SOFTFIRE

Software Defined Networks and Network Function Virtualisation
Testbed within FIRE+

Constructing a Federated Testbed and an Orchestrated Virtualisation Infrastructure

A Technical Overview

May 2017

Table of Contents

List of Figures

List of Tables

1 Introduction

Network Function Virtualisation (NFV) [1] is a recent and popular technology providing solutions for dynamically managing and orchestrating network functions on top of Virtualized Infrastructures. According to [2], NFV is the "*implementation of network functions in software that can run on a range of industry-standard server hardware, and that can be moved to, or instantiated in, various locations in the network as required, without the need for installation of new equipment*". By instantiating Virtual Network Functions (VNF) on conventional server hardware on an on-demand basis, network operators can quickly instantiate required network services, without the need for specialised hardware/equipment. By implementing network functions as software, and providing software as a service (SaaS) to clients, operators can scale their services according to dynamically changing user demand.

To support NFV in an operator network infrastructure, dynamic adaptation of data traffic flows is required, and hence another recent paradigm called Software Defined Networking (SDN) [3] provides the foundational blocks of next generation networks. SDN enables programming of the data (user) plane of off-the-shelf common networking equipment, and decouples control plane and user plane in network switches and routers.

The EU Project SoftFIRE (Software Defined Networks and Network Function Virtualisation Testbed within FIRE+) [4] has the goal of bringing NFV and SDN capabilities to a completely virtualised and multi-site federated infrastructure that spans across multiple countries in Europe. The testbed's foundational aim is to nurture an ecosystem of organizations willing to extend, consolidate, and possibly industrialise solutions in the realm of NFV/SDN with a specific reference to their adoption in 5th Generation (5G) mobile network architectures. SoftFIRE stresses out the importance of federation as a means: (*i*) to create an open environment capable of encompassing several programmable solutions in the field of NFV/SDN (*programmability*), (*ii*) to identify and solve the interworking issues of the technologies (*interoperability*), and (*iii*) to create a security framework for supporting the needs of NFV/SDN providers (*security*).

SoftFIRE regularly invites organisations via its Open Calls for experiments and provides the selected organisations with the federated testbed as an Infrastructure-as-a-Service (IaaS). Selected organisations can deploy their experiments on the virtualised infrastructure, perform experiments, and provide feedbacks about their findings to the project and to the general public.

This whitepaper describes a technical overview of the federated virtualised infrastructure provided by SoftFIRE, outlining its capabilities, and sharing the experiences gained in building such infrastructure.

2 Federation of Virtualisation Testbeds: A Recent History

Several federated testbeds supporting virtualisation exist in various parts of the world, with differing scales and capabilities. The largest of these testbeds is PlanetLab [5], which was established in 2002 and has grown to span over 1300 physical servers at over 700 sites across the world. Experimenters using PlanetLab are allocated a slice of the testbed's global resources, on which virtual machines (VM)s can be instantiated and fully controlled.

The KOrea advanced REsearch Network (KOREN) [6] is another federated testbed, located in Korea and spanning six different cities, connected by links with speeds of between 10 and 20 Gbps. At least one OpenFlow [7] switch and several servers are installed at each Point-of-Presence (PoP), and experimenters can reserve specific ports on the switches and control how traffic is forwarded over these ports.

The Research Infrastructure for large-Scale network Experiments (RISE) [8] is an SDN/OpenFlow testbed which uses the JGN-X network in Japan to provide experimenters with a software-defined network spanning over 10 domestic locations, and comprising over 70 switches and over 50 servers. Users of the testbed can set up their own slice and create VMs in under 10 minutes through the RISE management system.

The BonFIRE [9] testbed is a cloud-based infrastructure spanning across seven locations within Europe, offering experimenters with compute, storage, and networking resources. The testbed offers users an API to create, update, read, and delete resources throughout the lifetime of an experiment.

The testbeds mentioned so far provide wired infrastructure, but no wireless infrastructure. To address this, several federated testbeds have been built which link existing testbeds, bringing both wired and wireless resources together. For example, the OneLab [10] testbed integrates Internet testbeds such as PlanetLab, IoT testbeds such as w-iLab.t [11], and wireless testbeds such as NITOS [12]. The FED4FIRE [13] testbed also provides such an amalgamation of testbeds, but on a slightly larger scope. Finally, the Federated Testbed for Large-scale Infrastructure eXperiments (FELIX) [14] combines a smaller number of federated testbeds but over a large geographical area.

In this context SoftFIRE's distinctiveness is to create an environment addressing some important issues at the crossroads of research and industrialization. In fact, some issues tackled by the project are (i) the integration of NFV and SDN (claimed by the research community but poorly offered for experimentation), (ii) the integration of security within NFV/SDN, (iii) the possibility for developers to quickly use the platform for creating their applications, (iv) and the possibility to access physical radio resources. These features make SoftFIRE unique as compared to larger-scale or more specialised research projects.

This white paper describes the construction and orchestration of the SoftFIRE testbed, which provides a multi-site virtualisation environment. Apart from providing a distributed virtualisation infrastructure entirely built using open source software, SoftFIRE also enables connectivity to 5G mobile network core components, as well Radio Access Network (RAN) equipment.

3 The SoftFIRE Federated Testbed

The EU project SoftFIRE has designed and developed a framework for federating multiple testbeds, providing their functionalities as a service to external experimenters. The SoftFIRE federated infrastructure is illustrated in Figure 1 below.

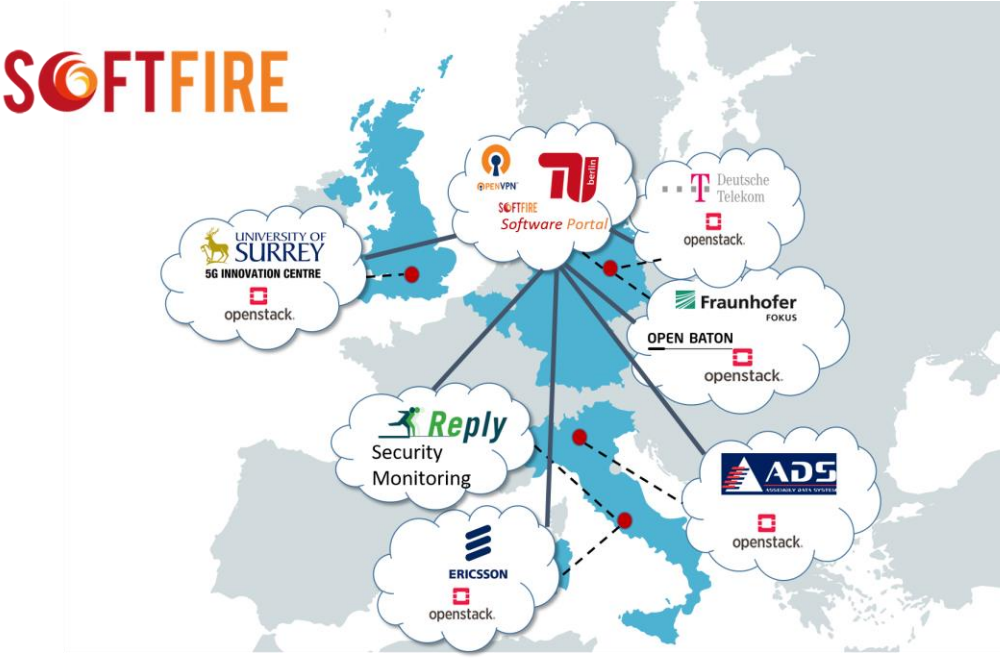

Figure 1: The SoftFIRE federated testbed.

Located in three different countries in Europe, SoftFIRE currently consists of the following individual testbeds:

- *RMED CloudLab* [15] provided by Ericsson, in Rome, Italy,
- *The 5G Playground (former FUSECO Playground)* [16] provided by Fraunhofer FOKUS and the Technical University of Berlin, in Berlin, Germany,
- *5G Innovation Centre (5GIC) testbed* [17] provided by the University of Surrey (UoS), in Guildford, United Kingdom,
- *Deutsche Telekom testbed* [18], in Berlin, Germany,
- *Assembly Data Systems NFV Lab testbed* [19], in Rome, Italy.

