ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 8(S2), 165–170, January 2015* DOI : 10.17485/ijst/2015/v8iS2/61217

Centralization of Network using Openflow Protocol

Ankita Vinod Mandekar[1*] and Krishna Chandramouli[2]

[1]School of Information Technology, VIT University, Vellore-632014, Tamilnadu, India; avmandekar@gmail.com
[2]Division of Cloud Computing, Vellore University, Vellore-632014, Tamilnadu, India; krishna.c@vit.ac.in

Abstract

Traditional network is used have distributed nature which face complexities while modifying, monitoring, securing the network. The centralization of network is proving very effective in terms for management, implementation of new applications, monitoring the network. The programmable network using programmable devices helps to implement centralization of network successfully. To reduce the latency in the network the control parameters of control plane are used for making the forwarding decision by the centralized controller. Software Defined Network (SDN) is emerging technology having the centralized policy to design cloud network topology. The abstraction of control plane from data plane is isolating the control parameters from the flow of packets for making an efficient forwarding decision by programmable device. This device is known to be controller; it also reduces the complexities to process the data overhead. The OpenFlow protocol is used for abstraction and transferring the control parameters over secure channel. The protocol enables the enterprise to design well managed and secure cloud. In this paper, the experimental test bed is built which provides the centralized System Center Virtual Machine Manager (SCVMM) controller in the private cloud. The cloud provides its virtual Platform as a Service (PaaS) to the client by creating multiple Virtual Machine instances on single machine. The Virtual Private Network is created by using the Network Virtualization Generic Routing (NVGRE) tunnelling Protocol for the client to reach up to the hosted platform.

Keywords: Hyper V Manger, Platform as a Service, Network Virtualization Generic Routing Encapsulation (NVGRE), OpenFlow, Software Defined network (SDN), System Center Virtual Machine Manager, Virtual Private Network (VPN)

1. Introduction

Today's traditional network is based on the routing of packet using different routing protocols such as Open Shortest Path First (OSPF), Border Gateway Protocol (BGP) and Enhanced Interior Gateway Routing Protocol (EIGRP). This protocols have certain limitation of hop count, converges slowly, no knowledge for bandwidth, prone to routing loops, multiple path for same source and destination, difficulties for deploying new protocol Internet Protocol Version6 (IPV6) and the applications due to physical limitations. The data with its header is forwarded using packet based network topology following different routes for same source and destination which results in reassembly of packets overhead and delay for delivery. Because of huge network infrastructure it's getting difficult to update the network devices. Using traditional networking techniques in the private network gives static network, less speed, inefficient network which requires large number of network devices. Cloud Computing is the network virtualization in which the systems share the network device and provides the Software, Infrastructure, Platform as a Service to the client. Using of traditional network results in less security, throughput, speed for managing the cloud. In Platform as a Service, the provider gives the platform to the client to save o-r access their data, application. In order to reach up to the cloud of service provider the client has to design the Virtual Network. Client can even locate one of the private network addresses on the service providers cloud. In this paper, the Operating Systems are virtualize on the top of "Microsoft Windows Server 2012 R2"[3] by creating multiple instances. Using Hyper Visor[9] multiple instances can be created on single machine and each instance can be providing Platform as a Service PaaS to the Client. Using Software Defined Network, the private cloud of the PaaS service provider

*Author for correspondence

can be managed efficiently. Software Defined Network is the centralized network built up using HyperVSwitches, SDN Controller (SCVMM) and Systems. HyperVSwitches are enabled with OpenFlow protocol[5] which separates the control plane from data plane. The forwarding of the flow is based on the flow table entry of switch and also SDN controller. The OpenFlow is Southbound API for SDN Controller which provides the required control parameters to make decision in forwarding when flow table entry is missing. The applications develop for managing bandwidth, access control list, design the topology, monitor traffic in the cloud is in the North bound of controller. The Virtual Private Network is created for the Clients of the cloud. The Client can reach up to the platform provided by the cloud using Network virtualizing Generic Routing Encapsulation tunnelling protocol. The virtual machine is hosted on the cloud infrastructure in the same private network of Client. Due to this the access of the virtual machine is transparent to the Client.

2. Architecture

In the Figure 1, the test bed name as SDNtestbed (SDT) is created with 3 systems in the PaaS providers cloud and 3 systems in customer's network. The PaaS provider's cloud is generated using the private space of Class C IP address form 192.168.0.0 – 198.168.255.255 with maximum number of systems in the network 65,536. The Domain Name System Server is used to assign the Domain for the cloud.

