Network Virtualization

Mr. Umang Nandu[*1], Mr. Naimin Sanghvi[#2], Ms. Dhwani Hingu[*3] Ms. Pooja Desai[@4]
[*] Student, Department of Computer Technology
[#]Student, Department of Information Technology
[@]Lecturer, Department of Information Technology
Shah & anchor Kutchhi Polytechnic, Mumbai
umangnandu@gmail.com[1], naiminsanghvi95@gmail.com[2], dhwanihingu16@gmail.com[3], pooja.desai@sakp.ac.in[4]

Abstract: Virtualization has not only become important in system VM, but also in storage and networks. And has proved to be a way to improve system security, reliability and availability, reduce costs, and provide greater flexibility. This paper will give us the clear idea about how the concept of virtualization has boosted the speed of computing, providing a secure access to harmful stuffs. It is an extremely lightweight technology. It is also referred to as Virtual Machine (VM) in broad concept. Virtualization has not only became important in system VM, but also in storage and networks. And has proved to be a way to improve system security, reliability and availability, reduce costs, and provide greater flexibility.

Keywords: *Network Virtualization, VLAN, VPN, VSN, VPN.*

*****

I. INTRODUCTION

Virtualization is a creation of a virtual (rather than actual) version of something, such as an operating system, a server, a storage device or network resources. ”Virtuality” differs from” reality” only in the formal world, while possessing a similar essence or effect. In the computer world, a virtual environment is perceived the same as that of a real environment by application programs and the rest of the world, though the underlying mechanisms are formally different. Virtual Machine (VM) provides a virtual platform or storage to the user, when there is less available physical memory on the system. The umbrella of technologies that help build such virtualized objects can be said to achieve tasks that have one common phenomenon, virtualization [1].

System virtualization adds a hardware abstraction layer, called the Virtual Machine Monitor (VMM), on top of the bare hardware. This layer provides an interface that is functionally equivalent to the actual hardware to a number of virtual machines [2].

The concept of Network Virtualization models the next-generation networking paradigm that can replace the existing Internet. Network Virtualization means the logical separation of a physical network into virtual networks.

It is the implementation of separate logical network environments (Virtual Networks, VNs) for multiple groups on shared physical infrastructure. The assignment of users to Virtual Networks depends on the successful authentication, because total privacy between groups have to be guaranteed. Data transport is achieved by a well-defined and controllable ingress/egress points.

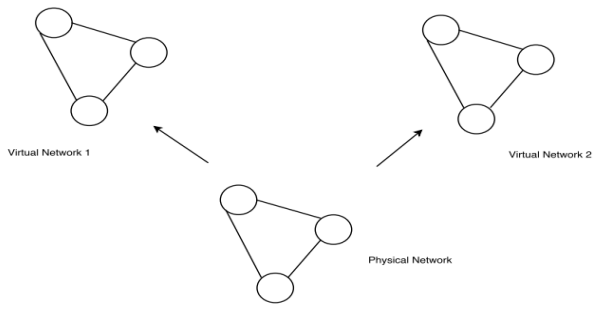

Figure 1. Virtual Network

II. HISTORICAL PERSPECTIVES

There are multiple co-existing logical networks. These are mainly classified into four main classes: virtual local area networks, virtual private networks, active and programmable networks, and overlay networks.

1.1 VIRTUAL LOCAL AREA NETWORK (VLAN)

A Local Area Network (LAN) is typically a collection of devices connected to a single switch. A VLAN typically involves grouping devices on a single switch into multiple broadcast domains and network segments. It is a solution to divide a single Broadcast domain into multiple Broadcast domains.

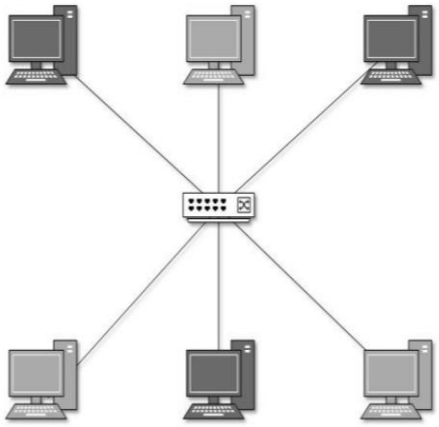

Figure 2. Virtual LAN.

