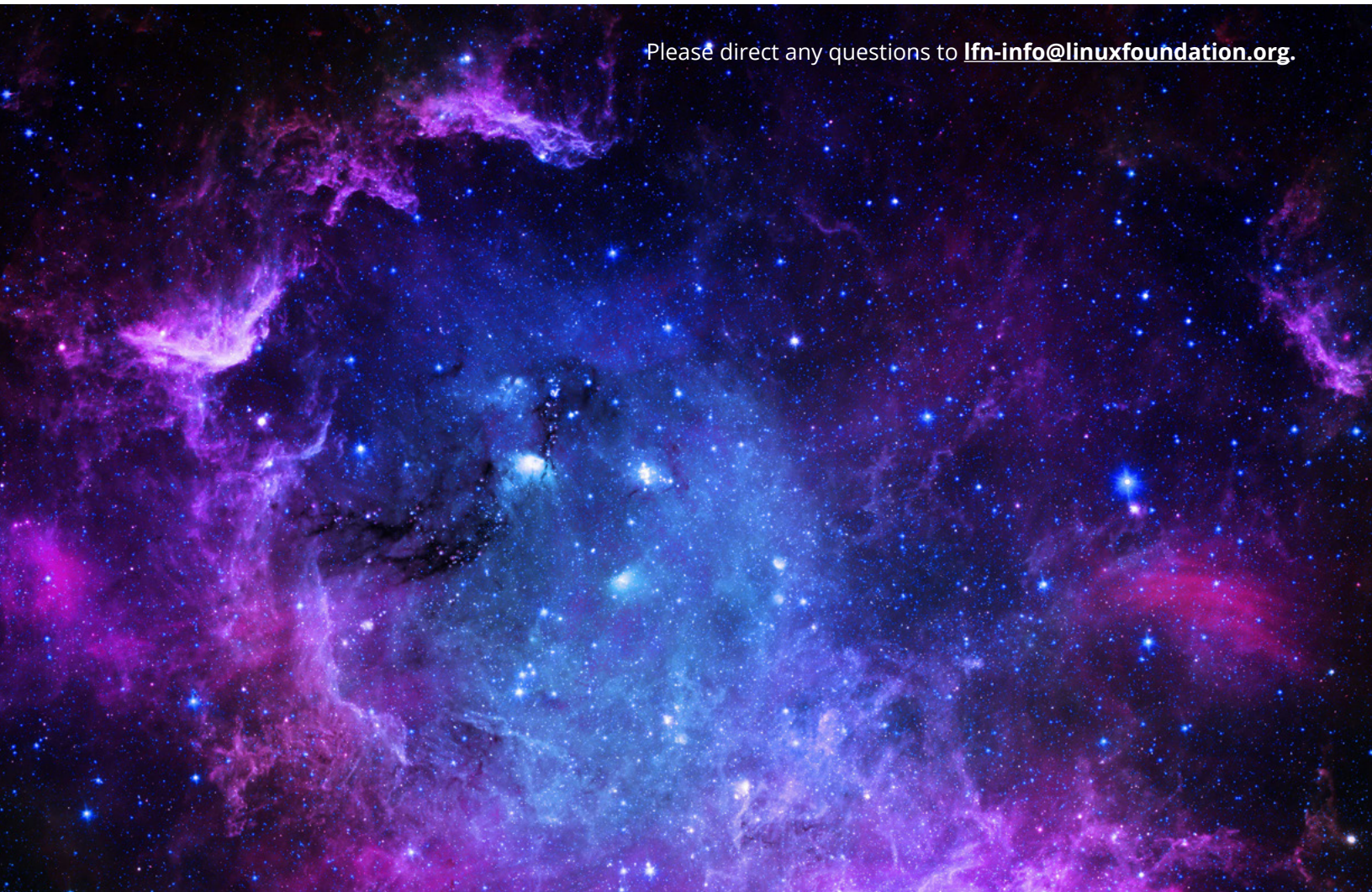
LF NETWORKING

LFN Developer & Testing Forum: January 2020

Results and lessons from the LF Networking Developer & Testing Forum, January 13-16, 2020, in Prague, Czech Republic.



