are:

---

[6] In this context, the term 'desktop' refers to the tradition desktop as well as to various mobile devices including laptops and smartphones.

- Server Based Computing (SBC)
- Virtual Desktop Infrastructure (VDI)

IT organizations have been using the SBC approach to virtualization for a long time and often refer to is as Terminal Services. In the SBC approach the terminal server functions in a fashion similar to a time-shared multi-user computer. Virtual Desktop Infrastructure (VDI) is a relatively new variation on the overall server-side form of virtualization where a VM on a central server is dedicated to host a single virtualized desktop.

Client-side application virtualization is based on a model in which applications are streamed on-demand from central servers to client devices over a LAN or a WAN. On the client-side, streamed applications are isolated from the rest of the client system by an abstraction layer inserted between the application and the local operating system. In some cases, this abstraction layer could function as a client hypervisor isolating streamed applications from local applications on the same platform.

Figure 3: Client-side and Server-side Desktop Virtualization
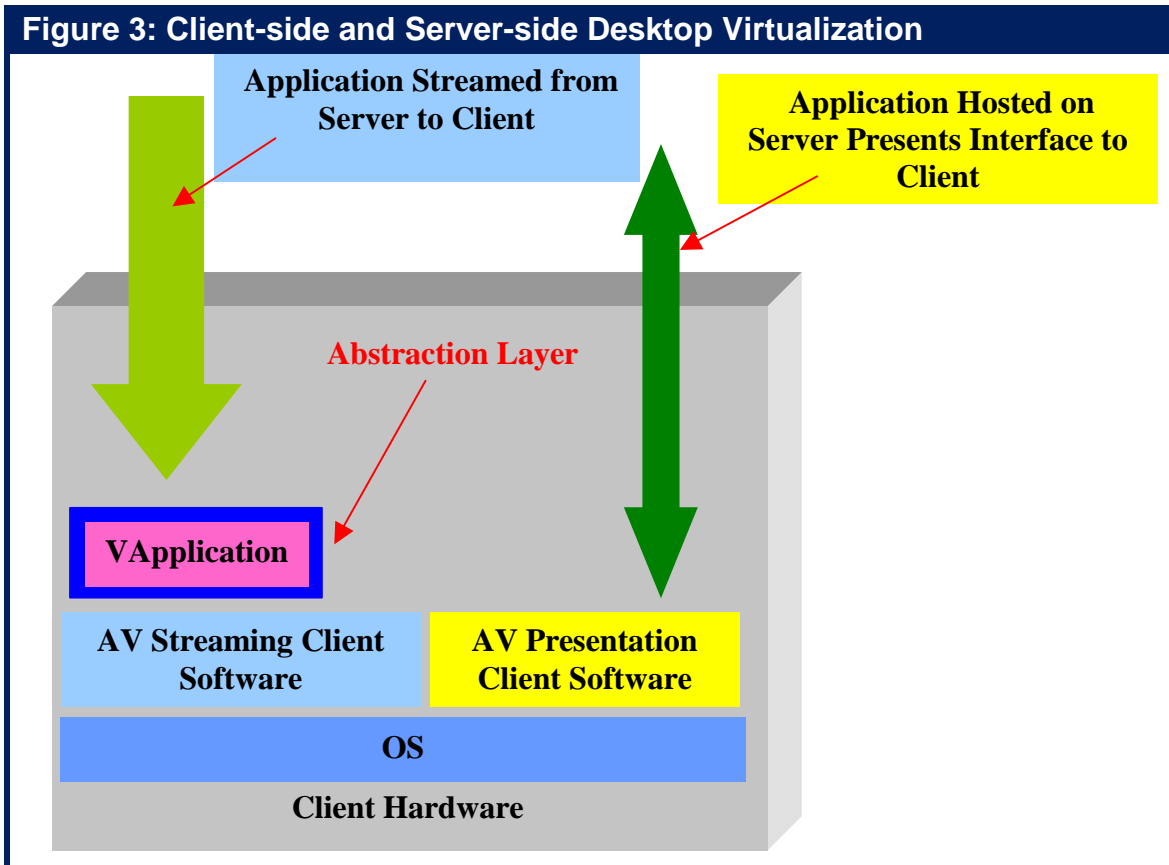
Figure 3 shows a client system that supports client-side and server-side virtualization models at the same time. For the server-side (or hosted) virtualization shown on the right-hand side of Figure 3, only screen displays, keyboard entries, and mouse movements are transmitted across the network. This approach to virtualization is based on display protocols such as Citrix's Independent Computing Architecture (ICA) and Microsoft's Remote Desktop Protocol (RDP). Hosted application virtualization does not require the client device to have a full-functioned operating system. As such, a primary advantage of hosted application virtualization is that the application can be securely accessed from home PCs, airport Internet kiosks, smart phones, and other thin client devices.

The left-hand side of Figure 3 shows a client system accessing a streamed client-side virtualized application. Application streaming is selective in the sense that only the required application libraries are streamed to the user's device. The streamed application's code is isolated and not actually installed on the client system. The user can also have the option to cache the virtual application's code on the client system. Caching greatly reduces the volume of download traffic for streamed applications and is particularly effective for applications that are infrequently updated. Caching also allows applications to be run locally on the client without the use of streaming in the event of network outages or other situations where the user's device lacks network connectivity.

Adoption of Desktop Virtualization

The data in **Table 3** shows the current and planned deployment of desktop virtualization as reported by the Interop Survey respondents. While a comparison of the data in Tables 2 and 3 indicates that there is less interest in desktop virtualization than there is in server virtualization, the data in Table 3 also indicates that within the next year:

- The number of IT organizations that have virtualized the majority of their desktops will almost double.
- The number of IT organizations that have not implemented desktop virtualization will be cut in half.

Table 3: The Percentage of Desktops that Already Have or Will be Virtualized					
	None	**1% to 25%**	**26% to 50%**	**51% to 75%**	**76% to 100%**
Have already been virtualized	49.5%	34.7%	8.9%	1.0%	5.9%
Expect to be virtualized within a year	22.0%	46.3%	18.3%	7.3%	6.1%

Respondents to the survey indicated that the primary factors driving their adoption of desktop virtualization are a reduction in the overall cost, primarily because of lower OPEX costs for maintenance and support; an improvement in data and application security and an enhanced ability to comply with security regulations.

Challenges of Desktop Virtualization

From a networking perspective, the primary challenge in implementing desktop virtualization is achieving adequate performance and an acceptable user experience for client-to-server connections over a WAN. The ICA and RDP protocols employed by many hosted application virtualization solutions are somewhat efficient in their use of the WAN because they incorporate a number of compression techniques including bitmap image compression, screen refresh compression and general data compression. While these protocols can often provide adequate performance for traditional data applications, they have limitations with graphics-intensive applications, 3D applications, and applications that require audio-video synchronization.

To respond to the challenges created by these types of applications, Citrix introduced High Definition user eXperience (HDX™) technology into XenDesktop 4. HDX is intended to support the remote display of multimedia, voice, video, and 3D graphics on client devices. Citrix HDX is comprised the following categories:

- HDX Broadcast – Ensures high-performance of virtual desktops and applications over any network, including high-latency and low-bandwidth environments.
- HDX WAN Optimization – Optimizes performance by caching bandwidth intensive data and graphics and delivering them from the most efficient location.
- HDX MediaStream – Accelerates multimedia performance through compression or when possible, through redirection and client-side rendering.
- HDX RealTime – Enhances real-time voice and video using advanced encoding and streaming to ensure a no compromise end-user experience.
- HDX 3D – Optimizes the performance of everything from graphics-intensive 2D environments to advanced 3D geospatial applications using software and hardware based rendering in the datacenter and on the device.
- HDX Plug-n-Play – Enables simple connectivity for all local devices in a virtualized environment, including USB, multi-monitor, printers and peripherals.

A relatively recently developed display protocol is the PC-over-IP (PCoIP) protocol from Teradici Corporation. PCoIP is a proprietary protocol that renders the graphics images on the host computer and transfers compressed pixel level data to the client device. PCoIP is compatible with *zero clients*. These are user display devices that have no operating system and no processor.

PCoIP is the display protocol used by the recently introduced VMware View 4 VDI product, which also supports RDP. A recently published document[7] stated that, "To support the lower bandwidth typically available over a WAN, the minimum peak bandwidth required for a PCoIP connection has been reduced to 1 Mbps." While the 1 Mbps required by PCoIP to support a single user represents a worst-case situation, it does underscore the fact that a significant amount of WAN bandwidth can be required to support desktop virtualization.

The bandwidth requirements of PCoIP also highlight the fact that before implementing desktop virtualization, IT organizations need to understand the network implications of that implementation. One of those implications is that other WAN traffic such as large file transfers, can negatively impact the user's experience with desktop virtualization. To avoid this situation, QoS needs to be implemented throughout the WAN.

Another implication of implementing desktop virtualization is that a large amount of WAN bandwidth may be required. As noted, IT organizations have been using the SBC approach to server side virtualization for a long time. As such, the bandwidth requirements of SBC are well known to be between 20 Kbps and 30 Kbps per simultaneous user[8]. Hence, if there are fifty simultaneous users in an office, that requires between 1 Mbps and 1.5 Mbps just to support desktop virtualization.

Identifying the bandwidth requirements of VDI is more difficult in part because it is a newer approach to desktop virtualization and in part because the bandwidth requirements will vary based on a number of factors. These factors include the particular display protocols being used and the types of tasks being performed. One recently published article[9] discussed the bandwidth requirements of VDI and stated, "If you're a typical worker who uses Microsoft Office and not much else, 200 kilobits of network bandwidth is probably enough. But for workers who need video streaming and 3D graphics rendering, those network requirements can scale to the hundreds of megabits."

A recent entry in The Citrix Blog[10] gave the following estimates (**Table 4**) for the amount of WAN bandwidth required by XenDesktop.

---

[7] http://www.teradici.com/media/resources/PCoIP-WAN-brief.pdf

[8] http://www.virtualizationadmin.com/articles-tutorials/terminal-services/performance/poor-bandwidth-latency.html

[9] http://www.pcworld.idg.com.au/article/341933/5_virtual_desktop_pitfalls/?