Following a successful integration of RMED CloudLab, 5GIC, and 5G Playground in 2016, the project is now expanding its testbed with the addition of the Deutsche Telekom [18] testbed located in Berlin, Germany, and the Assembly Data System NFV Lab testbed located in Rome, Italy. This will increase the capacity in terms of virtualised resources.

With its multi-site integrated testbed, SoftFIRE provides virtualised compute, storage, and networking resources available for executing on demand Virtual Network Functions. The aggregate capacity is summarised in Table 1.

Table 1. Virtualisation resources provided by SoftFIRE as of April 2017.

Testbed name	Number of CPUs	RAM (GB)	Disk space (GB)
5G Playground, Fraunhofer FOKUS, TU Berlin	56	256	274
RMED CloudLab, Ericsson	80	256	1600
Deutsche Telekom	10	20	50
5G Innovation Centre (5GIC), University of Surrey (UoS)	24*	96*	480*
Assembly Data System NFV Lab	16	47	900
TOTAL	202	722	4204

*Half of the resources at UoS are used by multiple 5G EPC Core VNFs, each dedicated to a single experimenter's use. The rest half is available for experimenter VNFs.

The rest of this White Paper is organised as follows. Firstly, an overview about physical resources and capabilities offered by the individual testbeds is given in Section 4. This section also provides the approach used for securely connecting those federated testbeds. Then, Section 5 presents the SoftFIRE Middleware, as the intermediary component between experimenters and the federated infrastructure. Finally, Section 6 provides the projects concluding remarks and suggestions on deploying and integrating a multi-site orchestrated virtualisation platform.

4 SoftFIRE's Component Testbeds

This section presents brief information on the individual testbeds forming the federated SoftFIRE infrastructure. As of May 2017, three testbeds have successfully been integrated, which are the Fokus 5G Playground testbed, University of Surrey 5GIC testbed, and Ericsson RMED CloudLab. Assembly Data Systems (ADS) NFV Lab and Deutsche Telekom (DT) testbeds are currently being integrated. This section briefly describes the currently integrated three testbeds, as well as the ADS NFV Lab testbed, which has completed its initial integration stage; whereas the DT virtualisation testbed is under integration work and not presented.

4.1 Ericsson RMED CloudLab

Ericsson SoftFIRE testbed is part of the Ericsson RMED CloudLab. Located in Rome, CloudLab's scope is to provide hands-on competence build-up, to show specific and concrete "proof" points for cloud computing, to house demonstrations to customers on specific virtualisation products, and to help customers resolve commonly encountered issues in virtualisation environments and to mitigate potential risks.

Main activities performed in CloudLab are:

- Experimenter demos,
- Deep dive on customer-specific requests,
- Fully customized Proof-of-Concept (PoC) demonstrations on customer premises,
- Validation and certification on customer specific stack / solutions.

Cloudlab in SoftFIRE provides an Infrastructure as a Service (IaaS), creating and managing large groups of virtual private servers in a single data center. It runs OpenStack Liberty as its infrastructure controller.

4.1.1.1. Building the Ericsson CloudLab segment for SoftFIRE

The SoftFIRE segment of CloudLab runs on Dell PowerEdge R620 server blades. There are three servers, one controller and two compute nodes, that OpenStack Liberty [25] runs on, as shown in Figure 2.

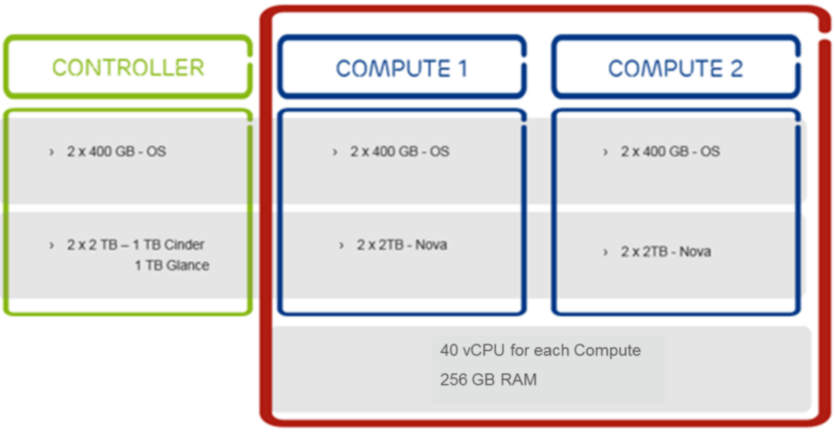

Figure 2: Ericsson CloudLab SoftFIRE segment IaaS nodes.

All servers are equipped with 2x400 GB disks in mirroring mode for OpenStack with 2 additional disks, each 2 TB, where OpenStack services run.

The installed OpenStack has a classical modular architecture where the main components are Nova (Compute), Cinder (block storage, i.e. volume), Glance (catalogue and repository for disk images), Keystone (authentication and authorization), Horizon (web-based user interface (UI)), and Neutron (networking).

To adapt the testbed to SoftFIRE, some software modifications have been made in the infrastructure, as follows:

- Instead of My SQL database, PostGres [27] is used;
- To extend OpenStack capabilities with SDN functionalities, OpenDaylight [28] SDN controller (ODL Boron SR-2) has been integrated with OpenStack Neutron service via the OVSDB 2.7.0 south-bound plug-in, which enables control and configuration of the attached Open Virtual Switch (OVS) [29]. This replaces the L3 Agent typically found in OpenStack installations. ODL provides the user with REST API to program flows.
- On the Compute Node, no DHCP and metadata are activated, and OVS is loaded via the networking-odl pseudo agent.

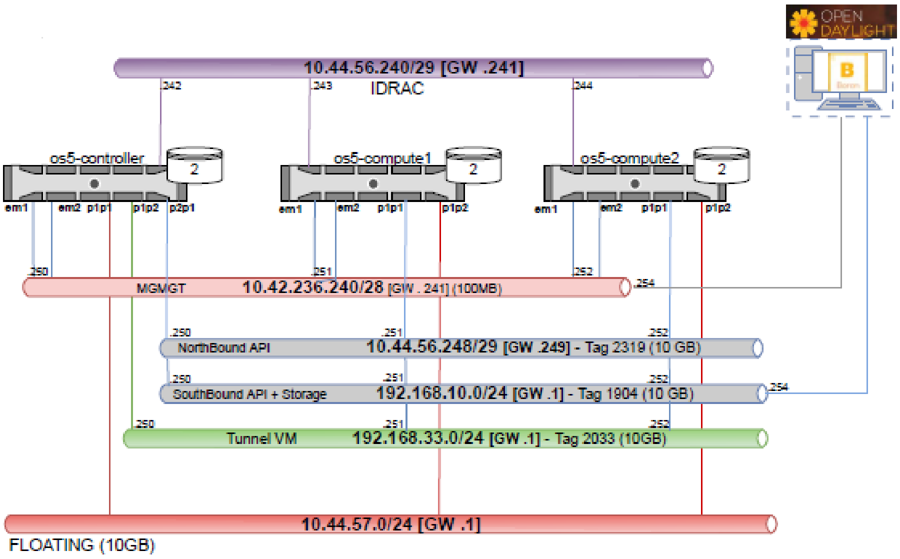

Figure 3: Ericsson CloudLab SoftFIRE segment network architecture.

Figure 3 illustrates the network design of CloudLab, which is composed of six networks.

- IDRAC: the console network,
- MGMT: Management of operation and maintenance,
- NB_API: Provides connectivity for OpenStack northbound API,
- SB_API: Provides connectivity for OpenStack southbound API, which is for OpenStack internal services,

- Tunnel network: Internal network in OpenStack, providing interconnection between VMs residing at different compute nodes,
- Floating network: External network (flat) in OpenStack providing connectivity to outside of OpenStack domain; VMs are assigned with floating IPs in this network.

