

THE IMPORTANT ROLE OF THE NETWORK IN A VIRTUALIZED WORLD

Meeting the Demands of a Transforming IT Landscape

Table of Contents

Executive Summary	3
Introduction	3
What Is Virtualization?	3
Types of Virtualization	4
Server Virtualization	4
Desktop Virtualization	4
Storage Virtualization	6
Application Virtualization	6
Implementing Virtualization Across the Network Infrastructure	7
Virtualization Services on the Network	8
Consolidation of Network Traffic	9
Increased Number of Network Connections	9
Desktop Quality Experience	9
Security	9
High-Performance Networks and Network Virtualization	9
Juniper's Network Virtualization Leadership	11
Conclusion	11
About Juniper Networks	12

Table of Figures

Figure 1: Server Virtualization and Hypervisor	4
Figure 2: Physical topology of VMware VDI infrastructure with VDM	5
Figure 3: Block Storage Virtualization	6
Figure 4: Application virtualization	7
Figure 5: Network's role in virtualization	8
Figure 6: One physical network—many virtual networks	10
Figure 7: Common network virtualization technologies	11

Executive Summary

Virtualization technologies have been at the forefront of the planning and implementation efforts for many IT professionals. While the basic capabilities have been incorporated into a variety of earlier products, it was the introduction of server virtualization that helped optimize x86 servers and enabled IT departments to realize significant cost savings that catapulted virtualization to become common terminology among IT professionals and CXOs. This renewed interest in virtualization technologies led to its use for other platforms such as desktops, storage devices, and even applications themselves. In the center of these virtualization trends is the network infrastructure “highway” that ties together all of these new services. In this capacity the network plays a key role toward ensuring that the implementation of these virtualization technologies does not impact the high-quality user experience end users have come to expect.

This paper provides a brief description of virtualization and offers details on the different types of virtualization technologies being used today throughout enterprise networks. It then takes a closer look at some of the challenges that might be introduced during implementation of these virtualization technologies onto an already overloaded network infrastructure. Finally, the paper discusses how implementing a high-performance network and network virtualization helps overcome these challenges.

CIOs should read this paper to help gain a better perspective when implementing virtualization technologies—such as server and storage virtualization—to realize the importance of a high-performance network infrastructure, and understand what types of network virtualization solutions are available to help ensure an effective and efficient virtualization environment.

Introduction

A basic premise of computing and IT has been the constant introduction of new technologies ranging from processors, to memory, to connectivity. This trend continues across IT organizations and includes constraints such as needing to show a measurable return on investment (ROI) and combating dwindling space, power, and cooling resources in data centers.

Virtualization has been a discussion point for many years as a technology to help increase an organization’s effectiveness while also meeting the financial and green requirements. Back in the mid-1960s, IBM introduced the CP-40—a research precursor to the BP-67—which in turn was part of IBM’s then revolutionary CP-67/CMS, a virtual machine/virtual memory time-sharing OS for the IBM System/360-67. In 1987 the Merge/386 made use of the virtual 8086 mode provided by the Intel 80386 processor, and supported multiple simultaneous virtual 8086 machines. The virtual machines supported unmodified guest operating systems and standalone programs such as Microsoft Flight Simulator. Finally, in 2006, VMware released VMware Server—a free machine-level virtualization product for the server market.

Multiple needs push the introduction of virtualization technologies into many data centers and across the distributed enterprise landscape. In preparation, it would be helpful to understand what types of virtualization there are and how prepared one’s network infrastructure and IT staff are to support them.

What Is Virtualization?

Virtualization has evolved to software technology that is helping to transform the IT landscape and fundamentally changing the way people utilize computing resources. Today’s powerful x86 computer hardware, which was designed to run a single OS and a single application, is being vastly underutilized in this capacity. One solution to this underutilization involves a type of virtualization that allows users to run multiple virtual machines on a single physical machine, thereby sharing the resources of that single computer across multiple environments. There are different implementations of these virtual machines where each can run different operating systems and multiple applications on the same physical computer.

Another type of virtualization involves making multiple physical resources (such as storage devices or servers) appear as a single virtual resource. This solution creates one virtual resource from one or more physical resources. For example, this virtualization allows the interconnection of multiple switches to form a single, logical device that is managed as a single chassis. Virtualization technology in this case provides the same level of availability, performance, and scale as a traditional modular chassis, with benefits that include smaller space and power requirements and a lower deployment cost.