Please direct any questions to **lfn-info@linuxfoundation.org**.

LF NETWORKING

Table of Contents

LF NETWORKING

Executive Summary

LF Networking (LFN) hosted a record breaking cross-community technical gathering, the LFN Developer & Testing Forum at the Prague Congress Center in Prague, Czech Republic, from January 13-16, 2020, attracting over 200 vendor and network operator participants representing several major LFN initiatives.

The event, a follow on to prior technical workshops, Developer Design Forums (DDF), and Plugfest events focused on bringing end users, vendors, system integrators, academic institutions, and individuals together to plan upcoming LFN project releases, to discuss technical priorities, and to perform hands-on testing and integration activities on current software releases. 210 individuals from 60 organizations including 15 end users, 6 research and nonprofit organizations attended the event.

The LFN projects and initiatives represented were the Common NFVI Telco Taskforce (CNTT), OPNFV, ONAP, and the OPNFV Verified Program (OVP). Building on the strategic promise of the LFN umbrella, this event strongly emphasized cross-project collaboration and joint activities, including project roadmaps, integration, and community strategy. The impact of these efforts should result in stronger collaboration and integration across all the projects in the future.

CNTT participants worked on the OpenStack-based Reference Architecture (RA) 1 and the Kubernetes-based RA2. Given its relative level of maturity, there was detailed planning work on Reference Implementation (RI) 1 and Reference Configuration (RC) 1 efforts. The main activities for the ONAP community were network slicing and related 5G topics, S3P (stability, security, scalability, performance), and looking at further cooperation opportunities with standards organizations. OPNFV participants discussed evolving the OPNFV mission to respond to CNTT needs for RI and RC leveraging OPNFV's five year history of developing rich continuous integration and NFV infrastructure (NFVI) testing tools. And for the first time at an event, the OVP Virtual Network Function (VNF) hacking track brought together commercial VNF suppliers, along with lab teams, and ONAP developers with the goal of achieving the first OVP results for commercial VNF products. The work accomplished during the hacking track laid the foundations for the successful conclusion on those first runs in the weeks following the event.

CNTT

VNF[1] developers have been forced to interoperate with innumerable variations of infrastructure platforms, most commonly, OpenStack or Kubernetes (K8s). This resulted in the potential for increased development, testing, and maintenance costs for VNF vendors. This also affected downstream costs and onboarding durations for the Communication Service Providers (CSPs).

CNTT was established in 2019 as a partnership between LF Networking and GSMA to normalize NFVI implementations, with the goal of reducing the number down to a discrete set, thus ameliorating the problems maintaining a large number of infrastructure architectures. As the name suggests, CNTT is a task force and not a formal project. For this reason, many of the deliverables will be provided by the OPNFV project. In addition to OPNFV, CNTT also works closely with ONAP and the Cloud Native Computing Foundation (CNCF) Telecom Users Group (TUG).

The CNTT sessions ranged widely from introductions designed to educate the larger community, working sessions, and deep dive discussions, to cross-community collaboration activities. At the highest level, the crux of the meetings was to complete the lifecycle of RA1 in terms of RI1 and RC1 and to publish an initial version of RA2.

Some of the educational sessions provided an overview of CNTT's structure and the state of the community:

State of the Community: The progress in just ten months has been inspiring. Across two releases (Botrange and Snezka), the community has released the RM 2.0 and RA1 1.0 specifications, established 8 workstreams, and demonstrated an impressive 160% growth with 39 member companies participating. The challenge moving forward is to continue to expand the contributor base, recruit adopters, establish the end-to-end framework (RA1→RI1→RC1), and finally better align with the industry as a whole including incorporating other open standards and open source projects. The success of the CNTT effort will be the ability to drive demand for the OVP badging as part of CSP Request for Proposal (RFP) processes. The community felt that achieving this goal requires evangelism and marketing across CSPs, vendors, and standards organizations. Another major challenge will be to make substantial progress on RA2 to streamline the adoption of Cloud Native Network Functions (CNFs), while understanding that the CNF architectures are still evolving rapidly. The ability to influence and drive how CNFs are built and what features are supported will be critical for the success of the project.

