International Journal of Networks and Communications 2012, 2(5): 105-111
DOI: 10.5923/j.ijnc.20120205.03

A Simplified Cloud Computing Network Architecture Using Future Internet Technologies

Yu-Hunag Chu, Yao-Ting Chen, Yu-Chieh Chou, Min-Chi Tseng*

Chunghwa Telecom Co., Ltd.Taiwan, R.O.C

Abstract Cloud computing is expected to provide quick, agile, stable and reliable services. Traditional cloud computing network architecture is too complicated to fulfil these services. Future internet is proposed to reinvent the Internet using a clean slate approach. Many new technologies including OpenFlow, Autonomic Computing, Content-Centric Network, Cross-layer communication and Locator/ID Separation Protocol are proposed to improve the limitations of current Internet. The main contribution of this paper is to propose a simplified cloud computing network architecture. This architecture first adopt OpenFlow switch simulate Firewall, SLB, and Switch simultaneously. The network devices are consolidated into one single device. Then, using Autonomic Computing concept can reduce operation cost and simplify management effort. Finally, Locator/ID Separation Protocol technology is adopted to enhance network security. This novel cloud computing network architecture is implemented and experimented in our laboratory. This novel network architecture results in huge cost saving both CapEx and OpEx.

Keywords Cloud Computing, Future Internet, OpenFlow, Simplified Architecture

1. Introduction

Cloud computing is expected to supply agility, scalability, fault-tolerance and SLA. The Cloud computing network is the fabric that provides secure user access and an infrastructure for the deployment, interconnection and aggregation of shared data center components as required, including applications, servers, appliances, and storage. A properly planned data center network protects application and data integrity, and optimizes application availability and performance. Data center services like security with firewall and intrusion prevention, and application resiliency with server load balancing techniques are included. It's expensive and complex to construct a fully secure multitenant Cloud computing center. It is too complex to dynamically provision so many devices for each service submission. The cloud computing network architecture needs to be redesigned and simplified. This paper proposes simplified network architecture. This architecture is cost effective and easily maintained, provisioned, and secured.

Future Internet is a general term for research activities on new architectures for the Internet. The research[1, 2, 3] focuses on solving present Internet's problems such as scalability, security, mobility, Quality of Service (QoS), robustness, and heterogeneity. The demand of future applications and services also accelerates the discussion and study of Future Internet, which is expected to overcome the limitations of current Internet and capably adapt to futuristic demands. In this article, we adopt OpenFlow[4, 5], Autonomic[6], and Identifier (ID) Locator split technologies to construct a novel simplified cloud computing network architecture. Besides on OpenFlow technology, the Firewall, server load balancer and Ethernet switch could be programmed, simulated and implemented on a single device. This new consolidated device is easily provisioned, programmed and managed. This simplified data center network architecture will decrease the OPEX and increase flexibility of cloud data center operation.

The rest of this article is organized as follows. Section 2 introduces existing cloud computing network architecture. Section 3 describes future internet technology. Section 4 is the simplified cloud computing network design. Section 5 implements the proposed architecture. Section 6 concludes this article.

2. Existing Cloud Computing Network Architecture

The existing cloud computing network architecture has a lot of different elements in service layer. It includes router, Firewall, Ethernet switch, Fiber channel switch, Server load balancing (SLB), and Volume Based Billing/Control (VBB/VBC) devices. Firewall is designed to permit or deny network transmissions based upon a set of rules. Cloud computing network use Firewall to protect the servers and

* Corresponding author:
minchi@cht.com.tw (Min-Chi Tseng)
Published online at http://journal.sapub.org/ijnc

storages. The SLB shares the loads between each server. The VBB/VBC is used for traffics volume billing.