Types of Virtualization

In review, there are many types of virtualization where some types virtualize one physical resource into many virtual resources and some turn many physical resources into one virtual resource. Across various enterprise environments, a few of the more common types of virtualization being implemented include:

- Server virtualization
- Desktop virtualization
- Storage virtualization
- Application virtualization

These next few sections provide a brief summary of these virtualization types and their basic concepts. By understanding these new technologies, you gain a greater appreciation of the increased demands they place on your network infrastructure.

Server Virtualization

Within IT data center environments, server virtualization has been getting most of the attention because of the many benefits associated with it. Server virtualization is a concept where one physical machine is divided into many virtual servers. The main incentive for IT organizations to use this technology is that many of the servers across the enterprise are underutilized, based on the existence of multiple processors, lots of memory, and huge amounts of disk space. By adopting server virtualization, IT organizations can then consolidate multiple servers into a single physical server, thereby reducing the number of physical servers required by optimizing the resources of the one server (see Figure 1).

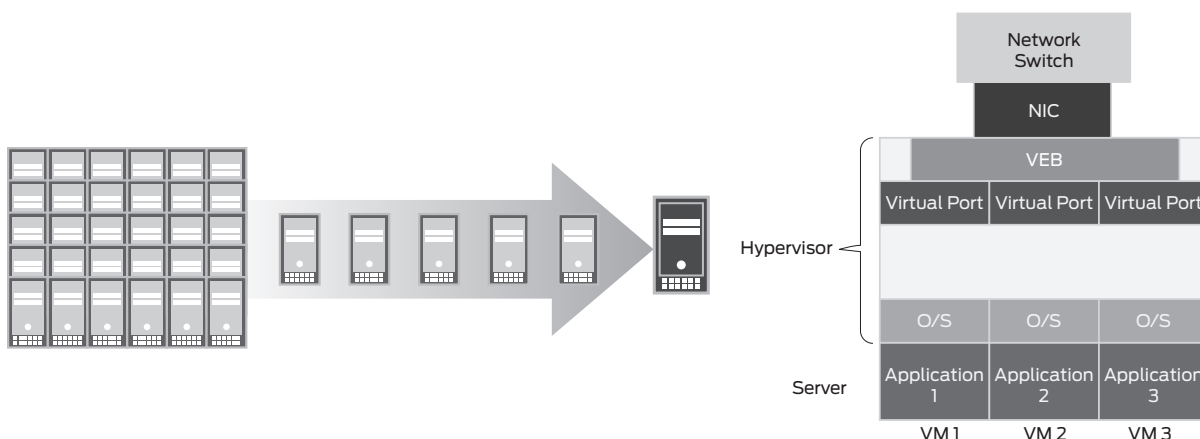


Figure 1: Server Virtualization and Hypervisor

This type of virtualization involves using something called a hypervisor (virtual machine monitor), which is a thin software layer that intercepts operating system calls to hardware. Basically, these hypervisors provide a virtualized CPU and memory for the services running on top of them. As a result, each virtual server is running its own OS, which is completely independent of the host operating system and other virtual servers that might be running on the host operating system.

Desktop Virtualization

Desktop virtualization is a technology that enables IT organizations to substantially increase the flexibility and manageability of their enterprise desktop environments. Currently, there are two types of desktop virtualization technologies being implemented:

1. Remote (server-based)
2. Local (client-based)

With server-based (or remote) desktop virtualization, a server in a remote location hosts the entire end user environment. This type of virtualization involves establishing a virtual desktop that connects to the remote server across a virtual desktop infrastructure or VDI (see Figure 2). Implementation of this model allows an IT organization's desktop PCs to be replaced with thin clients, which send all user input (keystrokes, mouse clicks, etc.) across the network to the server, which processes the input and sends the user interface back across the network to the user.