[1] Our use of the term VNF includes both Cloud Native Network Functions (CNFs) and Virtual Network Functions (VNFs)

CNTT Structure: CNTT specifications start with a single top level Reference Model (RM). The RM has a small number of Reference Architectures. Today there are two—RA1 based on OpenStack and RA2 based on K8s. Each RA has one Reference Implementation (RI) that serves as an example and a Reference Conformance program that is essentially a set badging mechanism for commercial NFVI and VNF products. While the above specifications reside in CNTT, the RI effort is expected to reside with OPNFV, while the RC will be split between OPNFV and OVP. The details of where all the components will ultimately reside is still to be worked out among the groups.

The key working meetings and deep dive discussions covered the following:

RM: The RM workstream discussed a number of relevant topics such as hardware variations, badge exception criteria under the assumption that not every vendor might pass 100% of the tests, and accommodating technologies such as SR-IOV[2] or PCI Express passthrough. There was also discussion of the impact of the differences between a VNF profile vs. an NFVI profile, performance testing, and the need to define common services such as Domain Name System (DNS), load balancers, and monitoring. There was also a discussion on the variations between workloads; for example, differences in IT and networking workloads that could result in different profiles such as basic, compute intensive, or network intensive.

[2] Note: Single Root I/O Virtualization (SR-IOV) is not an emerging technology but its use in NFV is

RA1: This workstream discussed topics such as mapping RM requirements to VNFs vs. NFVI, security, OpenStack versions, OpenStack services needed, Ceph storage, and hardware acceleration. The sessions also covered requirements in the areas of networking, traceability, APIs, discovery, load balancers, service function chaining (SFC), Ethernet virtual private network (EVPN), deployment topologies and the need for alignment with edge computing, public/multi-cloud architectures, operations, OpenStack lifecycle management and more. RI1 is considering incorporating technologies such as the OpenStack Airship installer, the OPNFV Iruya release, and the OPNFV Functest testing project. RC1, which is planned to have both an NFVI badge and a VNF badge, is aligning processes, tooling, and its marketplace of verified products with OVP. The launch of RA1, RI1, and RC1 is slated for this year and will be rolled out in three stages—Field Trial, Controlled Introduction, and General Availability (GA). The “Field Trial'' stage will use a few friendly NFVI and VNF vendors to help validate RC1. During the “Controlled Introduction” stage a few more vendors will be engaged, while the GA stage will allow any and all vendors to badge their systems. Vendors that want to participate early can do so by engaging with CNTT. The RI1/RC1 tracks made progress on lab specifications and delivery, software deployment, and integration with automated conformance suites, and identified cross-team collaborations for validation tools.

RA2: The use of K8s and CNFs for telco workloads is still very new, so the impetus of RA2 in 2020 will be to complete an initial draft. The discussions were about closing perceived gaps in networking, traceability, multitenancy, Continuous Integration/ Continuous Delivery (CI/CD), resilience, service mesh, support for VNFs (in addition to just CNFs), logging-monitoring-alerting, and secrets management. The team also discussed how to collect requirements across IT, network, and ML workloads. Specific technologies such as using Helm3 as a CNF descriptor, Akraino REC as a starting point for RA2, allowing the CNF user plane to reside on Smart NICs or other dedicated network fabric elements.

Community Collaboration: The main entities discussed during these tracks were:

- Global System for Mobile Communications (GSMA): Ultimately, the RM will become a GSMA permanent reference document (PRD), and the process to do so was discussed.
- OPNFV: OPNFV will be a key CNTT partner by working on RI and RC. The newly formed OPNFV Common Infrastructure Realization & Validation (CIRV) project will work on this along with other relevant projects such as OPNFV Functest (functional testing project) and VSPERF (virtual switch performance testing project).
- OVP: OVP phase 2 is important for the completion of RC2. The group also discussed how to better align OVP phase 2 with CNTT.

