*Proceedings of the Asia-Pacific Advanced Network* ***2014*** *v. 36, p. 125-131.*
*http://dx.doi.org/10.7125/APAN.36.18*
*ISSN 2227-3026*

# Network as a Service and its Key Challenges in Cloud Computing

**Mohammad Aazam and Eui-Nam Huh** *

Innovative Cloud and Security Laboratory, Computer Engineering Department, Kyung Hee University, Suwon, South Korea

E-Mails: aazam@ieee.org; johnhuh@khu.ac.kr

* Author to whom correspondence should be addressed; Tel.: +82-31-201-2454; Fax: +82-31-204-3778

**Abstract:** With the passage of time, cloud computing is gaining importance due its usability, flexibility, efficiency, and reachability. Virtualization is the key component in cloud computing. Through virtualization, not only software and hardware resources are efficiently used, but also a lot of money is saved. Virtual networking is also an emerging utilization, achieved through virtualization of resources. Keeping in view the importance of this area of research, this paper discusses about virtual networking and the key challenges involved in it and in virtual switch.

**Keywords:** virtual network switch; virtualization; cloud computing.

## 1. Introduction

Cloud computing is the paradigm of next generation computing, where not only the software resources, but the hardware resources are also outsourced [1]. Hardware resources are not limited to the CPU time, memory, and storage space, but it also refers to the whole networks being outsourced. Such networks are known as virtual networks, in terms of cloud computing. Virtual

networks have a great utility, since they not only save a lot of money for the user, but also provide diverse networking environments for academic and professional test bed setups.

Cloud computing provides four categories of services, namely: Software as a Service (SaaS), Platform as a Service (PaaS), Networks as a Service (NaaS), and Infrastructure as a Service (IaaS) [2]. SaaS refers to application working over the Internet which is available for the user on pay-as-you-go basis [3]. User does not need to store, install, and maintain the application. Instead, only Internet connectivity is required to access the service that has been rented out by the SaaS service provider on the cloud. PaaS is providing a platform to build applications and services, with all the toolkits and resources required to do so [4]. NaaS provides virtual network(s) to the users. User can have as many numbers of networks as required, with desired segmentation and policy enforcement. With NaaS, user can also have heterogeneous networks, for example, IPv4 and IPv6 segments working in co-existence or separately. IaaS provides computation and storage services on rental basis. Instead of purchasing expensive machines, servers, and storage devices, even for small tasks, user can outsource this task to the IaaS service provider [4]. With storage in IaaS, not only the data is stored by the IaaS service, but also, it makes the data universally accessible over the Internet.

## 2. Virtualization and Network as a Service

Making hardware and or software resources available to the user, without their physical presence directly under that user, is known as virtualization. Virtualization is the basis of cloud computing, through which, resources are outsourced on pay-as-you-go basis [1]. virtualized computing are based on the idea that users create individual virtual machines and virtual networks as execution environments for their tasks, allowing them to provide the required software resources, without being dependent upon the site administrators [5]. Virtualized environment is not only beneficial for the user, but also for the cloud service provider as well. In the user's perspective, instead of purchasing expensive hardware and then managing and maintaining it, user only has to pay the rent for what he has done on cloud environment [6, 7]. On the other hand, the cloud service provider has the opportunity to utilize all the resources in the best way by outsourcing to multiple users at a time, known as multi-tenancy in cloud computing. Unlike the traditional system, resources are not under-utilized, which creates more efficiency in the overall system and resources are used the way they should have been.

Virtualization also provides the privilege to create virtual networks. As discussed, Network as a Service (NaaS) is among the most useful services cloud computing provides. Sole users or whole organizations can take advantage of that, since NaaS provides all the kinds of virtual networking facility a user, academia, office, or a company needs to have. Diverse kinds of

networks can be created through virtual networking service, with customized policies enforced on different networks and/or subnets. Figure 1 shows the virtual networking scenario.