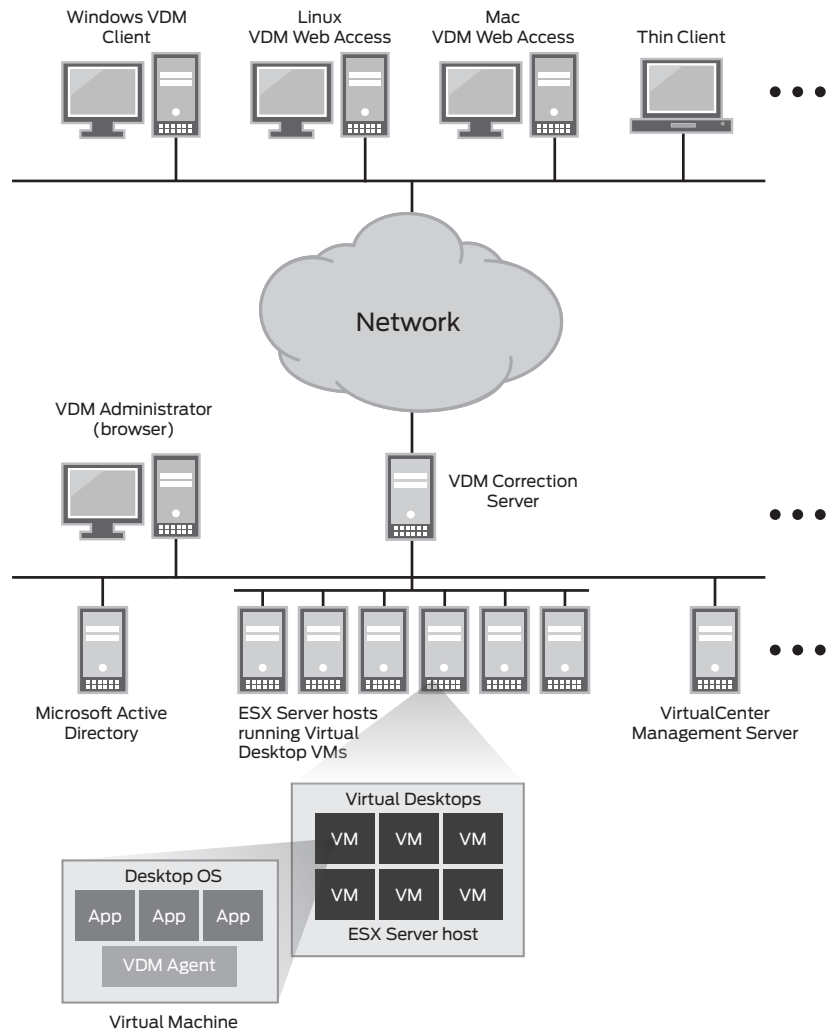


Figure 2: Physical topology of VMware VDI infrastructure with VDM¹

In the client-based (or local) desktop virtualization model, the local client (PC, laptop) hosts the virtual desktop itself—with an independent end user environment (the virtual desktop) running locally, in addition to a standard desktop operating system. In most IT implementations of this model, users interact with the virtual desktop just as they would with any locally installed application.

¹From www.vmware.com

Storage Virtualization

Many IT organizations are implementing storage virtualization within their data centers. This type of virtualization involves adding a new layer of software and/or hardware between storage systems and servers, where applications no longer need to determine on which specific drives, partitions, or storage subsystems their data resides. Servers detect this virtualization layer as a single storage device, and the storage devices determine the virtualization layer as their only server. In essence, through this layer of abstraction, distributed storage systems can be identified, provisioned, and managed as if they were a single consolidated resource.

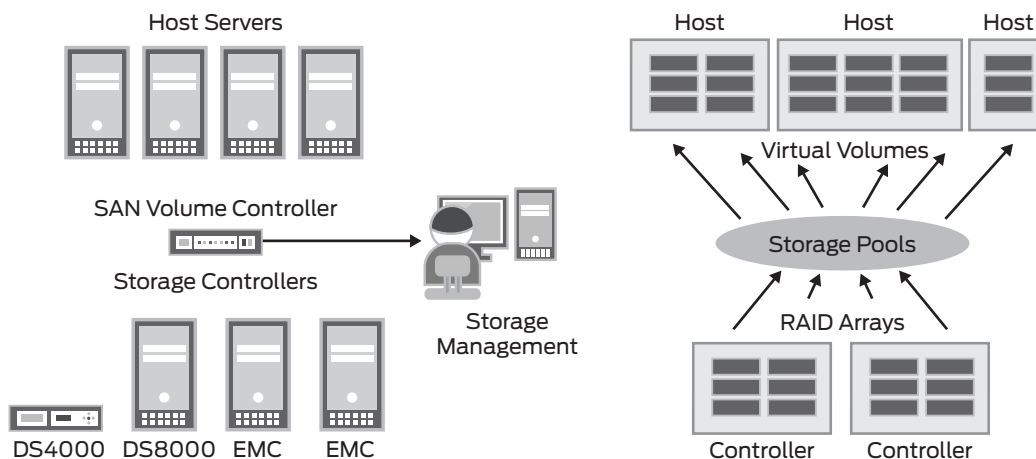


Figure 3: Block Storage Virtualization

In conjunction with the popularity of server virtualization, this type of virtualization is coming in as a close second. While there are many variations, storage virtualization implementations are normally structured in one of three basic ways:

