Implementation and Operation of User Defined Network on IaaS Clouds using Layer 3 Overlay

Ryo Nakamura, Yuji Sekiya and Hiroshi Esaki
The University of Tokyo, Bunkyoku, Tokyo, Japan

Keywords: IaaS, Cloud Network, Layer 3 Overlay Network, LISP, VXLAN.

Abstract: Server virtualization technology achieves ”Infrastructure as a Service (IaaS)” model services. Anyone can use virtual server resource easily without preparing computer hardware, thus IaaS environments provides multiple operational benefits to users. Therefore, today various types of users, both of personal users and enterprises users, deploy virtual resources on IaaS cloud. On the other hand, many enterprise users still have their own environments and operate them by themselves (i.e, on-premise environments). When they migrate the services from physical facilities to IaaS clouds, they have two problems. The first problem is that services are bound to IP addresses. The second problem is lack of flexibility in network design and management on IaaS clouds. To solve these problems, we propose an operation model to migrate on-premise services to IaaS clouds using LISP and VXLAN. Using our proposed method, users can migrate IP addresses and services among IaaS clouds. In this paper, we proposed new migration method of IP address among IaaS clouds and implemented the method using LISP and VXLAN software on Linux systems. Then we evaluate performance of our system and present a operation on actual IaaS clouds.

1 INTRODUCTION

Many virtual machines (VM) can work on single physical machine by virtualization technologies. Then, there are some service providers that provide virtual machine environments that are called Infrastructure as a Service (IaaS) to users. IaaS providers provide VM to users, and users pay fee depending on resources of VM. Today, these IaaS services are used by many consumers and enterprises. IaaS service offers many operational benefits such as reducing the costs of facilities and fault tolerance. Hence, enterprises tend to adopt IaaS clouds for benefits.

However, migrating existing services that are already operated in on-premise environment to IaaS clouds. The first problem is flexibility of IP addresses. Almost services are bound to IP address, e.g., www and IP address based access control (ACL). IP addresses that are used for service servers can be changed easily using the DNS system. However, changing IP addresses that are embedded into configuration such as ACL requires expensive operational costs. An IP address of IaaS provider is assigned to a VM. Thus, if a user want to migrate their services to IaaS cloud, IP addresses must be changed.

Besides, the layer 2 segment design and its construction on IaaS cloud should have also flexibility. In on-premise environments, layer 2 network segments are separated by policies and usages. This sort of network separations should be possible in IaaS cloud. Several IaaS clouds and researches provide functions to design flexible layer 2 network (Amazon, 2012)(Benson et al., 2011)(Cabuk et al., 2007). However, this flexibility is sometimes restrected by contracts and basically design of IaaS clouds.

The second problem is redundancy. If a user migrate their systems to IaaS cloud, the services are not so redundant. A service provider of IaaS cloud may construct their system highly redundant, however, there are some possibility of failures that deploying services on single IaaS cloud rather than on multiple IaaS clouds. Thus, the service which is migrated from on-premise environment to IaaS clouds must be constructed among several IaaS clouds.

In this paper, we present an approach that can isolate user networks from underlay IaaS clouds using layer 3 overlay networks. By using layer 3 overlay, user can define networks among several IaaS clouds with their own IP address prefixes. In order to achieve this isolation, we implemented Locator ID Separation Protocol and Virtual eXtensible LAN on Linux system. Finally, we evaluated implementations and present the operational model of our system.

Nakamura R., Sekiya Y. and Esaki H..
Implementation and Operation of User Defined Network on IaaS Clouds using Layer 3 Overlay.
DOI: 10.5220/0004373803660369
In *Proceedings of the 3rd International Conference on Cloud Computing and Services Science* (CLOSER-2013), pages 366-369
ISBN: 978-989-8565-52-5

2 APPROACH

In this section, we describe the requirements to migrate systems from on-premise environments to IaaS clouds, and the overview of proposed approach.

2.1 Requirements

Requirements to achieve migration from on-premise environments to IaaS clouds are shown below.

- Migrating IP address prefix from on-premise networks to IaaS clouds.
- Achieving flexible layer 2 network design on IaaS cloud.
- Constructing user networks among several IaaS clouds.