[10] http://community.citrix.com/display/ocb/2010/05/20/How+Much+Bandwidth+Do+I+Need+for+My+Virtual+Desktop

Table 4: VDI Bandwidth Requirements

Activity	XenDesktop Bandwidth
Office	43 Kbps
Internet	85 Kbps
Printing	553 – 593 Kbps
Flash Video	174 Kbps
Standard WMV Video	464 Kbps
High Definition WMV Video	1,812 Kbps

The entries in the right hand column of Table 4 represent the WAN bandwidth requirements for each simultaneous user of the corresponding activity listed in the left hand column. As before, if there were fifty simultaneous users in a branch office, the total WAN bandwidth requirement would be the sum of what was required by the fifty users. **Table 5** depicts one possible scenario of what fifty branch office users are doing and identifies that the total WAN bandwidth that is required by this scenario is just less than 16 Mbps.

Table 5: Bandwidth Requirements from a Branch Office

Activity	XenDesktop Bandwidth	Number of Simultaneous Users	WAN Bandwidth Required
Office	43 Kbps	10	430 Kbps
Internet	85 Kbps	15	1,275 Kbps
Printing	573 Kbps	15	8,595 Kbps
Flash Video	174 Kbps	6	1,044 Kbps
Standard WMV Video	464 Kbps	2	928 Kbps
High Definition WMV Video	1,812 Kbps	2	3,624 Kbps
Total WAN Bandwidth			15,896 Kbps

Compared with hosted applications, streamed applications are far less efficient as they typically use the same inefficient protocols that are native to the application. Furthermore, streamed applications create additional challenges for the IT organization because of the much larger amount of data that must be transmitted across the WAN when the application is initially delivered to the branch.

Meeting the Challenges of Desktop Virtualization

IT organizations that are implementing virtualized desktops should analyze the viability of implementing WAN and application optimization solutions such as those

described in the 2009 Application Delivery Handbook[11]. Some of the general WAN optimization techniques described in the handbook include:

- Compression
- Caching and de-duplication
- TCP Protocol optimization
- Application and protocol (e.g., CIFS, HTTP, MAPI) optimization
- Protocol (e.g., ICA, RDP, PCoIP) optimization
- QoS and traffic shaping

Although virtually all WAN Optimization Controllers (WOCs) on the market support the functions listed above, there are some significant differences in terms of how the functionality is implemented and how well it performs. For example, the ICA and RDP protocols can be difficult to optimize for a number of reasons. One of those reasons is that these protocols only send small request-reply packets. This form of communications is best optimized by byte-level caching that is not supported by many WOC vendors. In addition, some WOC vendors provide functionality not included in the above list. Implementers of desktop virtualization need to understand these differences in the context of the applications they want to virtualize and the models of desktop virtualization that they want to deploy. A recent report[12] provides insight into the primary WOC vendors and their products.

As shown in **Table 6**, techniques such as byte level compression, caching, protocol (e.g., ICA, RDP) optimization, and QoS can provide benefits for hosted applications. Before implementing them, however, an IT organization must determine which acceleration techniques are compatible with the relevant display protocols. For example, in order to be able to compress ICA traffic, a WOC must be able to decrypt the ICA workload, apply the optimization technique, and then re-encrypt the data stream.

In order to enable the growing population of mobile workers to access enterprise applications as easily as do workers in branch offices, the communications between the mobile worker and the data center (whether it is owned by the enterprise or a third party provider such as a cloud computing service provider) has to be optimized. One way to optimize this communications is to deploy client software on the user's mobile device that provides WOC functionality. Until recently, the typical device that mobile workers used to access enterprise applications was a laptop. While that is still the most common scenario, today many mobile workers use their smartphones to access enterprise applications. Therefore, over the next few years it is reasonable to expect that many IT organizations will support the use of smartphones as an access device by implementing server-side application virtualization for those devices. This

---

[11] http://webtorials.com/abstracts/2009-Application-Delivery-Handbook.htm
[12] http://searchenterprisewan.techtarget.com/generic/0,295582,sid200_gci1381156,00.html

Table 6: Applicability of Common WAN Optimization Techniques	Streamed Applications	Hosted Applications
Block Level Compression	X	
Byte Level Compression	X	X
Caching	X	X
Staging	X	
Protocol Optimization (e.g., TCP, IP, UDP)	X	X
Protocol Optimization (e.g., ICA, RDP)		X
Protocol Optimization (e.g., CIFS, HTTP, MAPI)	X	
QoS	X	X

means that in a manner somewhat similar to remote workers, mobile workers will access corporate applications by running protocols such as ICA and RDP over a WAN.

Just as was the case with workers who access applications from a fixed location, in order for mobile workers to be able to experience acceptable application performance, network and application optimization is required. In many cases the mobile worker will use some form of wireless access. Since wireless access tends to exhibit more packet loss than does wired access, the WOC software that gets deployed to support mobile workers needs functionality such as forward error correction that can overcome the impact of packet loss. In addition, as workers move in and out of a branch office, it will be necessary for a seamless handoff between the mobile client and the branch office WOC.

Many IT organizations resist putting any more software on the user's device. In addition, many users resent having multiple clients (e.g., WOC, SSL VPN, IPSec VPN, wireless/cellular access) that are not integrated on their access device. On a going forward basis, IT organizations should look to implement WOC software that is integrated with the other clients used by mobile workers.

A recently developed proprietary solution, the Experience Optimization Protocol (EOP)[13] is part of Quest Software's vWorkspace integrated platform for desktop virtualization. vWorkspace is intended to provide a unified solution for hosted applications delivered from heterogeneous environments of virtualized servers, terminal servers, or blade PCs. vWorkspace is compatible with multiple server hypervisors, but provides its own server-side and client-side software for application

---

[13] EOP and Xstream are alternatively looked at as display protocols and as optimization techniques.

delivery. For terminal services, there is some integration with Microsoft Remote Desktop Services.

The EOP display protocol accelerates the display of images and multimedia content. EOP's Xstream provides further acceleration of EOP and RDP traffic on high latency WAN links. vWorkspace also supports other remote display technologies, including HP's Remote Graphics Software (RGS), Wyse's Thin Client Experience (TCX) and Virtual Desktop Accelerator (VDA). RGS is a remote display solution that might be applicable to terminal-style access to hosted applications, but is optimized for collaborative screen-sharing sessions. Like PCoIP, RGS applies compression at the pixel level. TCX and VDA work in conjunction with ICA and RDP to enhance thin client access to hosted applications and desktops.

Table 7 provides an overview of the display protocols currently supported by VDI vendors. Table 7 is not intended to be a complete listing of display protocols. Rather, Table 7 is intended to highlight the breadth of protocols that IT organizations may need to support and optimize if they implement VDI.

Table 7: Vendor Support of Remote Display Protocols		
Vendor	**VDI Product**	**Display Protocols**
VMware	View	RDP, PCoIP
Citrix	XenDesktop	ICA, HDX
Microsoft	VDI Premium Suite	RDP7
Red Hat	Desktop Virtualization	SPICE
Quest Software	Vworkspace	EOP, RDP, EOP Xstream
Sun	Sun Ray	Appliance Link Protocol (ALP)

As previously noted, application streaming creates some significant WAN performance problems that require the deployment of a WOC. For example, the code for streamed applications is typically transferred via a distributed file system protocol, such as CIFS, which is well known to be a chatty protocol. Hence, in order effectively support application streaming, IT organizations need to be able to optimize the performance of protocols such as CIFS, MAPI, HTTP, and TCP. In addition, IT organizations need to implement other techniques that reduce the bandwidth requirements of application streaming. For example, by using a WOC, it is possible to cache the virtual application code at the client's site. Caching greatly reduces the volume of traffic for client-side virtualized applications and it also allows applications to be run locally in the event of network outages. Staging is a technique that is similar to caching but is based on pre-positioning and storing streamed applications at the branch office on the WOC or on a branch server. With staging, the application is already locally available at the branch when users arrive for work and begin to access their virtualized applications.

Whether it is done by the WOC itself, or in conjunction with the WOC, supporting application virtualization will require that IT organizations are able to apply the right mix of optimization technologies for each situation. For example, pre-staging and storing large virtual desktop images on the WOC at the branch office must be done in an orchestrated fashion with the corresponding resources in the data center. Another example of the importance of orchestration is the growing requirement to automatically apply the right mix of optimization technologies. For example, as noted protocols such as ICA and RDP already incorporate a number of compression techniques. As a result, any compression performed by a WAN optimization appliance must adaptively orchestrate with the hosted virtualization infrastructure to prevent compressing the traffic twice - a condition that can actually increase the size of the compressed payload.

Virtual Appliances

A *Virtual Appliance* is based on network appliance software, together with its operating system, running in a VM on top of the hypervisor in a virtualized server. Virtual appliances can include WOCs, ADCs, firewalls, and performance monitoring solutions among others[14]. An important set of synergies exist between virtual servers, virtual appliances such as a WOC or a performance monitoring solution and virtual desktops. Throughout the rest of this report, those synergies will be referred to as the Virtuous Synergies of Virtualization (VSV). The key components of the VSV are depicted in **Table 8**.

A cornerstone of the VSV is that virtual appliances are of particular interest to IT organizations in those instances in which server virtualization technology has already been disseminated to branch offices and has also been implemented in the data center. When server virtualization pervades the enterprise, a wide variety of networking functions can be deployed wherever needed easily and cost effectively with virtual appliances, without the installation of additional hardware.

In the branch office, a suitably placed virtualized server could potentially host a virtual WOC appliance as well as other virtual appliances. Alternatively, a router or a WOC that supports VMs could also serve as the infrastructure foundation of the branch office. Virtual appliances can therefore support branch office server consolidation strategies by enabling a single device (i.e., server, router, WOC) to perform multiple functions typically performed by multiple physical devices. These physical devices include a WOC, router, firewall, IDS/IPS, DHCP/DNS server, client-side application virtualization staging server, local application server, etc.

---

[14] The argument could be made that a virtual router is a virtual appliance. Virtual routers will be discussed in *Cloud Networking*.

One of the compelling advantages of a virtualized appliance is that the acquisition cost of a software-based appliance can be notably less than the cost of a hardware-based appliance with same functionality[15]. In many cases the cost of a software-based appliance can be a third less than the cost of a hardware-based appliance. In addition, a software-based client can potentially leverage the functionality provided by the hypervisor management system to provide a highly available system without having to pay for a second appliance[16]. As a result of these cost savings, IT organizations will be able to afford to deploy virtualized appliances more broadly than they would be able to deploy hardware-based appliances.

