Statseeker
every port. every minute. everywhere.

Virtualizing Your Network: Benefits & Challenges

What is Virtualization?

Gartner Research[1] defined network virtualization as the process of combining hardware and software network resources and functionality into a single virtual network. This offers access to routing features and data streams that can provide newer, service-aware, resilient solutions; newer security services that are native within network elements; support for subscriber-aware policy control for peer-to-peer traffic management; and application-aware, real-time session control for converged voice and video applications with guaranteed bandwidth on-demand.

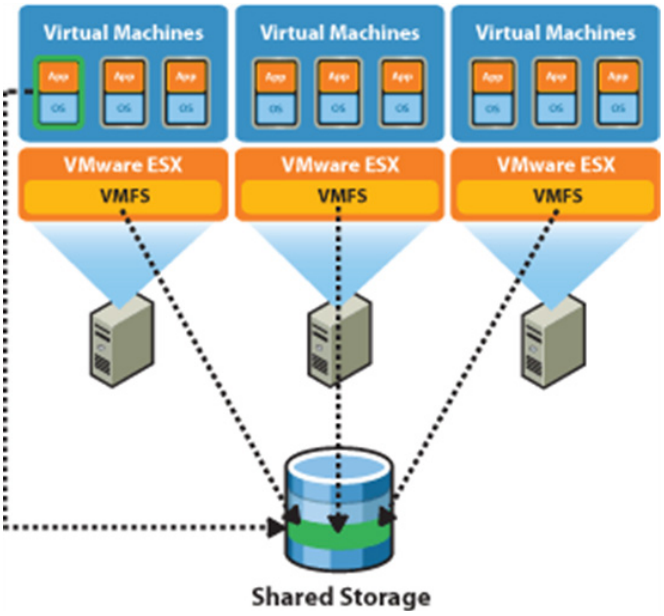
For the most part, when we speak of virtualization, we speak of hardware virtualization. That means that we create, on a host machine, a virtual machine that looks like another computer with an operating system and software. The software on the virtual machine is separate from the host machine's resources, and as far as it is concerned, it is running on its own computer (that we call the guest). Both in information technology (IT) and in operational technology (OT) environments the benefits of virtualization have led to its rapid adoption.

This white paper is not a prescriptive guide to network virtualization, rather it is a high-level overview focused on the benefits and challenges of network virtualization. While it will review the benefits, it will also cover the specific challenges network administrators and their respective businesses should understand to cost-effectively apply this technology to gain maximum results.

Virtualizing Computers and Servers

Full virtualization is the most common methodology for virtual machines. This means that the guest operating system runs unmodified on the virtual machine. This permits the centralization of all of the administrative tasks and enabling full scalability while maximizing hardware utilization. Many operating systems can be run in parallel on a single CPU.

Using virtualization, an IT organization can manage updates and changes to the operating system up to and including ignoring them. This can be critical in OT applications, where software has been designed to run on obsolete hardware and operating systems, and has not been updated. At the same time, this software is critical to the operation of the factory or process plant. Virtualization can give this software a longer operating lifecycle time, and can save both costs and intellectual property.

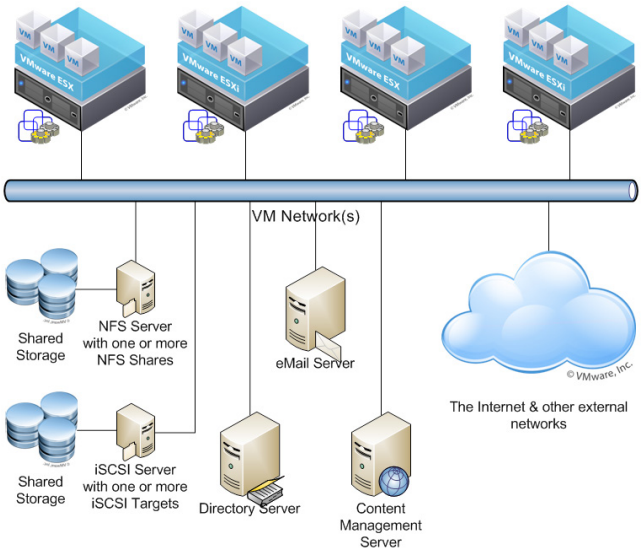


Desktop virtualization separates the logical desktop from the actual hardware. Virtual desktop infrastructure (VDI) permits the user to interact with the computer through another host computer or device on a network connection. The computer may be a server, enabling multiple user sessions at the same time. The latest trend in VDI is hosted virtual desktops (HVDs) in which the desktop is an image on a cloud-based server, managed by a hosting firm that specializes in HVD hosting.

