Network Working Group	K. Shima
Internet-Draft	IIJ Innovation Institute Inc.
Intended status: Informational	Y. Sekiya
Expires: April 19, 2012	The University of Tokyo
	K. Horiba
	Keio University
	October 17, 2011

Network Portability Requirements and Models for Cloud Environment
draft-shima-clouds-net-portability-reqs-and-models-01

Abstract

Recent progress of virtual machine technology made it possible to host various Internet service nodes in a so called cloud environment. The virtual machine hosting technology provides a method to migrate a virtual machine from one hypervisor to another. However, such a technology is mainly focusing on a migration between hypervisors attached to the same link, and tend not to consider migration over the Internet. This document mentions the purpose of that type of operation and describe several possible operation methods to provide network portability in cloud systems.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet- Drafts is at http://datatracker.ietf.org/drafts/current/.
Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."
This Internet-Draft will expire on April 19, 2012.

Table of Contents

1. Introduction

This document describes requirements and methodology of network migration for inter-datacenter and inter-clouds. The progress of virtualization technology changed the way to build Internet services completely. For example, the PaaS (Platform as a Services) is one of the innovative concept of computing service utilizing virtualization technology. It provides network-oriented service APIs to software layer which scales out by increasing the number of virtual nodes and scales in by decreasing the number of virtual nodes based on the load of the software requests.
A PaaS is built and provided in single datacenter by single organization nowadays, however, the needs of building distributed, inter-datacenter PaaS, and inter-connecting existing PaaS(es) are growing. Recently people expect sustainable service much more seriously than ever before. If a datacenter is encountered network circuit or power troubles,

administrators or users of PaaS want to move the virtual nodes in a datacenter to other datacenters or other PaaS(es) without service interruption.
In order to migrate virtual nodes between inter-datacenter and inter-clouds without service interruptions and changes, network portability technologies are required between the datacenters and clouds.

2. Network Portability Requirements

The requirements of network portability for migrating vitrual nodes between datacenters and between clouds are below.

*Providing the same user service networks between each datacenter and cloud

Each user has different service networks and it should be possible for users to use their networks on any datacenters or clouds. If the service infrastructure is operated by a single administrative organization, it is possible to use VLAN and VPN technologies to achieve this property, however, building user networks using such technologies is difficult in inter-datacenters or inter-clouds cases where administrative organizations differ. Since VLAN is a layer-2 technology and it requires direct circuit between datacenters, it is difficult considering the cost to keep the direct line. VPN is a cost-effective technology and it is possible to provide user networks on each datacenters and clouds, however, if the clouds are administrated by different organizations, it is difficult and costly for administrators to build a lot of VPN connection for all user networks.

*Movement policy management mechanism

When a network is moved from one datacenter or cloud system to another, it must be permitted and authorized by the destination system in some way.

*High-Availability of user networks

Even if using VLAN and VPN technologies, each user network has a single connecting point to the Internet. It may be a single point of failure of inter-datacenter and inter-clouds PaaS service. Network potability in inter-datacenters and inter-clouds should provide High-Availability capability.

3. Network Portability Models

We consider two kinds of network portability models in this draft. One is the host-oriented portability model, and the other is the network-oriented portability model.

3.1. Host-oriented Portability Model

In this model, each host (virtual machine) manages the network portability. To adpot this model, each host must be equipped with some kinds of host mobility support. Every time a host migrates from one hypervisor to another hypervisor and the attached network environment of the migrated host changes, the host must be trigger mobility function to adapt the current attached network environment. Examples implementation of this model are using host mobility protocols such as Mobile IP *[RFC5944]*, Mobile IPv6 *[RFC6275]*, HIP *[RFC5201]*, or LISP *[I-D.ietf-lisp]* and advertising host route entry from the moving node.

3.2. Network-oriented Portability Model

In this model, the network resource to which the host is attached before migration and after migration does not change. Since the migrated host doesn't notice the network environment change, it can continue to work after the migration. To provide the same network environment, the cloud system must support network resource migration between the previous location and current location of the host. Examples of this model is using VLAN, and using VPN connection.