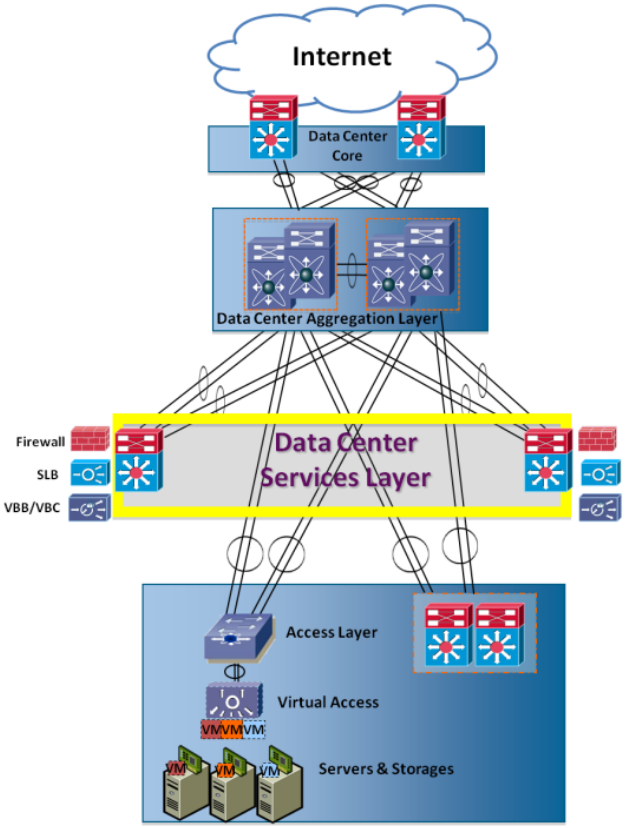

Figure 1. Existing Cloud Computing Network Architecture

Fig. 1 shows the existing cloud computing network architecture. There are lots of network and service devices to construct a cloud computing network. The data center uses a core router to connect the internet. There is an aggregation layer aggregating the services' layer devices. The services' layer is a complex layer. The application devices, such as Firewall, SLB and VBB/VBC, are in this layer. All the devices in services' layer connect to aggregation layer and switched/routed by the aggregation device. Subscriber could submit their service flexibility. Based on each service, the network architecture may be different. Some subscriber may choose SLB service and Firewall service. Some subscriber could choose flexible billing service based on fixed traffic volume. The network architecture could be varied based on different service provisioning.

The access layer includes virtual access devices, servers and storages. The access layer offers physical connectivity among servers and the network. This network architecture and configuration are quite complex, and the operation cost is very expensive.

3. Future Internet Technologies

3.1. OpenFlow

OpenFlow is one of the Future Internet technologies proposed by Stanford University in September 2007. The ambition of OpenFlow is allowed researchers to innovate and run experimental protocol in the networks. In order to maintain and support OpenFlow specification, a team of researchers from Stanford University established OpenFlow Switching Consortium in 2008. OpenFlow is added as a feature to existing Ethernet switches, IPv4 routers and Wi-Fi access points, with an internal flow-table, and a standardized interface to add and remove flow entries. OpenFlow Switching Consortium defines the flow table and OpenFlow controller. There is a remote controller[6] to control the OpenFlow enabled device. The latest version of the OpenFlow Switch Specification is version 1.3.0.

In traditional switches or routers, the data plane which forwards packets and the control plane which processes routing decisions are occurred on the same device. That makes network devices complex and inflexible. OpenFlow adopts the clean slate[7] design, which separates the data and control plane. OpenFlow is added as a feature to existing Ethernet switch, IPv4 router or wireless access point, along with an internal flow-table and an interface to add or delete flow entries. In general, the data plane is accountable for packet handling and forwarding, and the control plane is responsible for data flow processing. An external OpenFlow controller is in command of the duty of the control plane. With the feature, researchers can run innovation protocols on the production network to validate experimental protocols without limited by different vendors' network devices. OpenFlow controller controls the flow table and switch's status and flow information through OpenFlow protocol. The programmable characteristic of OpenFlow enables network administrators could provision and manage the OpenFlow enabled network dynamically. OpenFlow enables innovative ideas to emulate Ethernet switch, firewall, SLB and VBB/VBC in an OpenFlow enabled devices simultaneously. This new device can simplify the data center network architecture and reduce the investment cost of data center. Besides, it can increase management and maintenance efficiency.

