IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Volume-5, Issue-11 E-ISSN: 2347-2693

Network Hypervisors Pros and Cons: A survey

P. Sasibhushana Rao[1*], C. Kalyan Chakravarthy[2]

[1*]Dept. of CSE, AITAM (JNTUK), Srikakulam, India
[2] Dept. of CSE, MVGR, (JNTUK), Vizianagaram, India

Corresponding Author: sasipappu510@gmail.com, Tel.: 9550446625

Available online at: www.ijcseonline.org

Received: 13/Oct/2017, Revised: 25/Oct/2017, Accepted: 14/Nov/2017, Published: 30/Nov/2017

Abstract— In networking environment due to increasing demand of resources reliability, load balancing and efficient routing of data are still becoming a major issue. So I am proposing an efficient approach for solving all these issues using an innovative technique called Software Defined Networks(SDN).Software Defined Networks (SDN) has evolved as an emerging research area where it provides efficient network resources by separating data plane from control plane. Network virtualization allows sharing of physical resources by different users where each user executes their applications over its virtual network and its main features are isolation, multitenancy and simplified segmentation. The main component for virtualizing SDN is Hypervisor that abstracts physical SDN's into isolated virtual SDN's having its own controller. This paper presents different network hypervisors and its comparison shown will have a great impact on researchers building an efficient network infrastructure.

Keywords— *SDN, Hypervisor, Flowvisor, Multitenancy*

I. INTRODUCTION

Network Virtualization [1][2] refers to combining hardware and software network resources and its functionality into single virtual network. Its role is to improve resource allocation and permits network operators to check any changes made to the network and allows network users to share the given network in controlled and isolated manner[3][4]. The different contexts where the given network can be virtualized are network devices (control plane, data plane and management plane), network links and network services. The benefits of network virtualization are low cost, less space consumption, scalable, low power requirement and easy to manage [4][5].

To get quick glance on network virtualization first look closely at virtualization. Virtualization refers to abstracting computer hardware that permits the sharing and slicing of resources among the guest operating systems making each OS believe it has its own hardware[6][7]. Above the virtualization layer, consistent hardware abstraction allows different operating systems to build new approaches in their design. Below virtualization layer, different hardware can be used to map to hardware abstraction layer by having different instruction sets optimized for higher performance, lower power etc.[8].

So by analogy the network should have hardware abstraction layer by allowing multiple networks to run simultaneously without interference with each other on different hardware including switches, routers etc. to achieve the same benefits similar to computer virtualization [6]. New protocols and addressing formats should be executed simultaneously on different networks to enable different applications to improve their performance in the network [8].

This paper explores survey on Flow visor a network virtualization tool which act as hypervisor that resides between hardware and software on PC and splits the given physical network into network slices [9]. It uses Open Flow as hardware abstraction layer that resides between control and forwarding paths on network device. The resulting virtual network runs on existing or new low cost hardware which is compatible with current network [10]. The rest of the paper deals with installation process of flowvisor.

II. HYPERVISORS

Virtualization enables or allows multiple applications or operations to gain access to the hardware resources/ software resources of the host machine. Virtualization is a layer between the hardware and the operating system and it also provides access transparency. The hypervisors also known as the Virtual Machine Monitor (VMM), manages the applications and the operating system in general[4][6]. The following figure shows a virtual environment, where the hypervisor is right above the host hardware, and virtualizing guest machine with the full capability or more of the host machine[11][13].

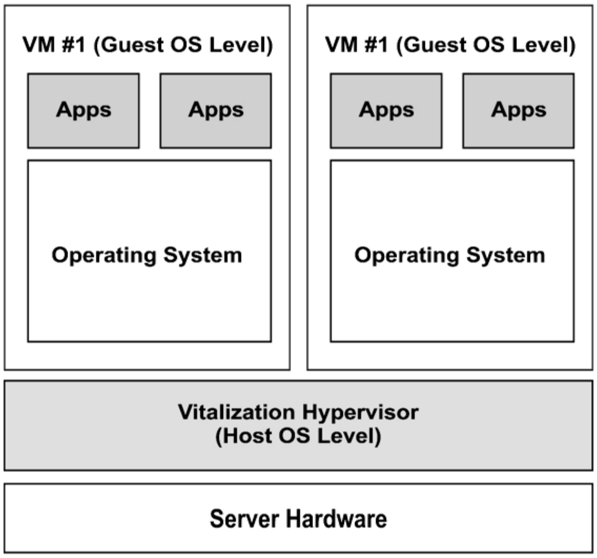

Fig 1: Architecture of Virtualization

III. Implementation Of Virtualization

Virtualization can be implemented in many ways using the following techniques[8][12]. They are:

