International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 05 • Number 2 • July – December 2013 pp. 131- 133 www.csjournals.com

Virtualization of Network Functioning

Peter Vinodchand. K. (Research Scholar)
Assistant Professor, Department of Computer Science
Government First Grade College. ALNAVAR.

Abstract: Network virtualization is reframing the rules for the way services are delivered, from the software-defined data center (SDDC), to the cloud edge. This approach moves networks from static, inflexible, and inefficient to dynamic, agile, and optimized networks. Modern networks must keep up with the demands for cloud-hosted, distributed apps, and the increasing threats of cybercriminals while delivering the speed and agility you need for faster time to market for your applications. With network virtualization, you can forget about spending days or weeks provisioning the infrastructure to support a new application. Apps can be deployed or updated in minutes for rapid time to value.

Introduction: (NV) Network Virtualization refers to abstracting network resources that were traditionally delivered in hardware to software. NV can combine multiple physical networks to one virtual, software-based network, or it can divide one physical network into separate, independent virtual networks. Network virtualization software allows network administrators to move virtual machines across different domains without reconfiguring the network. The software creates a network overlay that can run separate virtual network layers on top of the same physical network fabric.

Network virtualization decouples network services from the underlying hardware and allows virtual provisioning of an entire network. It makes it possible to programmatically create, provision, and manage networks all in software, while continuing to leverage the underlying physical network as the packet-forwarding backplane. Physical network resources, such as switching, routing, firewalling, load balancing, virtual private networks (VPNs), and more, are pooled, delivered in software, and require only Internet Protocol (IP) packet forwarding from the underlying physical network.

Network and security services in software are distributed to a virtual layer and are attached to individual workloads, such as virtual machines (VMs) or containers, in harmony with networking and security policies defined for each connected application. When a workload is enthused to another host, network services and security policies budge with it & when new

workloads are created to scale an application, necessary policies are dynamically applied to these new workloads, providing greater policy consistency and network agility.

Network Virtualization types:

Internal network virtualization: A virtualized internal network is a network that is restricted to one machine only. Hence it is also called "network in a box." It is essential to improve the efficiency of the network as communication over a network interface – which is also virtual – is allowed for communication.

External network virtualization: At least one local network is subdivided or joined into the virtual network in order to improve the effectiveness of big corporate networks or data center. The principle of an external network is the virtual local area network and the switch by utilizing these systems, that are physically attached to a similar local network into various virtual networks can be configured by the administrator. Virtual local area network permits the administrator to join systems on another local network into spanning the portions of a big network. Whereas in the internal network, to create a "network in a box" "hypervisor control programs or pseudo interfaces" with containers are joined to configure a single system.

Network virtualization abstracts all IT physical infrastructure elements (compute, network, and storage) away from proprietary hardware, pooling them together. From this pool, resources can be deployed automatically where they are needed most as demands and business needs change. This is especially relevant in the telecommunications industry, where traditional providers are challenged with transforming their networks and operations to keep up with technological innovation.

Whether it's virtual reality in remote surgery or smart grids allowing ambulances to safely speed through traffic lights, new advancements offer the promise of radically improved and optimized experiences. But the traditionally hardware-dependent networks of many service providers must be transformed to accommodate this innovation. Network virtualization offers service providers the agility and scalability they need to keep up.

Just as hyperscale public cloud providers have demonstrated how cloud-native architectures and open source development can accelerate service delivery, deployment, and iteration, telecommunication service providers can take this same approach to operate with greater agility, flexibility, resilience, and security. They can manage infrastructure complexity through automation and a common horizontal platform. They can also meet the higher consumer and enterprise expectations of performance, safety, ubiquity, and user experience. With cloud-native architectures and automation, providers can more rapidly change and add services and features to better respond to customer needs and demands.

Benefits of network virtualization

Network functions virtualization (NFV) is a way to virtualize network services—such as routers, firewalls, virtual private networks (VPNs), and load balancers—that have traditionally been run on proprietary hardware. With an NFV strategy, these services are instead packaged as VMs or containers on commodity hardware, which allows service providers to run their network on less expensive, standard servers thereby increasing flexibility and workload portability and providing the ability to spin workloads up and down with minimal effort.

Conclusion: With these services virtualized, providers can distribute network functions across different servers or move them around as needed when demand changes. This flexibility helps improve the speed of network provisioning, service updates, and application delivery, without requiring additional hardware resources. The segmentation of workloads into VMs or containers can also boost network security as they use less and less expensive hardware and also allows the network resources to be scaled elastically to address changing demands.

References:

https://www.vmware.com/topics/glossary/content/network-virtualization.html

https://www.techtarget.com/searchnetworking/What-is-network-virtualization

https://www.arista.com/en/solutions/network-virtualization

https://www.sdxcentral.com/networking/sdn/definitions/whats-network-virtualization/network-virtualization-and-how-it-works/