**NETWORK VIRTUALIZATION**

**Introduction:-**

The Internet has been stunningly successful in modeling the way we access and exchange information in the modern world. However, its sheer size has become the biggest impediment to its further growth. Due to its multi-provider nature, adopting a new architecture or modification of the existing one requires consensus among competing stakeholders. In recent years, the concept of network virtualization has attracted significant attention in the debate on how to model the next-generation networking paradigm that can replace the existing Internet. It is believed that network virtualization can eradicate the so-called ossifying forces of the current Internet by introducing disruptive technologies. Network virtualization is defined by decoupling the roles of the traditional Internet service providers (ISPs) into two independent entities ]: infrastructure providers (InPs), who manage the physical infrastructure, and service providers (SPs), who create virtual networks (VNs) by aggregating resources from multiple InPs and offer end-to-end services. Such an environment will proliferate deployment of coexisting heterogeneous network architectures free of the inherent limitations of the existing Internet.  
 **What is network virtualization?**

Virtualization is the ability to simulate a hardware platform, such as a server, storage device or network resource, in software. All of the functionality is separated from the hardware and simulated as a “virtual instance,” with the ability to operate just like the traditional, hardware solution would. Of course, somewhere there is host hardware supporting the virtual instances of these resources, but this hardware can be general, off-the-shelf platforms. In addition, a single hardware platform can be used to support multiple virtual devices or machines, which are easy to spin up or down as needed. As a result, a virtualized solution is typically much more portable, scalable and cost-effective than a traditional hardware-based solution.

When applied to a network, virtualization creates a logical software-based view of the hardware and software networking resources (switches, routers, etc.). The physical networking devices are simply responsible for the forwarding of packets, while the virtual network (software) provides an intelligent abstraction that makes it easy to deploy and manage network services and underlying network resources. As a result, NV can align the network to better support virtualized environments.

**Why Network Virtualization?**

The current network architecture used to build enterprise networks and data centers is outdated and cannot enable IT agility.

• Built on old protocols: Legacy infrastructure uses the archaic Spanning Tree Protocol (STP) to prevent routing loops and broadcast radiation by disabling ports that are not part of the “tree.” These disabled ports are made active in the event of a link failure on one of the active ports. This means that up to half of the ports in a network could be in “passive” mode, leading to a highly inefficient, underutilized network.

• Static architecture: Network infrastructure is very rigid and optimized for static environments. Network infrastructure provisioning can often have long lead times, and changes often must be made manually on a box-by-box basis. This process can lead to large amounts of human error.

• Not designed for modern compute models: Traditional networks are designed for best-effort traffic, such as e-mail and Internet browsing. Today’s IT strategies revolve around trends such as real-time collaboration, virtualization and cloud computing. This places the emphasis on the network evolving away from best-effort solutions and toward a network that features guaranteed delivery and low latency.

• Protocol overlays: With legacy network technologies, the same protocols and features need to be implemented at Layer 2 and then again at Layer 3, creating extra complexity due to the successive overlay of standalone protocols.

• High amounts of latency and insufficient resiliency: Legacy networks are architected with three or more tiers, and traffic is passed through each tier of the network core and then back through each tier. Each of these hops between network devices adds latency and creates points of failure that can impede the performance of mission-critical applications.

**Historical Perspective**

The concept of multiple co-existing logical networks appeared in the networking literature several times in the past, which can be categorized into four main classes

**Virtual Local Area Network**A virtual local area network (VLAN) is a group of logically networked hosts with a single broadcast domain regardless of their physical connectivity. All frames in a VLAN bear a VLAN ID in the MAC header, and VLAN-enabled switches use both the destination MAC address and the VLAN ID to forward frames. Since VLANs are based on logical instead of physical connections, network administration, management, and reconfiguration of VLANs are simpler than that of their physical counterparts. In addition, VLANs provide elevated levels of isolation.