4.2 Fraunhofer Fokus 5G Playground

The component testbed provided by Fraunhofer FOKUS in Berlin is realised as a slice of a much bigger testbed that is used to benchmark virtual 5G core network functions. This includes a dedicated part (tenant) of an OpenStack cluster to provide computing and storage resources. The connectivity to the distributed parts of the SoftFIRE component testbeds is realised by an IPsec secured VPN link to TUB. This is shown in Figure 4. The FOKUS testbed hosts the Open Baton orchestrator, which is used to orchestrate of the federated testbed. The FOKUS testbed also hosts an instance of the SEM.

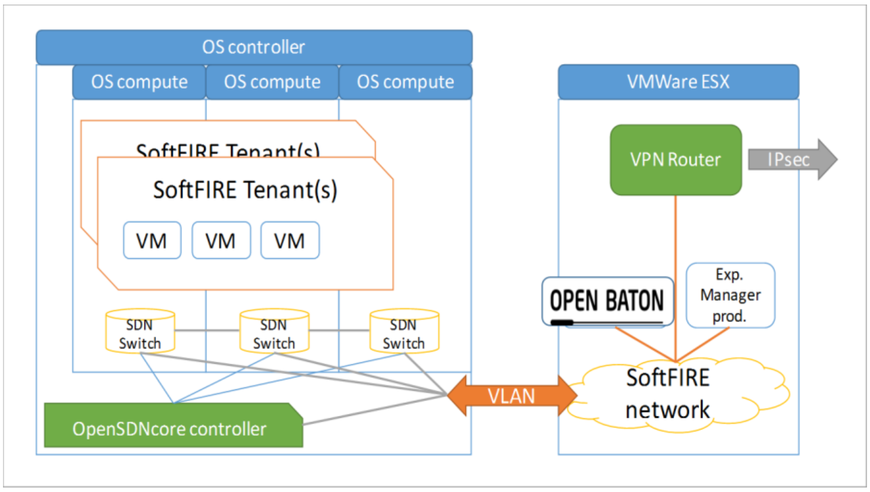

Figure 4: FOKUS testbed architecture.

In this component testbed, Compute resources are provided by an OpenStack Newton cluster installation that is dedicated to SoftFIRE. The setup is based on one combined OpenStack Controller, Compute, and Networking host node and two additional Compute nodes. The Controller also houses the OpenSDNcore [30] controller that acts as a master controller for each of the OpenSDNcore virtual switches that are deployed in each Compute host. The used servers are manufactured by Dell and are in the blade form factor.

Table 2 lists the details of the used server hardware in the Fokus component testbed. Storage capacity is provided by a central Storage Array Network (SAN) manufactured by NetApp accessed via a GBit Ethernet link. The Servers are connected to several adjunct networks that are used for management and storage access. Direct access to these networks is not possible from within the VM instances. Connectivity for the SoftFIRE VPN is realised as an external provider network that is connected via the OpenSDNcore virtual switches and dedicated to the SoftFIRE project.

Table 2. Fokus OpenStack hardware.

	Type	RAM	CPU	Storage
Controller & Compute 1	Dell PowerEdge M620	128 GB	2x Intel(R) Xeon(R) CPU E5-2640 v2 @ 2.00GHz (32vcores)	360 GB SSD 1 TB HDD NAS: 500 GB
Compute 2	Dell PowerEdge M620	128 GB	2x Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz (24vcores)	150 GB SAS NAS: 500 GB
Compute 3	Dell PowerEdge M620	128 GB	2x Intel(R) Xeon(R) CPU E5-2640 v2 @ 2.00GHz (32vcores)	150 GB SAS NAS: 500 GB

4.3 5GIC Testbed at University of Surrey (UoS)

The UoS SoftFIRE testbed segment is part of the overall UoS 5GIC testbed. Located in the UK, the scope of the testbed is to provide hands-on access to a 3GPP based campus RAN with indoor and outdoor coverage that is able to be interconnected with a variety of virtualized core slices, in order to develop Core Network 5G evolutions and demonstrate 5G use cases running over the resultant end-to-end (ETE) cellular network. In this manner, the testbed can be used to build industry core competence in 5G.

The network was initially built as a fixed ETE cellular system, but has now been evolved to provide a set of virtualised network capabilities that can be configured to connect with IP stubs towards the RAN to enable various network slices to be connected in circuit under the control of the federated SoftFIRE core.

It is envisaged that experimenters using the facilities of the UoS SoftFIRE testbed will be able to show specific and concrete “proof” points related to the 5G RAN and Core evolutions and demonstrate applications running over this infrastructure. These use case proof points can be used to support many types of use cases to highlight their benefits, explain to customers and industry partners how they work and demonstrate how 5G targets may be met, and what the pros and cons are for each demonstration.

The main activities performed are:

- Standard experimenter demonstrations
- Deep dive on experimenter specific request
- Proof-of-Concept (PoC) whilst connected to experimenters’ equipment or remote site
- Validation and Certification on customer-specific solution

The 5GIC UoS testbed is sharing a segment of the testbed with the SoftFIRE Federated Testbed (UoS SoftFIRE testbed segment). The scope of UoS SoftFIRE testbed segment in the SoftFIRE project is to provide the following component parts:

1) OpenStack (Newton version) system access to infrastructure that can be used to instantiate core slices for experimentation with the local RAN components,
2) Access to the 5GIC in-building LTE-A RAN,
3) Access to the 5GIC in-building Wi-Fi system for multi-access 5G use cases.

In order to deliver the infrastructure as a service (IaaS) capabilities for creating and managing as a data-centre, the following network hardware is provided for experimenter use, as shown in Table 3.

Table 3: Network equipment in the University of Surrey component testbed.

Description (single node configuration)	Quantity
Dell PowerEdge R920 (deployed as SoftFIRE OpenStack Controller and Compute server) Total 12 CPUs available for experimenter VMs.	1
Indoor, Wi-Fi Access Points Wi-Fi 802.11ac Access Points from Aruba	6
Indoor, LTE-A, FDD, Femto-cells	2

The UoS testbed provides several LTE-A core network software images and/or packaged components for experimenters to use, as listed in Table 4.

Table 4: Network services provided by the University of Surrey testbed

Network Service	Max number of instances on the UoS Testbed	Virtual Network Functions included in Network Service	Description
Control Plane Node (CPN)	1	HSS, MME, integrated (SGWc, PGWc, which are the control planes of SGW and PGW, respectively)	This Network Service (NS) slice is instantiated as soon as any EPC is required to be instantiated on the UoS testbed for Control Plane connectivity via the UoS LTE-A RAN. There is only ever one instance of the CPN NS for the whole UoS SoftFIRE network segment. All experimenters instantiated on the UoS testbed share this slice for LTE-A connectivity.
User Plane Node, Cluster Controller	3	CC, Integrated (SGWu, PGWu, which are the user planes of SGW and PGW,	This Network Service is instantiated per experimenter for LTE User Plane service and extended 5G Context Awareness Association to a group of cells known as a "Cluster" via the newly proposed 5G node called a Cluster

Network Service	Max number of instances on the UoS Testbed	Virtual Network Functions included in Network Service	Description
UPN (CC)		respectively)	Controller (CC). Each authorized experimenter is provided with a single instance of this VM on the UoS testbed.
User Plane Node, Cluster Member UPN (CM)	3	CM, Integrated (SGWu, PGWu, which are the user planes of SGW and PGW, respectively)	This Network Service is instantiated per experimenter for LTE User Plane service and extended 5G Context Awareness Association to a Cluster Member within a "Cluster" via the newly proposed 5G node called a Cluster Member (CC). CM has the interface to an experimenter-provided server application (that would run on an experimenter VM). Each authorized experimenter is provided with a single instance of this VM on the UoS testbed.