A Local Area Network (LAN) was originally defined as a network of computers within the same area. Today, Local Area Network is defined as a single broadcast domain. This means that if a user broadcasts information on his/her LAN, the broadcast will be received by every other user on the LAN. Here are the physical view of LAN and VLAN. The physical view of LAN is as follows:-

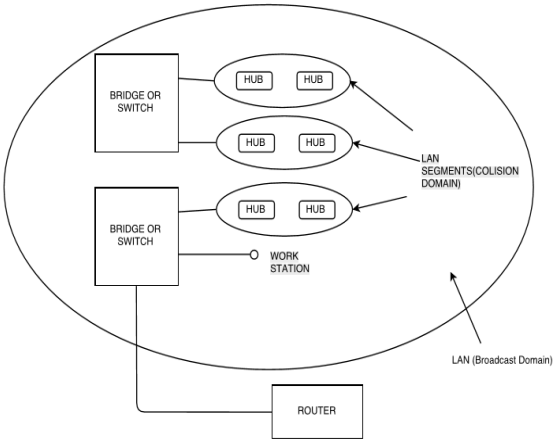

Figure 3. LAN physical view.

The physical view of VLAN is as follows:-

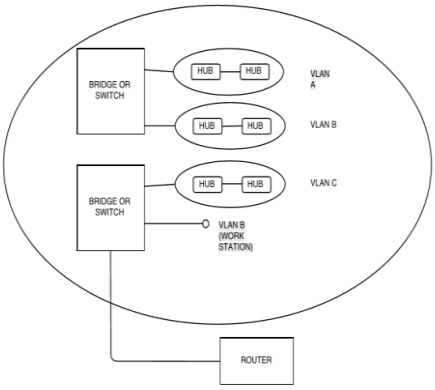

Figure 4. VLAN physical view.

1.2 VIRTUAL SERVICE NETWORK (VSN)

Virtual Service Network (VSN) is basically the generalization of Virtual Local Area Network (VLAN) concept to broader network. It define multiple network instances that share the physical resources and are properly segmented (functionality, access permissions, etc.). At every stage in this virtual chain, information is collected, transformed, packaged, and delivered to consumers at the next one, and finally to end-users. Business agreements regulate the terms and conditions of that information flow and use [3].

1.3 VIRTUAL PRIVATE NETWORK (VPN)

A VPN is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost.

Basically, a VPN is a private network that uses a public network (INTERNET) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as a leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee.

There are two types of VPN connections. :

2.3.1 Remote access VPN.

Remote access VPN connections enable users working at home or on the road to access a server on a private network using the infrastructure provided by a public network, such as the Internet. From the user's perspective, the VPN is a point-to-point connection between the computers (the VPN client) and an organization's server. The exact infrastructure of the shared or public network is irrelevant because it appears logically as if the data is sent over a dedicated private link.

2.3.2 Site-to-Site VPN

Site-to-Site VPN connections (also known as router-to-router VPN connection) enable organizations to have routed connections between separate offices or with other organization over a public network while helping to maintain secure communications. A routed VPN connection across the Internet logically operates as a dedicated WAN link when networks are connected over the Internet.

1.4 Active and programmable networks

Active and Programmable Network supports the co-existing networks through programmability. It customizes the network functionality through the programmable interfaces to enable

access to switches/routers. The Active code can call functions already installed and also allow user to execute own code at switches/routers. The operators must open networks to third parties, which are not used these days due to security reasons.

1.5 Overlay network

Overlay network works on the Application layer of the Virtual Networks. It is built upon the existing network using tunneling/encapsulation. It implements new services without changes in the infrastructure. It is totally Application specific, and not flexible enough.