2.1 Software Defined Testbed Cloud

2.1.1 Domain Name System Server

The Domain Name System is naming the systems, network devices, virtual Operating Systems in private network. The IP address provided to the devices converted to human readable form by assigning the unique domain name for the systems in same network. In SDT's PaaS providers cloud, the Host_SDT_1 is Domain controller and Domain Name System Server. The forest is created of 3 systems in the cloud by naming domain as "sdt.sdntestbed.com". It gives easy access to reach up to the PaaS providers cloud.

In Figure 2, the online systems under the domain "sdt.sdntestbed.com" are shown. The Domain Controller and DNS is on the Host_SDT_1. Domain Controller enables to check security policies and share the resources in the network. The Active Directory Domain System is enabled in the Host_SDT_1 to authenticate, imply security policies, and make updates on the systems under the "sdt.sdntestbed.com" domain.

2.1.2 Hyper Visor

Hyper-V is the software on the top of the operating system of the server. This software allows installing number on virtual machines on the top of the Hyper-V switch which is software based on the data link layer of network.

In Figure 3, the architecture of Hyper Visor is shown. In the PaaS provider's cloud, the Hyper Visor is installed in Host_SDT_1 and Host_SDT_2 on the top of system's operating system (OS) "Microsoft Windows Server 2012 R2". On top of this OS two Virtual Machines of Client_1 and Client_2 are installed at two different instant.

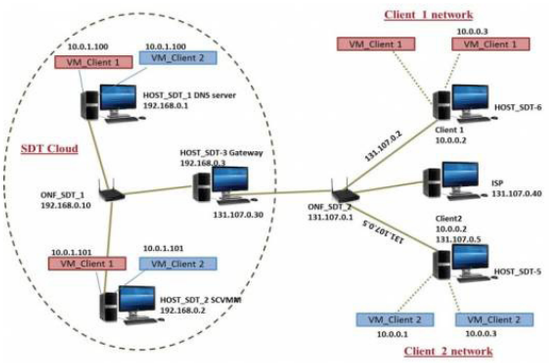

Figure 1. Architecture of SDT test bed.

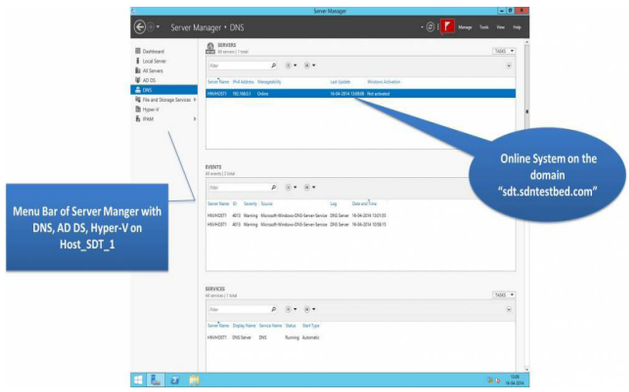

Figure 2. Domain Name System Server in SDT Cloud.

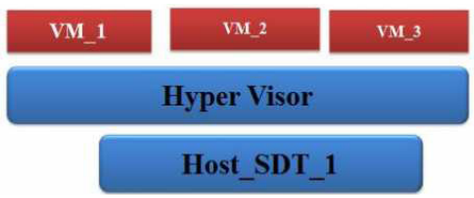

Figure 3. Hyper Visor Architecture.

2.1.3 System Centre Virtual Machine Manager (SCVMM)

SCVMM[4] is the virtual machine manager which keeps the log for online virtual machines. *The topology of virtual network in the cloud can be viewed. The whole cloud and their activities can be viewed on the controller. The virtual machine instance can be created, moved over Host_SDT_1 and Host_SDT_2 from this centralized controller. In SDNtestbed, the SCVMM is installed on Operating System (OS) "Microsoft Windows Server 2012 R2" of Host_SDT_2.

2.1.4 Virtual Gateway

The Microsoft Gateway configuration is enabled on the Host_SDT_3. This host is dedicated as gateway for connection of the systems and virtual machines inside the SDT Cloud to the external ISP network and vice-versa. The IP pool is created on gateway one is ranging from 192.168.0.0-198.168.255.255 and second is for the external virtual network from ISP address, 131.107.0.5 in subnet 255.255.255.0. Host_SDT_3 has two NIC card, NIC_1 is used for enabling first IP pool inside the cloud and NIC_2 for enabling the second IP from the external network.

2.2 Virtual Private Network for Client

The two different Virtual Private Networks (VPN) are created on the Host_SDT_2 for Client_1 and Client_2. Each VPN has an IP pool from 10.0.1.100-10.0.1.255. The private range of both VPN is same so the request form both customer is differs by unique VirtualSubnetId provided by Virtual Machine Manager and Client ID.