- **Host-based**—While the actual physical storage drives are handled via a traditional device driver, a software layer above the device acts as a special device driver that intercepts I/O requests, looks up metadata, and redirects I/O.
- **Storage device-based**—For this method, various types of array controllers, such as RAID, allow other storage devices to be attached downstream. There is a primary storage controller that handles pooling and manages metadata, allowing the direct attachment of other storage controllers.
- **Network-based**—In this scenario, the storage virtualization is seen as a network-based device. There is commonly a hardware device or switch-based implementation that generally uses Fibre Channel networks connected to a storage area network (SAN).

Application Virtualization

Another type of technology being used across enterprises is application virtualization. This is a concept where a service or application interprets that it is directly interfacing with the original operating system and all of the resources managed by it, when in reality it is not. In other words, this service/application virtualization unbundles the service/application from a physical OS and hardware. This is accomplished by the application virtualization layers replacing part of the runtime environment that the operating system normally provides. This layer intercepts and transparently redirects all file and registry operations to a virtualized location without the application even detecting it.

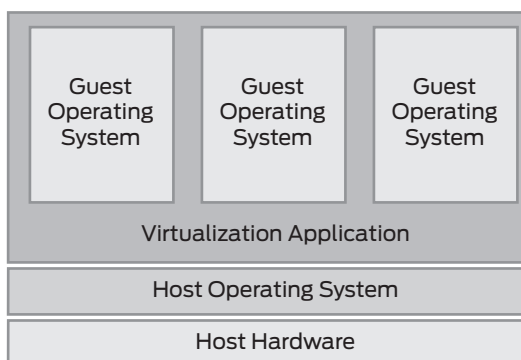


Figure 4: Application virtualization

By decoupling the service/application from the OS, this technology enables it to run as a network service. Since applications are not installed on the client, there is minimal impact on the host operating system or other applications.

As you can see, there are many types of virtualization technologies being implemented by IT organizations within their data centers and across their enterprise environments. The benefits of increased efficiency and lowered costs are evident. However, is it clear how successful these virtualization technologies are across one's existing network?

Implementing Virtualization Across the Network Infrastructure

The precursor to the Internet, the ARPANET, was designed to be a robust network by breaking down information into packets and transporting them independently to their final destination. This simplistic model provided a good environment that could survive disruptions in the network, while still offering a best-effort delivery scheme that is still in existence today within the Internet.

Older applications could run fine across this type of network environment as many of them operated, such as e-mail, as store-and-forward implementations. As originally designed, when packets travel from origin to destination across a network, there are several conditions that could affect the performance of applications or services that depended on delivery of these packets in real time.

- **Achieving sufficient throughput**—If all traffic (voice, data, and video) being transported across a single, physical network connection (such as 10 Mbps or a T1 line) are given equal priority, the load on the network can vary based on other users sharing the same network resources. Therefore, real-time applications might not receive adequate throughput across the network to provide the expected level of service to end users.
- **Handling of dropped packets**—A common function of buffers in networking equipment, such as routers, is when they become full they might be unable to deliver some packets and therefore “drop” them. Typically the network is set up so that the receiving end requests this packet be retransmitted. Depending on the size of the packet and the specific application being run, this retransmission of information could severely impact that application's performance.
- **Compensating for delay**—Sometimes packets can take a long time to reach their destination. This could be due to the specific network configuration, the available bandwidth, or type of networking equipment. These packets might just be held up in long queues or sent across multiple network hops. Again, this delay could impact the performance of applications waiting to operate in a real-time environment.
- **Handling jitter**—Since information is being broken up into packets, and each packet could take different routes to its final destination, it is not uncommon for these separate packets to have different delays. When the separate packets all reach their final destination, the receiving system must reassemble the packets and, if needed, handle the out-of-order sequence if the packets arrive in different sequence than when they were sent. These network delays, called jitter, also affect the application's performance.