4.4 Assembly Data System NFV Lab

The ADS SoftFIRE component testbed is located in Rome, and is made available to SoftFIRE with the aim of setting up additional NFV capabilities in the project, which are also to be included in ADS Software Factory which now provides a platform for customer demonstrations and PoC within the framework of SoftFIRE. The ADS component testbed is also an optimal working environment for the development and test of own-brand VNFs and for benchmarking cloud virtual network performance.

Currently the ADS component testbed consists of 5 nodes with the following roles:

Table 5: Network equipment provided by the ADS testbed

	Type	RAM	CPU	Storage
Director	Dell PowerEdge R610	16GB	2x Intel(R) Xeon(R) CPU E5504 @ 2.00GHz (8vcores)	136 GB 10K SAS
Controller	Dell PowerEdge R610	16 GB	2x Intel(R) Xeon(R) CPU E5504 @ 2.00GHz (8vcores)	136 GB 10K SAS
Compute 1	Dell	48 GB	2x Intel(R) Xeon(R) CPU	136 GB 10K

	PowerEdge R610		E5530 @ 2.40GHz (16vcores)	SAS CEPH: 1800 GB
Compute 2	Dell PowerEdge R610	48 GB	2x Intel(R) Xeon(R) CPU E5530 @ 2.40GHz (16vcores)	136 GB 10K SAS CEPH: 1800 GB
Ceph Storage Node	Dell PowerEdge R610	16GB	2x Intel(R) Xeon(R) CPU E5504 @ 2.00GHz (8vcores)	136 GB 10K SAS 4x 900 GB 10K SAS

The storage backend of the infrastructure is based on Ceph Software-Defined Storage [31], which provides high availability and high scalability object and block storage on general purpose hardware. The compute nodes leverage on the Ceph node (see Table 5); hence the VM image storage is not the on the same compute node, but it is fully decoupled from the compute resources.

ADS NFV infrastructure is based on RedHat OpenStack 10 (Newton), released on December 2016. This release is suggested for real production infrastructures for telecom operators, who need stable and supported virtualisation environments. RedHat OpenStack is based on the Triple-O project [32] (OpenStack on OpenStack), which installs two OpenStack instances, named *Overcloud* and *Undercloud*. The architecture is shown in Figure 5. The latter is a single-system OpenStack installation (the Director node) that includes components for provisioning and managing the Overcloud OpenStack nodes throughout the use of (i) Heat [33] stack templates that define the Overcloud Platform, and (ii) Ironic [34] module to manage bare metal instances. The Director node is not used by the workload cloud, but it is used only to provision and manage the nodes of the infrastructure.

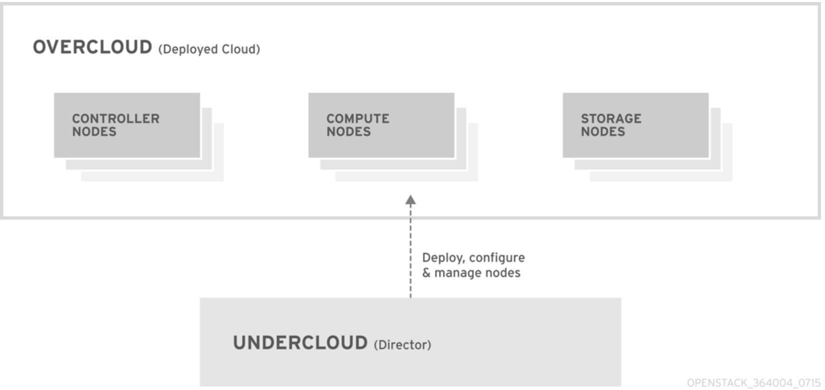

Figure 5: Triple-O Architecture

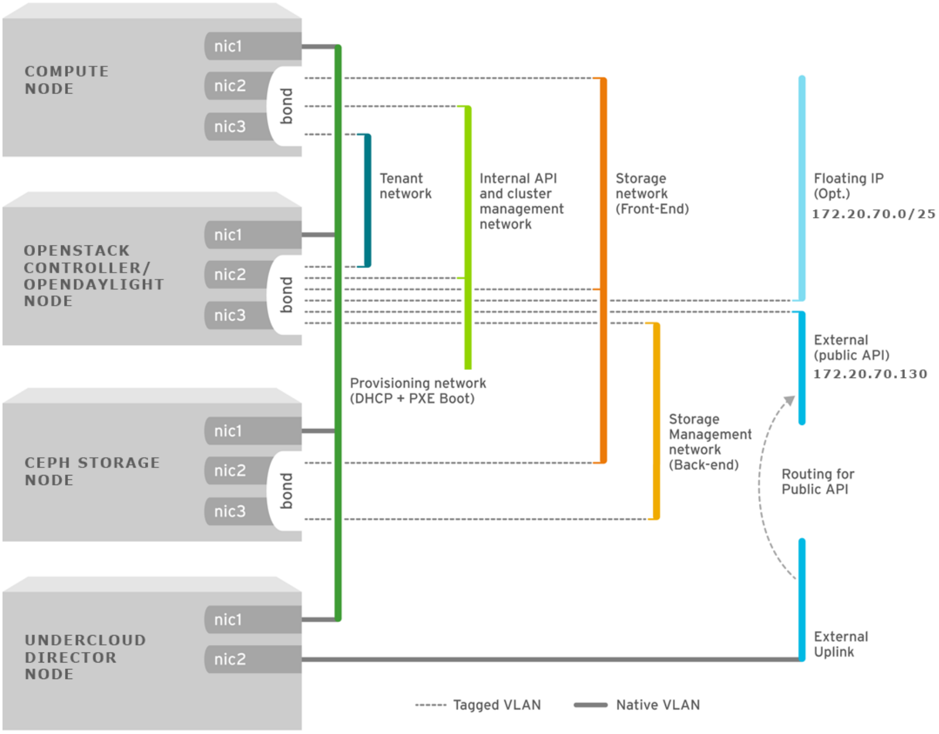

Figure 6: The ADS testbed network architecture.

The Openstack installation follows the reference design of RedHat, as illustrated in Figure 6. Control and service networks are isolated on separate VLANs, while interface bonding assures High Availability. The ADS component testbed also provides a platform for SDN experiments, hence the OpenStack installation is fully integrated with OpenDaylight as its networking backend, in order to provide more advanced SDN functionalities than those provided by default the OpenStack Neutron module. OpenDaylight is hosted at the Controller node, as shown in Figure 6.

5 Federation of Component Testbeds

5.1 Connectivity in the federated SoftFIRE testbed

The different testbeds in SoftFIRE are connected via secure communication links in a Virtual Private Network (VPN), specifically OpenVPN [20] [1]. Technical University Berlin (TUB) acts as the OpenVPN hub for SoftFIRE. As such, the TUB datacentre is in the middle of the SoftFIRE's VPN network, as illustrated in Figure 1. The VPN hub is capable of forwarding traffic between different SoftFIRE component testbeds. Incoming and outgoing network traffic is filtered based on whitelists that allow previously agreed protocols.

5.2 Virtual infrastructure manager: OpenStack

All the SoftFIRE individual testbeds make use of OpenStack (Figure 7). As an open source software, OpenStack [26] is considered as the de-facto Virtualized Infrastructure Manager in the NFV ecosystem. Development of OpenStack dates back to July 2010, from the collaboration between Rackspace Hosting [35] and NASA [36]. As an open source software, OpenStack is supported by a global community of collaborators and developers. The latest release deployed as the virtual infrastructure manager on SofftFIRE component testbeds is OpenStack Newton [37].

OpenStack manages Compute, Network, and Storage resources all over a datacentre. Separate projects have expanded the capabilities of OpenStack, such as Horizon, which provides a dashboard graphical user interface (GUI). OpenStack also exposes its command line interface which provides developers and users of OpenStack with an extensive set of API commands. Through the dashboard and the API, it is possible to manage the Compute resources, create and configure Networks, and manage Storage resources.