3.2. Identifier/Locator Split

In conventional Internet architecture, IP address is used to represent network identity and location at the same time. Then, routing scalability, mobility and multi-homing becomes challenges of current Internet. ID Locator split technology has been widely proposed to solve these problems. For example, the National Institute of Information and Communications Technology (NICT) in Japan proposed generic identifiers for ID/locator split internetworking[8]. ITU-T in SG-13 published the general requirements for ID/locator separation in NGN[9]. The Internet Engineering Task Force (IETF) conducts three working group in

ID/locator split research and proposed Locator Identifier Separation Protocol (LISP) Internet Drafts[7]. Once the locator and identifier of the host are separated, only locator will change as node moves and the identifier remains unchanged.

There are many drafts in IETF intending to propose

deployable protocol and solutions. There are host-based LISP and network-based LISP approaches. LISP inserts an additional identity layer between the network layer and Transport layer of OSI model. There are identifier and locator in new IP header. Identifier (ID) means "who", which is used to identify the node, such as hosts, servers, routers, etc. Locator (LOC) indicates "where", which provides the information of where to approach the host. The host- based solution proposes new LISP protocol from host point of view, and network-based LISP simplifies the changing and focuses on network devices only.

The mapping between identifier and locator is stored on the resolution system. Because ID must be unchanged and permanent, the ID could be used for identity verification. So, the LISP is easier to improve security than existing Internet.

3.3. Autonomic

Autonomic network is proposed for reducing network operation cost and increasing reliability. It can relieve the burden of system management and monitoring. The design of autonomic network is moving toward to self-management. Many European Union (EU) research projects focus on autonomic management and networking development. The noticeable projects include EU Autonomic Internet (AutoI)[10], EU Autonomic Network Architecture (ANA), EU Extending Features of IPv6 for Autonomic Networks and Services (EFIPSANS), and EU Component-ware for Autonomic Situation-aware Communications, and Dynamically Adaptable Services (CASCADAS).

Autonomic management exhibits self-CHOP properties: self-Configuring, self-Healing, self-Optimizing and self-Protecting. Autonomic systems can adjust themselves automatically according to pre-configured high-level policy. The autonomic feature can spontaneously detect problems, improve their performance and defend attacks.

4. Simplified Cloud Computing Network Design

The benefits of simplified cloud computing network architecture include network devices' consolidation, VLAN scalability achievement, on-demand provision, and security. The detailed description of these features showed as follows:

4.1. Cloud Computing Network Devices Consolidation

This paper proposes simplify the cloud network architecture by consolidate data center network layer and devices. This design could improve network operation efficiency, and reduce management and maintenance cost.