As the nature of application traffic continued to change, to help deal with these network performance conditions, networking vendors introduced technology that allowed the network to treat packets differently. This concept is often referred to as quality of service (QoS), and it addressed important concepts such as resource allocation and performance optimization. Differentiated services are provided where a user's traffic is divided into a small number of forwarding classes that result in differentiated treatment of the packets. Additional features found in MPLS technology—such as explicit route mechanisms, guaranteed QoS, and VPNs—can also help.

A successful implementation of virtualization technologies across an enterprise network requires the network to have the ability to rapidly scale and efficiently provide resources to real-time applications. This is paramount with the network being at the center of all these virtualization services. But, should you be concerned with what types of additional traffic might be introduced onto your network when implementing these virtualization services?

Virtualization Services on the Network

With all of these technologies pushing services to become even more distributed, and infrastructures continuing their trend of consolidation, the network plays a key role as the major “highway” transporting all of these virtualized services (Figure 5). Implementation of virtualization technologies across an enterprise requires the network to rapidly transport large amounts of data and handle the real-time remapping of network resources such as IP addresses, ports, and VLANs. Right in the middle, the network plays a critical role toward ensuring a successful implementation of virtualization and quality services to end users.

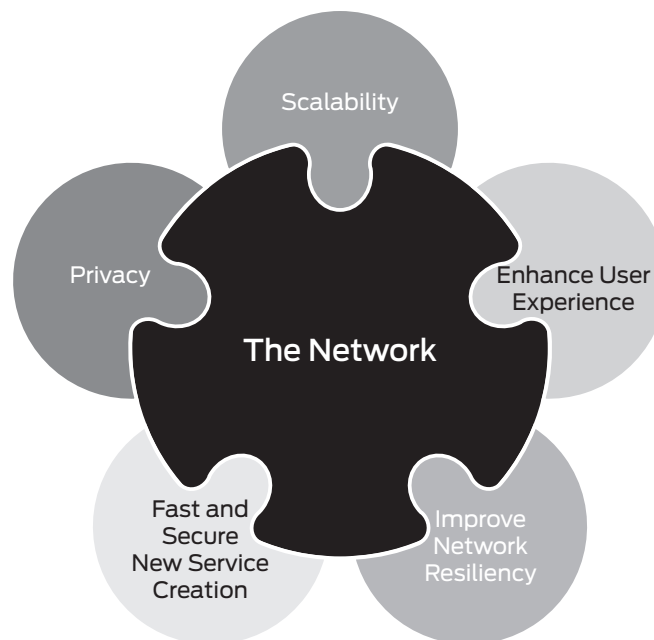


Figure 5: Network's role in virtualization

Let's take a look at a perfect example of this critical role of networks. Initial voice over IP (VoIP) deployments bear evidence of the importance the network plays in rolling out new technologies to help improve organizational efficiencies and improve operational costs. The implementation of VoIP connectivity for users and devices was a simple matter of adding ports for phones. However, the transmission of this time-sensitive voice traffic across networks that were not designed or built for this type of real-time environment resulted in poor call quality and unacceptable user experiences due to immature traffic handling and insufficient throughput. The end result for many of these early adopters of VoIP networks was building a second network, next to the existing network, that was dedicated just to handle this new VoIP traffic.

With this example in mind, when planning to implement one or more virtualization technologies onto your network, it would be prudent to review the additional requirements being placed on the network and any potential issues that might arise when introducing them into an already congested or poorly performing network infrastructure.

Consolidation of Network Traffic

As organizations adopt technologies such as server, desktop, and application virtualization to realize economic benefits, the implementation of these virtualization technologies causes an additional concentration of traffic in certain areas of the network. In many cases as organizations implement server virtualization, they also remove servers from remote offices and place them into a centralized data center. This consolidation of servers places additional traffic demands on the network as well as exposing the applications now running in a distributed environment to overloaded network effects such as latency, jitter, and packet loss. In addition, each of the servers running these virtualized services experiences an increased amount of network traffic both into and out of it.

Increased Number of Network Connections

Another impact to the network from the implementation of virtualization services is the increased number of network connections both within a virtualized device (server, storage, etc.) and between different virtualized devices. The virtual machines running within a single virtualized server and across multiple virtualized servers must connect to each other in real time to ensure continuous service to the users. For example, an end user might be interacting with multiple virtualized servers, between multiple virtualized storage servers, or between multiple application servers. This increased number of network connections could overload an already stressed network infrastructure.