- ONAP: There was discussion on how the VNF badge might be shared with ONAP. Furthermore, the opportunity to collaborate on RA2 was also covered.
- CNCF: RA2 is likely to generate upstream requirements for k8s similar to how OPNFV did so for OpenStack in its early days. There was a discussion on whether the CNCF Telecom User Group (TUG) might potentially be able to help with this.

CNTT Adoption: There were energetic discussions on how to increase the participation of existing contributors, grow the contributor base, and recruit vendors and CSPs to adopt the CNTT program. Ultimately, CNTT's success will be measured by its adoption in the vendor and operator communities.

ONAP

The ONAP community used this forum to plan subsequent releases. The main themes were 5G/network slicing, platform maturity, project and sub-committee planning, greater collaboration within ONAP projects and with 3rd party open source projects and standards organizations, process improvements related discussions such as the ONAP release cadence.

5G and Network Slicing

A significant number of sessions were dedicated to 5G and Network Slicing. These sessions highlighted some ground breaking work done by the ONAP community in this area. ONAP is finding itself in the unique position of being the de facto open

source reference implementation of 3rd Generation Partnership Project (3GPP), ETSI Zero touch network and Service Management (ZSM), and IETF Traffic Engineering Architecture and Signaling (TEAS) slicing related standards.

Network slicing was discussed in a robust manner—end-to-end, core network, transport, and cross-carrier slicing were all covered by different sessions. There was a sense of anticipation with the planned support for core slicing in the Frankfurt release. Multiple sessions covered the various different aspects of core slicing, the new ONAP Service Orchestrator (SO) workflows for Communication Service Management Function (CSMF), Network Slice Management Function (NSMF), and the Network Slice Sub-net Management Function (NSSMF) adapter. The speakers also discussed the impact of slicing to ONAP projects such as OOF (ONAP Optimization Framework), Policy, External API, SDC (Service Design & Creation), and A&AI (Active and Available Inventory) schemas. The talks also covered the two new dashboards in Frankfurt for CSMF and NSMF. The transport slicing presentation covered an introduction into the topic and how transport slicing fits into end-to-end slicing. This effort is being conducted in collaboration with standards organizations (see above) and is extending the Cross Domain and Cross Layer VPN (CCVPN) use case blueprint to include transport slicing. These talks also covered CNF support and other architectural considerations. The group discussed operator requirements around a slice being available across carriers, potential approaches to achieve this, and the need for new APIs and models in the ONAP Guilin release expected in late 2020.

Additional 5G topics covered the role of data lake services, 5G Network Resource Model (NRM) configuration via REST APIs using SO and CDS (Controller Design Studio), and the possible integration of ONAP4K8s (a profile of ONAP optimized for K8s clouds) with the 5G Cloud Native Network demo shown at KubeCon + CloudNativeCon NA 2019.

Platform Maturity

Platform maturity discussions were kicked off with a frank assessment of ONAP across seven factors—performance, stability, resilience, security, scalability, manageability, and usability. The assessment highlighted the importance of achieving greater platform maturity in the Frankfurt and Guilin releases and was followed by the need to review each project and CI/CD flows. Security was by far the most active area of platform maturity with discussions covering vulnerability, removal of root privileges for containers, user management, migration to newer Python and Java versions, improvements in CII (Core Infrastructure Initiative) badging, password removal, the use of an ingress controller, and the use of the Istio service mesh. The ONAP usability session examined topics such as potentially creating a reduced profile of ONAP with just the most important core components and improved documentation. Finally the integration team got a boost with the addition of new members and they addressed issues ranging from avoiding

merging new code when OOM gating fails (OOM gating is a CI process that runs a set of tests on patchsets submitted to the OOM repository), new testing strategies and approaches, and new tests around performance and robustness.