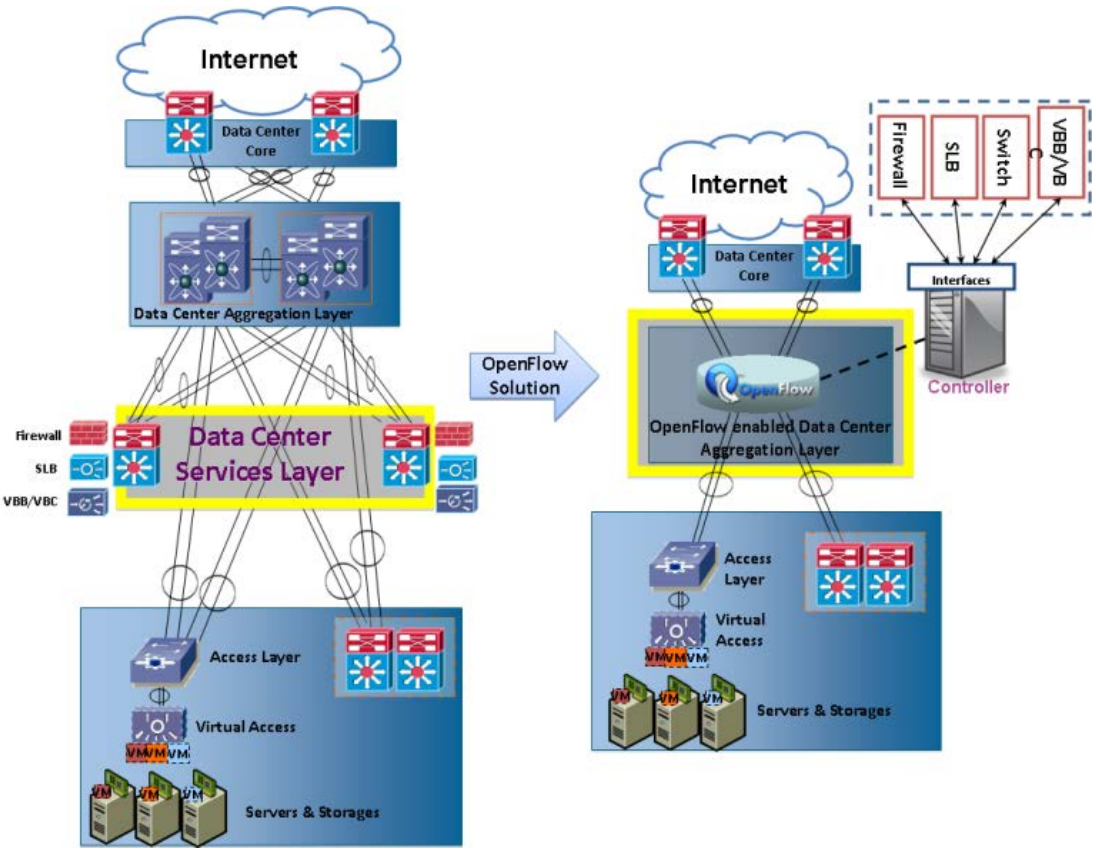

Figure 2. Simplified Cloud Computing Network Design

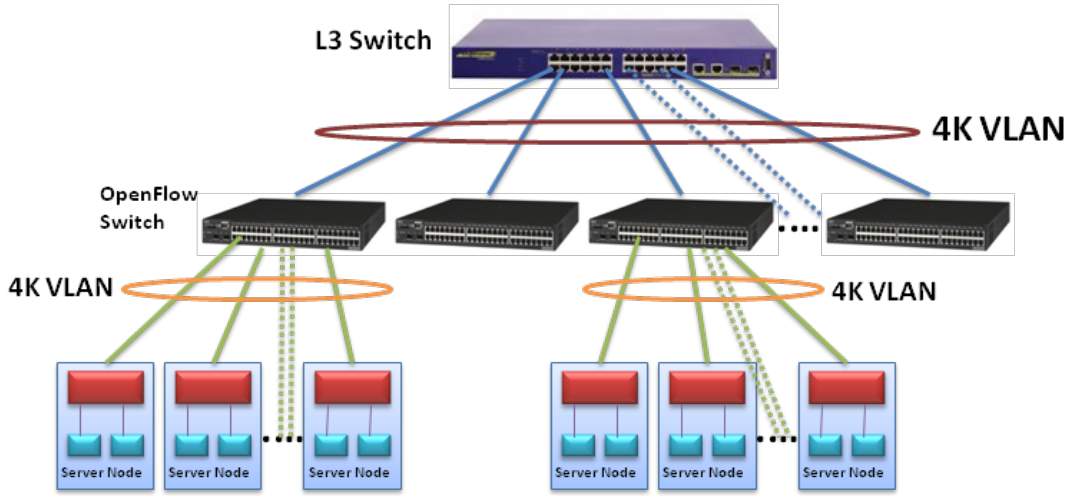

Figure 3. VLAN Scalability Concept

The comparison between traditional cloud computing network and simplified network architecture is shown in Fig. 2. The traditional data center network consists of data center core, data center aggregation layer, and data center service layer. Data center aggregation layer is the boundary between Layers 2 and 3. Data center service layer contains firewall, SLB and VBB/VBC, etc. The simplified cloud computing network design uses single OpenFlow enabled aggregation layer to simulate both data center aggregation layer and data center service layer. The OpenFlow enabled aggregation layer contains only OpenFlow enabled devices and the service layer is virtualized and become an application on the controller. This OpenFlow device can simulate all features of the service layer. The functions in the services layer are implemented by software and provisioning to the OpenFlow enabled switch by OpenFlow protocol and OpenFlow controller's interfaces. The OpenFlow controller's interface defines the flow table operation functions, for example: add, delete, modify, and getting information. The link status, node information, flow table and link utilization of OpenFlow enabled device can be easily monitored through controller's interface. The OpenFlow enabled switch could play the role of firewall, SLB, aggregation switch and VBB/VBC simultaneously based on 12-tuple flow table configurations. Service functions could be deployed and configured by OpenFlow controller. The service functions could also be placed outside the OpenFlow controller for easier management and scale point of view.

4.2. VLAN Scalability Achievement

Current cloud network is suffering from 4096 VLAN IDs limitation. It is impossible to isolate each tenant by dedicated VLAN ID for security requirement. As a result, multiple tenants may share one VLAN ID, which causes insecurity. The proposed simplified cloud network architecture could make VLAN ID number extended to 4069x4096. It is because OpenFlow Switch can modify VLAN ID and using one VLAN ID to represent 4096 VLAN ID. Fig. 3 shows