As discussed in the preceding section of this report, WOCs that implement the appropriate techniques can make virtual desktops a viable solution for provisioning and managing branch office desktop environments. While these advantages occur whether the WOC is hardware based or software based, the fact that a virtual WOC is so much more cost effective than a hardware based WOC means that they are more likely to be deployed. Because virtual WOCs can be deployed broadly in a cost effective manner, IT organizations are more likely to be successful with desktop virtualization.

Another advantage of a virtual appliance is that it offers the potential to alleviate some of the management burdens in branch offices because most of the provisioning, software updates, configuration, and other management tasks can be automated and centralized at the data center. In addition, as previously mentioned, in many instances the benefits of the dynamic movement of a VM from one server to another are maximized if the supporting infrastructure can also be dynamically moved. If virtualized appliances have been deployed, then it is notably easier than it is in a more traditional environment for various networking functions (WOC, ADC, firewall, etc.) to be migrated along with VMs in order to replicate the VMs's networking environment in its new location.

WOC and ADC virtualization can also be leveraged to provide "acceleration as a service" to facilitate and improve performance in deployments of service-oriented environments, including SOA and SaaS. In the case of SOA, Virtual WOC and ADC images can be easily deployed to be co-resident on the virtual servers that host the various components of a geographically-distributed SOA application. In the SaaS space, virtual WOCs and ADCs can be provided as a standalone managed software service or bundled with other managed software services to increase their performance as needed. One of the features that enables the overall system to dynamically increase performance of a SaaS solution is the ability to automatically add additional virtualized ADCs (a.k.a., autoscaling) as demand increases.

---

[15] The actual price difference between a hardware-based appliance and a software-based appliance will differ by vendor.

[16] This statement makes a number of assumptions, including the assumption that the vendor does not charge for the backup software-based appliance.

A virtualized ADC makes it easy for an IT organization to package and deploy a complete application. One example of this packaging is the situation in which an entire application resides on VMs inside a physical server. The virtualized ADC that supports the application resides in the same physical server and it has been tuned for the particular application. This makes it easy to replicate or migrate that application as needed. In this case, a virtualized ADC also provides some organizational flexibility. For example, the ADC might be under the control of a central IT group or it might be under the control of the group that supports that particular application. The later is a possibility because any actions taken by the application group relative to the ADC will only impact their application.

The recent formation of the Virtual Computing Environment (VCE) has placed more emphasis on the concept of pre-packaging data center solutions. The VCE is a coalition that is comprised of Cisco, EMC, and VMware and it has the stated mission of minimizing the risk for enterprises who are deploying pervasive virtualization en route to private cloud implementations. One of the key concepts that underlies the VCE is the concept of Vblock solutions. Vblock solutions are computing systems that are pre-integrated and pre-configured. A Vblock combines virtualization, networking, storage, security, and management.

As noted in the preceding section, one approach to monitoring and troubleshooting inter-VM traffic is to deploy a virtual performance management appliance or probe (vProbe). One of the characteristics of a virtualized server is that each virtual machine only has at its disposal a fraction of the resources (i.e., CPU, memory, storage) of the physical server on which it resides. As a result, in order to be effective, a vProbe must not consume significant resources. The way that a vProbe works is similar to how many IT organizations monitor a physical switch. In particular, the vSwitch has one of its ports provisioned to be in promiscuous mode and hence forwards all inter-VM traffic to the vProbe. As a result, the use of a vProbe gives the IT organization the necessary visibility into the inter-VM traffic.

As noted in the preceding section, a virtual firewall appliance can help IT organizations meet some of the challenges associated with server virtualization. That follows because virtual firewall appliances can be leveraged to provide isolation between VMs on separate physical servers as well as between VMs running on the same physical server. Ideally, the firewall virtual appliance would use the same software as the physical firewalls already in use in the data center. The security appliance can potentially provide highly integrated functionality to help secure virtual machines, applications, and traffic. This includes firewall, VPN, anti-malware, IDS/IPS, integrity monitoring (e.g., registry changes), and log inspection functionality.

Virtualized security management makes it is possible to meet critical regulatory compliance requirements for full application segregation and protection within the confines of virtualized physical servers. Through tight integration with the virtual

server management system, firewall appliances can also be dynamically migrated in conjunction with VM migration where this is necessary to extend a trust zone to a new physical location. In addition, hypervisor APIs, such as VMware's Vsafe, can allow physical/virtual firewall consoles to monitor servers for abnormal CPU, memory, or disk activity without the installation of special agent software. With some virtual switches, such as the Cisco Nexus 1000v, it is possible to establish private VLANs (PVLANs). PVLANs are useful in restricting traffic in flexible ways. For example, DMZ VMs on a PVLAN in "Isolated mode" are able to communicate only with hosts on the non-local network.

A potential issue to keep in mind is that each virtual appliance is running in a VM, so all of the challenges of managing a virtual server environment described earlier are also applicable to virtual appliances. In particular, visibility of VM-to-VM traffic would be more critical in order to troubleshoot a virtual server environment where traffic traverses several virtual appliances on its way to a destination VM located in the same physical server. In this instance, the deployment of one form of virtual appliance, a vProbe, eliminates some of the challenges associated with implementing other forms of virtual appliances; i.e., WOCs, ADCs and firewalls.

Table 8: The Virtuous Synergies of Virtualization
The fact that IT organizations have already deployed server virtualization means that it is easier and less costly to implement virtualized appliances.
Because it is easier and less expensive to deploy a software-based appliance than it is to deploy a hardware-based appliance, they are more likely to be broadly deployed.
Because software-based WOCs can be broadly deployed, they can enable the deployment of virtual desktops.
Because vProbes can be broadly deployed, they enable IT organizations to manage the performance of applications that run on virtualized servers.
Because virtual firewalls can be broadly deployed, they enable IT organizations to meet regulatory and compliance requirements for applications that run on virtualized servers.
As part of moving a VM, virtual appliances can be easily migrated along with the VM in order to replicate the VMs's networking environment in its new location.
Because vProbes can be broadly deployed, they eliminate some of the challenges associated with other forms of virtual appliances; i.e., WOCs, ADCs and firewalls.

One of the potential downsides of a virtual appliance is performance. The conventional wisdom in our industry is that a solution based on dedicated, purpose-built hardware performs better than a solution in which software is ported to a generic piece of hardware, particularly if that hardware is supporting multiple applications.

However, conventional wisdom is often wrong. Some of the factors that enable a virtualized appliance to provide high performance include:

- Moore's law that states that the price performance of off the shelf computing devices doubles every 18 months.
- The deployment of multiple core processors to further increase the performance of off the shelf computing devices.
- The optimization of the software on which the virtual appliance is based.

Because of the factors listed above and because of the advantages that they provide, IT organizations should evaluate the performance of a virtual appliance to determine if a virtual appliance is an appropriate solution.

Another critical factor when evaluating the deployment of virtual appliances in a dynamic, on-demand fashion is the degree of integration of the virtual appliance with the virtual server management system. Ideally this management system would recognize the virtual appliances as another type of VM and understand associations between appliance VM and application VMs to allow a coordinated migration whenever this is desirable. In addition to VM migration, integration with the virtual server management system should support other management features, such as:

- Provisioning of Virtual Appliances

  Software images can be deployed and provisioned from a central location to virtual servers anywhere within the organization's infrastructure.

- Resource Scheduling and Load Balancing

  The system manager can increase the resources available to virtual appliances to meet periodic surges in application traffic. Resource changes can be made manually, scheduled, or automatically triggered by changes in performance levels. Dynamic allocation of resources facilitates higher degrees of virtual server and virtual appliance consolidation in both the data center and the remote branch office.

- Virtual Machine File System

  Support for the VM file system allows virtual appliance images to reside on any networked or directly attached storage device supported by the virtual server infrastructure; e.g., SCSI, iSCSI, Fibre Channel SAN, SATA, etc.

- High Availability

    High availability virtual server features can be leveraged to maximize the availability of virtual appliances. High availability features can automatically restart a stalled virtual appliance on the same server or move the virtual appliance to a backup server (with appropriate network connectivity) via Live Migration.

- Business Continuance/Disaster Recovery

    Virtual server environments can support a variety of Business Continuance and Disaster Recovery tools. Integration with the virtual server management systems allows virtual appliances to benefit from these tools in the same way as applications that run in VMs benefit.

Conclusions

As shown in this report, there are significant advantages to server virtualization, desktop virtualization and appliance virtualization. As was also shown, there are also some Virtuous Synergies of Virtualization.

Of the three forms of virtualization described in this report server virtualization presents the greatest benefits. It also presents the broadest set of challenges, including the:

- Contentious Management of the vSwitch
- Breakdown of Network Design and Management Tools
- Multiple Hypervisors
- Limited VM-to-VM Traffic Visibility
- Inconsistent Network Policy Enforcement
- Complex Troubleshooting on a per-VM Basis
- Manual Network Reconfiguration to Support VM Migration
- Over-subscription of Server Resources
- Layer 2 Network Support for VM Migration
- Storage Support for Virtual Servers and VM Migration

At the present time, there is no overarching solution for the comprehensive management of a computing environment composed of virtualized servers, storage, and networks. Some the key developments that can help IT departments meet the challenges of virtualization include:

- Dynamic Infrastructure Management
- Virtualized Performance and Fault Management

- Distributed Virtual Switching
- Edge Virtual Bridges
- Orchestration and Provisioning

Desktop virtualization centralizes the management of complete desktops or individual desktop applications. Centralization simplifies management operations and allows a single maintenance operation to span a large number of virtualized desktops.   The two fundamental forms of desktop virtualization are:

- Server-side application/desktop virtualization
- Client-side application/desktop virtualization

From a networking perspective, the primary challenge in implementing desktop virtualization is achieving adequate performance and an acceptable user experience for client-to-server connections over a WAN. Protocols such as ICA and RDP can often provide adequate performance for traditional data applications, but they have limitations with supporting graphics-intensive applications, 3D applications, and applications that require audio-video synchronization. For this reason, myriad other protocols such as PCoIP and HDX have recently been deployed. In many cases, these protocols consume significant WAN bandwidth.

