How Standards and Open Source Interworking can Resolve Challenges Slowing down the Massive NFV Deployment

ZHOU Nan / Senior Standards Engineer
Kubi GAO / Senior Software Engineer
NFV History

ETSJ NFV ISG was founded in 2012 with Intel, AT&T, DT, BT, etc.
The first whitepaper was published in Oct 2012
The second whitepaper and 5 specs were published in Oct 2013
In 2014, 25 PoC, 10+ Specs and the third whitepaper were published by ETSI ISG NFV. 3GPP SA5 started NFV study item.

In 2017, HPE and many players reduced resource in ETSJ NFV ISG, DT initiated ZSM ISG.
In 2016, ISG Chair was re-elected, NFV commercial deployment was expected in 2020. NFV-ITI was initiated.
ETSI NFV ISG shifted to the Phase 2 from 2015, developing mandatory specs to help commercial deployment between 2016 and 2018. 9 specs were published. A TR was published by 3GPP.

- In the first whitepaper, the reason and challenges to implement NFV are given.
- The famous architecture was proposed in 2013 to specify different blocks (VIM, VNFM, Orchestrator, NFVI, VNF, etc.) and interfaces in NFV system. Ideally, carriers want different providers to provision different blocks, and each block can be replaced easily in a plug-and-play way.
- Interoperability was always the TOP issue needs to be resolved.
- ETSJ NFV ISG published many specs but most of them are optional.
- Time consuming for 3GPP, TMF, ETSI negotiating NFV standards.
Traditional Technology Landing Flow

Requirement → Standard Development → Certification → Interoperability Testing

- ETSI ISG NFV
- Standards Development
- 3GPP
- TMF
- Integration Testing
- Certification
- ETSI ISG NFV
- Interoperability Testing
- NFV ITI
- Carriers
- Requirements
- Use cases
- Deliver
All players wanted to accelerate NFV technologies since 2012, and they found the development process is slow via traditional SDOs. Therefore, they introduced open source to make the progress faster.

- Huawei introduced Yunify to ETSI in 2013
- AT&T and LF proposed open source plan in May 2014
- OPNFV was founded in Sept 2014
- OPNFV first ARNO was available in April 2015.
- In 2016, MANO open source projects Open-O, OSM were announced
- In 2017, Open-O and ECOMP are combined to form ONAP
- In 2018, ONAP Beijing was released
- OPNFV removed scope constraints in Dec 2015.
OPNFV facilitates the development and evolution of NFV components across various open source ecosystems. Through system level integration, deployment and testing, OPNFV creates a reference NFV platform to accelerate the transformation of enterprise and service provider networks. Participation is open to anyone, whether you are an employee of a member company or just passionate about network transformation.

**OPNFV defines use cases, integrates & tests what other projects (OpenStack, Kubernetes, ODL, OVS, fd.io) create!**
Most carriers choose model 1 with full stack islands.
Some carriers decouple HW from the SW stack with SW stack islands. HW is normally purchased with traditional server procurement procedures.
Few carriers, move one step further, decouple the VNFs from the rest of stacks. This requires a lot of integration work between VNF vendors and the underneath SW stack.
Carriers rarely decouple the full stack, not to mention being SI by themselves.
This is only about the vertical layers that each VNF vendor brings their own VNFM.
Challenges for NFV Massive Deployment

There are many issues when carriers want to massively deploy the NFV technologies:

- No stable API between layers
- Too many options for the full stack
- Considerable cost for integration and testing
- Vendor lock-in on platforms
Values Open Source Verification Bring to the NFV Industry

Verification: Setup a Baseline

- Increase Interoperability
- Reduce integration and testing cost
- Avoid Vendor Lock-In

WHY in Open Source?

- Many interfaces and blocks were developed in Open Source;
- Test cases are already developed in Open Source;
- Faster than SDOs;
- Not isolated from standards;
The Board and TSC approved the OPNFV Verified Program

OPNFV Verified Program (OVP) has been launched early this year

- OPNFV Verified Program (OVP) verifies that a commercial VIM/NFVI exposes the same
  - key APIs,
  - behaviors, and
  - characteristics
  as the OPNFV reference platform

- Main objective: Reduce VIM selection and VNF onboarding cost
  - Establish industry-accepted technical baseline
  - Simplify RFIs and RFPs
Overview on the OPNFV Verification Program

- **Test scope and coverage**
  - Based on tests developed by OPNFV and upstream communities

- **Releases of OVP**
  - **Release cadence**
    - 6 months between each type of release
    - 3 months shift between releases