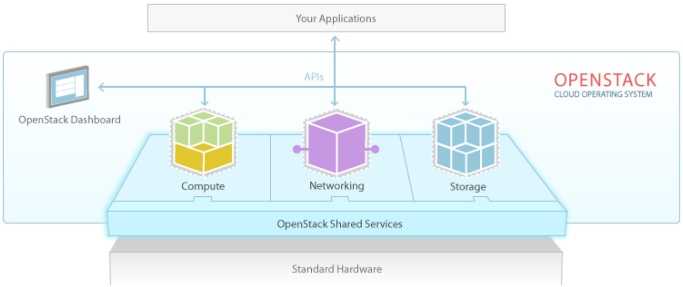

Figure 7: OpenStack virtual infrastructure manager.

In SoftFIRE, OpenStack exposes APIs to the upper layers for controlling virtualized resources later on used for hosting VNFs.

[1] OpenVPN is a Virtual Private Network software that uses Secure Sockets Layer/ Transport Layer Security (SSL/TLS) protocol to encrypt the encapsulated traffic and authenticate its peers.

5.3 The SoftFIRE middleware

The SoftFIRE Middleware provides the means for executing NFV/SDN experiments across the federated infrastructure. Figure 8 represents the high-level architecture of the SoftFIRE Middleware:

- The lower layer depicts the Virtualized Infrastructure Manager (VIM), OpenStack, utilized for controlling resources provided by each individual testbed. As already introduced in the previous sections, an OpenStack instance has been instantiated on each individual testbed.
- The intermediate layer represents the orchestration capabilities of the platform supported by Open Baton, a NFV MANO open source implementation.
- The upper layer is the set of tools and features needed to identify and support the experimenters and to map their requests on the available resources of the platform.

In the following sections, the description of the virtualisation and orchestration layer within SoftFIRE are provided following a bottom up approach.

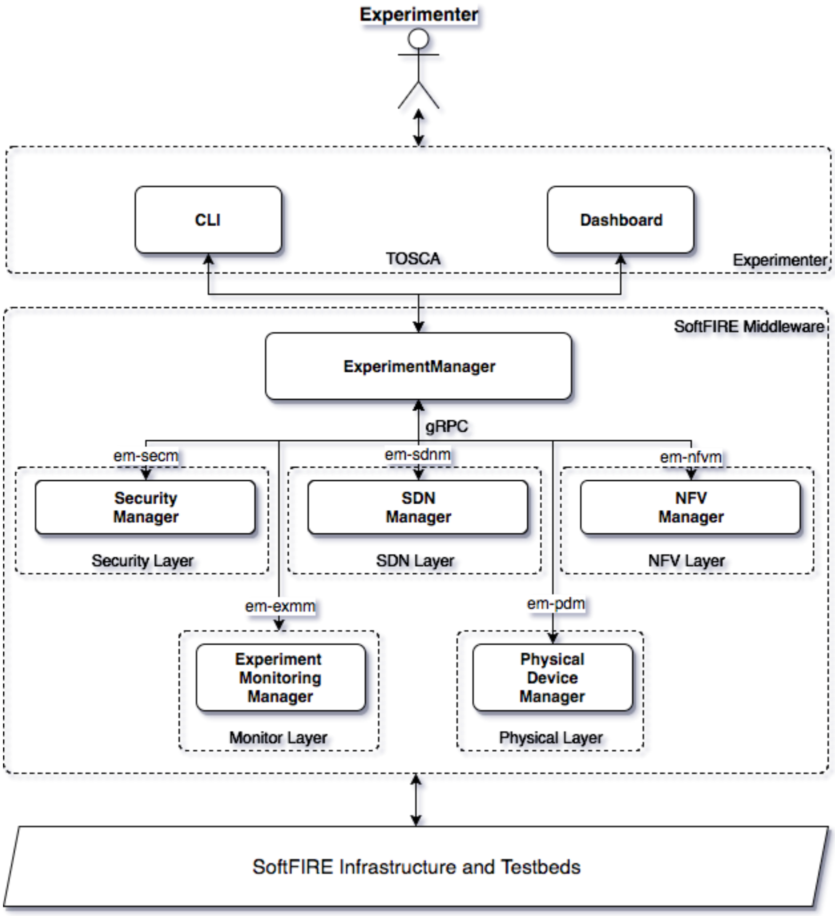

Figure 8: High-level SoftFIRE virtualisation architecture

5.4 NFV manager and orchestrator: Open Baton

The NFV Management and Orchestrator (NFV MANO) layer has been implemented using the Open Baton framework. Open Baton is an open-source ETSI MANO-compliant platform providing an extensible framework for managing and orchestrating VNFs. Open Baton provides mechanisms for deploying VNFs across the multi-site federated infrastructure.

5.4.1. Open Baton NFV orchestrator (NFVO)

The NFVO is designed to address the needs of cloud computing service providers as well as network operators, and is suitable for the virtualisation of 5G mobile networks, mission critical networks, machine-to-machine (M2M) networks, and multimedia networks. With this support for a broad umbrella of use cases, Open Baton enables virtual network service deployments on top of cloud-based infrastructures and thereby builds a bridge between cloud computing service providers that target at supporting network functions and network function providers that require the appropriate infrastructure support for the virtualisation of their network services.

In its first year, using the Open Baton orchestrator hosted in Fraunhofer FOKUS, the SoftFIRE project successfully demonstrated dynamic deployments of 5G network services on top of the University of Surrey testbed to network operators, SMEs, and government representatives on multiple occasions.

The software architecture of Open Baton is illustrated in Figure 9.

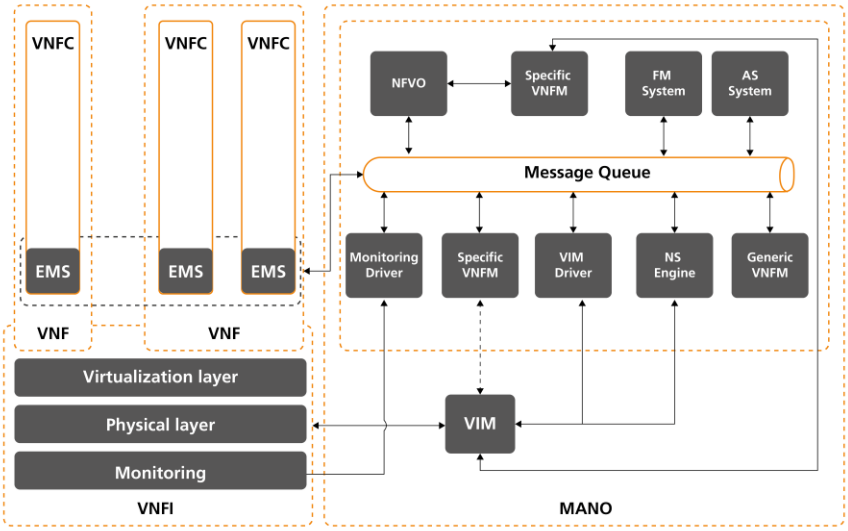

Figure 9: SoftFIRE's NFV Orchestrator: The Open Baton platform architecture

Open Baton is based on ETSI MANO v1.1.1 specification [38], which was published at the end of 2014. The platform can be easily installed on existing cloud-infrastructures like OpenStack, and consist of the following software components:

- NFV Orchestrator (NFVO) that dynamically orchestrates carrier-grade network functions and services as well as infrastructure resources. NFVO manages the lifecycle Network Services, including installation, deployment and configuration. It can also manage multiple PoPs. NFVP provides identity management and user separation, as well as support for interoperability of VNF Managers (VNFMs). VNF package management is also provided by NFVO,

- A generic Virtual Network Function Manager (VNFM) that dynamically manages virtual network the functions,
- A set of libraries (SDK) for the creation of customised VNFMs and for interfacing with the northbound REST APIs,
- A user-friendly dashboard through which the platform can be administered,
- An external module dedicated to execute fault management specific actions on deployed network services,
- An external module dedicated to perform auto-scaling on deployed virtual network functions,
- An extendible set of plugins that enable the communication with heterogeneous virtualised infrastructure manager and monitoring system.