Virtualizing Your Entire Network

Network virtualization is often defined as the process of combining hardware and software network resources and network functionality into a single, software based administrative entity - a virtual network. So, hardware functions like switches and network adapters (NICs), firewalls, network appliances like load balancers, network storage devices, are all combined into virtual devices instead of hardware. This can provide rapid scalability, as well as additional protection against hardware failure.

[1] Gartner Research - www.gartner.com/it-glossary/network-virtualization



Building a Greenfield Virtual Network

Virtualizing your network is very easy when you are building a greenfield network - one from scratch. You can design the network to be virtual from the beginning, and you can incorporate all the virtual tools you'll need to manage your network from the very start.

Organizing your virtual network can be relatively easy, and increase network efficiency. You can design your network so that your local area networks are subdivided into virtual networks and virtual local area networks.

You can dramatically improve efficiency and load balancing by doing this. You can also improve security by segmenting your network and establishing role-based and location-based permissions and procedures. Doing this in a virtual environment enables you to be agile about changing your network architecture as needed to cope with changing and increasing network loading and demand.

When it comes to network virtualization, the software defined network enabled approach allows network administrators and owners to integrate physical and virtual environments. While this technology has been around for years, only recently it has accelerated its adoption rate and is showing up in more and more network strategies.

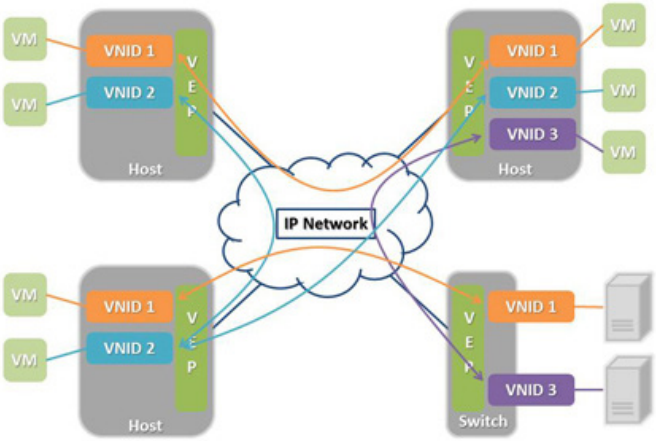
And why not? Significant agility, increased network visibility and lower operating costs are quickly realized for both new and existing network deployments.

Wireless networks and sensor networks that are part of the Internet of Things are candidates for virtualization, and this can be done easily by first segmenting the network and then using virtual NICs and other virtual devices, such as edge firewalls, as well as virtualized input/output (I/O) to provide agile network connectivity.

Adding Virtuality to Brownfield Networks

It is not as easy to add virtuality to an already existing, or brownfield, network as it is to start from scratch with a completely virtualized network. In the first place, you have a working network, and changing its topology or replacing components has to be done when the network is down. Very rarely is a working network down. So, what has to happen is that the virtualization architecture has to be designed, and the virtual network components constructed and tested alongside the non-virtual network you are replacing or revising, and then a hot cut over must be done, making sure that all of the features and functions of the original network segment are preserved.

One of the techniques that are often used is to make a virtual overlay above the brownfield hardware and firmware network. New functionality is done in the overlay, while the main network traffic continues in the brownfield network. As each segment of the network requires replacement, it can be left as a hardware network, or it can be virtualized, depending on cost and availability. The important thing is to keep the availability of the network as close to 100% as possible.



The Benefits of Virtualization

Virtualization has significant benefits both in computing and in networking. That's why both have been accepted so readily. This is especially true in OT networking and control systems, where the rest of the system is intended to live for 30 years, and the life of the computer and network components is less than two years. Virtualization also permits rapid changes and agile re-deployment, which is necessary for the Internet of Things.