In this research, to realize these requirements, we introduce layer 3 overlay networks. If using specific functions that depend on each IaaS cloud, migration can be realized. However, on assumption that a user network is constructed among several IaaS clouds, the network can not depend on these specific functions. Then, in our proposed method, layer 3 forms boundary between user network and IaaS clouds. All of functions to construct network are provided by over layer 3. Figure 1 shows the overview of proposed model. A user defined network is isolated from IaaS clouds through integration of LISP (Locator/ID Separation Protocol) and VXLAN (Virtual eXtensible LAN). The layer 3 topology in this system is defined by LISP that is IP over IP overlay protocol, and the layer 2 segment is defined by VXLAN that is ethernet over IP overlay protocol.

LISP (Farinacci et al., 2012) manages two aspects of the IP address, addressing and locator, in isolation. LISP manages pair of the prefix (EID), and the Routing Locator (RLOC) which accommodates the EID prefix. Then, LISP overlay routing table is constructed of this pair. By this approach, LISP achieves multipoint to multipoint layer 3 overlay IP routing. VXLAN (M.Mahalingam et al., 2011) is ethernet over IP overlay architecture. VXLAN Tunnel End Point (VTEP), is a gateway between VXLAN network and non-VXLAN network. VTEPs encapsulate broadcast, unknown unicast and multicast ethernet frame in IP multicast, and well-known unicast in IP unicast. Thus, VTEPs construct overlay forwarding database like ethernet switching. Therefore, VXLAN constructs the Forwarding Information Base for multipoint Ethernet over IP overlay network.

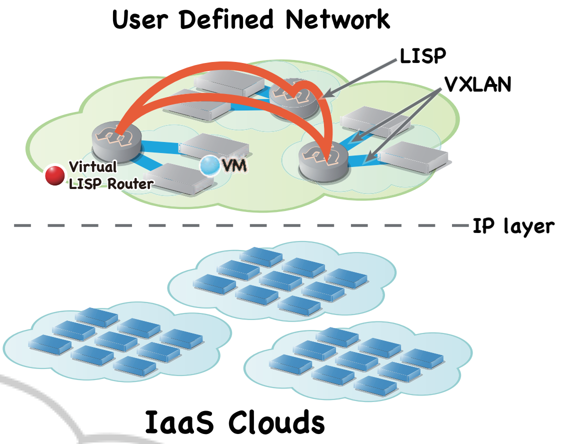

Figure 1: Isolation of user defined network and underlay IaaS clouds using layer 3 overlay networks.

2.2 Design Overview of proposed Approach

The proposed method achieves to isolate user networks from IaaS clouds. By this method, users can design and construct networks using own address prefixes freely without changes to underlay IaaS clouds, then users can migrate on-premise systems. LISP is used to achieve address prefix migration. LISP realizes network mobility through separation of EID and RLOC. Moreover, LISP avoids triangular routing between LISP sites by exchanging overlay routing table, then, applying a LISP site to a IaaS cloud enables IP address prefix migration and route optimization between IaaS clouds. Simultaneously, VXLAN is used to define layer 2 segments on IaaS clouds. VXLAN realize multi tenancy without changes to outer networks. VXLAN is originally assumed that it is used into underlay IaaS systems to separate user networks. However, By VMs directly terminate VXLAN, VM users can design and construct layer 2 segments freely without specific functions provided by IaaS clouds.

Figure 2 shows the overview of constructed system. User defined network is constructed among several IaaS clouds. Layer 2 segments in each IaaS cloud are constructed by VXLAN. Moreover, each layer 2 segment is accommodated by LISP router. An IP address prefix owned by user is associated with a VXLAN segment. In IaaS clouds, an IP address of IaaS provider is assigned to a VM. Then, A LISP router uses IaaS provider's address that is assigned as a locator address, and uses the prefix that is assigned to VXLAN interface as EID prefix. A LISP router advertises this prefix as EID prefix to the LISP overlay network. Thus, user defined network is constructed among several IaaS clouds over layer 3 networks.