5.4.2. Open Baton orchestrating VNFs across the federated infrastructure

In the federated infrastructure, each individual testbed provides its own installation of OpenStack, registered at the NFV Orchestrator level as multiple Point of Presence (PoP) as shown in Figure 10.

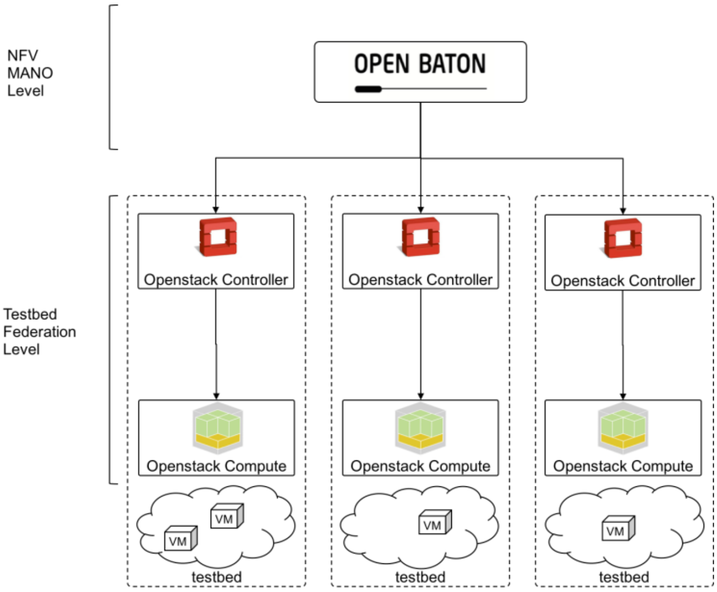

Figure 10: SoftFIRE's MANO strategy: Multiple controllers and single Open Baton orchestrator

In this setup, each OpenStack instance is completely separated from and unaware of the presence of other testbeds, however Open Baton provides a single view of the available resources to experimenters being the only access point towards the underneath infrastructure. The setup of a single NFVO controlling multiple PoPs provides the following benefits to the SoftFIRE federated testbed:

- Possibility for each testbed provider to choose the best OpenStack version to use,

- Exploitation of the user/experiment separation capability provided by Open Baton,
- Exploitation of the multiple-PoP management capability provided by Open Baton
- No need for additional functionalities in the northbound of OpenStack for user management and resource separation,
- Reduction of the number of Open Baton machines to be maintained by the federated testbed owners.

5.5 The Experiment Manager as enabler for FIRE experimentation

One of the major functionalities which has to be provided by the SoftFIRE middleware is to control the full life-cycle of an experiment on top of such a distributed and heterogeneous infrastructure. Being a project part of the FIRE research activities, one of the major objective is to facilitate the way external experimenters are interacting with the federated infrastructure. During the initial phase of the project, experiment control has been provided via the FITeagle toolkit. FITeagle follows the Slice Federation Architecture (SFA) specification, and provides mechanism for discovering, provisioning, monitoring and disposing very heterogeneous resources. SFA provides an easy way to describe resources via the Resource Specification (RSPec) language. With those RSPec definitions, resources could become part of a catalogue exposed to experimenters.

However, one of the major limitations encountered with this approach was that most of the resources available in the underneath infrastructure are typically described using cloud-based reference model, like the Topology and Orchestration Specification for Cloud Applications (TOSCA). TOSCA is also one of the major candidates foreseen by the ETSI NFV community for modelling network services.

The project SoftFIRE is currently evolving the current architecture of the SoftFIRE middleware in order to (i) enable various different functionalities at the orchestrator level, (ii) support remote control of mobile devices, and (iii) expose SDN functionalities over multiple testbeds. One of the major decisions taken was to use TOSCA as reference model for describing an experiment consisting of different types of resources: NFV, SDN, Monitoring, and Security.

The Experimenter Manager is the result of this restructuring and consolidation of the SoftFIRE middleware architecture. Figure 11 illustrates the middleware architecture under development by the SoftFIRE project in 2017. Open Baton will be the manager of virtual resources, whereas a new SDN manager will provide SDN functionalities. Furthermore, a security manager will support allocation of security functions. Finally, a Monitoring Manager will monitor all functionalities. These managers are currently under development. The SoftFIRE Experiment Manager (SEM) will provide the access to these different managers, so that experimenters can perform the desired actions via a related manager, while the SEM abstracts the underlying implementation from the experimenter.

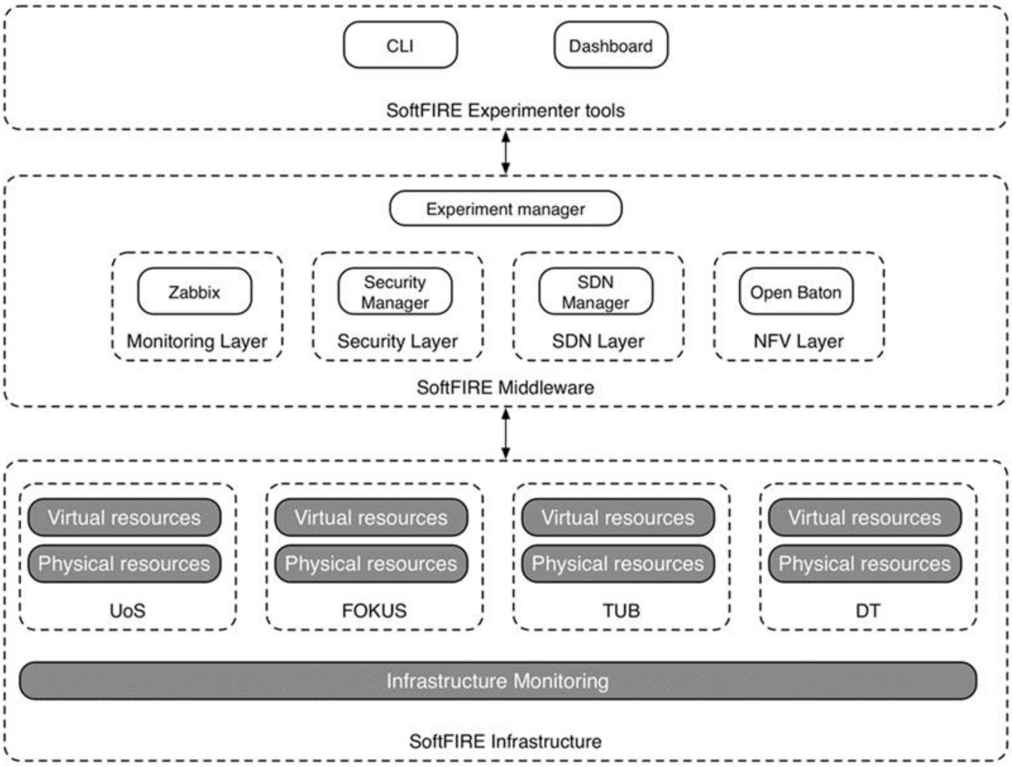

Figure 11: The SoftFIRE middleware architecture

5.6 Usage of the SoftFIRE infrastructure

A possible scenario depicting the usage of the SoftFIRE infrastructure is outlined in the following Figure 12. First, the testbed grants access to an experimenter, and then allocates requested resources to the experimenter. To get access to the platform, the experimenter first receives a certificate from the Experimenter Manager. This is then followed by request for resources initiated by the experimenter. The Experimenter Manager relays such request to the corresponding entity (a Manager) related with that request.

The SoftFIRE Experiment Manager also isolates different experiments so as to avoid conflicts and interruption between different experiments.