  - **Releases**:
    - Release OVP 1.0.0 (2018.01)
    - Release OVPN 6.0.0 (Fraser)
    - Release OVP 2.0.0 (2018.07)
    - Release OVPN 7.0.0 (Gambia)

  - **Timeline**:
    - February 2018
    - April 2018
    - August 2018
    - October 2018

- **Ways of Participation**
  - **Self testing**: Deploy and run Dovetail in private lab
  - **3rd party labs**: Utilize services offered by selected labs (under development)
Main components of OVP

1. Dovetail: automated test and reporting tool leveraging OPNFV and upstream test tools
2. OVP web portal: upload, display, and review results
Compliance Verification Workflow

1. Submission of participation form
2. Testing
3. Submission of results
4. Notification of reviewers
5. Community review of test results
6. Grant of use of program marks
Compliance Verification Workflow

As OPNFV continues to advance state-of-the-art in open source NFV, overcoming interoperability challenges in the NFV ecosystem has become a top priority. Open source, community-driven initiatives with mechanisms for validating and verifying NFV deployments are now critical to growing the marketplace for NFV products and services.

The OPNFV Verified Program (OVP) demonstrates the readiness and availability of commercial products based on OPNFV as well as expands the market for OPNFV-based infrastructure and the applications designed to run that infrastructure. Verified products and services submitted by respective vendors and service providers become compliant by implementing explicitly defined interfaces, behaviors and key features — while retaining distinct and value-added innovations across features and capabilities.

We're pleased to announce that the OVP is officially open! Applicants can self-test or utilize the service of third-party testing organizations. The process can take a few weeks so we encourage interested parties to learn more and get started today. Please email verified@opnfv.org with any questions.

Key Benefits of Vendor Participation

OVP Web Portal
Today’s OVP Test Suite

**OPNFV Verified 2018.01**

**Mandatory test cases**
- OpenStack interop API tests (205 tests)
- Basic layer 2 packet forwarding (2 tests)
- OpenStack control service high availability (8 tests)

**Optional test cases**
- IPv6 tenant networks (25 tests)
- BGPVPNs (4 tests)
- Fundamental VIM capabilities (30 tests)

**Os_interop**: 全部来自tempest测试用例集，openstack官方认证项目osinterop的2016.08测试集，涵盖network, image, compute, volume, identity

**vPing**: vping_ssh, vping_userdata

**HA**: cinder-api, glance-api, nova-api, neutron-server, haproxy, keystone, cpu load, disk load.

**IPv6**: 选自tempest的ipv6相关测试用例

**BGPVPN**: 来自opnfv社区sdnvpn项目

**VIM capabilities**: 选自tempest中的scenario测试用例，覆盖forwarding packages, security group, dynamic network, vm lifecycle and multinode.
The Rolling Test Suite for OVP

**OPNFV Verified 2018.0x**

### Functest test cases
- Tempest compute (smoke)
- Tempest identity v2 (smoke)
- Tempest identity v3 (smoke)
- Tempest image (smoke)
- Tempest network (smoke)
- Tempest volume (smoke)
- Tempest Neutron Trunk ports
- Tempest BGPVPN Tempest tests
- Security: Patrole RBAC tests
- VNF testing vIMS
- VNF testing vEPC

### Yardstick test cases
- High-availability of one controller (restart)
- High-availability of message queue
- High-availability of Neutron L3 agent
- High-availability of OpenStack database

### Bottlenecks test cases
- Stress Testing

- **smoke**: tempest中所有标签为smoke的测试用例，基础的API测试
- Neutron trunk: tempest plugin测试用例，针对neutron trunkport的测试
- BGPVPN: tempest有关bgpvpn的plugin测试用例
- Patrole: tempest plugin，检测环境的role权限管理功能
- vIMS: 部署cloudify和ims，运行测试用例检测
- vEPC: 使用juju部署一个vEPC，测试attach流程

- **HA restart**: ipmi登录控制节点shutdown
- **HA message queue**: 杀消息队列进程
- **HA neutron l3**: 杀neutron_l3_agent
- **HA database**: 杀数据库服务进程

- **Stress**: Bottlenecks瓶颈测试项目，检测同时起20组虚机的能力
Open Source Verification in Nutshell is Another Form of Standards

Linux Foundation Networking

- Umbrella project covering 6 networking projects

Linux Foundation Networking

propose expanding the program in 2018 to include VNF compliance

OCI Certification Program (DRAFT)

This is a draft process for the OCI Certification Program. The OCI Certification Working Group (CertWG) is responsible for drafting the process around OCI Certification.