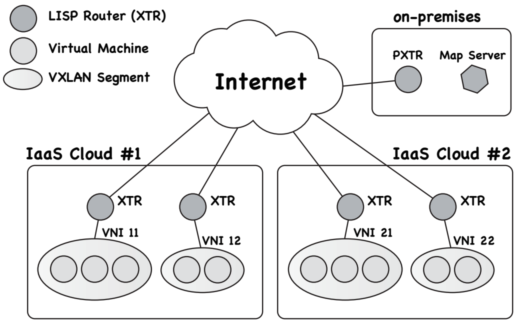

Figure 2: The overview of proposed system.

2.3 Implementation and Operation

We implemented LISP and VXLAN in Linux user space, and they can be configured through Vyatta. In proposed system, LISP router including VXLAN function is deployed as a virtual router into IaaS clouds. Thus, we implemented them as vyatta extension. Vyatta, is open source routing suite, provides CLI to configure many open source software for networking. Furthermore, vyatta is provided VM image. By implementing LISP and VXLAN as vyatta extension, anyone can use proposed system in cloud environments with some networking functions that vyatta provides. These implementations, that are called lixy and vxlan-vyatta, are published.

We deployed proposed system into the two actual IaaS clouds. The first IaaS cloud is WIDE Cloud (WIDE Project, 2012) that is academic IaaS environment. WIDE Cloud is constructed from over 20 HVs around Japan, and some HVs are located in foreign countries. It is controlled by WIDE Cloud Controller that is developed by WIDE project. All of HVs connect to a large scale layer 2 segment that accommodates VMs using vlan and vpn tunnels. And another cloud is constructed independently at Keio University using WIDE Cloud Controller too.

We deployed Vyatta with LISP and VXLAN extensions to these IaaS clouds. We extend LISP beta network (Lisp, 2012) to these clouds using proposed system. The wide-xtr that is located in WIDE backbone registers assigned prefix to the map server of beta network periodically. Moreover, two XTRs that are located in two IaaS clouds, register a part of assigned prefix and own address as a locator address a map server that is located in WIDE backbone. In this way, we separate assigned prefix into two small prefixes that are used on two clouds. Moreover, layer 2 segments in each cloud are constructed from VXLAN. Thus, we use LISP beta network prefix without any changes to underlay IaaS clouds using proposed method.

3 PERFORMANCE EVALUATION

In our proposed method, all of traffics from VMs go through layer 3 overlay. Layer 3 overlay causes degrading bandwidth because MTU is decreased due to layer 3 encapsulation. Thus, this point is obvious bottleneck of this system. This section shows the performance evaluation result of LISP and VXLAN that we implemented.

3.1 Performance Degradation due to Fragmentation

First of all, we evaluated implementations to clarify the performance degradation due to fragmentation. Therefore, we tested the throughput of implementations changing message size of test traffic that is UDP payload length from 50 bytes to 1500 bytes with 50 bytes step on a physical node environment.

Figure 3 shows throughput of LISP and VXLAN on physical nodes. With the result of LISP test, when message size 1450 bytes message, throughput was 952Mbps, and when the message size was 1500 bytes, throughput was 917Mbps. LISP encapsulates IP packets in LISP header, so that, when message size is over 1422 bytes, packets are fragmented by LISP router. With this result, performance degradation due to fragmentation is about 3.7%. With the result of VXLAN test, when message size was 1400 bytes, throughput was 924Mbps, and when message size was over 1400 bytes, throughput degraded. VXLAN encapsulates ether frames in VXLAN header, so that, when message size is over 1408 bytes, packets are fragmented by VXLAN node. With this result, performance degradation due to fragmentation is about 25%.

3.2 Performance on Virtual Environment

Implementations are assumed to be used as VM on IaaS clouds, and so we evaluated performance on a virtual environment. With the result of above experiments, if the message size is over the threshold, performance is degraded. Therefore, we evaluated the performance on a virtual environment with the largest message size that packets were not fragmented.