In most cases, the successful deployment of desktop virtualization will require the deployment of WAN optimization techniques that focus on the particular characteristics of the traffic that is associated with desktop virtualization.   For example, protocols such as ICA can be difficult to optimize in part because these protocols only send small request-reply packets and in part because in order to compress ICA traffic, it is necessary to decrypt the workload, apply the optimization technique and then re-encrypt the traffic. In addition, protocols such as ICA and RDP already incorporate a number of compression techniques. As a result, any compression performed by a WAN optimization appliance must adaptively orchestrate with the hosted virtualization infrastructure to prevent compressing the traffic twice - a condition that can actually increase the size of the compressed payload.

An important set of synergies exist between virtual servers, virtual desktops and virtual appliances such as a WOC or a performance monitoring solution. Perhaps the most important synergy is that virtual appliances are of particular interest to IT organizations in those instances in which server virtualization technology has already been disseminated to branch offices and has also been implemented in the data center.   Another synergy stems from the fact that software-based appliances cost notably less than hardware-based appliances. This means that virtual appliances can be deployed more broadly which enables the broad deployment of desktop virtualization. A third synergy is that if virtualized appliances have been deployed, then it is notably easier than it is in a more traditional environment for various

networking functions to be migrated along with VMs in order to replicate the VMs's networking environment in its new location.

In the branch office, a suitably placed virtualized server could potentially host a virtual WOC appliance as well as other virtual appliances. Alternatively, a router or a WOC that supports VMs could also serve as the infrastructure foundation of the branch office. Virtual appliances can therefore support branch office server consolidation strategies by enabling a single device to perform multiple functions typically performed by multiple physical devices. A critical factor that must be considered when evaluating the deployment of virtual appliances in a dynamic, on-demand fashion is the degree of integration of the virtual appliance with the virtual server management system. Ideally this management system would recognize the virtual appliances as another type of VM and understand associations between appliance VM and application VMs in order to to allow a coordinated migration whenever this is desirable.

Rethink the Network Farm

Certe⊙n®
Accelerate Your Business

Certeon aCelera Virtual Appliance: High Performance, Scalability, and Value for Today's Dynamic Enterprise

"Productivity isn't everything, but in the long run it is almost everything." Paul Krugman, New York Times columnist and professor of Economics and International Affairs at Princeton University

High performing key applications and services are core to running a productive company. IT executives need to deliver consistent high performance services across the enterprise whether it is meeting a storage environment recovery point objective or a customer relationship management system page load time. This commitment to productivity is critical to every company's ability to generate revenue and deliver services; however, achieving this goal is difficult due to a wide variety of technical and organizational challenges.

Technologies such as virtualization and cloud computing all provide compelling solutions to many of the challenges faced by IT management trying to increase productivity while lowering costs. Unfortunately, the ability to successfully deliver the real benefits of these 21st century technologies across the globe is often dependent on 20th century appliance technology for wide area network (WAN) optimization. Appliances do not support the dynamic nature of these solutions. Virtual appliances seamlessly integrate with these and emerging technologies that enable enterprises to deliver resources and services to all users without compromising on performance, scalability, or cost reduction.

Certeon is the leading supplier of 21st century WAN optimization software solutions. aCelera virtual appliances enable enterprises to improve application performance across the WAN by up to 95 percent while reducing WAN bandwidth consumption by 65 to 95 percent. These dramatic results enable companies to leverage their virtualized infrastructures, networks, and application environments to create new revenue and service opportunities. aCelera leverages enterprises' growing virtual infrastructures, in both data centers and branches, allowing IT management to realize clear TCO benefits from saved acquisition, operations, real estate, power, cooling and maintenance/support costs in ways not possible with hardware-based WAN optimization solutions.

Figure 1: Typical deployment
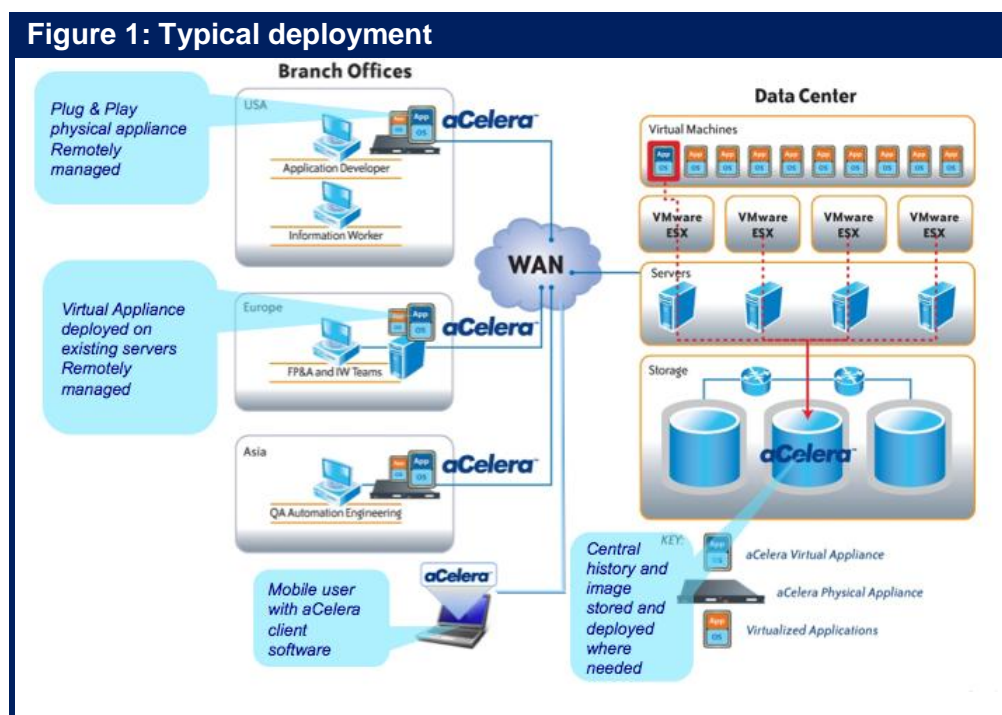
aCelera Virtual Appliances vs. Network Farm Appliances

aCelera is software running on any major hypervisor that can be provisioned and scaled using the system resources of the virtual machine (VM) environment. Hardware WAN optimization and application acceleration solutions typically host some virtualization capabilities by providing a limited virtualization session on top of the appliance's standard operating system. These appliances do not support hypervisors because the appliance design requires complete control of the system resources (CPU, memory, storage) and allocates limited capabilities for other applications**.**

aCelera WAN optimization virtual appliance software delivers:
- **Acceleration:** All WAN traffic is optimized without single purpose hardware
- **Ease of Maintenance:** VMware® VMotion and Microsoft® Quick Motion capable - a running image of aCelera can be moved from one virtual machine to another over the network without disrupting operations or traffic flow
- **High Availability:** In the event of a hard failure, virtualization management software can automatically spin up an aCelera instance on designated backup server ensuring reliable performance in the event of a failure
- **Central Management:** The aCelera instance can be deployed and provisioned via the aCelera CMS and monitored by VMware VirtualCenter or Microsoft SCVMM from central data centers to any aCelera across the enterprise
- **Dynamic Resource Scheduling (DRS):** DRS provides the ability to scale or manage Disk, CPU and memory resource allocation across virtual machines
- **True Branch in a Box Capability:** aCelera virtual appliances can share server resources with ANY other VM applications on industry standard hardware
- **Multi-purpose:** The aCelera virtual appliance can be deployed as many times and anywhere that makes sense for your application environment's topology and load: (**Figure 1**)
  - Application Acceleration
  - File Delivery Optimization
  - Backup and Replication
  - Client Support

Bottom line: Hardware appliances cannot take advantage of the scalability, flexibility and manageability benefits of virtualization. aCelera virtual appliance software leverages all of these capabilities.

Virtualization of Enterprise Network Features

Conditioned to buying their way out of transport challenges by adding capacity with next generation hardware or additional network bandwidth, enterprises are finding more challenges when dealing with today's virtualized server and storage environments. Many enterprises are thinking of moving internal IT to a private cloud service model in order to achieve the level of agility they need to respond to the changing business environment. Most have already taken the first step by applying virtualization to production IT; however, virtualization of WAN optimization and other network services is also required since an efficient and cost-effective network is key to delivering on the dynamic needs of the enterprise.

Deploying network technologies conventionally - piling proprietary boxes on top of each other in a farm - is no longer the way to go. A networking appliance farm including WAN optimization, just like a server farm, drives up capital costs, operational expense and energy consumption. Virtualization technologies have successfully reduced server and storage farm sizes and complexity. Now is the time to use virtualization to downsize the network and optimization appliance farm. The currently accepted way of delivering network services is unacceptable. Hardware appliances are inflexible, inefficient and unable to change fast enough to meet business demands. Virtualized WAN optimization appliances make an entire network more scalable and more reliable.

aCelera: Scalable Performance and Lower TCO

aCelera software is delivered as a virtual appliance supported on industry-standard servers running hypervisors such as VMware ESX and Microsoft® Hyper-V and as software installed on industry standard laptop systems. aCelera software packages are delivered over a network and installed by Certeon CMS in data centers, at remote sites, or on end user PCs

in less than 30 minutes. aCelera creates a virtual WAN Infrastructure or "WAN-in-a-box" and delivers a responsive, global and scalable WAN that can scale to meet your application and user performance needs.

Every network has two ingredients: nodes and connections. In the global networks that enterprises are now assembling, the number of the nodes is collapsing, due to virtualization, while the quantity of connections and the demands placed on these connections is exploding, mainly due to virtualization, the advent of managed services and cloud computing. aCelera provides exceptional performance by leveraging every ounce of resource available in the virtualized environment.

aCelera software exceeds the scalability and performance requirements of today's enterprises and reduces WAN optimization TCO by 60 percent when compared to hardware WAN optimization deployed in an appliance farm.

Pound for pound aCelera supports 50 percent more concurrent accelerated connections than hardware WAN optimization appliances. aCelera is designed to leverage enterprise virtualization scalability and is ready for the usage demands of managed services and cloud computing (**Figure 2**).