a) Server Consolidation: This combines or centralizes the workloads of various physical machines that are not fully used to lesser machines that can run safely and transparently over shared hardware infrastructure and then virtualized as different servers, increasing its efficiency, workability, speed etc.
b) Application Consolidation: This is giving legacy or outdated applications the environment to utilize new hardware and operating system by virtualizing the new hardware and providing access to other guest machines to utilize the application.
c) Multiple Execution: Virtualization can help create more than one environment for program or application execution ad also the quality of service can be increased by ensuring that specific amount of resources is allocated appropriately.
d) Virtual Hardware: The virtualization of hardware that is unavailable to users is achieved in virtualizinghardware. Examples of such hardware are: SCSI drivers, Virtual Ethernet Adapters, Virtual Ethernet Switches, and Hubs etc
e) Debugging: The virtual environment can help in debugging of applications or software that are complicated such as an operating system or a device driver. This is achieved by allowing the user to execute the software in a virtualized environment with all the full control of the software available in the environment, giving the programmer or developer the perfect environment for debugging.
f) Multiple Simultaneous Operating System: Virtualization enables the facility of having and running more than one operating system simultaneously, and also having different applications according to the users demands.The guest machine runs on the virtualized application or software that in turn runs above the host machine operating system.
g) Business Continuity: This is achieved by putting the entire system files into a single file that can be replicated and restored on any server. This reduces downtime.
h) Sandboxing: Virtual Machine helps in providing secure and isolated environments for applications that are less trusted in the virtualized operating system. Virtualization helps in creating a secure computing environment.
i) Software Migration: This ease the migration or moving of software form one server to another, thereby helps mobility.

Advantages of Virtualization [6][11]

Security: A security breach on one of the virtual machines does not affect the other VM because of isolation which is achieved by the different compact environment that have different or separate security measures in the different guest machines.

Reliability and Availability: When there’s a software failure in one virtual machine or guest machine, it doesn’t affect other virtual machines.

Cost: It is cost effective by combining small servers to secure a more powerful server. The cost effectiveness of virtualization runs down to the hardware, operations (man power), floor space etc

Adaptability to Workload Differences: In virtualization when workload changes or varies, the workload degree can be optimized easily by shifting the resources and priority allocations between or among virtual machines. Processors can also be moved from one virtual machine to another.

Load Balancing: The software state of a VM is relatively condensed by the hypervisor, this makes it possible for migration of the entire virtual machine to another platform, it improves load balancing.

Legacy Applications: This enables the running of legacy applications on old OD in the guest machines. For example if an enterprise decides to migrate to a different OS, it is possible to maintain the old legacy applications on the old VM or guest machine.

IV. Types Of Hypervisors

Hypervisors as stated earlier is a software that manages different operating system or different instances of the same operating system in one physical computer or host machine, has two distinct types namely: Type 1: Native or bare Metal and Type 2: Hosted hypervisors.[4]

A. Type 1: Native or Bare Metal Hypervisor

These are software that run directly above the hardware of the host machine. It also monitors the operating system that runs directly above the hypervisor and also monitors the operating system that runs on the guest machine. This is because the guest machine operating system runs on a different or isolated level that is directly above the hypervisor. Examples are Oracle VM, Microsoft Hyper-V, VMWare ESX and Xen etc. [6][11]

The following figure shows native hypervisor

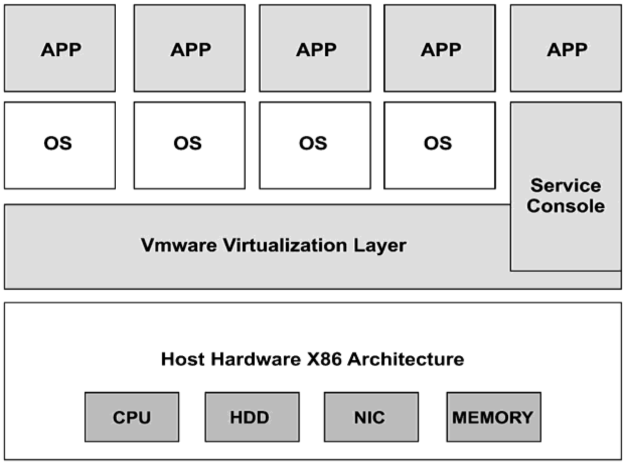

Fig 2:Native or Bare Metal Hypervisor

B. Type 2: Hosted Hypervisor

The hypervisor is hosted or installed on an already existing operating system and it houses other operating system that is above it. In this type of hypervisor, any problem occurring with the host operating system will affect guest machine operating system that is running on the hypervisor and also it affects the hypervisor itself, although sometime the hypervisor running above the operating system might be secured but the guest operating system wouldn't be.[4][8] Examples of such are Oracle VM Virtual Box, VM Ware Server and Workstation, Microsoft Virtual PC, KVM, QEMU and Parallels. The hosted architecture of hypervisor, relies on host operating system for device support and physical resource management.[6]