OpenFlow Switch connected to servers and L3 switch. In the server side, each OpenFlow switch can accommodate up to 4096 VLAN ID. After flow table translation, there is only one VLAN ID used to represent these 4096 VLAN ID packets to the L3 Switch. On the other hand, packets send from L3 switch to OpenFlow switch, OpenFlow switch will change the unique VLAN tag to corresponding tenant VLAN tag according to destination MAC and IP address. Then, VLAN space is extended to 4096x4096. At the same time, tenant security is satisfied for isolated by dedicated VLAN ID.

4.3. On-demand Provision

Cloud computing is agile because on-demand provisioning of virtualized resources. When a user subscribes the cloud computing service, the virtual machine and network devices would be provisioned immediately for these requests. However, the traditional network devices aren't designed for dynamically provisioning. On the other hand, OpenFlow is created to be programmable protocol. It's easier to use OpenFlow to provide the dynamic network provision. OpenFlow enabled cloud computing network is an on-demand provisioned cloud computing network. The network provision can also be triggered by web portal, which is the cloud computing service portal.

The new proposed cloud computing services and network service are depicted in Fig. 4. Firstly, customer can access the web portal via the internet. There are service platform and network platform support the web portal. There are cloud services and network services provided by the cloud provider. The cloud services include at least cloud IaaS service, IP Multimedia Subsystem (IMS) VoIP service, Hami book store, and Hadoop big data service. The network services contain per flow billing service, traffic engineering enabled service, DDoS defender security service and firewall security services. Once one subscriber submits the cloud services, the service platform would provision both the cloud service and network service immediately.

The OpenFlow controller is in charge of network devices provisioning. When the cloud services and network features are provisioned successfully, the subscriber will start to use the subscribed services eventually.

