Verification of NFV Services: Problem Statement and Challenges

draft-irtf-nfvrg-service-verification-00

M-K. Shin, ETRI, K. Nam, Friesty
S. Pack, KU, S. Lee, ETRI
R. Krishnan, Dell, T. Kim, LG U+

NFVRG Meeting@IETF94, Yokohama, Japan
Overview

- NFV relocates network functions from dedicated hardware appliances to generic servers, so they can run in software. However, incomplete and/or inconsistent configuration of VNF and FGs (aka, service chain) may lead to verification issues.

- This draft discusses properties to be checked on NFV services. Also, we present challenging issues related to verification in NFV environments.

Table of Contents
1. Introduction
2. Problem statement
   2.1 Dependencies of Network Service Components in NFV framework
   2.2 Invariant and error check in VNF FGs
   2.3 Load Balancing and Optimization among VNF Instances
   2.4 Policy and State Consistency
   2.5 Performance
   2.6 Security
3. Examples - NS policy conflict with NFVI policy
4. Requirements of verification framework
5. Challenging Issues
6. Gap analysis - open source projects
7. Security considerations
Changes since IETF93

- Adopted as a RG document
- Address all the comments from last meeting
  - New sections added
  - Implementation examples (section 3)
    - NS policy conflict with NFVI policy
  - Gap analysis of relevant works in open source projects (e.g., OPNFV, ODL, etc.) (section 6)
- And many editorial updates
Example - NS policy conflict with NFVI policy

Another target of NFV verification is conflict of NS policies against global network policy, called NFVI policy.

<Example conflict case #1>
- NS policy of NS_A (composed of VNF_A and VNF_B)
  - Resource constraints: 3 CPU core for VNF_A and 2 CPU core for VNF_B
  - Affinity rule between VNF_A and VNF_B
- NFVI policy
  - No more than 4 CPU cores per physical host
- Conflict case
  - The NS policy cannot be met within the NFVI policy

<Example conflict case #2>
- NS policy of NS_B (composed of VNF_A and VNF_B)
  - Affinity rule between VNF_A and VNF_B
- NFVI policy
  - Place VM whose outbound traffic is larger than 100Mbps at POP_A
  - Place VM whose outbound traffic is smaller than 100Mbps at POP_B
- Conflict case
  - If VNF_A and VNF_B generate traffic in 150Mbps and 50Mbps, respectively,
  - VNF_A and VNF_B need to be placed at POP_A and POP_B, respectively according to the NFVI policy
  - But it will violate the affinity rule given in the NS policy
Example - NS policy conflict with NFVI policy

<Example conflict case #3>
- NS policy of NS_C (composed of VNF_A and VNF_B)
  - Resource constraints: VNF_A and VNF_B exist in the same POP
  - Auto-scaling policy: if VNF_A has more than 300K CPS, scale-out
- NFVI policy
  - No more than 10 VMs per physical host in POP_A
- Conflict case
  - If CPS of VNF_A in POP_A gets more than 300K CPS,
  - and if there is no such physical host in the POP_A whose VMs are smaller than 10,
  - VNF_A need to be scaled-out to other POP than POP_A according to the NFVI policy
  - But it will violate the NS policy
Next step

- We are now implementing verification services for vEPCs and reflect them in next revision as more specific examples.
- Add more specific verification services for vCPE and vFW, as well as vEPC (or publish them in a separate document)
- We’ll identify gaps in the implementation and/or existing open sources and suggest ways to fill those gaps.