Originally hypervisors were developed to suit server platforms, later on the virtualization of Desktop, PC operating systems were achieved. A challenge that held the virtualization of PCs operating system was the virtualization of the x86 based CPU architecture[4][9][11]The following figure shows hosted hypervisor

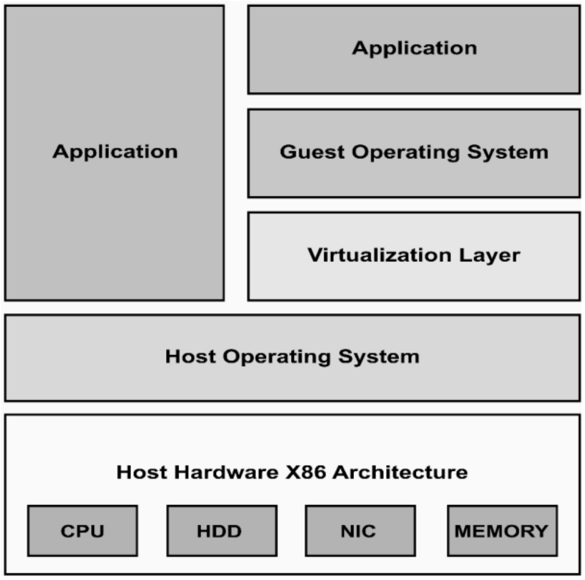

Fig 3:Hosted Hypervis

V. FLOWVISOR

FlowVisor sits between the underlying physical hardware and the software that controls it which is shown in figure below[14][16]

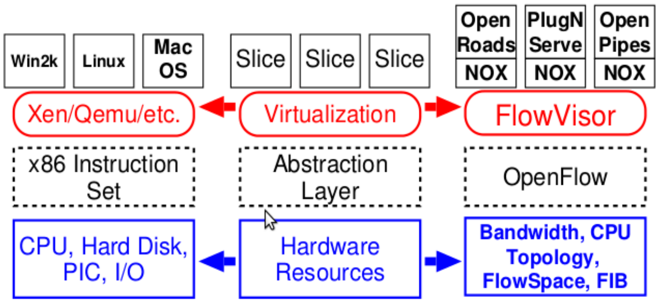

Fig 4: Placement of Flowvisor

It is like an operating system uses an instruction set to control the underlying hardware, FlowVisor uses the OpenFlow protocol to control the underlying physical network. Open-Flow exposes forwarding control of a switch's packets to a programmable entity, i.e., the OpenFlow controller.FlowVisor hosts multiple guest OpenFlow controllers, one controller per slice, making sure that a controller can observe and control its own slice, while isolating one slice from another (both the datapath traffic belonging to the slice, and the control of the slice).

OpenFlow provides an abstraction of the networking forwarding path that allows FlowVisor to slice the network along the five required dimensions, and with the following main characteristics[15]

a) FlowVisor defines a slice as a set of flows running on a topology of switches.2

b) FlowVisor sits between each OpenFlow controller and the switches, to make sure that a guest controller can only observe and control the switches it is supposed to.

c) FlowVisor partitions the link bandwidth by assigning a minimum data rate to the set of flows that make up a slice.

d) FlowVisor partitions the flow-table in each switch by keeping track of which flow-entries belong to each guest controller.

A. FLOW SPACE

The set of flows that make up a slice which can be thought of constituting a well-defined subspace of the entire geometric space of possible packet headers.Because FlowVisor defines a slice as a set of flows defined by set of non contiguous regions. Flowvisor slices traffic using flowspaces.Flowvisor makes decision of isolating slices by making sure that their flowspaces doesnot overlap with each other in given topology[17][14][15]. It can also decide which switches can be used to communicate from one slice to another which can also make packet to belong to one or more slices which can be explained in fig below where Alice and Bob are taken for example assuming each having their own OpenFlow Controller.

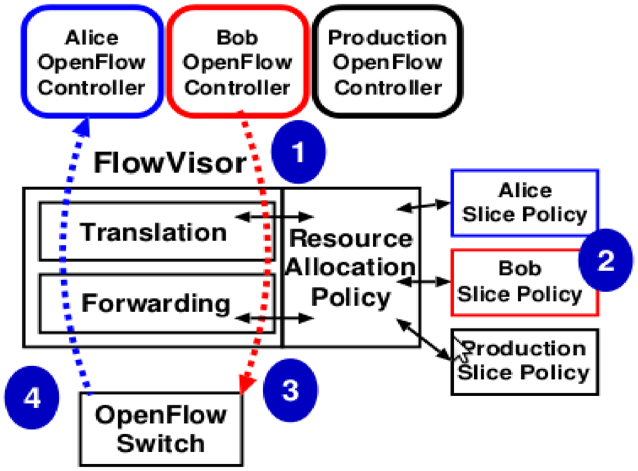

Fig 5: Intercepting Open flow messages from guest controller

B. Design Goals[15]

- It should be transparent to network controller
- strong isolation must exist between network slices
- slice policy should be extensibly defined with documentation

VI. Conclusion And Future Scope

The paper deals with Network Virtualization which refers to combining hardware and software network resources and its functionality into single virtual network. Its role is to improve resource allocation and permits network operators to check any changes made to the network and allows network users to share the given network in controlled and isolated manner. The paper also discussed Hypervisor and its implementation and different types of hypervisor are elaborated in detail.