**Virtual Private Network**   
A virtual private network (VPN) is a dedicated network connecting multiple sites using private and secured tunnels over shared or public communication networks like the Internet. In most cases, VPNs connect geographically distributed sites of a single corporate enterprise. Each VPN site contains one or more customer edge (CE) devices that are attached to one or more provider edge (PE) routers. Based on the protocols used in the data plane, VPNs can be classified into the following broad categories:

***Layer 1 VPN*** : Layer 1 VPN (L1VPN) framework emerged in recent years from the need to extend L2/L3 packet-switching VPN concepts to advanced circuit-switching domains. It provides a multiservice backbone where customers can offer their own services, whose payloads can be of any layer (e.g., ATM and IP). This ensures that each of the service networks has independent address space, independent Layer 1 resource view, separate policies, and complete isolation from other VPNs.

***Layer 2 VPN*** : Layer 2 VPNs (L2VPNs) transport Layer 2 (typically Ethernet) frames between participating sites. The advantage is that it is agnostic about the higher-level protocols and consequently, more flexible than L3VPN. On the downside, there is no control plane to manage reachability across the VPN.

***Layer 3 VPN***: Layer 3 VPN (L3VPN) is characterized by its use of Layer 3 protocols in the VPN backbone to carry data between the distributed CEs. There are two types of L3VPNs: In CE-based VPN approach, the provider network is completely unaware of the existence of a VPN. CE devices create, manage, and tear up the tunnels between themselves. Sender CE devices encapsulate the passenger packets and route them into carrier networks; when these encapsulated packets reach the end of the tunnel, i.e., receiver CE devices, they are extracted and actual packets are injected into receiver networks. In PE-based approach, the provider network is responsible for VPN configuration and management. A connected CE device may behave as if it were connected to a private network.

***Higher Layer VPNs*** : VPNs using higher (e.g., transport, session, or application) layer protocols also exist. SSL/TLS-based VPNs are popular for their inherent advantages in firewall and NAT traversals from remote locations. Such VPNs are light-weight, easy to install and use, and provide higher granularity of control to their users

**Network Virtualization Environment**

Unlike the existing all-IP Internet, a virtualized networking environment is a collection of multiple heterogeneous network architectures from different service providers. Each service provider leases resources from one or more infrastructure providers to create virtual networks and deploys customized protocols and services.

***Business Model*** ***:*** The main distinction between the participants in the network virtualization model and the traditional model is the presence of two different roles: infrastructure providers and service providers, as opposed to the single role of the ISPs.

***Infrastructure Provider(InP):*** Infrastructure providers deploy and actually manage the underlying physical network resources. They offer their resources through programmable interfaces to different service providers. Infrastructure providers distinguish themselves through the quality of resources they provide, the freedom they delegate to their customers and the tools they provide to exploit that freedom.

***Service Provider(SP):*** Service providers lease resources from multiple InPs to create and deploy virtual networks by programming allocated network resources to offer end-to-end services to the end users. A service provider can also provide network services to other service providers. It can also create child virtual networks by partitioning its resources and can act as a virtual InP by leasing those child networks to other service providers.

***End User:*** End users in the network virtualization model are similar to that of the existing Internet, except that the existence of multiple virtual networks from competing SPs provides them a wider range of choice. Any end user can connect to multiple virtual networks from different SPs for different services.

**Architecture**

In a network virtualization environment (NVE), the basic entity is a virtual network (VN). A VN is a collection of virtual nodes connected together by a set of virtual links to form a virtual topology, which is essentially a subset of the underlying physical topology. Each virtual node is hosted on a particular physical node, whereas a virtual link spans over a path in the physical network and includes a portion of the network resources along the path.

Each VN is operated and managed by a single SP, even though the underlying physical resources might be aggregated from multiple InPs. Suppose there are two virtual networks, VN1 and VN2 created by the service providers SP1 and SP2, respectively. SP1 composed VN1 on top of the physical resources managed by two different InPs (InP1 and InP2) and provides end-to-end services to the end users U2 and U3. SP2, on the other hand, deployed VN2 by combining resources from infrastructure provider InP1 with a child VN from service provider SP1. End users U1 and U3 are connected through VN2.

The owner of a VN is free to implement end-to-end services by deploying custom packet formats, routing protocols, forwarding mechanisms, as well as control and management planes. As mentioned earlier, end users have the choice to opt to any VN. For example, end user U3 is subscribed to two virtual networks VN1 and VN2 managed by SP1 and SP2, respectively.