In addition, a decision was made to replace the Use Case Subcommittee with a new Requirements Subcommittee. At the outset of the ONAP project 3 years ago, it was important to have a few select use case blueprints to show concrete value from the project and to provide guidance to developers. However, after the El Alto release, there was an increasing realization that the Use Case Subcommittee has outlived its purpose and the community would be better served by a team that would prioritize functional requirements, and more importantly, non-functional requirements. Ultimately this will contribute to greater platform maturity.

Project Planning

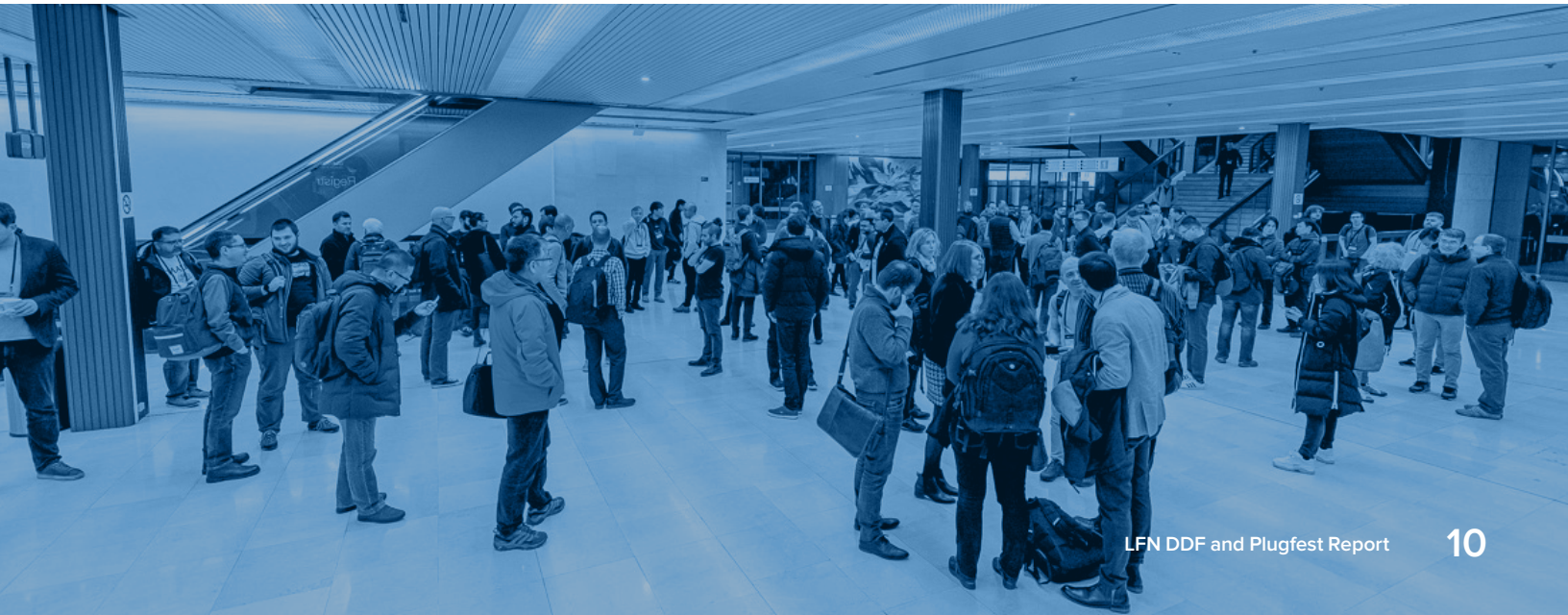
Several projects used this event as an opportunity to meet face-to-face and conduct planning for the Frankfurt and Guilin releases. The SO team considered architecture enhancements to support CNFs, custom resources, custom controllers, dynamic/custom BPMN workflows, and to improve TOSCA (a modeling language) support through the inclusion of the Puccini compiler. The OOM team discussed their roadmap around Kubernetes 1.6 and Helm 3 support, database consolidation, storage and security enhancements, and the use of a service mesh. Next the CDS initiative discussed support for K8s.