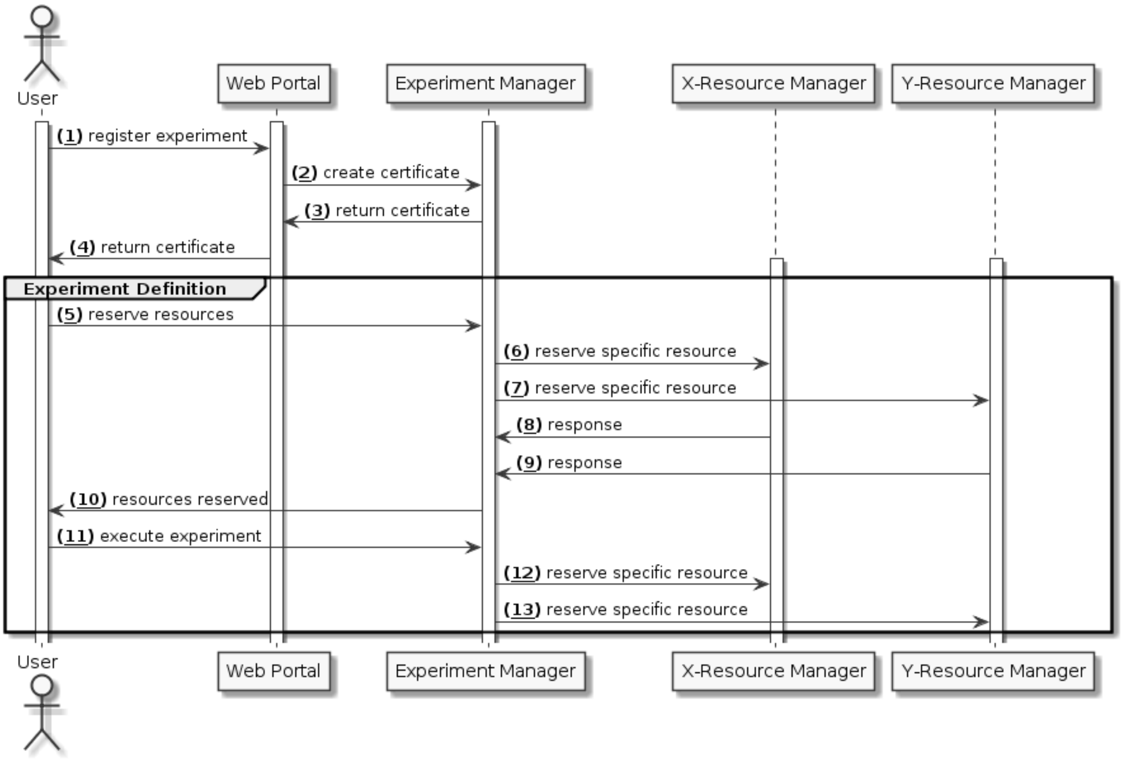

Figure 12: Experimenter use of the platform.

6 Concluding Remarks and Lessons Learned

The SoftFIRE project is strongly willing to bring the issues and the results of its experiments to the general public. There are several high-level remarks to bring upfront and some more detailed issues to present to the community. This section briefly introduces the high level issues and then provides a view on the problems encountered by the project during its first year and its first round of experimentation.

6.1 A high level view

Interoperability issues are inevitable when integrating multiple heterogeneous networks. Different component testbeds are likely to have different requirements, regulations, and restrictions. Secure connection between testbeds is undeniably a must; however such communication must be continuously maintained. Connectivity losses between sites defeats the purpose of an integrated testbed. As with any network deployment, individual component testbeds must be maintained when failures/malfunctions occur. This requires not only development effort, but also IT support, which must be taken into account when planning a testbed integration.

An easy to use programming interface is essential to realise effective use of the platform by experimenters. The key point of consideration is the heterogeneity of experimenter needs; a federated testbed must have a minimal set of requirements, some basic capabilities exposed to experimenters, as well as a set of restrictions imposed on them. While providing ease of use of a wide range of programming capabilities, such interfaces must also enable certification, security, and isolation between users of the platform.

Use of open source software is often challenging when different software pieces need to be integrated. One example is the integration of the OpenStack infrastructure manager and the OpenDaylight SDN controller. The community support on such integration depends on different versions of the open source software pieces, which makes it difficult to realise their effective and timely integration. Furthermore, the integration of an infrastructure orchestrator with multiple OpenStack instances running at multiple sites is challenging, requiring considerable development effort towards providing suitable plugins, proxies, and managers. Such intermediate software pieces need to be adaptable to different APIs exposed by different open source software distributions.

Last but not the least, security and safety mechanisms must be in place to protect the infrastructure from malicious users, and to avoid unintentional damage to experimenter software caused by improper use of the platform by experimenters.

6.2 Lessons learned

6.2.1. Interoperability perspective

Achieving full interoperability of the whole SoftFIRE Testbed has required a lot of design sessions and troubleshooting, with a considerable impact on the individual companies' IT security policies. The interconnection between the different testbeds has taken substantial effort to realise. As a result of this effort, various results have been obtained:

- The project infrastructure need to be tuned up by means of a number of internal measures to be taken at individual component testbeds,
- The SoftFIRE inter-operability test (InterOpTest) event in Berlin, which took place in September 2016, successfully demonstrated the operation of the platform, and proved that a multi-site virtualisation platform can provide quick services to end customers,
- Starting from November 1 2016, the SoftFIRE federated testbed has been made available to experimenters to carry out their experiments,
- During that period, the platform had to be consolidated in order to better adapt and support the requirements of developers. The tuning up has been carried out with the support of the experimenters, creating a community of software virtualisation experts,
- The Platform has supported several projects running in parallel up until end of February 2017. All the running projects were able to achieve their expected results, proving the project's claim to be an operational virtualisation infrastructure provided to experimenters as a service.

Despite its achievements, the project has also encountered various challenges. Above all, the project has made considerable effort to integrate FIRE tools with the newer approach undertaken by the NFV/SDN community. It has finally been concluded that these two approaches do not match perfectly, which is a crucial finding that is directly useful for the NFV/SDN community. As a result, the project has moved to a TOSCA-based approach through a new middleware, called the Experimentation Manager, which can support various types of resources for experimenter use.

In order to measure the features and the capabilities of the SoftFIRE federated testbed and in general as a contribution to the NFV/ SDN/ 5G community, the SoftFIRE project has defined a set of KPIs (ranging from platform programmability to security). Some of them have also been implemented in order to measure the behaviour of platform. This is a valuable contribution (in line with the project objective to measure the QoS offered and supported by the platform) because newer software platforms need to be assessed by new sets of KPIs that measure not just the platform performance, but also the capability to quickly implement and run solutions whilst also providing fundamental security measures.

6.2.2. Programmability perspective

In order to lay the foundation for measuring the "programmability" of the platform, an initial definition is needed. In this sense, project SoftFIRE has defined "programmability" by means of a set of goals; i.e. a platform is highly programmable if it achieves the following:

a. Minimal additional software development whilst integrating an application/service on the platform (in other terms the additional development needed to adapt the envisaged properties to run on the chosen platform),
b. Maximal number of services, interfaces (APIs), and libraries should be made accessible to a programmer,

c. The right set of tools and mechanisms should be offered to programmers, which are useful for software development and management, without overwhelming or superimposing certain tools and methodologies,
d. Various popular set of tools that allow rapid and efficient testing and deployment of applications and services on the platform should be offered.

With this empirical definition of "programmability" in mind, a high programmability of the platform has been targeted, by means of two actions and their related results:

1. SoftFIRE internal development of use cases; i.e., experiments carried out by the SoftFIRE team internally, in order to implement and run interesting applications,
2. Experimentations carried out under the umbrella of the First Open Call launched by SoftFIRE; i.e., experiments carried out autonomously by developing teams.