Desktop Quality Experience

The network also plays a key role in determining a quality experience for end users when running a desktop virtualization environment. With the desktop virtualization server residing in a remote location from end users, the quality of their experience is dependent on available network bandwidth, acceptable latency, and minimal packet loss across the network connections.

Security

The introduction of virtualization technology into an organization's network creates several new security challenges. For example, in a virtualized environment the compromise of a single physical server could affect numerous virtualized services and a larger number of users. There are three key security challenges:

1. IT organizations using normal network-based security platforms are not able to monitor traffic passing back and forth between virtual machines. Thus, worms and other malicious traffic could propagate unchecked.
2. Use of virtualized services across a distributed network environment results in multiple flows per transaction that make it difficult to enforce access entitlements and might create throughput issues for security enforcement systems due to multiple, high-bandwidth TCP sessions needing inspection.
3. Since all of the virtualization technologies require use of the network for transport, these implementations require heightened security to prevent denial-of-service (DoS) and other malware attacks that could result in critical information not being available or being corrupted.

It should now be clear that each type of virtualization technology provides unique benefits to an IT organization. However, having taken a closer look at how implementation of these various virtualization services can impact a network, the next question that comes to mind is how can you better prepare for this?

High-Performance Networks and Network Virtualization

The network plays an increasingly critical role in delivering the IT applications and services such as virtualization. From applications in the data center to office workers with PCs to mobile users with notebooks and smart phones, to IP cameras and networked sensors, the network is the common platform that delivers these services.

High-performance networking and security products of today are able to meet stringent business requirements and deliver a consistent experience and cost efficiencies. By using standards-based solutions and architectural innovation in software, silicon, and systems, these high-performance products are also able to massively scale based on three dimensions:

- **Connectivity**—of users and devices to the network
- **Capacity**—as measured by network throughput delivering application response time
- **Control**—which is characterized by security, traffic separation, and user experience

More recently, networking vendors introduced a concept called network virtualization, which brings an even higher level of flexibility, scalability, and security to the network infrastructure. Network virtualization combines the hardware, software, and functionality resources within a network infrastructure by “virtually” splitting up available bandwidth into independent, secure channels that can be assigned to different devices or services. In addition, since all of the separate physical networks can now be combined into one physical network running many virtual networks, the management is simplified (Figure 6).