Subcommittee/Use Case Planning

The ControlLoop (CL) Subcommittee is looking at including applications other than just the Policy framework, DCAE (Data Collection Analytics and Events) and CLAMP (Closed Loop Automation Management Platform) in a Control Loop. The Subcommittee proposed a TOSCA based application model covering any application extension involved in ONAP Control Loop. The Modeling Subcommittee reviewed ongoing activities, feedback from TM Forum, information model documentation, and Swagger API documentation. Next, the Change Management use case team discussed strengthening the build and replace workflow, progress on granular change support via VNF Component (VNF-C) and schema changes, and improvements in PNF software upgrades. The team is also looking at the upgrade of complex services, parallel SO workflows, and K8s support. K8s is interesting because it has the potential to simplify change management given its native features such as scaleout, health checks, and upgrade.

Other ONAP Topics

Additional topics such as collaboration with standards organizations including 3GPP, TM Forum and their Catalyst projects, CNTT, ETSI NFV and MEC (Multi-Access Edge Computing) were also covered. The community discussed the need to improve lifecycle management of projects (proposal→archiving), reducing the release cadence to accommodate three annual releases, more effective marketing promotion of ONAP, and ONAP training. Artificial Intelligence (AI) was a popular topic, where one talk covered cross-project AI for network intelligence and how it fits in the DCAE/CL framework. Another talk covered the use of Tensorflow AI/ML inference engine for intelligent energy optimization of an EPC core based on training data from China Mobile. Finally there were topics around multi-tenancy in ONAP and the creation of an OVP verified VNF catalog.



OPNFV

The OPNFV community members reflected on the need to evolve the OPNFV mission statement and to solidly align the project with CNTT. The participants observed that when OPNFV was created over five years ago, the urgent need of the day was to close gaps in upstream projects such as OpenStack and OpenDaylight and to make them suitable for NFV use cases. This was done by working directly with various upstream projects. However, interest in OPNFV scenarios based on different installers and the portfolio of feature projects has declined relative to the testing projects. At the same time, with the emergence of CNTT and given that the RI and RC activities of CNTT require development and implementation tasks, OPNFV has evolved into the natural home for this work. The combination of the above factors means that OPNFV needs to reframe its focus, and there was significant discussion on this topic. The evolved mission will be based on inputs from a working group of the OPNFV Technical Steering Committee (TSC) and the LFN Strategic Planning Committee (SPC).

Given the overall sentiment, there were numerous sessions dedicated to collaboration with CNTT. Specifically, as discussed above, a new OPNFV project Common Infrastructure Realization & Validation (CIRV) was approved. CIRV will focus on creating RI and RC. The RI discussions revolved around release management, release engineering, scenario testing, cookbook and configuration creation, deployment specifics, and the CI/CD pipeline. The Functest project will fill a bulk of RI1 testing needs, and there were several sessions around this topic. In fact, LaaS (Lab-as-a-Service) along with a couple of OPNFV PODs and Functest are already being used to address RC testing needs. Another discussion posited that the CNTT suite of Reference documents/definitions will not be complete without performance benchmarking of the Reference Infrastructure, using Reference VNFs (or workload). This work is in-progress in parallel to other OPNFV work that attempts to anticipate CNTT's needs.

One discussion reviewed the CNTT/OPNFV situation from a VNF's point of view. VNF vendors will be required to certify their products against RI1 to get an OVP VNF badge. For this reason, RI will need to be fully documented through a cookbook so VNF vendors can set up the environment and run the tests. Of course, subsequent to getting a badge, a VNF vendor may have to conduct additional testing against the CSP's chosen NFVI vendor's OVP (RC) compliant NFVI stack as well.

Additional CNTT related discussions ranged from validation of the hardware as a step 0 of CNTT testing, leveraging the current OPNFV CI pipeline and test results database for the RC1 cookbook, using the Airship installer for RI1, and setting up formal communication channels between OPNFV and CNTT.