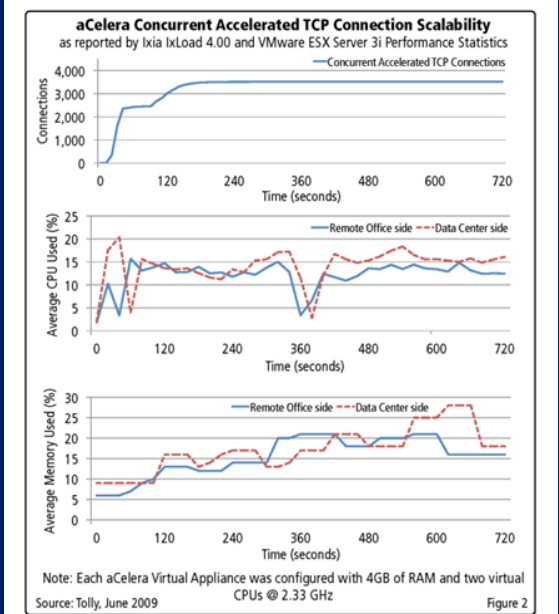## Replacing the Network Farm with Dynamic Virtualized WAN Optimization

aCelera enables IT managers to operate applications, desktop, and server infrastructures where they will be most effective: in branch offices, centralized data centers or even in on-premise or off-premise cloud infrastructures.

Figure 2: Tolly #209129/CPU and Memory used by aCelera

Note: Each aCelera Virtual Appliance was configured with 4GB of RAM and two virtual CPUs @ 2.33 GHz
Source: Tolly, June 2009   Figure 2

With the increasing popularity of virtualization in the enterprise, Certeon's aCelera Virtual Appliance software delivers a software application acceleration platform that can reduce hardware footprint

The use of hardware-based WAN optimization technology in heavily virtualized enterprise environments will not provide the required application performance or meet IT managements' need for flexibility. Proprietary WAN optimization appliances with hosted virtualization do not stand up to anyone's definition of a virtualized or cloud service. Hardware centric approaches to delivering virtualized network resources like WAN optimization creates castaway technology - islands of virtualization capabilities surrounded in a sea of proprietary technology.

aCelera virtual appliances deliver performance benefits and advantages without the downsides of additional hardware costs and management. aCelera virtual appliances leverage the virtual infrastructure and can easily be scaled on existing platforms or migrated to more powerful platforms and processors when business conditions dictate.

Certeon's aCelera software embodies all of the performance advantages of WAN optimization with the flexibility, scalability, manageability and cost-savings of virtualization. aCelera can be deployed in virtualized private, public, and hybrid cloud computing environments and is poised to meet the evolving needs of the dynamic enterprise.

http://www.certeon.com

Leveraging Virtualization in the Branch Office

Blue Coat

Consolidate, optimize delivery and contain costs

Global enterprises everywhere are looking for new cost-effective ways to deliver critical applications to an increasingly distributed workforce. The challenge at the branch, however, is particularly difficult. In an environment where you're trying to reduce costs and consolidate devices and equipment, you face a diverse set of issues:

- Business apps are slow
- The network is nearing full utilization and WAN costs continue to grow
- You have to deal with procurement and management costs for servers, storage and other devices
- Consolidation/IT initiatives are delayed
- You need to deploy new services capabilities to match business needs

Balancing these issues is no easy task. How can you cost-effectively optimize WAN bandwidth when you have to manage record levels of network traffic, expand remote storage and backup capacity, increase branch office productivity and help your business reach customers wherever they happen to be?

There is a solution.

You can deal proactively with all these issues, including the need for cost reduction and superior application delivery, with a combination of Blue Coat and VMware technologies. You can then implement:

- **Virtualization** that consolidates infrastructure and expands services
- **WAN Optimization,** packaged as a virtual appliance, that reduces WAN costs and accelerates application performance
- **Delivery of applications, network and application services** that match business needs
- **Industry-standard servers** that provide a flexible, powerful and cost-efficient platform for consolidation

Here's how you can apply this solution to your enterprise:

1. Virtualize your branch infrastructure.
Consolidate resources while expanding services.

Virtualization with VMware offers a unique opportunity to consolidate branch office infrastructure, with flexibility to deliver specific services to each site – with high availability.

Blue Coat's market-leading WAN Optimization software is now being delivered as a virtual appliance that runs on any industry-standard platform certified on VMware 3.5 or 4.0. This means that WAN Optimization runs on the same platform

as Microsoft Windows Server – along with business applications and other key services. The hypervisor can isolate issues with any resident virtual machine (VM), so the instability of a server OS won't take down the system or the other VMs.
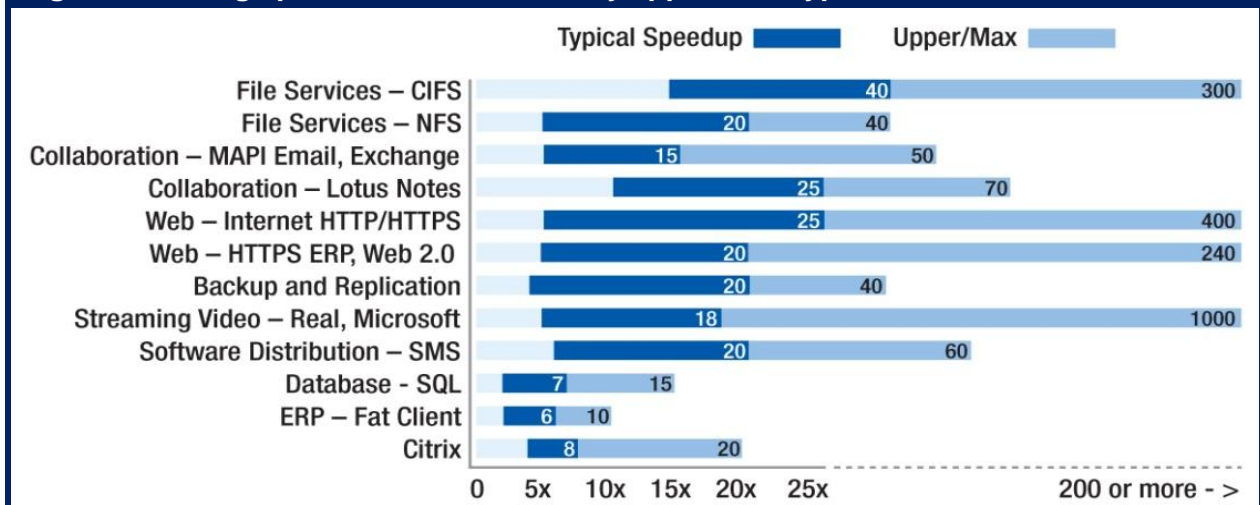
2. Apply Blue Coat WAN Optimization to your network.
Accelerate your business applications and reduce WAN costs.

The Blue Coat solution accelerates the broadest range of applications in the industry, including files, email, backup, video and software-as-a-service (SaaS) applications. You can improve application performance and conserve WAN bandwidth by applying the right mix of Blue Coat acceleration capabilities across your distributed enterprise:

- *Protocol optimization:* Improves application performance over the WAN by reducing the effects of latency on inefficient protocols or applications originally architected for the LAN.

- *Object caching:* Dramatically accelerates Web applications and workflows that depend on centrally stored files by delivering remote content locally.

- *Byte caching:* Reduces bandwidth consumption for repetitive data elements transmitted over the WAN, even across disparate applications.

- *Compression:* Reduces the effect of latency for any compressible data traversing the WAN.

- *Bandwidth management:* Prioritizes enterprise-critical application delivery over the WAN.

- *Video caching and live stream-splitting:* Saves bandwidth by enabling you to download a single live stream once and distributing it to multiple users. Files can also be pre-populated and cached for on-demand use in native protocol.

**Figure 1. Average performance increase by application type**

3. Deliver site-specific applications, network services, and application services.

Match the business requirements at every site.

In addition to Blue Coat WAN Optimization, a consolidated, virtualized platform can deliver key network and application services. That includes Microsoft Windows Server 2008 – the industry standard for IT services like DNS, DHCP, authentication and print services, required for high-availability distributed sites.

What does your business need at the branch? A point-of-sale application? An inventory system? Video surveillance? Customer or patient history? What changes do you foresee? A flexible open system allows you to run required applications at your sites – key to maintaining an agile architecture.

LOB APP/Key Service
POS   Customer
Inventory Comms
Financial   Kiosk
Comms   ...
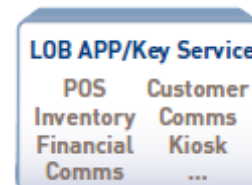
4. Consolidate with industry-standard servers.

Use powerful, flexible, cost-efficient platforms.

Today's industry-standard servers are multi-core, multi-processor, expandable-memory systems with large hard-disk capacity. Their flexibility and compute power give you the most cost-efficient consolidation platform available.

There's more. The x86 architecture combines with virtualization to assure complete compatibility with open, cost-efficient platforms from strategic suppliers like Dell, HP, IBM, Lenovo, and Fujitsu. That means that a system from your trusted server vendor can give you a 4-20x price/performance edge over proprietary router and appliance platforms. You'll be able to use your platform of choice to deliver WAN optimization with key branch office applications and services, and as a result:

- Maintain branch office productivity
- Reduce WAN costs
- Accelerate business applications
- Control costs through server consolidation

To sum up

The Blue Coat WAN optimization solution is now available as a virtual appliance that runs on VMware on industry-standard servers. You can use VMware to consolidate branch infrastructure and reduce costs. The server that hosts Blue Coat can also serve applications and services needed by the branch office. Blue Coat can accelerate business applications and reduce WAN costs. This combination of technologies gives you control, flexibility, and cost containment to handle changing needs.

About Blue Coat

Blue Coat is the technology leader in Application Delivery Networking (ADN). Blue Coat ADN infrastructure provides the visibility, acceleration and security capabilities required to optimize and secure the flow of information to any user, on any network, anywhere. This application intelligence enables enterprises to tightly align network investments with business requirements, speed decision-making and secure business applications for long-term competitive advantage. To learn more, please visit us at **www.bluecoat.com**.

Cisco Server Virtualization
for the Branch Office

CISCO

Overview

Server virtualization has brought a large number of new features into the data center that a traditional server cannot provide; such features include live virtual server migration, dynamic resource allocation, live CPU and memory increases, and distributed software switches. Gartner predicts that by the end of 2012, 50 percent of all Intel x86 data-center server workloads will be running on virtualized hardware[17]. The rapid growth of server virtualization in the corporate data center is an indicator of the appeal of this technology. Increasingly, the virtualization technology is also finding its way into the branch office.

