

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: April 21, 2016

T. Kim  
E. Paik  
KT  
October 19, 2015

Considerations for Benchmarking High Availability of NFV Infrastructure  
draft-kim-bmwg-ha-nfvi-00

Abstract

This documents lists additional considerations and strategies for benchmarking high availability of NFV infrastructure when network functions are virtualized and performed in NFV infrastructure.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

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 21, 2016.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Considerations for Benchmarking High Availability of NFV Infrastructure . . . . .	3
2.1. Definitions for High Availability Benchmarking Test . . . . .	3
2.2. Configuration Parameters for Benchmarking Test . . . . .	3
3. High Availability Benchmarking test strategies . . . . .	4
3.1. Single Point of Failure Check . . . . .	4
3.2. Failover Time Check . . . . .	5
4. Security Considerations . . . . .	6
5. IANA Considerations . . . . .	6
6. Normative References . . . . .	6
Authors' Addresses . . . . .	6

## 1. Introduction

As both amount and variety of traffic massively increase, operators are adopting SDN and NFV, the new paradigm of networking, in order to secure scalability and flexibility. Service provider and vendors are developing SDN and NFV solutions and VNF(Virtual Network Function) to reduce CAPEX and OPEX, focusing on the increment of the scalability and flexibility of the network with programmable networking.

To replace the legacy network devices with VNFs and to select the fittest one from various products of vendor, operators want to ensure the availability and resiliency of the VNF products and their infrastructures. There also exist fears on the immeasurable failures.

Among VNFs, vEPC is getting many attentions and some telecommunications company already deployed vEPC partially. Currently in 4G mobile communication, the availability reaches 99.9999%; downtime being 3 seconds per year. Therefore, VNFs like vEPC (virtual Evolved Packet Core) must guarantee the 6-nines to replace hardware dedicated network functions. From the telecommunication company's point of view, the availability is the most important feature, and the benchmarking tests for the high availability of VNFs and NFV infrastructure are also important. This document investigates considerations for high availability of NFV Infrastructure benchmarking test.

## 2. Considerations for Benchmarking High Availability of NFV Infrastructure

This section defines and lists considerations which must be addressed to benchmark the high availability of VNFs from the NFV infrastructure perspective.

### 2.1. Definitions for High Availability Benchmarking Test

Generally, availability is defined as follows, where MTBF stands for Mean Time Between Failure) and MTTR stands for Mean Time To Recovery.

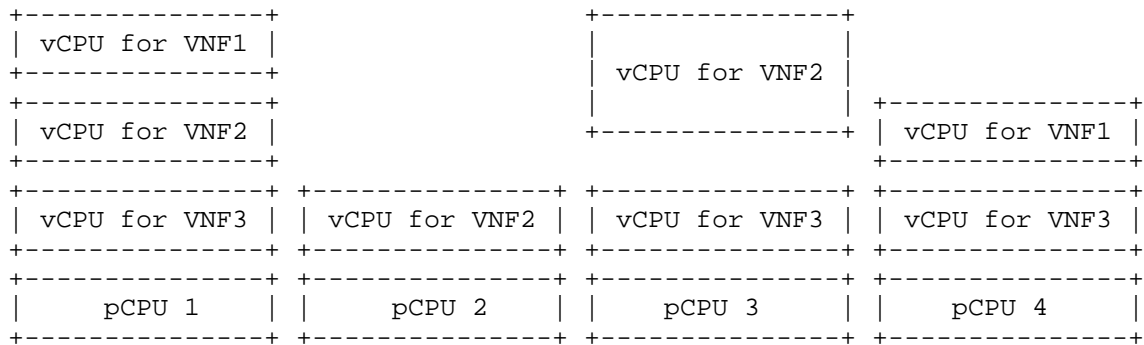
Availability :  $MTBF / (MTBF + MTTR)$

A failover procedure is as follows.

Failure -> Detection -> Isolation -> Recovery, therefore the time to take failover starts from the time when a failure happens.

### 2.2. Configuration Parameters for Benchmarking Test

- o Types of VNFs; depending on the type of VNF, followings are different.
  - 1. What kind of operations they do
  - 2. How many CPUs, MEMs, Storages they need
  - 3. What kind of traffic pattern they usually face
- o The specification of the physical machine which VMs
- o The mapping ratio of hardware resources to VMs(virtual machine) where VNF runs, such as vCPU:pCPU (virtual CPU to physical CPU), vMEM:pMEM (virtual memory to physical memory), vNICs as shown below.
- o Types of hypervisor and the different limitations of their roles.
- o Cloud Design Pattern of NFVI
- o The composition of network functions in VNFs : for example, sometimes in vEPC implementations, PGW(Packet Data Network Gateway) and SGW(Serving Gateway) are combined or PGW+SGW+MME.