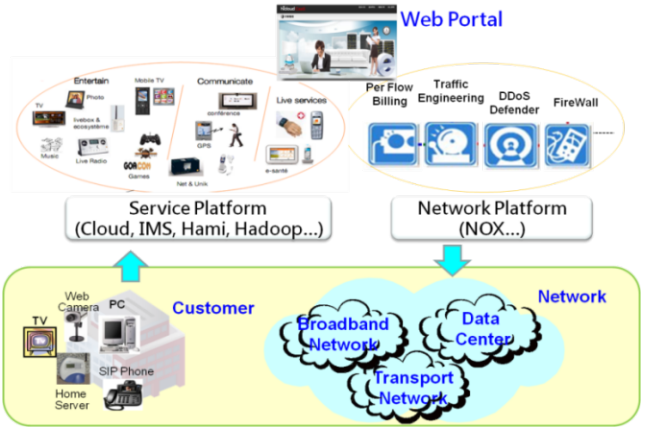

Figure 4. On-demand provisioning

4.4. Security Network

There are many cloud computing security topics such as: Data Protection, Identity Management, Application Security, Privacy, Availability, and, etc. In this paper, we focus on identity management and availability to improve cloud computing network security. Identity management allows every client to have its own identity to access cloud service. In general, the identity check is on the server side. The network security is responsible by intrusion detection system (IDS) and Intrusion Prevention System (IPS) in a data center. This solution is inefficient because the attacker's traffic will occupy the network resource from attacker to data center. If the network device can have the capability to check each packet's identity, there is no need to send the identity packet to the server for confirmation. With OpenFlow and LISP technologies, OpenFlow enabled switch can verify packet's ID on OpenFlow controller (NOX) as the identity check. Only valid ID's packets are allowed to enter the cloud data center.

Besides, there still have many security threats behind, such as IP spoofing, Distributed Denial of Service (DDoS) attacks, intrusions, worm infections, etc. The OpenFlow-based DDoS defender is implemented on OpenFlow controller[11] by the concept of Autonomic Computing. In cloud computing network, DDoS defender is activated on OpenFlow enabled switches to intensify network robustness. Moreover, IPS is deployed to block and prevent intrusion.

The deployment of secure cloud computing network which integrated with on-demand provision application is shown in Fig. 5. Once the cloud service is subscribed, the client's ID will be registered on the OpenFlow enabled switches. Only the recognized traffic could be allowed to access to the server farm. When an OpenFlow enabled switch receives a packet which is not matched on the flow table, the packet would be blocked or sent to the OpenFlow controller for analysis. The controller would verify whether the ID is on the list of granted clients. If the ID is unregistered or invalid, the packet would be dropped or sent to security equipment, such as IDS/IPS, for further investigation. For a highly secure network point of view, the network must enable the features of OpenFlow ID check, DDoS defender and IPS appliance.

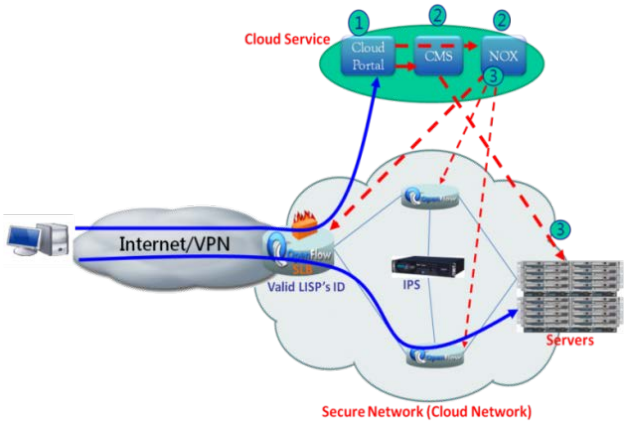

Figure 5. On-demand provision and security network

5. Implementation of Simplified Cloud Computing Network Architecture

To achieve the proposed architecture design, we use OpenFlow enabled switch to replace existing SLB, Firewall and Ethernet switch. Fig. 6 shows the test environment of this experiment. There are Cisco router, NEC IP8800, OpenFlow controller and Spirent TestCenter in this test environment. Spirent TestCenter emulates two web servers, one FTP server, one Mail Server, and three clients simultaneously. Cisco router is the L3 core router. NEC IP8800 is the OpenFlow-enabled switch which simulates firewall, Ethernet switch and SLB concurrently. The applications run on the OpenFlow Controller to provision the NEC IP8800.