This paper explains how virtualization unlocks new capabilities and provides a brief overview of Cisco® Services Ready Engine Virtualization (Cisco SRE-V), Cisco's server virtualization solution for the branch office. Cloud-based services, virtual desktop infrastructure, and virtualized disaster-recovery backup sites are all made possible by virtualization. Cisco SRE-V enables consolidation, energy savings, improved server uptime, and rapid application provisioning—and it reduces both equipment and operating costs.

Introduction

Server virtualization addresses the challenges of managing large server infrastructure in data centers that consumes significant energy and requires sophisticated planning to account for unexpected loads. Server virtualization inserts a thin layer of software (hypervisor) between the server hardware and the operating system to help manage these servers.

The hypervisor provides virtual hardware containers for hosting application and operating-system environments (virtual servers), as shown in **Figure 1**. Virtual servers are faster to provision than their physical counterparts; require less space, power, and cooling than multiple physical servers; and can be cloned, moved, or clustered on demand and without service interruption.

Figure 1. Intel x86 Server Virtualization Architecture
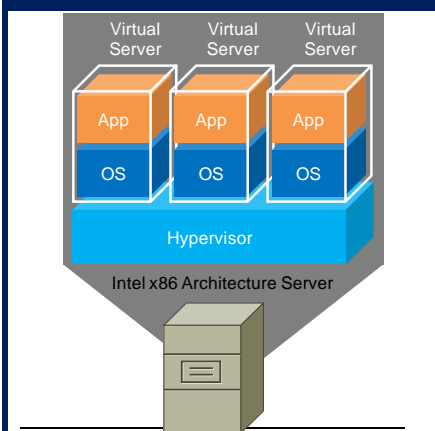
A hypervisor imposes the following set of attributes on virtual servers that traditional x86 servers lack:

- Isolation: A virtual server is confined to one container and is unaware of other virtual servers.
- Multiplicity: A virtual server shares hardware concurrently with other virtual servers.
- Abstraction: A virtual server is hardware-independent and can run on various platforms.

[17] http://www.gartner.com/it/page.jsp?id=1211813

- Encapsulation**:** A virtual server stores its complete point-in-time execution state in a file.

These fundamental attributes are the building blocks of higher-level functions introduced by server virtualization.

Application Provisioning Options for the Branch Office

Enterprise applications such as SharePoint Server, SQL Server, Exchange Server, print services, Dynamic Host Configuration Protocol (DHCP) server, Domain Name System (DNS) server, Microsoft Active Directory Domain Services, and performance-critical line-of-business applications are typically provisioned in one of the following ways (**Figure 2**):

- Dedicated physical server for each application: This setup isolates applications from each other for organizational, security, performance, or application availability reasons. However, it increases equipment and operating costs.
- Multiple applications share one physical server: This setup minimizes total cost. However, it creates access control, operational efficiency, application availability, and time-to-deployment complexity.

Figure 2. Application Provisioning Options on Physical Servers
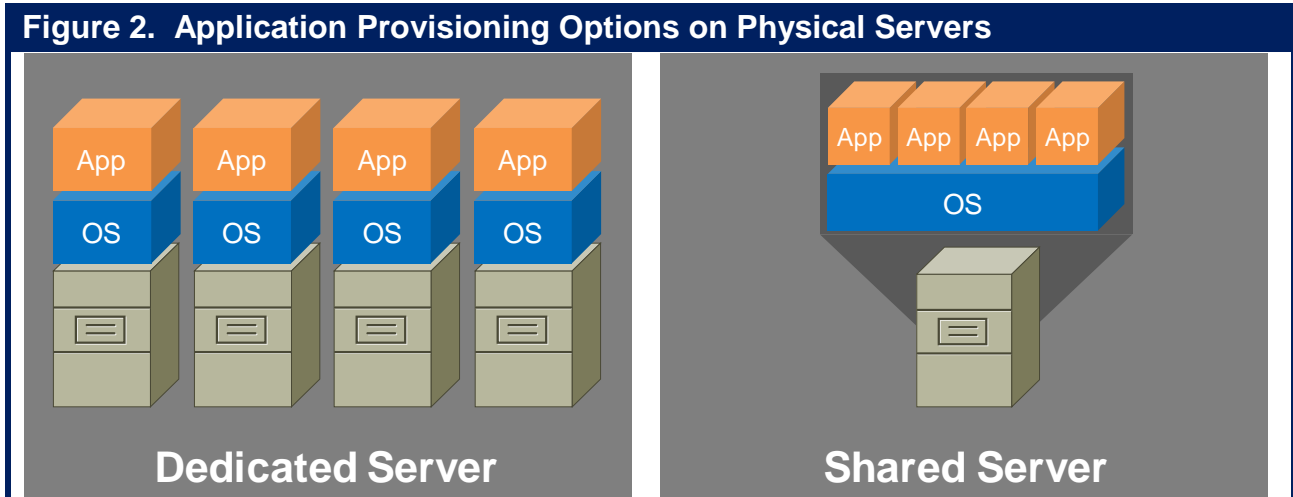
Server virtualization eliminates the worst of each while offering the best of both deployment scenarios. The isolation and multiplicity attributes of virtual servers described previously enable the following provisioning options (**Figure 3**):

- Dedicated virtual server for each application, all hosted on one physical server: This setup isolates applications from each other, while lowering costs, increasing application availability, strengthening access control, and improving time to deployment.
- Dedicated virtual server for each application hosted across multiple physical servers: In addition to the benefits discussed previously, this setup improves application availability and disaster recovery for a marginal increase in cost.

Figure 3. Application Provisioning Options on Virtual Servers
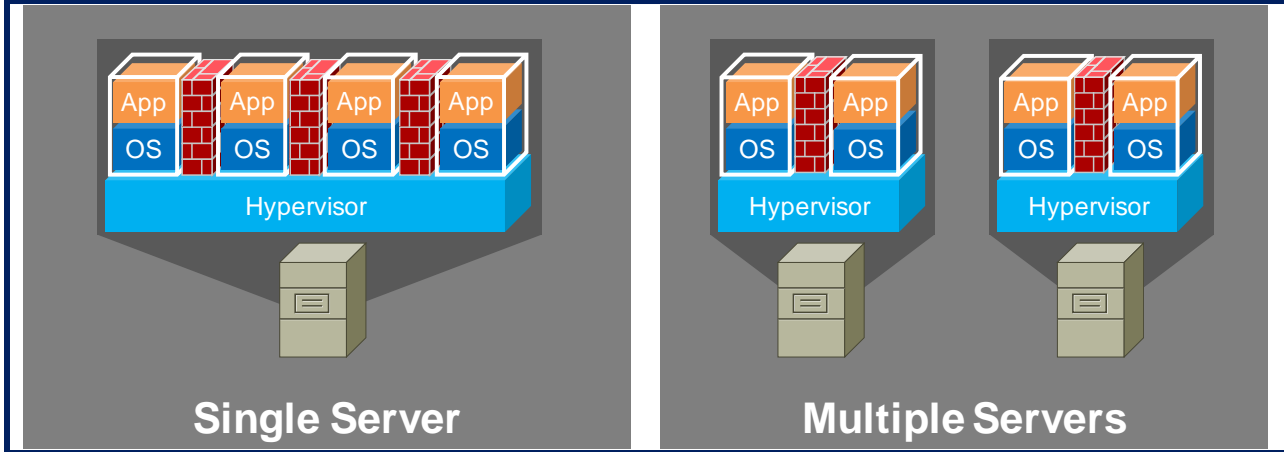
These provisioning options bring the following benefits:

- Lower infrastructure and operating costs: Most server hardware is underused. Consolidating multiple applications to run on a single physical server eliminates unnecessary servers and increases use of the remaining servers. Cost savings extend beyond server hardware, and include less cabling, Ethernet ports, power supplies, patch panels, surge protectors, and rack and physical space.

- Shorter application downtime and response time: Multiple applications hosted on one operating system share and compete for resources. Isolating applications from each other ensures that an action of one application does not affect the rest of the system.

- Faster time to deployment for applications: Multiple applications hosted on one operating system have various dependencies. Isolating applications from each other ensures that a change in one application is transparent to the other applications.

Cisco Server Virtualization Solution

Cisco Services Ready Engine Virtualization (SRE-V) combines the on-demand application provisioning capabilities of the Cisco Services Ready Engine (SRE) service module and the hardware-like reliability and performance of the hypervisor into a server virtualization platform. The Cisco SRE-V is a jointly developed solution from Cisco Systems and an industry-leading virtualization solution provider. This solution enables the consolidation of all network and application services into a single-box solution. Unlike standalone x86 servers with virtualization, the Cisco SRE-V combined with the multiservice Cisco Integrated Services Routers Generation 2 (ISR G2) provides more agile, simpler, and lower-cost branch-office infrastructure integrated into a single, high-performance, feature-rich device.

The Cisco SRE is designed to help organizations place services more efficiently. On-demand application provisioning provides the option to remotely deploy networking or computing service into

any office at any time. Deploying Cisco SRE with the Cisco ISR G2 removes the burden of having to decide initially which services have to be provisioned, provides the flexibility to change service placement decisions in the future, eliminates onsite visits, and eliminates a costly infrastructure lock-in.

The Cisco SRE-V enables one or multiple instances of Microsoft Windows Server to run directly on the Cisco ISR G2. This solution is industry's first and only solution for hosting services such as routing, switching, security, voice, video, wireless, computing, storage access, server virtualization, and Microsoft Windows core services (core Windows applications and services such as Active Directory Domain Controller) and line-of-business applications (point-of-sale software) in a single device. Cisco SRE- provides the following benefits:

- Cost savings: The Cisco SRE deployed on the Cisco ISR G2 delivers cost savings by eliminating onsite visits and infrastructure changes, lowering energy consumption, and attaching SRE hardware support services to the ISR G2 at no cost.
- Consolidation: With fewer servers and appliances, less cabling, fewer Ethernet ports, fewer power supplies, and less rack and physical space, a hard-wired physical infrastructure that needs frequent onsite support is replaced by a **soft-wired, virtual** infrastructure that is easier to manage remotely.
- Integration: Virtual servers hosted on Cisco ISR G2 routers running Microsoft Windows Server can now directly take advantage of router and switch features such as VLANs, demilitarized zones (DMZs), access control lists (ACLs), firewall, and quality of service (QoS)—without affecting performance. By unifying routing, switching, computing, and storage access, the Cisco ISR G2 provides more flexibility, more granular control over security, and higher performance.