In addition to CNTT topics, there were other OPNFV discussions as well. One discussion covered the evolution of the CI pipeline as Jenkins Jobs are proving to be difficult to write. Another session focused on potentially transforming the OPNFV Physical Descriptor Format (PDF), that describes the underlying POD, to an Airship installer Manifest. The VMware team covered VMware Integrated OpenStack (VIO) reference implementation. Next, with the Pharos POD architecture specification having been more or less constant for many years, there was a discussion on Pharos 2.0. The OVP team discussed the possibility of incorporating ONAP for NFVI badging. Moreover, the testing community reviewed how OPNFV Barometer could help with ETSI NFV Management and Orchestration (MANO) and VNF testing by injecting test metrics. Finally, the testing participants also examined the need to validate the various different OPNFV manifests (PDF, SDF or scenario descriptor file, IDF or installer descriptor file) in a pre-deployment setting to ensure a successful deployment outcome which is especially needed during automation.

OPNFV Verification Program (OVP)

OVP is an open source, community-led compliance and verification program to demonstrate the readiness and availability of commercial NFV products and services using OPNFV and ONAP components. The main OVP activity at this event was a “VNF Hacking Track” where VNF vendors got an opportunity to get exposed to the OVP VNF verification badging program. In addition, there were several discussions on OVP 2.0 and the alignment between OVP, CNTT, OPNFV, and ONAP.

VNF Hacking Track

The goal of this hands on testing track was to provide a collaborative and safe environment for VNF vendors to help them get comfortable with OVP testing and establish ONAP interoperability. From an OVP developer point of view, this track was also meant to help debug the OVP tooling and VNF verification tests.

Three lab environments were available through remote access for this hacking track. These labs hosted both ONAP and OpenStack:

Lenovo

OpenStack POD:

- **Hardware:** Lenovo ThinkSystem SR630/SR650 servers, Lenovo ThinkSystem NE2572/NE0152T switches
- **Software:** WindRiver Titanium Cloud R5

ONAP POD :

- **Hardware:** Lenovo ThinkSystem SR650 servers, Lenovo ThinkSystem NE2572/NE0152T switches
- **Software:** Aarna Networks ONAP Distribution 3.0 (Dublin release), OPNFV Fraser release (APEX OpenStack scenario)

University of New Hampshire - InterOperability Laboratory (UNH-IOL)

Environment 1

- ONAP El Alto release
- OpenStack Rocky (3.16.2) release

Environment 2 (on OPNFV Lab-as-a-Service)

- Aarna Networks ONAP Distribution 3.0 (Dublin)
- OPNFV Fraser release (APEX OpenStack scenario)
- Microsoft Azure
- ONAP El Alto release on Azure VMs
- OpenStack devstack (as the cloud provider being orchestrated by ONAP)

Roughly five organizations participated in this track. The testing consisted of compliance tests (static tests meant to validate the VNF descriptors) and validation tests that ran onboarding, deployment, and termination tests on an actual ONAP instance. The testing was successful in achieving the two stated objectives. It helped VNF vendors get comfortable with the OVP badging program and it helped the OVP contributors flesh out issues with the tooling. The ready access to various ONAP experts was tremendously valuable in making the session a success.

OVP Planning

In addition to the above hacking track, there were several sessions dedicated to OVP 2.0 planning. The gist of this planning was to collaborate more closely with CNTT and CNCF with the goal of supporting badging. Other topics such as the exact role of OVP for CNTT RC, additional tooling required for OVP testing (especially from a MANO point of view), and identification of gaps in ONAP-related OVP testing were also discussed.

Participants

The following companies participated in the event. Many thanks to all the participants.

