Verification of NFV Services:
Problem Statement and Challenges

draft-irtf-nfvrg-service-verification-03

M-K. Shin, ETRI, K. Nam, Friesty
S. Pack, KU, S. Lee, ETRI
R. Krishnan, Dell

NFVRG Meeting@IETF98, Chicago
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 chains) 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
   - 5.1 Consistency check in distributed state
   - 5.2 Intent-based service composition
   - 5.3 Finding infinite loops in VNF FGs
   - 5.4 Real-time verification
   - 5.5 Languages and their semantics
   - 5.6 Stateful VNFs with multiple physical views
6. Gap analysis - open source projects
7. Security considerations
History

- (-00) Adopted as a RG document (Nov. 2015)
  - New sections added
    - Implementation examples (section 3)
    - NS policy conflict with NFVI policy
    - Gap analysis of relevant works in open source projects (section 6)

- (-01) A new challenging issue added (Mar. 2016)
  - Stateful VNFs with multiple physical views (section 5.6)

- (-02) Some text clean-up (Sep. 2016)

- (-03) Survey ETSI NFV TST docs and be aligned with the aspects of pre-deployment testing (Mar. 2017)
Example - NS policy conflict with NFVI policy

- Example factors of the NS policy are resource constraints (or deployment flavor), affinity/anti-affinity, scaling, fault and performance management, NS topology, etc.
- Example factors of the NFVI policy are NFVI resource access control, reservation and/or allocation policies, placement optimization based on affinity and/or anti-affinity rules, geography and/or regulatory rules, resource usage, etc.

<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 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

This examples are mainly related to other NFVRG docs- draft-irtf-nfvrg-policy-based-resource-management
The verification framework addressed in this document follows [ETSI-NFV-Testing], which covers
1) assessing the performance of the NFVI and its ability to fulfil the performance and reliability requirements of the VNFs executing on the NFVI,
2) data and control plane testing of VNFs and their interactions with the NFV Infrastructure and the NFV MANO, and
3) validating the performance, reliability and scaling capabilities of network services.

Next step

- Need inputs on security aspect