Summary

Organizations have much to gain by deploying server virtualization in their data centers and branch offices. The virtualization technology not only solves common IT infrastructure problems, it also introduces new capabilities not available with traditional servers. Server virtualization offers a rich set of functions that can unlock new capabilities. Cisco SRE-V combined with the multiservice Cisco ISR G2 provides more agile, simpler, and lower-cost infrastructure integrated into a single, high-performance, feature-rich device. In summary, Cisco SRE-V improves the speed of application deployment, application uptime, and performance guarantees—and reduces both equipment and operating costs.

For more information about the Cisco Branch-Office Virtualization Solution, please visit: http://www.cisco.com/go/isrG2.

Automation and Orchestration of Dynamic Virtual Services

LINE SIDER
TECHNOLOGIES

Does your network have what it takes to support cloud computing?

Virtualization Challenges Conventional Wisdom about Today's Networks

It's everywhere. Virtualization is a top priority for IT organizations. Datacenters, users and applications have all become fluid elements in this new dynamic computing model. However, the network wasn't designed for this new dynamic reality.

Stress fractures have begun to appear in the network triggered by the increasing adoption of virtualization around datacenter compute and storage platforms. The virtualization of datacenter resources, while good for the efficient utilization of costly physical resources, is placing enormous demands on the underlying network and operational support teams in terms of increasing support costs and time spent implementing changes to the infrastructure driven by the dynamic nature of virtual services. Traditional network designs and the tools that control and manage them cannot keep pace with the dynamic nature of virtual services.

This sharp increase in cost and time is a direct result of the amount, and the complexity, of changes that are required across deployed devices and active configurations in order to maintain access and security models for dynamic virtual resources and services being delivered to end-users. While the increase in cost/time is troubling, more alarming is the constant changes being made to the infrastructure exposes gaps in existing security models and enterprise security frameworks that could be disruption of access, the loss of critical business services or even worse, the destruction or loss of data and other valuable assets of the enterprise.

Support teams are being overloaded by demand, and the existing network management tools they have available have not been designed to deal effectively with this volume or type of network change. Existing tools have simply reached their limits.

A New Approach - Network Services Virtualization with OverDrive

LineSider Technologies has created OverDrive, the industry's first network first network automation and orchestration solution that enables enterprises and service providers to dramatically reduce network operations costs associated with virtualization and cloud computing. OverDrive works without scripts or templates to automate and virtualize network infrastructure so the network becomes fluid and responsive to changes in today's computing environments. This helps dramatically reduces operations costs and provides the flexibility, agility, and scalability required to support dynamic computing environments.

OverDrive extends the power and dynamic capabilities of the virtualized datacenter to the network infrastructure by abstracting devices and services into a model that enables OverDrive to define cloud services that combine server, storage and network (access and security models) into a single holistic service that can be delivered to end-users on demand.

Components of the OverDrive network virtualization solution include; Control Center that defines controls and manages all services, Network Virtualization Engine that transforms policies into actionable service directives, Device Service Controllers (DSC) to manage the device-level configurations across the deployed network.
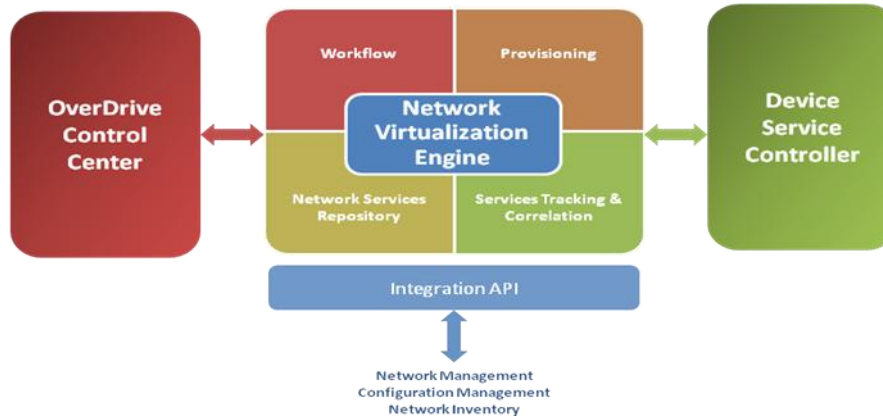
OverDrive Features

Business Policy Driven

Using OverDrive's Control Center, business rules are captured using common semantics. The OverDrive policy acts as the 'control' document for governance and ongoing change management.

Automates Device Level Configurations

OverDrive automates the initiation, deployment, control, and management of network services using business-level policies. Once created, policies are translated directly into device-level configuration syntax and pushed-out to routers, switches, firewalls and other devices deployed on the network. This is all done automatically, without the need for pre-written configuration templates, scripting tools or tedious command line sessions.

Automates Network Service Delivery

OverDrive policies control and define the underlying network infrastructure services that provide end user access and security to both physical and virtual resources.

Eliminates Security Gaps

As users, virtual resources or underlying network services and devices change across the service delivery infrastructure, access and security models break down requiring costly manual involvement to identify the problem and rebuild the service. OverDrive ensures that underlying access and security parameters remain in effect and will automatically notify administrators if for some reason a defined access or security policy is violated.

Identifies Potential Conflicts

Changes made to a production environment has the potential to cause a conflict or interruption of deployed services. OverDrive understands the complex interdependencies between resources in both physical and virtual computing environments and alerts the network administrator about configuration, access, and security conflicts prior to changes being pushed out to devices that may impact the production environment.

Enforces Compliance

OverDrive provides a complete solution that satisfies multiple audit controls and reporting requirements for Sarbanes-Oxley, HIPPA, PCI and other federal mandates in regulated industries. With OverDrive, policies control and define all

aspects of network-based access and security configurations. All changes are made at the policy level where a full and complete history of changes is tracked and managed.

Integrates into Existing Network Support Platforms

OverDrive has been designed to integrate with and share information across the existing back-office systems used to control the network infrastructure. OverDrive has a powerful SOAP/REST API that can produce or accept structured XML data feeds to be shared with other configuration, network and performance.

Create Dynamic Fluid Networks with OverDrive

As most early adopters of highly virtualized and cloud networking environments are realizing, true on-demand computing can only be fully realized when the underlying network infrastructure is as flexible and liquid as the dynamic needs of the business end-users. Platforms, such as OverDrive, that virtualize network services and transform the legacy infrastructure into a responsive, dynamic delivery apparatus are essential to creating a fluid, dynamic networking environment.

For more information on OverDrive, visit **www.linesider.net**.

Optimizing Application Delivery in a Virtualized World

zeus

Beyond Server Virtualization

Server Virtualization has dramatically changed the landscape in the datacenter. Organizations are consolidating workloads from underutilized servers and are seeing large reductions in datacenter space, power, cooling and administration requirements. Standardization onto a small number of common hardware platforms is speeding up the server deployment process and reducing the overall cost of hardware maintenance. However, server consolidation is just the beginning of what can be achieved. Virtualization unleashes applications and compute workloads, breaking the ties that hold them to physical servers. This new-found freedom makes possible an entirely new datacenter architecture where the hardware serves the applications and the applications serve the business, rather than the other way round.

The Zeus philosophy is that throwing additional hardware at a performance problem or paying for more bandwidth can and should be avoided. These are overheads that will either depreciate in value or add to operational costs, or both. Virtualization of key network services such as Load Balancing and Application Delivery Controllers is the logical next step in any virtualization strategy.

If your organization has decided to Virtualize, why run applications such as your Application Delivery controller on a dedicated, proprietary appliance at the edge of the infrastructure? The Zeus Elastic Application Delivery platform runs natively in your virtualization environment.

Lower Total Cost of Ownership

For Rodgers Townsend, the "green appeal" of Virtualization was a consideration. Server consolidation and the reduced server room footprint equate to energy and hardware savings, but the instant scalability was the key differentiator. "Zeus Traffic Manager VA is unique in that it's the only application delivery solution available as a virtual appliance," says Jonathan Knorr, IT Director, Rodgers Townsend, "Because the Zeus software is infinitely more scalable than F5's hardware line, when further capacity is required, all we need to do is buy another licence, which can be received and deployed much faster than any physical appliance."

Zeus Elastic Application Delivery Platform

The Zeus Elastic Application Delivery Platform ensures that no matter where your users are and where your applications are, your users get the best possible level of service and your applications run as cost effectively as possible.
It enables you to deliver fast, secure and available applications across any combination of physical, virtual and cloud infrastructures with a single point of application delivery control and monitoring across all locations.

The Zeus Elastic Application Delivery Platform incorporates the industry's fastest software Application Delivery Controller for local traffic management, Global Load Balancing to balance between datacenters and Multi-Site Management to maintain consistent policy and configuration across datacenters.
The Zeus Elastic Application Delivery platform runs on most major virtualisation technologies, including VMware, OracleVM, KVM, Xen and Microsoft HyperV.

Bound for the Cloud?

If and when you decide to migrate to a cloud computing provider, hardware appliances will become obstacles. Zeus considers them to be "anchors" that make your infrastructure inflexible. When form and function are locked together, the ability to adopt more efficient solutions is hindered.

Many organisations have already begun moving their IT infrastructure into a Virtualised environment, but for others complete Virtualisation is a little – or a long – way off. Rather than clear and defined lines, we are seeing more

organisations running on a hybrid of traditional hardware as well as more sophisticated Virtual and Cloud solutions. This means that developers need the ability to choose where they deploy their applications without impediment, and to be able to move them when required. Moving an application from a Physical to a Virtual environment and into the Cloud should add scalability, greater agility of service and commercial flexibility with all other criteria unchanged.

Cloud ready

What this has done is remove the 'old world' barriers to the way we view traffic management and web application development. Organisations can now create exceptional applications, manage the traffic to those applications to control operational cost and complexity, and deliver those applications successfully to end users, no matter whether the applications are located in a physical datacentre, on a Virtualised platform or in any infrastructure Cloud. The rate of change demanded of on-line applications and services requires an ever faster time-to-market, developers have to create these sophisticated services quickly and reliably while meeting the demands for performance, scalability and availability. This in turn places greater demands on the infrastructure that supports them.