Firstly, Spirent TestCenter emulates clients that possess public IP address (200.1.1.1~4) as shown in Fig. 6. On the other hand, servers are placed on the private networks. The NAT function will translate servers' private IP address (192.168.1.0/24) to public IP address (100.1.1.100). As a result, clients can access the FTP server successfully even though FTP server is in the private network. Secondly, one ACL rule is set up to block TCP port 23 on NEC IP8800. Fig. 7 shows the traffic of TCP port 23 is dropped. Thirdly, the SLB function is verified. Fig. 7 shows the two HTTP servers will equally receive request packets from the clients. From the test result, OpenFlow switch is capable of providing Firewall, SLB and switch functions.

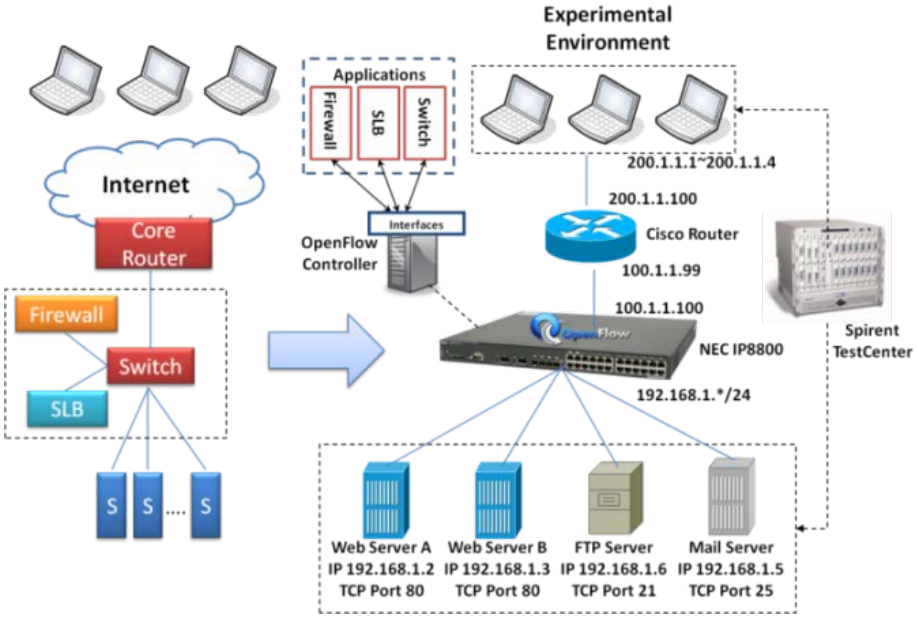

Figure 6. The experimental environment

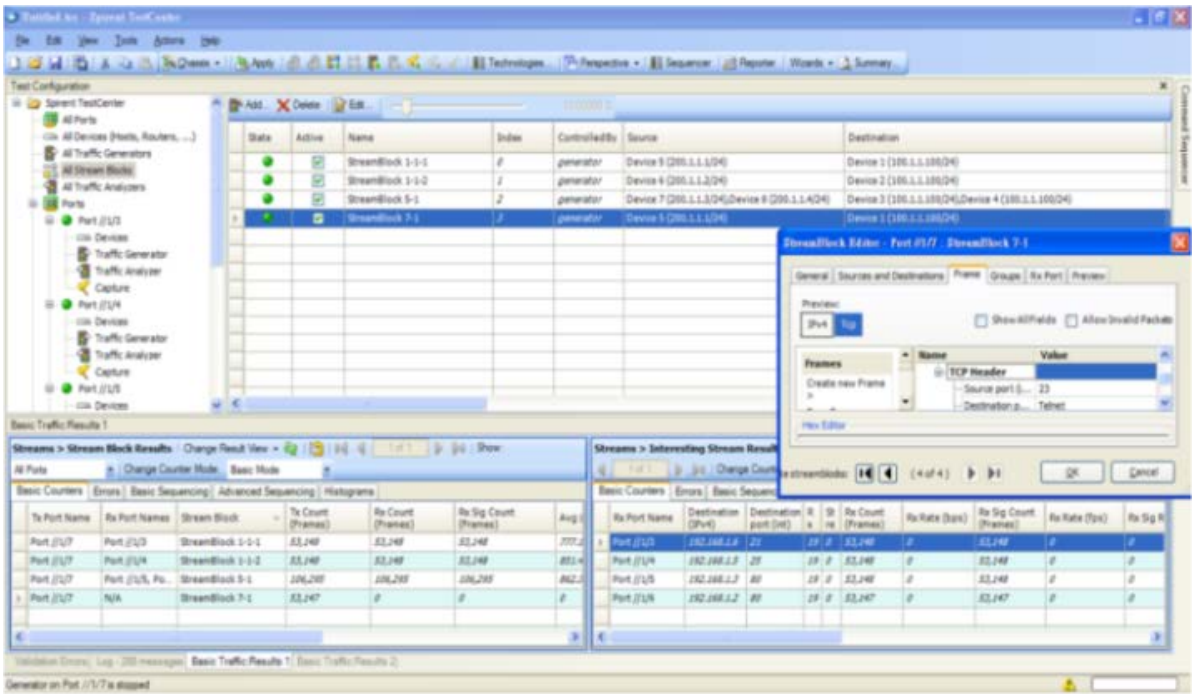

Figure 7. The experimental result

6. Conclusions

Cloud computing has become one of the hottest topics in recent years. Traditional cloud computing network architecture is too complicated to fulfil diverse cloud services. This paper proposes a simplified cloud computing network architecture leveraging clean-slate concept. The advantages of this architecture include network device consolidation, VLAN scalability, on-demand provision, and security improvement. The experimental result shows that one OpenFlow switch can play Firewall, SLB and Switch concurrently. The unpermitted traffic of TCP port 23 can be blocked. User web request can be equally balanced to backend servers. Nevertheless, this experiment is manual provision. The web-based auto-provision feature will be implemented in our further research.

REFERENCES