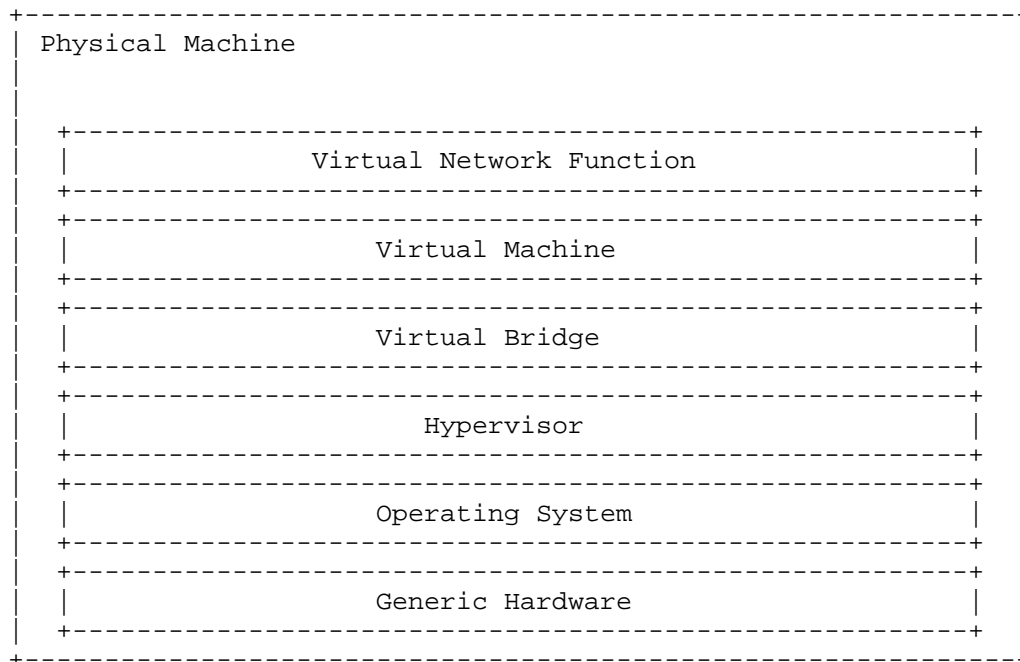
### 3. High Availability Benchmarking test strategies

This section discusses benchmarking test strategies for high availability of NFV infrastructure. For the continuity of the services, these two must be checked.

#### 3.1. Single Point of Failure Check

All devices and software have potential failures, therefore, redundancy is mandatory. First, the redundancy implementation of every sing point of NFV infrastructure must be tested as shown below.

- o Hardware
  - \* Power supply
  - \* CPU
  - \* MEM
  - \* Storage
  - \* Network :NICs, ports, LAN cable ..
- o Software
  - \* The redundancy of VNFs
  - \* The redundancy of VNFs path
  - \* The redundancy of OvS
  - \* The redundancy of vNICs
  - \* The redundancy of VMs



### 3.2. Failover Time Check

Even though the components of NFV infrastructure are redundant, failover time can be long. For example, when a failure happens, the VNF with failure stops and should be replaced by backup VNF but the time to be shifted to the new VNF can be varied with the VNF; stateless or stateful. Namely, redundancy does not guarantees high availability and short failover time is required to reach high availability. This section discusses strategy about measuring failover time.

In order to measure the failover time presicely, the time when failure happens must be defined. Followings are three different criteria which is the time when failure happens.

1. The time starts when failure actually happens
2. The time starts when failure detected by manager or controller
3. The time starts when failure event alerts to the operator

As the actual operations in VNFs and NFV infrastructure start to be changed when failure happens, the precise time of the failure happened must be the 1. When measuring the failover time, it starts

from the time when the failures happens at a point in NFV infrastructure or VNF itself.

#### 4. Security Considerations

TBD.

#### 5. IANA Considerations

No IANA Action is requested at this time.

#### 6. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.

#### Authors' Addresses

Taekhee Kim  
KT  
Infra R&D Lab. KT  
17 Woomyeon-dong, Seocho-gu  
Seoul 137-792  
Korea

Phone: +82-2-526-6688  
Fax: +82-2-526-5200  
Email: [taekhee.kim@kt.com](mailto:taekhee.kim@kt.com)

EunKyoung Paik  
KT  
Infra R&D Lab. KT  
17 Woomyeon-dong, Seocho-gu  
Seoul 137-792  
Korea

Phone: +82-2-526-5233  
Fax: +82-2-526-5200  
Email: [eun.paik@kt.com](mailto:eun.paik@kt.com)  
URI: <http://mmlab.snu.ac.kr/~eun/>