The last section of paper deals with Flow visor and its design goals which are useful for slicing traffic in efficient manner.

References

[1]. Kilian Rausch, *Network Virtualization - An Overview, Network Architectures and Services*, July 2011

[2]. H. Wen , Network Virtualization-An Overview, Wireless Virtualization, Springer Briefs in Computer Science,2013.

[3]. N.M. Musharraf, K. Chowdhury, R. Boutaba, *A survey on network virtualization.* J. Comp.Telecommun. Networking 54(5), 862–876 (2010)

[4]. Gregor Schaffrath,Christoph Werle§ Panagiotis Papadimitriou, Anja Feldmann, Roland Bless, Adam Greenhalgh,Andreas Wundsam, Mario Kind, Olaf Maennel, Laurent Mathy, *Network Virtualization Architecture:Proposal and Initial Prototype*, ACM, August 17, 2009.

[5]. Raj Jain and Subharthi Paul, *Network Virtualization and Software Defined Networking for Cloud Computing: A Survey*, IEEE Communication Magazine, November 2013

[6]. Morty Eisen, *Introduction to Virtualization*, IEEE Circuits and Systems (CAS) Society, April 28,2011.

[7]. Daniel A. Menasce, *Virtualization: Concepts, Applications, And Performance Modeling*, National Geospatial-Intelligence Agency (NGA)

[8]. Michael Pearce, Sherali Zeadally, Ray Hunt,*Virtualization: Issues, Security Threats,andSolutions*, ACM, 2013.

[9]. Victor T. Costa, Luís Henrique M. K. Costa, *Vulnerabilities and solutions for isolation in FlowVisor-based virtual network environments*, Journal of Internet Services and Applications,2015

[10]. Amanpreet Kaur, Sawtantar Singh Khurmi, "*A Study Of Cloud Computing Based On Virtualization And Security Threats*", International Journal of Computer Sciences and Engineering, Vol.5, Issue.9, pp.108-112, 2017.

[11]. Gabriel Cephas Obasuyi, Arif Sari, *Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment*, Scientific research publications, 2015

[12]. Anand More, Priyesh Kanungo, "*Use of Cloud Computing for Implementation of e-Governance Services*", International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.3, pp.115-118, 2017.

[13]. Marisol García-Valls, Tommaso Cucinotta,Chenyang Lu,*Challenges in real-time virtualization and predictable cloud computing*, Elseiver,2014

[14]. Rob Sherwood, Glen Gibb , Kok-Kiong Yap ,Guido Appenzeller ,Martin Casado , Nick McKeown, Guru Parulkar, *Flowvisor: A Network Virtualization layer*, Openflow lab, 2009

[15]. Yiannis Yiakoumis, Kok-Kiong Yap, Sachin Katti, Guru Parulkar, Nick McKeown, *Slicing home networks*, Home nets, 2011.

[16]. Wanqing You, Kai Qian, Xi He, Ying Qian, *Towards Security in Virtualization of SDN*, International Journal of Computer, Electrical, Automation, Control and Information Engineering , 2014

[17]. Masayoshi Kobayashi, Srini Seetharaman, Guru Parulkar, Guido Appenzeller, Joseph Little, Johan van Reijendam, Paul Weissmann, Nick McKeown, *Maturing of OpenFlow and Software Defined Networking through Deployments*, Elseiver,2012

Authors Profile

Mr. P.Sasibhushana Rao pursed Bachelor of Computer Science and Engineering from JNTUK in 2009 and Master of Computer Science and Engineering from JNTUK in year 2012. He is currently pursuing Ph.D. In JNTUK and currently working as Assistant Professor in Department of Computer Science and Engineering ,AITAM, Srikakulam. His main research work focuses on Cryptography Algorithms, Network Security, Computer Networks. He has 5 years of teaching experience.

Dr. C. Kalyan Chakravarthy pursed Master of Computer Science and Engineering from GITAM. He pursued Ph.D. in Andhra University in the area of Wireless Networks and currently working as Professor in Department of Computer Science and Engineering since 2006. He is a member of ISTE & IEI. His main research work focuses on Wireless Networks, Software Defined Networks and Internet of Things. He has 16 years of teaching/industrial Experience.