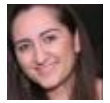
CLOUD / JANUARY 4, 2018

What Is Network Virtualization?



Diana Shtil

Network virtualization describes hardware, software, and network functionality combined into a single, virtual network. This allows developers and engineers to test software that is under development or in the simulation stage. But there's a lot more to network virtualization. What makes it such a great resource for developers? And why should you virtualize your network? Find answers to these questions here.

As on-premises server environments become more expensive and complex, organizations are virtualizing more and more of their traditional infrastructure. In fact, a 2016 Gartner report found that, on average, enterprises are already pursuing network virtualization and implementing virtual machines to great effect, and have virtualized 75 percent or more of their data centers.

By implementing network virtualizing, the network administrator can automate many of the tasks previously performed manually, making the network much easier to scale. Additionally, network virtualization software allows a single hardware platform to support multiple virtual devices that can be used as needed to cut costs and increase flexibility.

But what *is* network virtualization? In this post we will be providing a definition, as well as some quick insights into how to put it to work for your business.

Making the switch to network virtualization? Gigamon GigaSECURE® can help ensure that your vital network data stays safe.

What Is Network Virtualization?

Network virtualization in computing is the procedure that separates the management plane from the control plane by combining hardware (such as switches and routers) and software network resources into a single, software-based administrative entity called a virtual network. This is often used in conjunction with software containers.

The virtual network simulates the functionality of traditional hardware; once a software-based view of the network has been created, the hardware is then only responsible for forwarding packets while the virtual network is used to deploy and manage network services. Additionally, software virtualization can be used to create network overlays — layers of network abstraction that run on top of the physical network. Storage virtualization — managing all storage as a single entity — is sometimes included as an aspect of network virtualization.

Currently, there are two types of network virtualization:

- **Internal Virtualization**
  Internal virtualization is designed to use software containers to replicate the functionality of a single network.
- **External Virtualization**
  External virtualization combines multiple local networks into a single “virtual” network to improve the network efficiency.

Many organizations are also taking advantage of cloud technologies to further their network virtualization objectives. Network virtualization in cloud computing follows the same basic idea, but instead relies on cloud-based resources to create a working virtual network.

Simply put, the question “what is network virtualization?” can be answered as the ability to run networks uncoupled from your hardware. This allows for certain advantages.

Why Virtualize Your Network?

If you’re interested in the benefits of network virtualization, here are the most important advantages to consider:

1. **Boost IT Productivity:** Network virtualization can reduce the cost of purchasing and maintaining hardware, which is especially useful and logical for organizations with bursty workloads that would require over-provisioning to keep up with demand. Also, as data volume and speed increase, the ability to scale efficiently allows security teams to maintain better network visibility.
2. **Improved Security and Recovery Times:** Network virtualization software allows organizations to control which types of traffic go through the physical network. Many attackers rely on the fact that once they’ve breached the security perimeter, there are few, if any, security controls in place. Network virtualization allows organizations to better combat security threats by creating micro-perimeters within the network. With this control, known as micro-segmentation, they can keep sensitive data within a certain virtual network that only authorized users can openly access. For example, an organization could secure VoIP data by placing it within its own virtual network with restricted user access. According to Forrester Consulting: “‘Micro-segmentation provided through network virtualization paves the way for implementing a Zero Trust model. Where previous security models assumed the threat was outside the network, Zero Trust assumes even the network is insecure.” Additionally, network virtualization software can reduce or even eliminate outages created by hardware failures and improve disaster recovery times. Disaster recovery with traditional network hardware requires many manual, time-intensive steps, including changing the system’s IP address and updating the firewall. Network virtualization eliminates these steps.
3. **Faster Application Delivery:** Without network virtualization, network provisioning is a time-intensive, manual process. As a result, any time an application requires you to provide fundamental network changes, the application deployment time is extended. Moreover, the risk of a deployment failure increases significantly when organizations perform manual

deployments. Since network virtualization automates network configuration, they can instead cut application deployment time from weeks to minutes. Reducing deployment time can have a significant impact on a company’s bottom line, allowing for faster new-product rollouts or major application updates.

Gigamon as a Network Virtualization Solution

To monitor and secure virtual workloads, it is critical to have immediate and deep visibility of network activity across the entire infrastructure. Application and security monitoring technology need to be able to analyze security threats, congestion points and application behavior. To accomplish this, data from the physical and virtual network must be readily accessible.

Gigamon offers an integrated network virtualization platform solution using the GigaSECURE® Security Delivery Platform for both VMware NSX and ESX network virtualization. With this network virtualization platform, security operations and networking teams can automate external traffic visibility of both physical and virtual workloads and networks while benefiting from the efficiency of network virtualization. In fact, 2019 marked the sixth consecutive year with Gigamon ranking as the market leader in the IHS Network Monitoring Equipment Annual Market Report. This demonstrates that when it comes to understanding and taking advantage of the new avenues offered by network virtualization (as well as other network related issues), successful organizations are relying on superior Gigamon visibility and analytics platforms for optimum site performance.

To learn more, please read our “Enhanced Monitoring for VMware Infrastructure” solution brief.