Safety and Robustness

Virtualizing computers and servers, as well as network components, can add a significant measure of both safety and robustness to the network.

Storing images of the virtual machines off site, in the cloud, or at another location means that if the site has an accident, or the site network is destroyed by weather (like Hurricane Katrina did to many petrochemical plants) it will be easy to re-construct the systems, re-use the disk images, and be back in business months earlier than if the systems were not virtual. In addition, virtual systems have a failover mode, where a defective disk simply switches to a backup on the fly, and the failed component can be repaired, while the system continues to run.

Lifecycle Management

As we have noted, especially in OT systems, such as building automation, factory automation and process control system networks, there is a fundamental issue with lifecycle. The control system, its I/O, and the final control elements (valves, etc.) are intended to last the life of the project - easily 30 years. Unfortunately, through the action of the market and Moore's Law[2], computer, server, and network components have a lifecycle of about 18 months. This disparity is well known in project work, where the time from project initiation to startup of the network and control system may be as long as 48 months. So, when the end-user receives control of the system, it is obsolete by as much as 36 months, and may not be maintainable.

Virtualization solves this problem by creating virtual machines that run on operating systems that would otherwise be obsolete and no longer maintained. As an extreme example, there might be a laboratory information management system (LIMS) that operates on Windows 95, and which would have to be completely re-written to run on a modern operating system. Running this application on a virtual machine allows the user to continue to use the application, and the operating system it was written for, without worry that it is obsolete and not maintainable.

Security

Completely virtualizing your servers and networks allows you a measure of security that you didn't have before. Just virtualization won't necessarily make your system safe, but it will get rid of much of the chance for hardware to be compromised by, say, inserting a USB stick, or a CD-Rom or DVD with malware on it. Virtualization severely reduces the number of physical devices that you need to have control over, too.

You also have the ability of much more easy network segmentation, and more direct control with policies and procedures. This means a great deal when you have a dynamic network where the edges are variable, due to user devices going in and out of the network.

Challenges with Virtualization

While there are great benefits from virtualization, there can also be serious challenges. One of the challenges is that the IT staff, OT staff, or sysadmins must truly know their servers and network. Especially in a virtualization overlay on an existing physical network, the administrator must know exactly what their system is doing, what they want it to do and how it will be laid out for future expansion.

You can't just throw another managed switch on a line and call it good. You need to make sure that the data center you are virtualizing has adequate and appropriate electric power and backup generation in case of power outages. You need to make sure that the building you're in has adequate heating and cooling resources, and that it is secure from physical penetration.

From your design, you need to make sure that the virtualized system has enough availability to operate better than the old system did. Consider this:

Changing Best Practices

This means that system administrators need to borrow from OT systems the concept of front end engineering design (FEED). The virtualized network must be specified at least as well as you would specify a physical set of hardware and software. A FEED must be clear and complete, and supported by all the stakeholders in the system.

Changing Standards

"The nice thing about standards is that there are so many of them," said legendary computer scientist Andrew S. Tanenbaum. Tanenbaum may be cynical, but he is not wrong. One of the things that can bite a virtual system is a change in a standard that makes the way the system is virtualized not work, or not work well.

The system administrator needs to stay abreast of standards better than if they were just running a standard hardware/firmware system.

One of the issues virtual systems must deal with is the hardware. Often, the idea that the system is virtual is taken to mean that you can run the system on significantly less costly servers and other hardware. This is far from true. In fact, the hardware and firmware you use in a virtual system needs to be much more robust than a conventional system.

Changing the Architecture of the Network

From the very beginning you should implement a network information management tool, such as Statseeker. In any virtual environment, it is even more critical than in a standard networking situation, to be able to see down into the system - to be able to see all the devices and nodes, virtual or not, that are on your network. Statseeker gives you the ability to scale (read: contained CAPEX/OPEX cost) from a small system to a huge system of various interfaces. Otherwise, you'll drive yourself crazy trying to troubleshoot the virtual system.

