An IPv6-Enabled Software-Defined Networking Architecture

Chia-Wei Tseng[1,2], Yao-Tsung Yang[1,2], Li-Der Chou[2]

[1]Broadband Network Laboratory
Chunghwa Telecom Laboratories
Taoyuan, Taiwan
chiawei@cht.com.tw[1], yaovct@cht.com.tw

[2]Dept. of Computer Science and Information Engineering
National Central University
[3]National Center for High-performance Computing
Taoyuan, Taiwan
cld@csie.ncu.edu.tw

***Abstract*—Software-Defined Networking (SDN) is a new potential approach that can separate and provide abstract elements to build computer networks. Internet Protocol version 6 (IPv6) is a mature, proven and deployed globally technology, and also the future of the internet infrastructure. It can identify, localize and route traffic across the Internet. In this paper, we combine the existing IPv6 protocol and the SDN, known as SDNv6, to provide the smarter and reliable network communication architecture.**

Keywords- IPv6, SDN, OpenFlow, network architecture

I. INTRODUCTION

SDN is an approach to building computer networks that separates and abstracts elements of these systems. Several works have addressed the architecture of total control of the network including the SDN layer and transport layer [1],[2],[3]. Currently, SDN is realized in OpenFlow [4]. The key attributes of SDN include separation of data and control planes, a uniform vendor-agnostic interface between control and data planes, a logically centralized control plane, and slicing and virtualization of the underlying network. SDN also introduces the benefits of a centralized approach to network configuration.

In various network setups and operations, IPv6 is bringing many unique benefits when it is combined with emerging technologies such as Autonomic Management & Control, Clouds Virtualization, SDN, IoT/M2M, etc. These benefits include host automation, and scalability in addressing, route aggregation and forwarding and traffic steering functions [5]. IPv6 enables the transformation that occurs at the networking infrastructure level providing resources and functions to make SDN and network virtualization easy to scale.

In this paper, We propose an architecture that combines the features of IPv6 and SDN. With IPv6 support in SDN architecture, the architecture can now take full advantage of the future Internet.

II. PROBLEM DESCRIPTION

The shortage of IPv4 addresses has created widespread use of private address spaces, which are not directly accessible from the Internet. The current connectivity scenarios encompass the need for M2M communication , which is revolutionizing the modern network revolution. Another issue with the current network is the difficulty of easy and scalable functional enhancement. Most device manufacturers develop network device software along with their proprietary hardware to enable the hardware to perform operations appropriate for each communication. Besides these technical limitations, the requirements of new scenarios comprise aspects such as energy consumption, economic and social needs [6]. How to control and manage these networks has become the most important task of the current network architecture [7],[8].

There are two technologies that can help resolve these problems. One of the results of this effort in creating a future Internet is the IPv6 technology. Another of the results of this effort in creating a future Internet is the Software Defined Networking (SDN) design.

Our main goal is to design a SDN architecture based on the IPv6 technology that will eliminate the constraints of VM host minimize control overhead and complex configuration and at the same time improves the maximum utilization of network bandwidth. Figure 1 is an example to illustrate SDNv6 architecture.

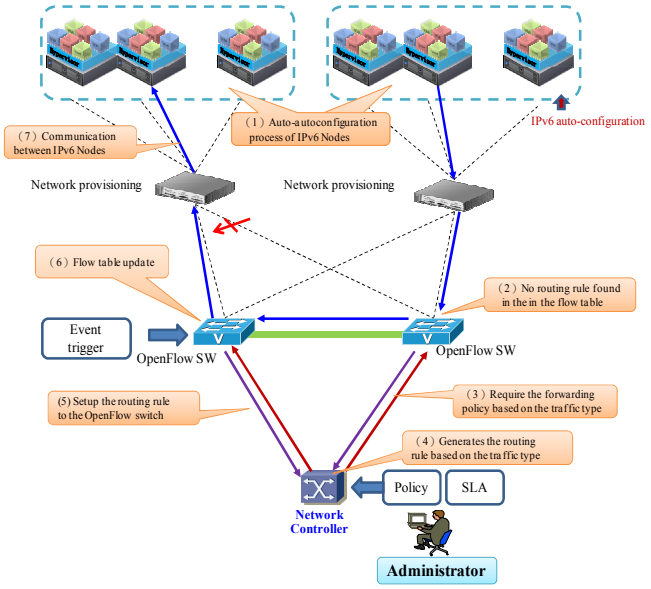

Fig. 1 SDNv6 Architecture

This research was supported in part by National Science Council of the Republic of China under grants NSC 99-2221-E-008-041-MY3 and NSC 100-2218-E-008-012-MY3.

III. PROPOSED IPv6 ENABLED SDN ARCHITECTURE

There are four components in the SDNv6 architecture.

1) VM Hypervisor: VM Hypervisor is a machine that hosts other virtual machines using VMware virtualization software.

2) Network Provisioning: The Network Provisioning device provide IPv6 autoconfiguration function that allows the various VM host attached to an IPv6 network without manual configuration.

3) OpenFlow Switch: An OpenFlow Switch is a software program or hardeare device that forwards packets in SDN environment.