4. Implementation Examples

In this section, we show some of the implementation example of network portability in cloud system. Section 4.1 describes an example of the network-based network portability implementation using wide area VLAN configuration. Section 4.2 describes another example of the network-based network portability implementation using NEMO BS. *[RFC3963]* Section 4.3 describes an example of the host-based network portability implementation using Mobile IPv6. Section 4.4 describes another example of the host-based network portability implementation using host route technology. Section 4.5 shows yet another example of host-based approach.

4.1. Wide area VLAN-based Network Porability

One possible solution to provide network portability in a cloud system is that to provide a seamless layer 2 network to the entire cloud system. Recently, since the wide area connectivity is getting faster and faster, so it becomes realistic to extend a layer 2 network from one site to other site where is geographically far.
In this case, the hypervisor and host configuration become simple. All the hypervisors are attached to the same layer 2 link which is widely extended to every sites which consist the entire cloud system. A host is configured with the network which is bridged to the wide area layer 2 network.
The migration procedure does not require any additional configuration or operation. Since all the hypervisors share the same layer 2 network,

hosts can migrate to any one of the hypervisors attached to the layer 2 network.
The policy management of the network resource mobility is performed as a part of the VLAN management. Whether the destination service provider accept network resource migration or not is same as whether they accept to offer their VLAN resource to the source service provider.
For the redundancy, the same technologies for VLAN can be used.

4.2. NEMO-based Network Porability

Another way to provide network portability is to use network mobility technology such as NEMO BS *[RFC3963]*. In this model, the cloud operator puts several mobile routers (MRs) in the cloud and assigns mobile network prefixes (MNPs) to each of the MR. The MRs are basically hidden to the users of the cloud system. Users do not need to know what is happning when the network migration occurs.
The MRs are prepared as virtual machines in the cloud system as same as other normal host machines. Since the MNP bound to each MR moves with the MR, all the hosts attached to the MNP must also move with the MR. Below is an example operation of the migration procedure performed in this case.
The cloud system first prepares a home network prefix used as a base network of all the MRs in the cloud system, and prepares a home agent (HA) to serve the network mobility function. Each MR has two network interfaces; one is for the local attachment point to get a care-of address, the other is for the presistent network to host other virtual machines which move with the MR.
As many virtual machies as possible can be put on the persistent network of the MR, however, when network migration is performed, all the machines inside the persistent network must be moved altogether. So, if we want to move a virtual machine one by one, we must put only one virtual machine in the persistent segment. It depends on the configuration of the service system. For example, if we design a kind of web service system that consists of a web server and a backend database server, then we may put these two into the one persistent network. Because those two servers must be on the same segment anyway, simultaneous migration will not be a limitation in this scenario.
The persistent networks that are bound to MNPs are virtual networks defined in hypervisors. The requirement to the virtual network is that the network must be identified by a virtual machine with a static identifier (e.g. the name of the virtual network) independent of the hypervisors on which the virtual machine runs. For example, if a virtual machine attaches to a virtual network whose name is 'mobile-net-1' on hypervisor A and migrates to hypervisor B, then the hypervisor B must be able to provide a virtual network which is identified by the name 'mobile-net-1'.
Whem a network is migrated, all the related virtual machines must be moved to the same destination hypervisor. That includes a MR, all the hosts attached to the MNP of the MR. Once a MR migrates to other

hypervisor, it will detect the external interface status and find that the network is changed. The MR then initiates the procedure of NEMO BS, acquires a new care-of address, and registers its new location to the HA. For the hosts inside the MNP, no additional action is required, since the network environment of the MNP is maintained by the MR and no change happens to that network.

The policy management of the network resource mobility is performed as a part of mobility management policy of NEMO BS. For example, some kind of roaming mechanism between the source and destination service providers and service level agreement are used to implement the policy management.

Similar to Mobile IPv6, the system may need to deploy some mechanisms to add high availability function to the home agent, since it is a single point of failure of Mobile IPv6-based mechanism. The mechanism for high availability of home agents is out of scope of this document.

4.3. Mobile IPv6-based Network Porability

In this case, all the hosts (which are virtual machines in a cloud system) are assumed to have Mobile IP function. A home agent must also exist as a part of the cloud system to serve home network of the mobile hosts.