**Architectural Principles**

Network virtualization propounds the following principles for the next-generation networking paradigm:

**Coexistence**   
Coexistence of multiple VNs is the defining characteristic of an NVE. It refers to the fact that multiple VNs from different SPs can coexist together, spanning over part or full of the underlying physical networks provided by one or more InPs. In our example, VN1 and VN2 are two coexisting VNs.

**Recursion**   
When one or more VNs are spawned from another VN creating a virtual network hierarchy with parent-child relationships, it is known as recursion as well as nesting of VNs. Service provider SP1, in our example, leased away a portion of its allocated resources to SP2, to whom it appears simply as a virtual InP.

**Inheritance**   
Child VNs in an NVE can inherit architectural attributes from their parents, which also means that the constraints on the parent VN automatically translate to similar constraints on its children. For example, constraints imposed by InP2 will automatically be transferred to VN2 from VN1 through inheritance. Inheritance allows a SP to add value to the spawned child VNs before reselling them to other SPs.

**Revisitation**   
Revisitation allows a physical node to host multiple virtual nodes of a single VN. Use of multiple logical routers to handle diverse functionalities in a large complex network allows a SP to logically rearrange its network structure and to simplify the management of a VN. Revisitation can also be useful for creating testbed networks. Our example shows revisitation in the virtual network VN2.

**Design Goals**

Flexibility  
Manageability  
Scalability  
Isolation  
Stability and Convergence  
Programmability  
Heterogeneity  
Legacy Support

**Implementation Examples**

Some of the implementation examples of network virtualization are given in the following paragraphs:   
  
**a)**  **Router architecture for virtualization support**   
To support virtualization capability, the router architecture has three layers viz. router hardware, router software, and control framework layers. The router hardware typically consists of a switching component for packet forwarding and flow table. The router software performs router’s main operations such as running routing protocols and building routing table. The router software may include virtualization layer in order to support virtualization in router. The virtualization layer typically creates and manages logically isolated virtual systems, which can run various 6 components on the native hardware. Thus, the virtualization layer can support virtualization of router hardware resources by creating the isolated virtual systems, i.e. virtual router. The virtual router is a software implementation of a router that executes the same operations as a physical router. It is an isolated partition of a real router. Multiple virtual routers can coexist over the virtualization layer and each virtual router is completely isolated from the others. In order to provide the management of virtual routers, the virtualization layer can include the virtual machine monitor or hypervisor function. The control framework performs the interaction between the virtual or physical router and other network entities. Control framework defines interfaces, message types including basic protocols and required functions, message flows between router and network entities. The network entities may include networking elements such as routers, switches, and so on. It also may include logical entities such as registry for managing of LINPs, network resources, and user information. Each LINP and virtual routers are managed by resource manager that are implemented in the control framework of the physical router. The resource manager is in charge of creating and managing LINPs and virtual routers in the physical router.

**b)**  **Application virtualization**

Each application accesses the LINP to control the functionality of the LINP, such as routing. Multiple applications may access the same LINP. The task of Application platform is to receive requests from the application, to access LINP to control the functionality of the LINP, and to access virtualized network management to reconfigure LINP.

**Benefits of Network Virtualization**

Virtualization technology offers a unique opportunity for organizations to improve efficiency and scalability and reduce overall operational costs and complexity. It provides an efficient way to centrally manage network resources, simplifying provisioning and maintenance tasks.

Virtual Networks attempt to better utilize networking infrastructure by reusing individual routers or links (i.e., either physical or logical networking resource) for multiple concurrent network instances, or to aggregate 4 multiple such resources to obtain increased capabilities. These resources can be any network component, including routers, hosts, links, and services, (e.g., name mapping services). Increased capability can refer to aggregate capacity provided by bundles of links or groups of routers, or increased fault tolerance of a cluster of primary and backup service systems.

Network virtualization when done at the device level reduces the number of physical network devices, or when done at the network level, by creating multiple logical networks, enables full utilization of one physical network. In brief, following are some of the benefits of network virtualization:   
− It helps in de-ossifying the current network architectures.  
− It allows multiple virtual networks to coexist over a shared physical− infrastructure.   
− It provides paths to the future networks approaches.  
− It allows the deployment of new business roles and players.  
− It reduces/shares cost of ownership.  
− It optimizes the resource (network infrastructure) usage.