[1] A. Feldmann, "Internet Clean-Slate Design: What and Why?" Computer Communication Review, ACM SIGCOMM, vol. 37, no. 3, pp. 59-64, 2007.

[2] AKARI Architecture Design Project, "New Generation Network Architecture—AKARI Conceptual Design (Ver.

2.0)" 2007.

[3] ISO/IEC JTC 1/SC 6, "Working Draft Technical Report Text for JTC 1/SC 6 Future Network: Problem Statement and Requirements," 2009.

[4] The OpenFlow Switch Consortium.http://www.openflowswitch.org.

[5] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. Openflow: enabling innovation in campus networks. SIGCOMM Comput. Commun. Rev., 38(2):69–74, 2008.

[6] C. Jelger, C. Tschudin, S. Schmid, and G. Leduc, "Basic Abstractions for an Autonomic Network Architecture," in Proceedings of AOC'07, June 2007, Helsinki, Finland.

[7] D. Farinacci, V. Fuller, and D. Oran. "Locator/id separation protocol (LISP). Internet Draft," January 2007. Available online at: www.ietf.org/internet-drafts/draft-farinacci-lisp-00.txt.

[8] V. P. Kafle, K. Nakauchi, and M. Inoue, "Generic identifiers for ID/locator split internetworking," Proc. ITU-T Kaleidoscope event, Innovations in NGN – Future Network and Services, Geneva, Switzerland, May 2008.

[9] General requirements for ID/locator separation in NGN (Y.2015), ITU-T, January, 2009.

[10] AutoI http://ist-autoi.eu/autoi/index.php

[11] Yu-Hunag Chu, Min-Chi Tseng, Yao-Ting Chen, Yu-Chieh Chou, Yan-Ren Chen, "A Novel Design for Future On-Demand Service and Security", IEEE ICCT 2010

[12] ONF White Paper, "Software-Defined Networking: The New Norm for Networks", April 13, 2012.

[13] Software Defined Network(SDN) http://pomi.stanford.edu/content.php?page=research&subpage=openflow