Each host attaches to any one of the virtual or bridged networks that hypervisors provide. Based on the procedure of the Mobile IPv6, the host configures its care-of address using some kinds of address configuration mechanisms provided at the attached network, and register it with its home address to the home agent. The detailed Mobile IPv6 operation procedure and configuration procedures is not described here.

When a host is migrated from one hypervisor to another hypervisor, the network to which the migrated host attached changes, if the hypervisors are not attached to the same network segment. The migrated host detects the new network environment using the Mobile IPv6 function, and acquire a new care-of address of the network under the new hypervisor.

As same as the NEMO BS case, the policy management of the network resource mobility is performed as a part of mobility management policy of Mobile IPv6. For example, some kind of roaming mechanism between the source and destination service providers and service level agreement are used to implement the policy management.

Similar to Mobile IPv6, the system may need to deploy some mechanisms to add high availability function to the home agent, since it is a single point of failure of Mobile IPv6-based mechanism. The mechanism for high availability of home agents is out of scope of this document.

4.4. Routing-based Network Portability

Using host route entry is another way to implement host-based network portability. In order to use this mothod, every host which is moving between different networks must run routing daemon program on it. The node advertises its host route entry to the upstream router of the attached segment periodically.

As you can see, this method needs access right to the routing repository of the attached cloud system. Also, distributing host route entry is impossible from different AS domain. So this method is usually limited to one administrative domain.
The policy management of the network resource mobility is performed as a part of route filtering mechanism. The destination service provider has to configure their routers to accept routing information sent from legitimate moving virtual machines.
To achieve redundancy, any kind of redundancy mechanisms of routing layer can be used.

4.5. LISP-based Network Portability

LISP is a two layer communication protocol that aims to separate locator layer and identifier layer. Applying this technology to a host enables the host to move everywhere in the Internet.
In this scenario, every network segments where virtual machines are supposed to be migrated must have LISP capability, that is, every network must have at least one XTR node to intercept traffic from the LISP-based virtual machines and tunnel it to the other end of XTR or ITR which is the tunnel end node of the destination identifier of the traffic. Also, because this mechanism is using LISP, the entire system must have some kind of locator-identifier mapping system which is being discussed in the LISP Working Group.
The policy management of the network resource mobility is performed as a part of the LISP operation. The XTR node of the destination service provider must be configured to accept the legitimate LISP-based virtual machines.
The redundancy will be provided as a part of the LISP operation too.

5. Acknowledgements

We thank the members of the WIDE project for discussion on this network migration technologies, and their bravery to use the experimental cloud system we constructed.

6. IANA Considerations

This memo includes no request to IANA.

7. Security Considerations

The management NEMO HA shuld be secure and the tunnels between NEMO nodes should use secure transportation, such as SSL or IPsec.

8. References

[RFC3963]	Devarapalli, V., Wakikawa, R., Petrescu, A. and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.

[RFC5201]	Moskowitz, R., Nikander, P., Jokela, P. and T. Henderson, "Host Identity Protocol", RFC 5201, April 2008.
[RFC5944]	Perkins, C., "IP Mobility Support for IPv4, Revised", RFC 5944, November 2010.
[RFC6275]	Perkins, C., Johnson, D. and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.
[I-D.ietf-lisp]	Farinacci, D, Fuller, V, Meyer, D and D Lewis, "Locator/ID Separation Protocol (LISP)", Internet-Draft draft-ietf-lisp-15, July 2011.

Authors' Addresses

Keiichi Shima Shima IIJ Innovation Institute Inc. 1-105 Kanda-Jinbocho Chiyoda-ku, Tokyo 101-0051 Japan EMail: keiichi@iijlab.net

Yuji Sekiya Sekiya The University of Tokyo 2-11-16 Yayoi Bunkyo-ku, Tokyo 113-8658 Japan EMail: sekiya@wide.ad.jp

Katsuhiro Horiba Horiba Keio University 5322 Endo Fujisawa, Kanagawa 252-0882 Japan EMail: qoo@sfc.wide.ad.jp