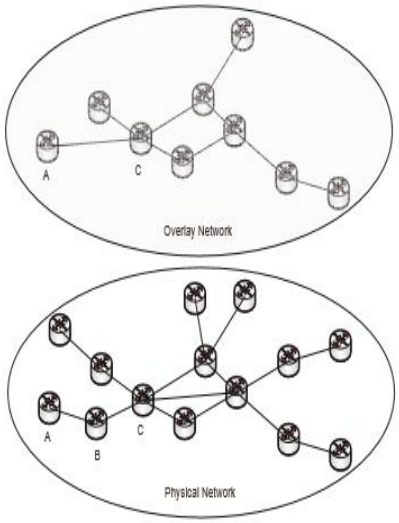

Figure 5. Overlay Network [4].

III. ARCHITECTURAL PRINCIPLES

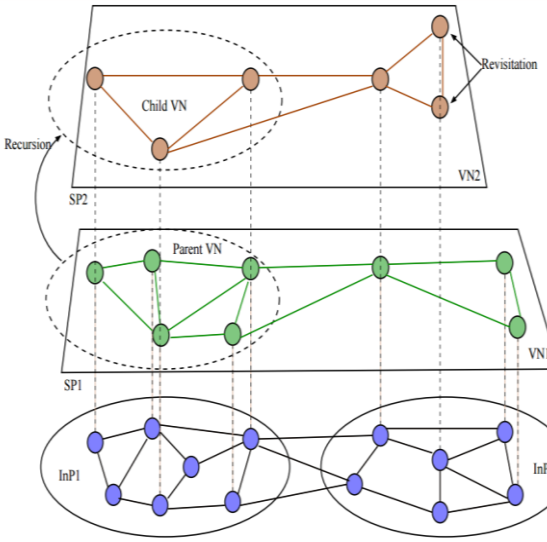

Figure 6. Architectural Principles [4]

The principles are described as follows:

3.1 Concurrency.

Concurrency refers to the multiple service provider competition. Different multiple virtual networks coexist which leads to diversity.

3.2 Nesting.

Nesting refers to the virtual network hierarchy, where child virtual network derive from parent virtual network.

3.3 Inheritance.

The child VN inherits architectural attributes from the parent virtual network. It creates the value added services.

3.4 Revisitation.

I is a single physical node which hosts the multiple virtual nodes. It also deploys diverse functionalities and simplifies operation and management as well.

IV. ADVANTAGES OF NETWORK VIRTUALIZATION

1. As the number of physical devices reduces, the cost decreases.
2. There is less consumption of space due to division of a single network system into multiple and virtual network systems.
3. The power consumption requirements get reduced.
4. It is easier to manage as there are less physical device requirement.
5. It provides security by compartmentalizing environments with different security requirements in different networks.

V. CONCLUSION

In this paper we have discussed the Network Virtualization concept. Briefly explained the Virtual Local Area Network (VLAN), Virtual Service Network (VSN), Virtual Private Network (VPN), Active and Programmable Networks, Overlay Structure. The advantages of Network Virtualization are also stated clearly.

REFERENCES

[1] Susanta Nanda Tzi-cker Chiueh. A Survey on Virtualization Technologies. *SUNY at Stony Brook Stony Brook, NY 11794-4400*. http://www.ecsl.cs.sunysb.edutrTR179.

[2] Daniel A. Menasc´ e. VIRTUALIZATION: CONCEPTS, APPLICATIONS, AND PERFORMANCE MODELING. *Fairfax, VA 22030, USA.* http://cs.gmu.edu~menascepapersmenasce-cmg05-virtualization.

[3] Mauro Regio. Government Virtual Service Networks. *Proceedings of the 35th Hawaii International Conference on System Sciences – 2002.* https://www.computer.org/csdl/proceedings/hicss/2002/1435/05/14350124.pdf

[4] George N. Rouskas. Network Virtualization: A Tutorial. In *NC STATE.UNIVERSITY.* North Carolina State University. http://rouskas.csc.ncsu.edu/Publications/Talks/OFC-2012-NV.pdf.