Figure 4 shows performances of LISP and VXLAN on a virtual environment using kernel virtual machine (KVM). The x axis means the direction of test traffic. The performance of LISP implementation is degraded to less than a half of the performance of the physical node environment. In addition, the performance of virtual node to physical node is 25%

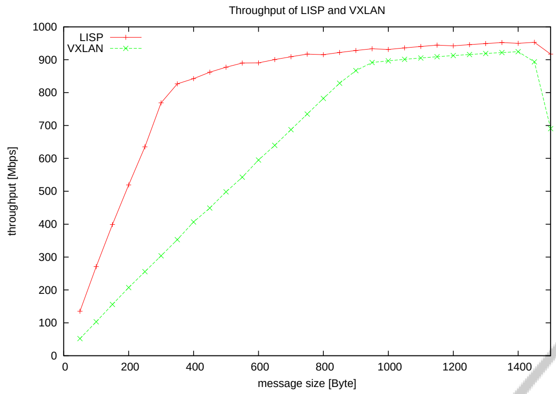

Figure 3: UDP throughput measurement of LISP and VXLAN implementations.

lower than physical to virtual. When packets come from edge network of LISP router, router has to look up LISP map table and encapsulates packets. Therefore, this result shows that looking up LISP map table and encapsulation overhead causes of 25% degradation of performance on a virtual environment. The performance of VXLAN implementation is also degraded to less than a half of the performance of physical. In addition, virtual to physical case performance is half of physical to virtual case. When the test traffic was transmitted from VM, vCPU usage on VM was full.

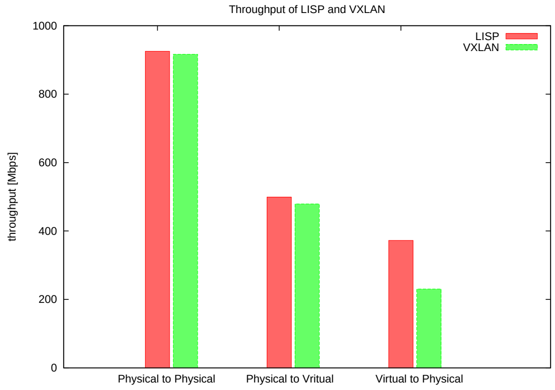

Figure 4: UDP throughput of LISP with 1422 bytes message, and UDP throughput of VXLAN with 1408bytes message.

3.3 Consideration

With these results, performances of each implementation are over 900Mbps on a physical environment. However, on the virtual environment, performances are degraded to less than a half of the performance of physical. Thus, using this implementation, enterprise systems without large scale services like office branch systems can be migrated to IaaS cloud. However, performance degradation in a virtual environment can not be ignored.

4 CONCLUSIONS

Also we deployed them in our actual IaaS cloud and evaluated the implementations.The evaluation results show that the implementations have some performance degradation of network communications, however, it is acceptable degree of degradation for small enterprise systems. Although current performance of our systems is not feasible to accommodate large scale systems that require high performance. Moreover, flexible layer 2 design in IaaS clouds is achieved by VXLAN. VXLAN requires IP multicast to underlay IaaS system and IP multicast does not work globally today. As a result, migratable layer 2 domain is limited in a IaaS cloud. Therefore, our future works are improving packet transfer performance on virtual environments, and design a more flexible method for constructing layer 2 network among several IaaS clouds.

REFERENCES

Amazon (2012). Amazon EC2. http://aws.amazon.com/ec2.

Benson, T., Akella, A., Shaikh, A., and Sahu, S. (2011). CloudNaaS: a cloud networking platform for enterprise applications. In *Proceedings of the 2nd ACM Symposium on Cloud Computing*, SOCC '11, pages 8:1–8:13, New York, NY, USA. ACM.

Cabuk, S., Dalton, C. I., Ramasamy, H., and Schunter, M. (2007). Towards automated provisioning of secure virtualized networks. In *Proceedings of the 14th ACM conference on Computer and communications security*, CCS '07, pages 235–245, New York, NY, USA. ACM.

Farinacci, D., Fuller, V., Meyer, D., and Lewis, D. (2012). Locator/ID separation protocol (LISP) draft-ietf-lisp-23. Internet Draft, IETF Network Working Group.

Lisp (2012). LISP beta network. http://www.lisp4.net/beta-network.

M.Mahalingam, D.Dutt, K.Duda, P.Agarwal, Kreeger, L., Sridhar, T., M.Bursell, and C.Wright (2011). draft-mahalingam-dutt-dcops-vxlan-00.txt. Internet Draft, IETF.

WIDE Project (2012). WIDE Cloud. https://wcc.wide.ad.jp/.