Company	Description	URL
Aarna Networks	ONAP products and services vendor	aarnanetworks.com
Amdocs	Software and services provider to communications and media companies	amdocs.com
AT&T	Telecommunications service provider	att.com
Avast	Computer security company	avast.com
Bell Canada	Telecommunications service provider	bell.ca
Benu Networks	SD-Edge platform software company	benunetworks.com
Berner Group	Strategic umbrella with products and services across industries	berner-group.com
Canonical	Cloud, desktop, device open source software	canonical.com
China Mobile	Telecommunications service provider	www.chinamobileltd.com
CodiLime	Provider of network engineering services	codilime.com
Comptel	Provider of professional and technical services	comptelinc.com
Dell	Compute, storage, networking vendor	dell.com
Deutsche Telekom	Telecommunications service provider	telekom.com

Ericsson	Network equipment vendor providing communication technology and services	ericsson.com
F5 Networks	Networking vendor providing application delivery and security	f5.com
Frinkx	Network automation software vendor	frinkx.io
Fujitsu	Information and communication technology (ICT) company, offering products, solutions, and services	www.fujitsu.com
Futurewei	Research and development of information and communication technologies	futurewei.com
GMX	Internet service provider	gmx.net
Granton	IT consultancy	granton.cz
GSMA	Industry organization representing the worldwide mobile industry	gsma.com
Highstreet Technologies	Managed cloud services for enterprise applications and IT infrastructure	highstreetit.com
Huawei	Network equipment vendor providing communication technology and services	huawei.com
IBM	Compute, storage, networking vendor	ibm.com
Intel	Semiconductor and computing vendor	intel.com
Juniper	Networking vendor	juniper.net
KDDI	Telecommunications service provider	kddi.com
Keysight Technologies	Helps companies accelerate innovation to connect and secure the world	keysight.com
Lenovo	A multinational technology vendor	lenovo.com
The Linux Foundation	Non-profit organization that accelerates open technology development and commercial adoption	linuxfoundation.org
Loodse	Enterprise software platform that enables automated multi-cloud operations	loodse.com
Matrixx	Software company providing a digital commerce platform for 5G	matrixx.com
Nokia	Network equipment vendor providing communication technology and services	nokia.com
NTT	Telecommunications service provider	ntt.com
OpenStack Foundation	Open source software foundation	openstack.org/foundation

Orange	Telecommunications service provider	orange.com
PANTHEON.tech	SDN/NFV software and services	pantheon.tech
Red Hat	Enterprise software company with an open source development model	redhat.com
Samsung	Consumer electronics and technology vendor	samsung.com
Solutions by STC	ICT subsidiary of the Saudi Telecom Company	stcs.com.sa
Spirent	Test and measurement vendor	spirent.com
Swisscom	Telecommunications service provider	swisscom.ch
T-Mobile Czech Republic	Telecommunications service provider	t-mobile.cz
T-Mobile Poland	Telecommunications service provider	t-mobile.pl
Tata Communications	Telecommunications service provider	tatacommunications.com
Technische Universitaet Chemnitz	University in Chemnitz, Germany	tu-chemnitz.de
Telecom Italia	Telecommunications service provider	telecomitalia.com
Tieto	Software and services company	tieto.com
ULAK Haberlesme	Provider of mobile and broadband communication systems	ulakhaberlesme.com.tr
UNH-IOL	Independent interoperability and conformance testing for data, telecom and storage networking	iol.unh.edu
University of Surrey 5G Innovation Centre	University in the UK with 5G focus	surrey.ac.uk/5gic
Verizon	Telecommunications service provider	verizon.com
VMware	Software vendor with compute, cloud, networking and security, and digital workspace offerings	vmware.com
Vodafone	Telecommunications service provider	vodafone.com
ZTE	Network equipment vendor providing communication technology and services	zte.com.cn

Table 1: Participating Organizations

LF NETWORKING

Conclusion

The 2020 LFN Developer & Testing Forum had a record 210 attendees—including representatives from 15 end user companies—collaborating face to face as an open community that achieved outputs far greater than the sum of the many LFN parts. Attendees had the opportunity to get to know each other better, to plan upcoming LFN project releases and initiatives, and perform hands-on testing and integration activities. Eighty-one percent of survey respondents rated the overall event a 4 or 5 out of 5.

Stay tuned for updates on future LFN technical community events. Updates will be made on wiki.lfnetworking.org/display/LN/Technical+Community+Events and respective project mailing lists.

References

Links to presentations and Zoom session recordings
https://wiki.lfnetworking.org/pages/viewpage.action?pageId=25364127.