4) Network Controller: The policy based network controller is responsible for the maintenance of the flow tables of one or more switches that are under its control and responsible for the handling of unmatched packets.

Figure 2 is an example to illustrate SDNv6 reference model. SDNv6 decomposes the architecture into three layers: Service plane, Control and Management layer infrastructure layer. In SDNv6 architecture, for more intelligent and smart control. The main ideas of the proposed architecture are as follow:

- Virtualization Network Interconnectivity

Virtual connection is constructed in the virtualized SDN environment. With the SDNv6 environment, an arbitrary number of virtual machines can be quickly created and deployed to any location with arbitrary network topologies. The separate management domain and configuration can provide the logical separation for its function, resource sharing and fault isolation allowing the network designers to construct cloud environments that are more flexible than those we are using today.

- Automatic IPv6 network configuration

In IPv4 environment, IP address, network mask, default gateway and possible domain setting are required in the host network configuration. In SDN network with enormous VM hosts, manual configuration is virtually impossible and pose a big challenge for network management. With IPv6 auto-configuration, IPv6 enabled VM host can leverage the neighbor discovery mechanism to learn the network topology and simplify the network management loading.

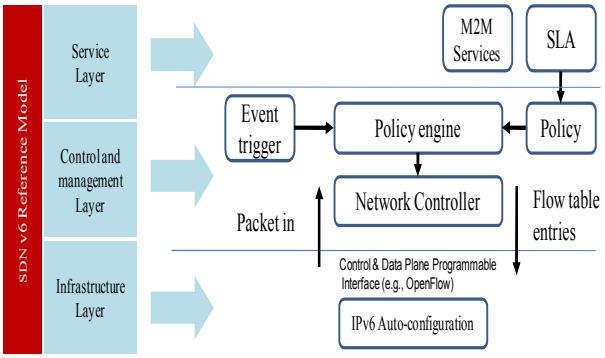

Fig. 2 SDNv6 Reference Model

- Event Trigger based Traffic Control Strategy

Although the OpenFlow specifications are standardized, the controller's behavior and the automatic traffic control are not. For smart and proactive network management, event trigger based traffic control mechanism is required. The event trigger based traffic composed two scenarios: the proactive and passive scenarios. In the proactive scenario the terminal node will issue a request the network resource (e.g., bandwidth or QoS) requirements to the OpenFlow switch when it needs the network service. The OpenFlow switch, upon receiving this information, will trigger the event to the controller for adjustment of the corresponding forwarding policy. The proactive scheme can provide better QoE for users. In the passive scenario when the SLA changes or the network congestion occurs, the network administrator must intelligently trigger the event to the controller for adjustment of the corresponding forwarding policy improving the network reliability guarantee and providing better network QoS.

IV. EXAMPLE CONSIDERATIONS IN SDNV6

Recently SDN are radically transforming data center networking architectures. As cloud business becomes more pervasive, distributed and large-scale data centers hosting a multitude of customers who must be kept securely segmented from each other will eventually become the standard. Not only do these data centers need to handle the very large number of addresses present on the Internet, but they must do so in a virtualized manner with integrated mobility. The major drawbacks of the traditional data center are listed as follows:

- VLAN and switching boundaries are not flexible nor easily extensible. As requirements grow or shrink, computing and storage resources need to be allocated with major operational overhead.
- IP address maintenance and VLAN limits will become challenges as the data center scales, particularly when strong isolation is required or in service provider environments.

For the above reasons, we will discuss the virtual data center use case with SDNv6 in this section.

Case 1: L3 Virtual Data Center Network

The virtual machines can trigger the event to require the network resource or service function like bandwidth, server load balance (SLB), firewall..etc.

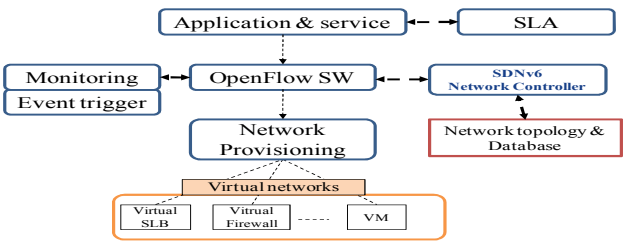

Fig. 3 L3 Virtual Data Center Network Case

In Figure 3, large numbers of virtual machines are expected in this virtual network domain. This type of networking requires simple and robust auto-configuration features. The IPv6 auto configuration allows the various virtual machines attached to an IPv6 network to connect to the internet. Even in the absence of a network provision, hosts on the same link can automatically configure themselves with link-local addresses and communicate without manual configuration.

Case 2: Inter-Connected Virtual Data Center

The data center servers may virtualize applications, processors and devices for the end nodes. In Figure 4, the virtual machines may be located on multiple data centers. The large address space of IPv6 has been designed to allow for multiple levels of subnetting and address allocation from the Internet backbone to the individual subnets within data centers. For performance and reliability considerations, the traffic from the virtual machines need to be inter-connected or aggregated over the network connections/tunnels that have been discovered and provisioned using SDNv6.