In the first case, the SoftFIRE project has developed use cases that have been proved internally and some of them have been shown internationally, specifically in the context of 5G networks. The goal in doing so has been to provide some examples inherent to the issues to be encountered by 5G network operators when adopting NFV/SDN solutions. Virtual IMS is one example to be considered under this perspective and the project's work undergoing in the realm of 5G network slicing is an attempt to move forwards in this area. For instance, so far, in 2017 a 4-slice, Rel-14 CPN/UPN core network slicing demonstration has been realized on the UoS testbed, with 3 of the slices deployed using Open Baton demonstrating both local and remote network slicing control.

SoftFIRE has received a strong request from its experimenters to offer access to programmable resources. In fact, some of the executed experiments have stressed the need for certain programming capabilities offered by the platform resources. SoftFIRE has built special solutions backed up by the availability of some network resources in order to support these programming needs.

6.2.3. Security perspective

With respect to Security, the SoftFIRE project has been working on the definition of security requirements that brought to the identification of a high-level security framework. Towards this, a monitoring system has been built, which receives log files and other information by the different components of the platform, and processes them in order to detect risks and potential threats to the platform. This required a solid design of the solution and related implementation. An initial version of the monitoring functionalities has been demonstrated during the inter-operability test in Berlin.

Security is considered as an integral part of the design of the Federated Testbed. OpenVPN, tunnelling and encryption were implemented between the component testbeds to provide a secure internetworking solution, while also segregating the infrastructure from the public Internet. In fact, (Experimenter) access to the SoftFIRE Federated testbed is implemented using an OpenVPN server that connects all clients directly into the SoftFIRE subnet. Access to the VPN is protected by certificates that are signed by a PKI hosted and integrated into the SoftFIRE infrastructure.

The project is further developing a Security Manager in its new middle-ware architecture, that governs and controls further security measures during experimenter access to the platform.

The implemented security results will be further elaborated and will have an impact on how SoftFIRE will further progress. In particular:

- Introduction of new functions appealing to the experiments requirements (Programmability)
- Consolidation and introduction of new security features (Security).

The First Wave of Experimentation has provided the project team with (i) the perspectives of experimenters and (ii) the challenges encountered by the platform providers, in terms of security. This will make it possible to make the upcoming Open Calls more feasible to support.

6.3 Final remarks

Last but not the least, of fundamental importance are the features of the experiments that run on a federated environment, especially when the network runs virtualised resources. It is of utmost importance to plan how many experimenters/users are on the network and how many virtual machines exist, and the amount of resources consumed in aggregate and individually by different experimenters. Improper planning can easily stretch infrastructure and staffing resources.

Although it has various challenges as outlined above, an integrated federated testbed paves the way to the future network function virtualisation realisations, such as operator control of a virtual mobile network with network slicing, or flexible and scalable multi-site virtual infrastructures to be provided by datacentre operators. Towards this, the SoftFIRE testbed has enabled a multi-site virtualisation platform – one of the most recent such deployments in the world readily used by experimenters.

Bibliography

[1] “Network Function Virtualisation: State-of-the-Art and Research Challenges”, Rashid Mijumbi, Joan Serrat, Juan-Luis Gorricho, Niels Bouten, Filip De Turck, Raouf Boutaba, *IEEE Communications Surveys & Tutorials*, vol 18, no 1, 236-262, September 2015,

[2] "Network Functions Virtualisation— Introductory White Paper", ETSI, 22 October 2012, retrieved 20 June 2013.

[3] “Software-Defined Networking: A Comprehensive Survey”, Diego Kreutz, Fernando M. V. Ramos, Paulo Esteves Veríssimo, Christian Esteve Rothenberg, Siamak Azodolmolky, Steve Uhlig, *Proceedings of the IEEE*, vol 103, no 1, pp 14-76, January 2015,

[4] EU SoftFIRE project, https://www.softfire.eu/

[5] PlanetLab, https://www.planet-lab.org/

[6] The KOrea advanced REsearch Network (KOREN), http://www.koren.kr/koren/eng/

[7] OpenFlow, https://www.opennetworking.org/sdn-resources/openflow

[8] Research Infrastructure for large-Scale network Experiments (RISE), http://www.jgn.nict.go.jp/rise/english/index.html

[9] EU BonFIRE project, http://www.bonfire-project.eu/home

[10]OneLab future Internet testbeds, https://onelab.eu/

[11] EU CREW project, w-iLab.t testbed, http://www.crew-project.eu/wilabt

[12] Network Implementation Testbed Laboratory (NITOS), http://nitlab.inf.uth.gr/NITlab/nitos

[13] Federation for Future Internet Research and Experimentation (FED4FIRE), https://www.fed4fire.eu/

[14] Federated Testbed for Large-scale Infrastructure eXperiments (FELIX) https://www.surf.nl/binaries/content/assets/surf/nl/2016/20160630-presentatie-felix---peter-hinrich.pdf

[15] Ericssion RMED CloudLab, https://www.ericsson.com/portfolio/services-and-solutions/learning-services/education-centers/rmed

[16] Fraunhofer Fokus, FUSECO Playground, https://www.fokus.fraunhofer.de/go/en/fokus_testbeds/fuseco_playground

[17] 5G Innovation Centre, University of Surrey, http://www.surrey.ac.uk/5gic

[18] Deutche Telekom testbed, https://www.telekom.com/en/company/special--5g-haus

[19] Assembly Data Systems NFV lab testbed, https://www.assembly.it/

[20] OpenVPN, https://openvpn.net/

[21] OpenBSD, https://www.openbsd.org/

[22] VMware, http://www.vmware.com/

[23] OpenBaton, https://openbaton.github.io/

[24] Zabbix, http://www.zabbix.com/

[25] OpenStack Liberty, https://www.openstack.org/software/liberty/

[26] OpenStack open source cloud computing software, https://www.openstack.org/

[27] PostGreSQL, https://www.postgresql.org/

[28] OpenDaylight, https://www.opendaylight.org/

[29] Open Virtual Switch, http://openvswitch.org/

[30] OpenSDNcore, http://www.opensdncore.org/

[31] Software-Defined Storage, https://www.mirantis.com/software/ceph/

[32] The RDO project Triple-O, https://www.rdoproject.org/tripleo/

[33] OpenStack Heat, https://wiki.openstack.org/wiki/Heat

[34] OpenStack Ironic, https://wiki.openstack.org/wiki/Ironic

[35] Rackspace, www.rackspace.com

[36] NASA, https://www.nasa.gov/

[37] OpenStack Newton, https://www.openstack.org/software/newton/

[38] ETSI MANO specification, http://www.etsi.org/deliver/etsi_gs/NFV-MAN/001_099/001/01.01.01_60/gs_NFV-MAN001v010101p.pdf

List of Acronyms and Abbreviations

Acronym	Meaning
5G	Fifth Generation Mobile Network
API	Application Programming Interface
CC	Cluster Controller
CM	Cluster Member
CPN	Control Plane Node
CPU	Central Processing Unit
ETE	End-to-End
IaaS	Infrastructure as a Service
LTE-A	Long Term Evolution Advanced
MANO	Management and Orchestration
M2M	Machine-to-Machine
NFV	Network Function Virtualisation
NFVO	Network Function Virtualisation Orchestrator
ODL	OpenDaylight
OVS	Open Virtual Switch
PGW	Packet data network Gateway
PoP	Point of Presence
RAN	Radio Access Network
SDN	Software Defined Network
SEM	SoftFIRE Experiment Manager
SGW	Serving Gateway
SSP	SoftFIRE Software Portal
SAN	Storage Area Network
UPN	User Plane Node
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNF	Virtual Network Function
VNFM	Virtual Network Function Manager
VPN	Virtual Private Network

SoftFIRE

Disclaimer

This document contains material, which is the copyright of certain SoftFIRE consortium parties, and may not be reproduced or copied without permission.

The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the SoftFIRE consortium as a whole, nor a certain part of the SoftFIRE consortium, warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, accepting no liability for loss or damage suffered by any person using this information.

SoftFIRE has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement no. 687860.