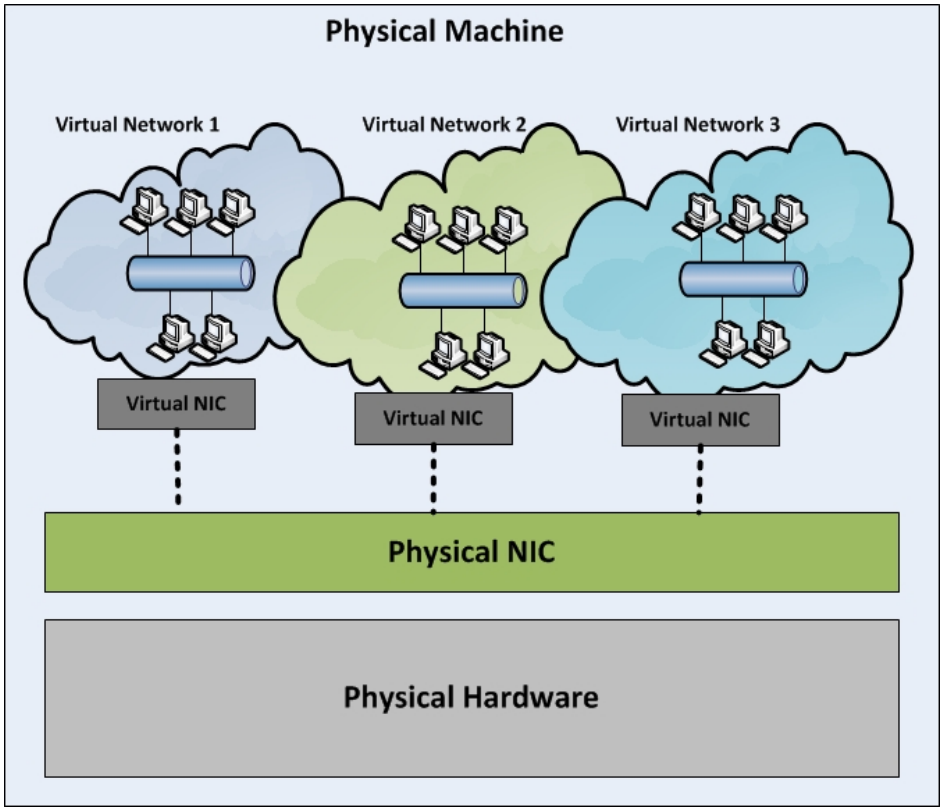


**Figure 1. Virtual networking**

## 3. Virtual Network and Switch Challenges

Since virtual networking provides user the privilege to create and manage different kinds of networking scenarios, with least amount of cost, since user has to bear the cost of usage and not the whole infrastructure, so users tend to create networking scenarios according to their needs, which leads to some complexities. So, due to this, besides all these benefits virtual networking bears with it, there are some challenges. This section discusses about those challenges.

- Shared network layer vulnerability

To accommodate the VM's working for the same company or organization communicate with each other, they are allocated in the same shared network [8], based on the assumption that VM's that belong to a same virtual shared network are trustful to each other. This 'assumption' makes this shared network layer vulnerable to attacks.

- VM exit

To emulate the interface, virtualization tool or hypervisor must use hardware virtualization extensions to trap each attempt to access the device. Every attempt to access the hardware creates a VM exit, which is disastrous for the performance. So, emulated interfaces are used only if necessary.

- Switch and traffic management

Much of the traffic between VM's on a same host does not leave the host and go to the physical network [8]. So that traffic cannot be monitored or managed by physical devices (firewall, Intrusion Detection System/Intrusion Prevention System). This creates issue in managing the traffic as well as the switch.

- I/O bandwidth

With more VM's, more traffic is generated and thence more processing is required from the physical CPU to move that traffic within VM's [8]. This creates a huge I/O bandwidth for the server and switch to manage. Efficiently handling this I/O bandwidth is an issue for a server as well as virtual switch.

- Security

For the purpose of security, only NAT is used in virtual networks. Having only NAT for the purpose of security is not good enough [1, 9, 10]. Since NAT can be traversed through IPv4-in-UDP tunneling, so this solution is not always workable. Also, as discussed previously that VM's working for the same organization are treated to be on the same network and they are allowed to communicate with each other. This also causes security vulnerability.

- IPv4-IPv6 coexisting virtual networks

One of the most significant things with virtual networking can be to create such scenarios, where IPv4 and IPv6 coexist. Since, IPv4 has exhausted and migration towards IPv6 is already underway, so, both these versions of IP are going to coexist for a reasonable time. During that period, viable solutions, according to the needs of user as well as organizations, including the service providers, effective solutions are required. Research is still going on in this regard. Tunneling is considered to be the best possible solution for this purpose [11], [12], and [13]. Since, tunneling involves some overhead, so, virtual networking can provide a very good mean to analyze that, before deploying practically, according to the needs of service provider or organization and the traffic involved. Other

than that, cloud service providers also have to have such kind of networking scenarios, since the requesting user can be using other version of IP, as compared to the server. A physical machine can have various IPv4 and IPv6 virtual machines or virtual networks, creating a hybrid IPv4-IPv6 networking environment.