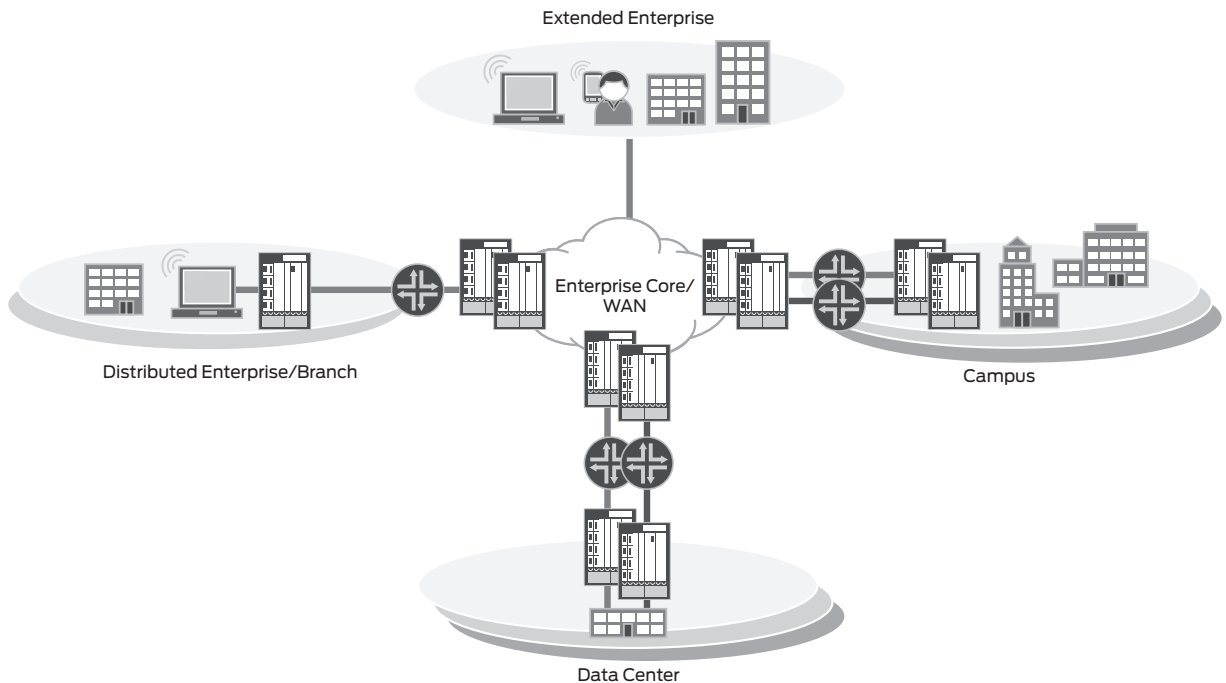


Figure 6: One physical network—many virtual networks

Network virtualization can deliver numerous benefits. It can boost network scalability, performance, and resiliency; support traffic segmentation and privacy; enhance end user experience; and make it possible to deploy new applications and services on the network in minutes. Some common network virtualization technologies being implemented, as shown in Figure 7, include:

- **Network Service Virtualization**—This type of virtualization improves network utilization, scalability, and resiliency by virtualizing the transport of traffic using virtual connectivity. It also virtualizes network services such as Layer 2 VPN (L2VPN), Layer 3 VPN (L3VPN), VPLS, and Psuedowire—and offers many options for secure virtual connectivity.
- **Network Device Virtualization**—This method improves network device utilization and manageability, by improving routing utilization and simplifying configuration when managing virtual routers or physical interfaces.
- **Network Link Virtualization**—In this case, the virtualization improves network link utilization, scalability, resiliency, and security using technologies such as traffic segmentation, traffic prioritization, and link aggregation.

Network Service Virtualization	L2VPN L2 Point-to-Point	L3VPN L3 Multipoint-to-Multipoint		VPLS L2 Point-to-Multipoint	
	Privacy	MPLS Traffic Engineering		Scalability Resiliency	
Device Virtualization	Virtual Router Scalable Routing Separation	VRF Lite Routing Separation	Logical Systems Routing and Management Separation	Bridge Group Simplifies Configuration	Virtual Switch Scalable Switching Separation
	VLAN Traffic Segmentation Priority	LAG Scale Bandwidth Resiliency	GRE Tunnel non-IP Traffic	MPLS LSP Traffic Segmentation Priority	

Figure 7: Common network virtualization technologies

Juniper's Network Virtualization Leadership

Juniper Networks delivers innovative software, silicon, and systems that transform the experience and economics of networking for global service providers, leading enterprises, and public sector organizations. Our core routers, switches, and security hardware and software run the world's largest and most demanding global networks. Since 1996, we have helped our customers stay ahead of the demands posed by the exponential growth in network users and endpoints, while meeting the business imperatives for high performance, reliability, and absolute security.

At Juniper, we have a unique and fundamentally different way of looking at the challenges of the global network. We've developed and productized some of the industry's most groundbreaking innovations across every aspect of networking technology. This includes a dedication toward developing new pure-play IP solutions based on a unique single architecture, single OS, and single release train that ensures performance, reliability, and security at the scale that customers demand of their networks—without compromise.

We are taking this same approach toward building innovative network virtualization solutions that help our customers continue to transform the experience and economics of their networking infrastructures. Juniper offers a myriad of network virtualization technologies and uniquely offers them in one OS—with Juniper Networks® Junos® operating system, running consistently across Juniper's switching, routing, and security platforms.

Conclusion

The spread of virtualization technologies across an enterprise infrastructure has brought about exciting times. IT professionals are now able to maximize computing resources and provide a higher level of flexibility and manageability for desktops, applications, and devices that function as true "network" services. However, the introduction of these new virtualization technologies onto an existing network infrastructure requires those same IT professionals to understand (1) how well their existing network handles increased traffic demands, (2) any impacts to the network from the new virtualization services, and (3) what types of solutions are available to ensure these new services run effectively and efficiently. The good news is there are a variety of high-performance networking and network virtualization solutions available today that can help. Leading networking vendors such as Juniper Networks offer a broad portfolio of innovative software, silicon, systems, and network virtualization technologies to help you install, integrate, and manage all of these new technologies.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.