Our proposal is to construct an overlay network for a group of VMs. Each host is represented by an individual virtual machine. With the standard IPv6 features, the network provisioning can automatically assign IPv6 addresses and device numbering to each virtual machine providing the interconnection between VMs. In this figure, all VMs in the same group will share a common network identification (such as VLAN). When the VMs communicate with one another, they are not aware of the underlying networks. This requires the SDN to aggregate the VMs traffic over a selected set of network connections which should control adequate delay and bandwidth guarantees. For smart and effective network control, the monitoring function can provide real time network topology surveillance for SLA enforcement monitoring. The event trigger functions can trigger notification for network administrator to respond first hand for network abnormality providing intelligent and smart control for more efficient network performance.

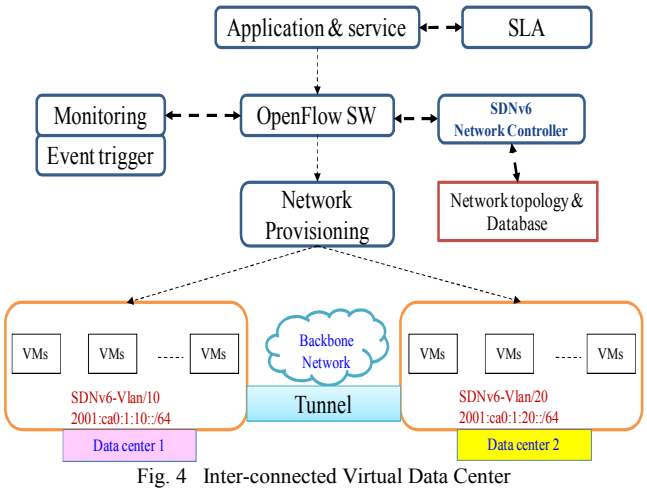

Fig. 4 Inter-connected Virtual Data Center

V. CONCLUSION

IPv6 enabled SDN architecture is the network paradigm for future Internet applications. In this paper we discuss the motivations and progress made towards the development of Software Defined Networking architecture based on IPv6 technology for future networks. Benefits related to using SDNv6 are summarized as follows:

- SDNv6 allows network owners and operators to regain more control of their infrastructure, achieving customization and optimization, and reducing the overall capital and operational costs.
- SDNv6 can mitigate many hardware restrictions and provide virtual network topologies to support innovative services.
- SDNv6 can simplify IP address management by leveraging IPv6 address space and auto-configuration features for end node configuration needs.

This paper only proposes the conceptual SDNv6 network architecture. Future works will be focused on detailing SDNv6 use cases and performance on different scenarios especially in the enterprise network environments.

REFERENCES

[1] S. Azodolmolky, R. Nejabati, E. Escalona, R. Jayakumar, N. Efstathiou, and D.Simeonidou, "Integrated OpenFlow–GMPLS control plane: an overlay model for software defined packet over optical networks," Opt. Express, vol. 19, no. 26, pp. B421–B428, Dec 2011.

[2] Myung-Ki Shin ; Ki-Hyuk Nam ; Hyoung-Jun Kim , "Software-defined networking (SDN): A reference architecture and open APIs," ICT Convergence (ICTC), 2012 International Conference, Daejeon, South Korea, Oct. 2012.

[3] Staessens, D. ; Sharma, S. ; Colle, D. ; Pickavet, M. ;Demeester, P. , "Software defined networking: Meeting carrier grade requirements," Local & Metropolitan Area Networks (LANMAN), Local & Metropolitan Area Networks (LANMAN), 2011 18th IEEE Workshop on, pp.1-5, Oct. 2012.

[4] OpenFlow(6.September.2012).[Online].Available: http://www.openflow.org/

[5] Xiaohan Liu, Gang Qin, Shuangjian Yan, Ze Luo, Baoping Yan, "VNET6: SOA Based on IPv6 Virtual Network," Cloud and Service Computing (CSC), 2012 International Conference, pp.32-39, Nov. 2012.

[6] G. Tselentis, A. Galis, A. Gavras, S. Krco, V. Lotz, E. Simperl, B. Stiller,
and T. Zahariadis, Towards the future internet emerging trends fro m European research. Amsterdam :: IOS Press,, 2010.

[7] L.-D. Chou, Y.-S. Chen, Y.-T. Yang, T.-C. Chang, C.-K. Shieh, S.-W. Huang, "Implementation of Virtual Network Management System with SLA on NetFPGA," Proceeding of the 14th Asia – Pacific Network Operations and Management Symposium (Best Paper Award), Seoul, Korea, Sep. 2012. Project Number : NSC 100-2218-E-008-012-MY3

[8] L.-D. Chou, Y.-T. Yang, W.-P. Chang, T.-C. Chang, Y.-M. Hong, C.-K. Shieh, S.-W. Huang, "The Implementation of Multilayer Virtual Network Management System on NetFPGA," Proceedings of the First International Workshop on Future Internet and Cloud Networking(FICN), Tainan, Taiwan, pp.988-991, 7-9, Dec. 2011. Project Number : NSC-100-2218-E-008-012-MY3