**Standardization Efforts**

Standardization Bodies like ITU-T and IETF are working in the area of Network Virtualization. ITU-T has created a FG-FN(Focus Group on Future Networks) and this focus group has considered Network Virtualization as one of the future technology and is working on a document “Framework of network virtualization for Future Networks”.

IETF has also set up a Virtual Networks Research Group (VNRG) which provides a forum for interchange of ideas among a group of network researchers with an interest in network virtualization in the context of the Internet and also beyond the current Internet. The VNRG will consider the whole system of a VN and not only single components or a limited set of components and it will identify architectural challenges resulting from VNs, addressing network management of VNs, and exploring emerging technological and implementation issues. Initial set of work items of VNRG are:  
− concepts/background/terminology  
− common parts of VN architectures  
− common problems/challenges in VN  
− descriptions of appropriate uses  
− some solutions (per-problem perhaps)

**Current market trends**

Network virtualization is offered by several equipment and software vendors through:  
  
 • Network hardware like switches and network adapt ers. These are also known as network interface cards (NICs)   
• Network components like Load balancers, Firewalls, Virtual LANs (VLANs) and containers such as virtual machines (VMs)   
• Storage equipments  
 • M2M elements such as telecommunications 4G HLR and SLR devices   
• Mobile elements (End users devices/equipments like smart phones)   
• Ethernet and Fibre Channel media

Operators that can benefit from virtualization could be:   
• Mobile/fixed network operators   
• Network as a service provider   
• Virtual mobile/fixed network operator   
• Virtual wholesalers   
• Exchange brokers   
• Resellers   
• Virtual network providers   
• Resource providers

**Network virtualization and automation:**

The unique architecture of [virtualization makes automation much easier](http://searchservervirtualization.techtarget.com/answer/Can-virtualization-automation-software-save-me-money) to implement compared with traditional physical environments.  
The virtualization layer turns hardware into software, which is emulated hardware presented to the servers running on a host. This makes integration and automation much easier because you can use [application programming interfaces (APIs)](http://searchexchange.techtarget.com/definition/application-program-interface) to interact directly with virtual machines (VMs). As a result, you can automate many common tasks such as creating VMs, changing power states, managing snapshots and conducting host/storage migrations.  
In larger IT environments, the process of creating VMs en masse can be quite time-consuming. Virtualization is all about efficiency, and automation tools and workflows can help you maximize efficiency. Whether or not you’re moving to a cloud environment, third-party automation tools can greatly reduce the effort it takes to manage a virtual environment.  
When we talk about automating tasks in the data center, the word scripting typically comes to mind. Many scripting languages, such as PowerShell and [Perl](http://searchstoragechannel.techtarget.com/tip/Using-Perl-to-script-backup-jobs), can be used to perform automation in a virtual environment. Using these languages to develop scripts, however, requires programming skills and can be very time-consuming. Scripts are often built in-house, where programming skill levels may vary. As a result, scripts can be buggy, inefficient and poorly documented.  
Many third-party tools help admins automate certain tasks without requiring any programming knowledge.   
While creating a VM is much easier than procuring a physical server, configuring virtual hardware is still a multistep process. This can be a tedious task in large environments, where many servers or desktops may need to be created at one time.

VM sprawl, the uncontrolled growth of virtual machines, is always a concern. VMs are often created with more resources than they need. Automation tools can help you keep tight control of a virtualized environment by introducing discipline. Automation can do the following things for your data center:  
-- greatly reduce administrative effort;  
-- reduce human error;  
-- minimize time between when request is made and its completion;  
-- prevent VM sprawl with a workflow process that requires approval to create new VMs; and  
-- help monitor the lifecycle of VMs and ensure that they are removed when they are no longer needed.

Some of the automation tools are :

CA Virtual Automation.  
Embotics V-Commander.  
ManageIQ EVM Automate.  
Quest Cloud Automation Platform.  
VMware yCloud Director.