You will also need to avoid VM sprawl, and storage will need to be centralized and not located at each computer. And in doing that, you need to make sure that security is not dropped off. In a virtual network, combining Statseeker with a good vulnerability scanner is critical to proper security implementation.

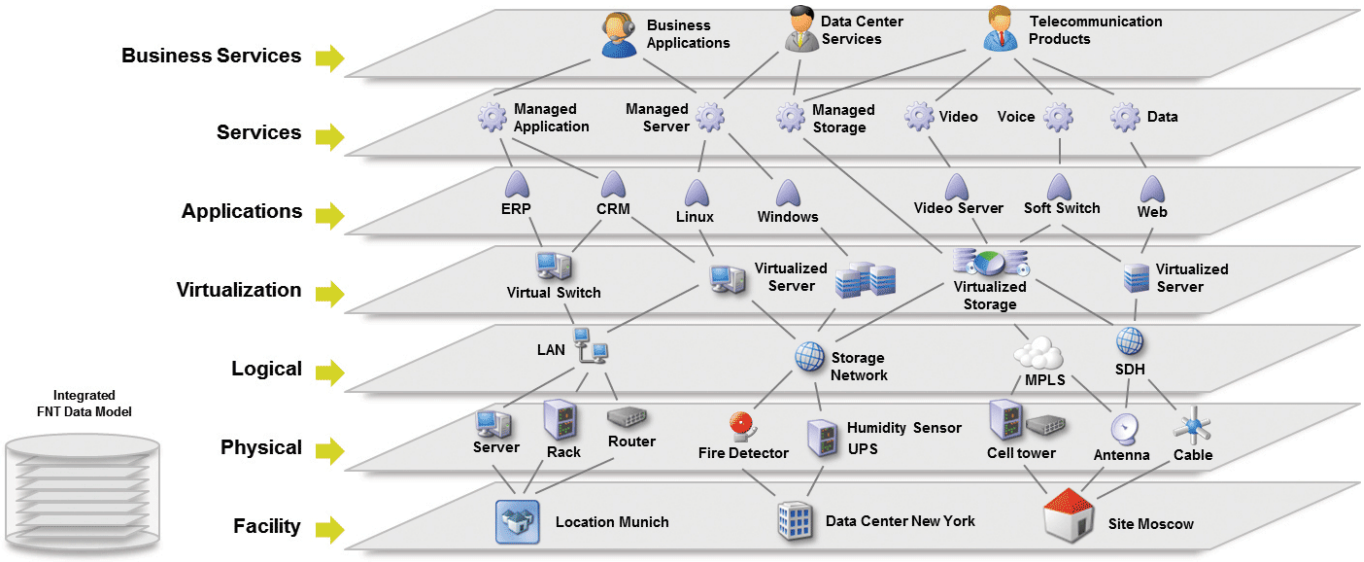
New Skills and Organization for IT and Admin Staff

You and your staff need to have training and experience in handling virtualization and virtual networks. The system is not the same as a standard system, it's just virtual. It needs to be operated, designed, and maintained differently, and those skill sets must be available to you before you start virtualizing your systems.

The IoT, the Cloud and Virtualization

Virtualization is ubiquitous, and the sensor-centric networks that make up the IoT are becoming ubiquitous as well. Most data goes to the cloud, where virtual servers and hosted desktops permit DaaS (Data as a Service) applications to be ubiquitous as well. Virtualization technology is implemented in thousands of devices and systems already, and the idea is that IoT and Cloud computing will make our lives better.

[2] Gordon E. Moore, co-founder of Intel, 1st to observe a doubling every year in the number of components per integrated circuit



Virtualization and Its Impact on Network Monitoring

Network monitoring in a standard hardware/firmware system has often been considered a “nice to have” rather than a “critical need.” As we move to virtual systems, the ability to see all the way down through the network, in real-time becomes a critical need.

Since you are operating a virtual network, you can’t just walk out there and lay hands on the server, or the network appliance, that is giving trouble. You must have some way to get performance data and diagnostic data from the virtual system, just as you would from a standard, physical hardware and firmware system. Statseeker provides the tool you need to do that. It is simple to implement, simple to operate, requires only a single server, and provides the deep granularity you need to make your virtual network behave.