2.2.1 Internet Service Providers Network

Host_SDT_4 is the system where the IP pool is created from 131.107.0.1 – 131.107.0.255. The distribution of the IP is made as shown in Table 1.

Table 1. Public IP address

Host	IP addresses
ONF_SDT_2	131.107.0.1
Host_SDT_3	131.107.0.30
Host_SDT_4	131.107.0.40
Host_SDT_5	131.107.0.2
Host_SDT_6	131.107.0.5

2.2.2 Client_1 and Client_2 Architecture

The DNS entries are made under the domain name "Client1.com". The virtual machines are installed on the top of physical Operating system "Microsoft Windows Server 2012 R2". The distribution of the private IP address is made by creating the IP pool with subnet 10.0.0.0/24. Using this IP range the Client_1 can use the systems in the same network. Similarly, the private network is configured for Client_2. Similarly, the private network is configured for Client_2.

3. Methodology

3.1 Software Defined Network

Software Defined Network (SDN)[6] is emerging technology for centralization of the network using the programmable devices as Openflow enabled Switches, Controller. In this paper, the controller System Centre Virtual Machine Manager (SCVMM) and TP-LINK TL-wr1043nd routers are used to create the SDTs Cloud.

3.1.1 System Center Virtual Machine Manager (SCVMM)

It is the software which centralizes the private network of cloud.

Features supporting PaaS:-

- On network traffic congestion as there are number of virtual machines on the single system, SCVMM can migrate the virtual machine logically to the other system with less load. This provides load maintenance in the cloud.
- The disk resources which are reserved by the virtual machine can be removed or added as per the clients request for the centralized manager SCVMM.
- Maintenance and Management of the whole cloud is centralized on the SCVMM.
- The cloud vendor can add the plugins on the top of SCVMM to increase the functionality of SCVMM controller.

In Figure 4, SCVMM manages the virtual machines hosted remotely in the same network. The access list of the systems in the network is maintained which gives access to the authenticated systems and virtual network in the cloud.

3.1.2 TP-LINK TL-WR1043 Routers

Figure 5, shows the separation of control plane from the data plane on the OpenFlow enabled Router. This router inter-connects the systems in the cloud. This is enabled with OpenFlow version 1.3.0 protocol[7] by upgrading the image file from the firmware of router to OpenWRT version 1.8. The router can be access by using Putty software for allocating IP address and modifying the upgraded version of OpenFlow as the research in Southbound API that is OpenFlow protocol is still going on. The up gradation of protocol can be installed easily.

3.1.3 OpenFlow Protocol

The current network uses the decision made by network devices to forward the packet based on the routing protocol like BGP, OSPF etc. Due to increasing traffic in the network, the implementation of new routing protocols like ZRP is made to avoid the congestion overhead. Further, more parameters of network as security, reliability, throughput needs the new protocols for network devices like routers, switches. This is resulting in the highly complex protocols designing and their implementation.

1. Openflow protocol[5] is to overcome this static nature of the network infrastructure. It provides Flow-Based routing. Regardless of vendors of network devices the common attributes are considered for forwarding the flow. Openflow protocol separates the Control plane and Data plane.
2. It uses the header fields shown in Table 2 in flow table with control parameters Ingress port, Ether Src (Ether Source),Ether Dst (Ether Destination), Ether Type, VLAN, IP Src (IP Source), IP Dst (IP Destination), IP protocol, Src Port (Source Port), Dst Port (Destination Port).
3. Counters to get the number of packets sent for each flow and determine the statistics for the flow.
4. Depending on the action entry the decision is made to forward the packet to the destination as per the flow table header attribute, drop the packet of send to the SDN controller over the secure channel. These parameters are only involved in making the routing decision while data is isolated to avoid data overhead.

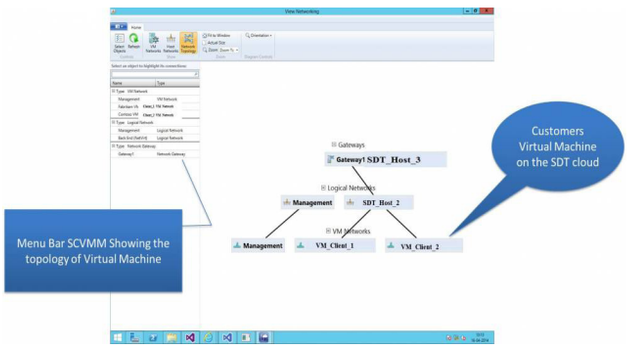

Figure 4. SCVMM Controller.