- Quality of Service provisioning

As the amount of data increases and the type and unpredictability also comes into play, QoS becomes an issue. At any moment, any type and amount of data can be triggered. It may also be an emergency data as well. Dynamic prioritization of the requests would be required on cloud side. QoS would mostly be measured in terms of bandwidth, delay, jitter, and packet loss ratio [14]. Depending upon the type of data and its urgency to be sent to the sync node, QoS must be supported.

- Location of data storage

Location also matters for critical and latency or jitter sensitive data. Time sensitive data, like video, should be stored in the closest possible physical location to the user, so that minimum possible time should be involved in accessing big data. For multimedia data, nearest possible virtual storage server must be allocated. It also possible that studies on live migration should be extended and enhanced. For types of data which require collaborations, like collaborative work on cloud storage services, like Dropbox or GoogleDrive, allocating resources of nearest possible available pool of resources and also, migrating data contents to the closest possible location makes it more efficient and network friendly for both the parties, the service provider and the service consumer.

## 4. Conclusions

Benefits of cloud computing cannot be denied. But the issues involved in it must also be considered and focused in the research and development, to make this paradigm more acceptable for the user as well as the service provider. Virtualization holds a key in cloud computing, but it has some issues involved in it. Those issues, focusing more on virtual networking and virtual switch have been gathered and discussed here in this paper. This will allow the research and development sector, working on virtual networks, to focus on these issues and further developments to be done accordingly, keeping in view these problems.

## Acknowledgment

This research was supported by the MSIP (Ministry of Science, ICT & Future Planning), Korea, under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National IT Industry Promotion Agency)" (NIPA-2013-(H0301-13-2001)). The corresponding author is Prof. Eui-Nam Huh.

**References**

1. Ryan Shea and Jiangchuan Liu, “Network Interface Virtualization: Challenges and Solutions”, IEEE Network Journal, October 2012.
2. W Ma et al., “The Survey and Research on Application of Cloud Computing”, in the proceedings of 7th International Conference on Computer Science and Education, 02-04 November, 2012, Wuyishan Mountain, China.
3. Y. Jadeja et al., “Cloud Computing - Concepts, Architecture and Challenges”, in the proceedings of International Conference on Computing Electronics and Electrical Technologies, Nagercoil, India, 21-22 March, 2012.
4. Minqi Zhou et al., “Services in the Cloud Computing Era: A Survey”, in the proceedings of 4th International Universal Communications Symposium, Beijing, China, 18-19 October, 2010.
5. Roland Schwarzkopf, Matthias Schmidt, Christian Strack, Simon Martin and Bernd Freisleben, "Increasing virtual machine security in cloud environments", Journal of Cloud Computing, July 2012
6. Alex Comninox, “Emerging Issues: Cloud Computing Learning”, South African Internet Governance Forum 2011
7. Siani Pearson et al., “Privacy, Security and Trust Issues Arising from Cloud Computing”, in the proceedings of 2nd IEEE International Conference on Cloud Computing Technology and Science, Indianapolis, USA, Nov. 30- Dec 03, 2010.
8. Hanqian Vu et al., “Network Security for Virtual Machine in Cloud Computing”, in the proceedings of 13th International Conference on Computer and Information Technology, Dhaka, Bangladesh, 23-25 Dec., 2010
9. G Aljabbari and Evren Eren, “Virtual WLAN: Extension of Wireless Networking into Virtualized Environments”, International Journal of Computing, 2011
10. Judith Hurwitz et al., “Security issues with cloud computing virtualization”, available at: http://www.dummies.com/how-to/content/security-issues-with-cloud-computing-virtualizatio.html

11. M Aazam et al., “Deployment and Performance Evaluation of Teredo and ISATAP over Real Test-bed Setup”, in the proceedings of ACM Management of Emergent Digital EcoSystems 2010, Bangkok, Thailand, 26-29 Oct., 2010
12. Mohammad Aazam et al., “Comparison of IPv6 Tunneled Traffic of Teredo and ISATAP over Test-bed Setup”, in the proceedings of IEEE International Conference of Information and Emerging Technologies 2010, Karachi, Pakistan
13. Mohammad Aazam, Eui-Nam Huh, “Impact of IPv4-IPv6 Coexistence in Cloud Virtualization Environment”, Springer Annals of Telecommunications, vol. 68, August 2013, DOI: http://dx.doi.org/10.1007/s12243-013-0391-6
14. Mohammad Aazam, Adeel M. Syed, Eui-Nam Huh, “Redefining Flow Label in IPv6 and MPLS Headers for End to End QoS in Virtual Networking for Thin Client”, in the proceedings of 19th IEEE Asia Pacific Conference on Communication, Bali, Indonesia, 29-31 August, 2013