Infrastructure and the OPNFV Reference Platform

There are a number of pain points related to the infrastructure supporting the OPNFV Reference platform.

As a **VNF Provider**, I use the OPNFV platform to validate portability of my VNFs across different NFVI infrastructure deployments so that problems in my customer’s operational deployments are minimized.

As a **NFV Operator**, I use the OPNFV platform to ingest and administer servers, switches and other whiteboxes so that the ingestion and administration costs of new hardware resources is minimized.

As a **NS Operator**, I use the OPNFV platform to deploy VNF instances across a large number of NFVI-PoPs so that the same operations work at all NFVI-PoPs.

The NFVI (on which the OPNFV reference platform is expected to run) is expected to exist at different size nodes at different locations. Much of the preliminary work assumes a generic large data center environment, however, access nodes would be much smaller and Enterprise CPE environments even smaller. Enterprise CPE locations seem to be early deployments of NFV services such as Naas and vCPE according to market researchers (STL) (tehnativo) (Nexcom). There are a number of industry efforts in the access space dealing with different I/O options e.g. CORD that define POD specifications for access nodes (amongst other things). At larger scale the OPNFV platform needs to be operational on large scale data centers and large federations of data centers.

As a **NS Operator**, I use the OPNFV platform to deploy VNF instances across a number of NFVI-PoPs of different scale (e.g., CPE, access, Small, medium large, federated) so that the same operations work at all NFVI-PoPs, and the same onboarding processes work for all VNFs regardless of their intended deployment location.

The current OPNFV NFVI on which the build/test infrastructure is deployed is Pharos labs that defines (amongst other things) a Pharos Node specification. The build/test CI process at OPNFV proceeds in terms of scenarios which are essentially a combination of platform components and tests. The community is discussing scenario consolidation, however the current scenario notion does not seem to support different infrastructure variants.

Bryan Sullivan: Especially as ONAP focuses on automation of workloads across VIM+NFVI instances, it is a key opportunity for OPNFV to show active support for a diversity of open source VIM+NFVI platforms, at least OpenStack-based and Kubernetes/Docker (“cloud-native”), and deployments including the set of included VIM+NFVI components (“scenarios”) and hardware configuration. In that effort however we need to address the development overhead of adapting the platform scenarios to varying hardware platforms, finding ways to expand the variety of VIM+NFVI platforms/scenarios supported by OPNFV while not permuting the work required to develop them. Following are the ways that we are pursuing this:

- **ONAP-Automated OPNFV (Auto)** project, which will include distributing ONAP components into edge cloud platforms for local semi-autonomy
- **Multi-Access Edge** project proposal
- **Armada** project proposal (evolving OpenStack-based cloud control planes for better efficiency and resilience, especially at the edge)
- Experimenting with cloud-native VIM+NFVI platforms (Docker-CE, Rancher) with ONAP integration in advance of proposals for OPNFV projects
- Projects specifically focusing on workload management through ONAP Multi-VIM across multiple OPNFV platform deployments including private (datacenter, edge, enterprise) and public