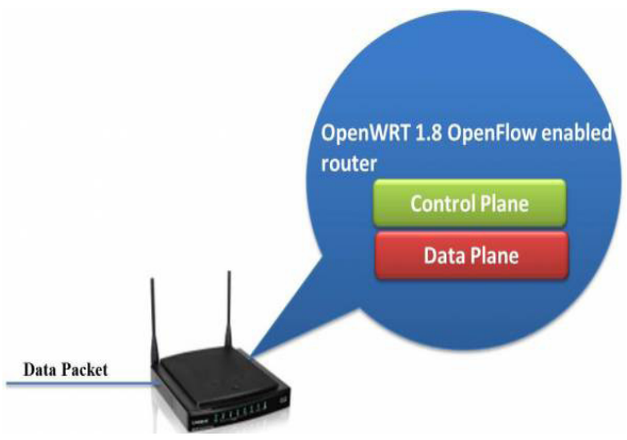

Figure 5. OpenWRT Router.

3.2 Virtual Private Network

3.2.1 Network Virtualization Generic Routing Protocol

The tunnelling protocol to create the Virtual Private Network (VPN) involves three types of protocols:-

- Passenger Protocol: For encapsulation of the data sent over the local network.
- Carrier Protocol: For carrier service.
- Transport Protocol: For encapsulation of two preceding IP.

In this paper, the SDT cloud provides the virtual platform for the Client with the private IP address of Clients local network. The Network Virtualization Generic Routing Encapsulation[4] (NVGRE tunnelling protocol used for encapsulation of the packet from the source located in Clients local network.

Table 2. Header fields of OpenFlow control parameter

Ingress Port	Ether Source	Ether Dst	Ether Type	VLAN Id	IP Src	IP Dst	IP Proto	Src Proto	Dst Proto

Working of NVGRE protocol:

1. The source located in the Clients private network send the packet over the network for system with IP address "10.0.1.101". Router checks its routing table and it finds that the destination is not in local network then the packet is encapsulated to create NVGRE tunnel. During encapsulation the transport protocol encapsulate the virtual packet with preceding packet and appropriate Public Address (PA) option of IP. Point To Point (PPTP) link from the source router ONF_SDT_2 to destination router ONF_SDT_1 is virtually made. As shown in Figure 6. Packet is encapsulated with unique VirtualSubnetId and Client ID.
2. A destination router ONF_SDT_1 removes the encapsulation and gets the original packet. With the help of appended Public Address, VirtualSubnetId, Client ID the Gateway, DNS server determines the destination Virtual Machine.

4. Discussion

In this paper, two technologies are used one for managing the private network and second for increasing the speed of virtual private network.

1. Software Defined Network using SCVMM controller and OpenWRT routers is implemented for centralizing the SDT cloud network. Centralization of network gives the managed, secure network. The plugins are installed on top of the controller to enable use of valid access list, list of virtual network hosted on the cloud.
2. The Virtual private Network is built using NVGRE protocol makes more accurate to reach up to the destination as Virtual Subnet ID and Client ID is encapsulated with original packet.
3. Virtualization of Operating System on top of "Microsoft Windows Server 2012 R2"[1] on single system makes the use of less infrastructure for many virtual operating system that is platform for the Clients on the SDT cloud.

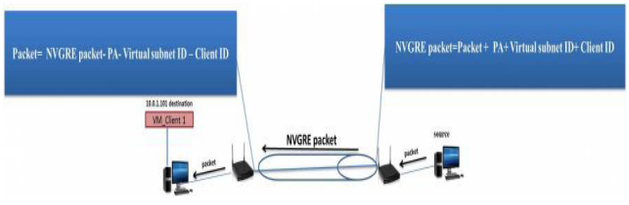

Figure 6. NVGRE Tunnel.

Supported Hypotheses:

1. In 2008, Enabling Innovation in Campus Network[1] proposed by Nick McKeown, Tom Anderson, Hari Balakrishnan. In this paper the campus network is design using OpenFlow protocol. The need of programmable network and its advantages are explain.
2. A survey of Software-Defined Networking: Past, Present and Future Programmable Networks[2] by Bruno Astuno A. Nunes and Marc Mendonca. In this paper, the awareness of programmable network using SDN is focused and describes the advantages using OpenFlow Protocol.
3. OpenFlow-Based Server Load Balancing Gone Wild by Richard Wang, Dana Butnariu and Jennifer Rexford has proposed that the hosting service provided by data centre needs load balancing while traffic congestion and that is managed by the programmable network using SDN.
4. Global Environment for Network Innovation (GENI) is providing the virtual environment for research on the security, Software Defined Networks (SDN), application. The scientist, students making research in networking are implementing their ideas on this test bed.