Making sure your application infrastructure is 'cloud-ready' is not as difficult as it might sound. At first glance, cloud-based applications may not look significantly different to applications running in traditional Physical or Virtualised datacenters. One of the key aspirations of Cloud however, is that it will allow organisations to exchange some of those enormous capital infrastructure costs for pay-by-use operational costs, and through elasticity and improved infrastructure utilisation, reduce the overall costs. So, crucially, one of the first steps is to audit the application infrastructure, picking out any components that are implemented in hardware appliances – firewalling, intrusion detection, web application firewalls, load balancers etc – and replace them with software alternatives when the next technology refresh comes round. If necessary, walk round the datacenter with a pack of post-it notes tagging any brightly-coloured single-purpose appliances with the label 'anchor', because those appliances are going to weigh your applications down and prevent you from ever moving to the Cloud.

Case Study: Yottaserve

Yottaserve offer "hosting without toasting" and deliver application analysis, web hosting and consultancy for companies that have websites rich in Web 2.0 content.

Yottaserve chose Zeus Traffic Manager VA (Virtual Appliance) in favor of other costlier solutions that required the purchase of hardware to provide their application delivery. Zeus Traffic Manager VA is a great fit for YottaServe's virtualized hosting environment because it can be run from the existing SAN and if the hardware hosting the Zeus software were to fail, a new instance can be started automatically and be back in action in a matter of seconds – no need to wait for hours or days for a replacement.

"Once Zeus Traffic Manager VA is put in front of the simulated traffic, I watch my customer's jaw drop, as the difference is phenomenal," said Jeff Rhys-Jones, Founder Yottaserve. Jeff adds, "Using Zeus Traffic Manager VA, we were able to demonstrate that placing Zeus software in front of the application transformed the number of concurrent users from ten into thousands – with no application modifications needed."
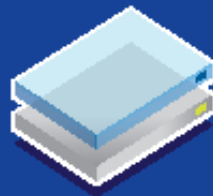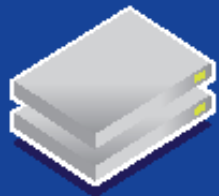
EXPAND networks | VIRTUALLY EVERYWHERE ™

Market Overview

WAN optimization needs have changed from traditional bandwidth enhancement and application acceleration capabilities, to a more application-aware approach that integrates monitoring and layer 7 QoS functionality to enables visibility and control over all applications traversing the WAN.

Addressing performance and productivity challenges of an increasingly mobile and remote workforce, as well as being conducive to virtualized environments, WAN Optimization has moved from tactical deployment to strategic imperative that is a key enabler of IT initiatives today.

Meeting Global Business Challenges - The Proximity Gap

One size of WAN Optimization doesn't fit all. Solutions should be focused upon addressing specific enterprise needs, and for this, some WAN Optimization solutions are more equal than others. Expand is focused on enabling accelerated delivery and guaranteed performance of business critical applications and services within virtualized WAN environments and across distributed enterprise infrastructures.

As organizations struggle to meet global business challenges, while consolidating IT data and applications, they create a proximity gap between users and resources as the users and data center services move physically further apart from each other. This causes applications, files & services delivered over the WAN to suffer from performance challenges and can result in poor user productivity, failed IT projects, and impact the bottom line.

Expand addresses the proximity gap by placing users in virtual proximity of their applications and data center services. Tightly integrating technologies provide greater control and optimization of the WAN, assuring the quality of user experience across complex network environments by delivering 4 to 10 times the bandwidth and delivering a constant SLA for the user via Acceleration, Optimization & Layer 7 QoS techniques over the existing WAN infrastructure.

Enabling Strategic Initiatives

Expand Networks' technology delivers maximum results by focusing on enabling the following strategic initiatives:

- VDI - Expand is the only vendor that can successfully accelerate within Virtual Desktop Infrastructure (VDI) environments with applications such as Microsoft Terminal Services (RDP), Sun Sunray (ALP), and Citrix XenApp (ICA) as well as being able to securely enable VMware/Terradici PCoIP offerings. Unlike competitive offerings, Expand works on the IP layer, this enables Expand to accelerate _all_ IP & uniquely UDP applications over the WAN.
- Server Based Computing and Virtualization - Expand's WAN Optimization software can be effectively integrated into virtual environments, such as VMWare Vsphere (ESX, ESXi). Today Expand is the only vendor that can successfully optimize server based computing protocols such as Microsoft Terminal Services (RDP), Citrix XenApp (ICA) and Sun Ray (ALP).

Key Technologies – Any Application, Any Network

- **Automatic Layer 7 application Monitoring & QoS engine**: provides unprecedented levels of visibility and control over a comprehensive list of 400 plus applications.

- **Compression technology**: **U**sing low latency, lossless techniques that work on all applications, Expand Networks consistently deliver average bandwidth increases between 100% and 400%, with peaks of over 1,000%.

- **Byte-level caching techniques** are unique in its memory acceleration, not hard drive, for real-time interactive and small packet applications, ensuring no duplicate data traverses the WAN and leaving the limited network resource to work on the business critical traffic.

- **Optimization and TCP Acceleration** overcomes latency and can accelerate <u>any</u> application across <u>any</u> network to deliver a guaranteed and constant experience for the remote user. Expand Networks' interactive application **acceleration** enables more user sessions per remote location as well as speeding response times across the board.

- **WAFS & Virtual Server –**with integrated 'virtual server' technology, Expand enables complete branch office server consolidation by replacing the need for an additional branch office file server, ensuring delivery of local DNS, DHCP and Print server functionality via the "Virtual Server features".

Expand Enables Server Consolidation and Data centre Centralization Success at Kingspan Group

Currently embarking on a company-wide centralization programme, Kingspan Group PLC - a global manufacturer of sustainable products for the construction industry - is consolidating its business operations into a centralized data center and has chosen Expand Networks Virtual and Physical Accelerators to provide WAN optimisation services.

This follows a successful deployment at Kingspan Environmental, a division of Kingspan Group, where Expand enabled the implementation of a server consolidation strategy to simplify IT infrastructure and reduce costs. With business critical applications moving further away from users, Kingspan Environmental needed to ensure that WAN connectivity to remote office sites could cope with the increased demand the applications placed on the network.

Expand prioritised Citrix traffic and maximised the throughput of the existing connections in order to maintain a consistent level of service to distributed offices., KingSpan Environmental then quickly moved to consolidate remote file servers with WAFS. The Accelerators provided:

- Reduced WAN latency and congestion and significant cost savings
- Improvements in application performance of up to 2000%,
- QoS function ensures the critical Citrix applications are prioritised and always available.
- Wide Area File Services (WAFS) enabled the complete removal of remote file servers, replacing the remote office server functions including Print server.

Looking to mirror this success, Kingspan Group has now enhanced its Expand deployment with the Virtual Accelerators in its new central data center and has also implemented ExpandView for the simple management of all its appliances. The Accelerators will control Citrix services and ensure network performance and application delivery for users as it embarks upon its transition to a centrally managed IT environment.

"Peter Donnelly at Kingspan comments, *""The key to a successful consolidation or centralization strategy is understanding and considering the effect it will have on the network and its users. Expand's integrated multi-service capabilities are delivering the network performance needed to maintain productivity and increase efficiency. The technology has year on year for the last 7 years capped our WAN cost at Expand enabled sites, where other non expand sites have seen costs goes up by as much as a factor of 3. "*

- Server Consolidation - Expand's WAN Optimization solution with its integrated 'virtual server' technology enables complete server consolidation by replacing the need for an additional branch office file server. Expand's unique "Virtual Branch Server" feature sets also enable to customer to replace features that used to be delivered by a remote server, such as DCHP, DNS and Printing, all within the AoS and not via third party plug-ins like other vendors.

- Satellite Environments - satellite links fast becoming a scarce commodity, Expand's WAN Optimization solution, with integrated Space Communication Protocol Standard technology, helps distributed organizations overcome the traditional low bandwidth, high latency obstacles that impede the speed and performance of applications and services over satellite links.

Flexible Deployment from Datacentre to the Desktop

Ensuring transparent integration into your existing network in your choice of **virtual or physical** platforms, Expand's technology is unique in its combined ability to be deployed within a virtualized infrastructure and to accelerate and control virtualized traffic out of it. As a truly virtualised solution Expand can also be deployed under traditionally challenging and extreme conditions such as on aircraft, mobile environments and remote and unattended locations.

In addition, increased mobility and collaboration has become a critical enabler to breaking down traditional organisational boundaries and improve decision making, customer responsiveness and business productivity. Expand Networks' product range is designed to provide the same seamless user experience wherever users are – Headquarters, branch office, home office, airport, client site, train – putting all data and applications in virtual proximity of users – virtually everywhere.

APPLIANCE ACCELERATOR (ACC) - Expand Accelerators can be deployed in small and regional branch offices, as well as in data center environments that require scale and flexibility to survive in some of the largest and most complex networks. Expand Accelerators are available in both a hard drive and a non hard drive offering, and the optimization throughput ranges from 128 Kbps to 250 Mbps depending on product choice. Expand provides a pay as you grow licensing model for both datacentre and branch Accelerators, enabling users to simply upgrade a license to unlock more capacity support.

VIRTUAL ACCELERATOR (VACC) - The Virtual Accelerator solution for virtualised datacentre environments delivers the most advanced levels of VMware integration of any leading WAN optimization vendor in the market today, enabling IT to leverage VMware's suite of services to deploy, manage, maintain and assure the Virtual Accelerator within the virtualized infrastructure. The VACC can also be deployed on servers at the branch office that have become redundant as a consequence of server consolidation, enabling the recycling of otherwise surplus hardware and supporting an efficient IT strategy.

Deployed on VMware Server version 1.0 and 2.0, ESX version 3.5 and up and ESXi version 3.0 and up, the Virtual Accelerator fully integrates into the virtual infrastructure. Scalability is achieved by running multiple instances of the Virtual Accelerator on one or multiple physical servers and the VACC introduces high availability support that enables organizations to move the Virtual Accelerator from one server to another without losing the warm cache.

MOBILE ACCELERATOR CLIENT (MACC) - The Mobile Accelerator Client (MACC) with unique HIVE technology transforms the economics of WAN Optimization for smaller branch offices and mobile workers within medium to large sized businesses. The MACC's Intelligent location detection provides increased flexibility and mobility as users can move around & the client will provide full WAN Optimization capabilities regardless of location while also providing a distributed 'Virtual Cache' for the small branch office (collective branch) avoiding the procurement dilemma of appliance versus multiple clients and IT footprint issues.