5. Result and Conclusion

The Software Defined Test bed has centralization of the systems in cloud with SSCVM programmable controller and tunnelling of virtual private network using NVGRE protocol.

1) Software Defined Network for SDT cloud.

In Figure 7, the Host_SDT_1, Host_SDT_2 and Host_SDT_3 are three systems in SDT Cloud. The Host_SDT_2 is enabled with SCVMM controller and showing the network topology which is centralized and managed on the Host_SDT_2.

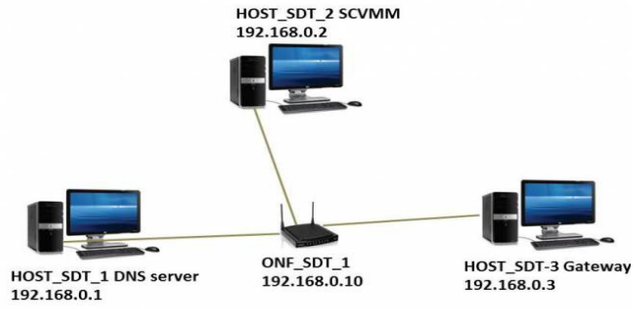

Figure 7. Centralized Software Defined Network.

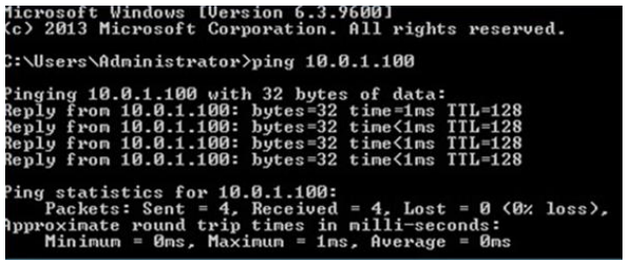

Figure 8. Ping report to client's application on SDT Cloud.

2) Virtual Private Network using NVGRE tunnelling protocol.

In the Figure 8, the ping command shows that the Client system can successfully reach the application hosted on platform addressing "10.0.1.100" Virtual IP address of SDT Cloud.

1. Centralized programmable device SCVMM Controller manages, monitor the physical as well as virtual systems in the cloud.
2. The OpenFlow enabled Switch have flow table with attributes as matches, ingress port, and decision flow. If match is missed in the flow table then it is forwarded to controller. The programmable device controller decides its topology and the flow are processed. The traffic from same source and destination follows same topology. Thus, the flow based forwarding results in increasing throughput. Using this technology, the proper distribution of bandwidth is made to provide the uniform and fast access to virtual Operating System located on the server.
3. Use of Hyper V Manager for creating virtual instances results in less infrastructure requirement which is cost effective.
4. The NVGRE tunnelling protocol provides secure and specific reachability to the destination on virtual network of cloud.

6. Acknowledgement

We acknowledge VIT University, Vellore for the encouragement and permission to publish this paper. We would like to thank Programme chair for M.Tech (IT), Prof. Sathiyamoorthy E., Associate Professor, for his support.

7. References

1. Laadan O, Jason N. Operating System Virtualization: Practice and Experience. Proceedings of the 3rd Annual Haifa Experimental Systems Conference (SYSTOR 2010); 2010 May; Haifa, Israel.
2. Boutaba R, Ng W, Leon-Garcia A. Web-based Customer Management of Virtual Private Networks. 2009 Jun.
3. Virtualization in Cloud Computing. 2014 Mar. Availaible from: http://www.slideshare.net/markanamehul/virtualization-in-cloud-computing-ppt.
4. Laadan O, Nieh J. Test Lab Guide: Windows Server 2012 R2Hyper-V Network Virtualization with System Center 2012 R2 VMM.
5. McKeown N, Anderson T, Balakrishnan H. OpenFlow: Enabling Innovation in Campus Network. 2008 Dec.
6. Nunes BAA, Mendonca Marc. A survey of Software-Defined Networking: Past, Present and Future Programmable Networks. 2010 Apr.
7. Open Network Foundation: OpenFlow Switch Specification version 1.3.1 (wire protocol). 2012 Sep.
8. Enterasys Secure Network: Software Defined Network (SDN) in the Enterprise. 2013 Jun.
9. VMware Network Virtualization Design Guide. Technical white paper. 2013 Jan.