ETSI GR NFV-TST 004 V1.1.2 (2017-07)

GROUP REPORT

Network Functions Virtualisation (NFV); Testing; Guidelines for Test Plan on Path Implementation through NFVI

Disclaimer

The present document has been produced and approved by the Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference

RGR/NFV-TST004ed112

Keywords

NFV, NFVI, SDN, testing

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Network Functions Virtualisation (NFV).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

There are many technological options available to implement paths through the Network Function Virtualisation Infrastructure (NFVI) to realize Virtual Network Forwarding Graphs (VNFFG) or Service Function Chains (SFC). In the present document, paths can be composed of physical and virtual links (including wide-area network links connecting locations and their NFVI), physical and virtual switches and routers, and other virtual network functions (VNF). VNFs are composed of one or more VNF Components (VNFC). VNFC are synonymous with Virtual Machines (VM) or OS containers (OSC) as in ETSI GS NFV 003 [i.21]. A VM or OSC is referred to with the general term virtualization container in the present document.

The present document is motivated by the design needs of many NFV actors. Service Providers and NFVI Operators need to select the best alternatives in order to implement cost-effective services. NFVI Providers and VNF Providers need to understand the preferred alternatives so they can support them efficiently. What configurations work well in combination, and possibly enhance performance? How can the actors above begin to objectively evaluate the various alternatives? These questions are to be evaluated before NFV deployments, and re-evaluated as new technology alternatives emerge.

The present document recognizes the need to evaluate the various path-implementation alternatives operating together, and begins by providing a high level test plan. Ultimately, the results from tests comparing the alternatives may influence the architectural choices when implementing the NFV framework.

1 Scope

The present document provides guidelines for test plans that assess different approaches to defining SDN Applications, different ways of arranging and federating SDN Controllers, and arrangements of network switching/forwarding functions (both physical and virtual) to create the various path-implementations between and among NS Endpoints and VNFs. These guidelines support development of detailed test plans, and ultimately influence the NFV framework (when testers share their results from testing arrangements encouraged by these guidelines). The test plan guidelines should be sufficiently abstract to include all envisioned possibilities, and will also pursue the details of technologies of interest. Although the primary emphasis of testing is the performance and benchmarking of systems composed of the components above, the attempts to combine different protocols and functions will undoubtedly uncover combinations which are non-interoperable, and these should be noted.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GS NFV-EVE 005 (V1.1.1) (2015-12): "Network Functions Virtualisation (NFV); Ecosystem; Report on SDN Usage in NFV Architectural Framework".

[i.2] IETF RFC 6241(June 2011): "Network Configuration Protocol (NETCONF)".

[i.3] ONOS^{TM}.

NOTE: Available at http://onosproject.org/.

[i.4] OpenDaylight^{TM} .

NOTE: Available at http://www.opendaylight.org/.

[i.5] OpenContrail^{TM}.

NOTE: Available at http://www.opencontrail.org/.

[i.6] Floodlight^{TM}.

NOTE: Available at http://www.projectfloodlight.org/floodlight/.

[i.7] OpenStack$^{TM\ SM}$.

NOTE: Available at https://www.openstack.org/.

[i.8] IETF RFC 4271 (January 2006): "A Border Gateway Protocol 4 (BGP-4)".

[i.9] IETF RFC 5440 (March 2009): "Path Computation Element (PCE) Communication Protocol (PCEP)".

[i.10] OpenFlow ^{SM}.

NOTE: Available at https://www.opennetworking.org/sdn-resources/openflow.

[i.11] P4^{TM} language for programming the network dataplane.

NOTE: Available at http://p4.org/.

[i.12] ETSI GS NFV-INF 003 (V1.1.1) (2014-12): "Network Functions Virtualisation (NFV); Infrastructure; Compute Domain".

[i.13] VLOOP-VNF.

NOTE: Available at https://lists.linuxfoundation.org/pipermail/opnfv-tech-discuss/2015-May/002601.html.

[i.14] IETF RFC 7348 (August 2014): "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks".

[i.15] IETF RFC 7432 (February 2015): "BGP MPLS-Based Ethernet VPN".

[i.16] IETF RFC 1701 (October 1994): "Generic Routing Encapsulation (GRE)".

[i.17] Internet Draft (Work in Progress): "Geneve: Generic Network Virtualization Encapsulation, draft-ietf-nvo3-geneve-04".

[i.18] Internet Draft (Work in Progress): "Network Service Header, draft-ietf-sfc-nsh-11".

[i.19] Internet Draft (Work in Progress): "Benchmarking Methodology for SDN Controller Performance, draft-ietf-bmwg-sdn-controller-benchmark-meth-03".

[i.20] ETSI GS NFV-INF 010 (V1.1.1) (2014-12): "Network Functions Virtualisation (NFV); Service Quality Metrics".

[i.21] ETSI GS NFV 003 (V1.2.1) (2014-12): "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.22] ETSI GS NFV-TST 001 (V1.1.1) (2016-04): "Network Functions Virtualisation (NFV); Pre-deployment Testing; Report on Validation of NFV Environments and Services".

[i.23] IETF RFC 2544 (March 1999): "Benchmarking Methodology for Network Interconnect Devices".

[i.24] IETF RFC 2889 (August 2000): "Benchmarking Methodology for LAN Switching Devices".

[i.25] ETSI GS NFV-IFA 003 (V2.1.1) (2016-04): "Network Functions Virtualisation (NFV); Acceleration Technologies; vSwitch Benchmarking and Acceleration Specification".

[i.26] Internet Draft (Work in Progress): "Benchmarking Virtual Switches in OPNFV, draft-ietf-bmwg-vswitch-opnfv-01".

[i.27] Open Platform for NFV VSPERF Project.

NOTE: Available at https://wiki.opnfv.org/display/vsperf.

[i.28] IETF Benchmarking Methodology Working Group (BMWG).

NOTE: Available at https://datatracker.ietf.org/wg/bmwg/documents/.

[i.29] ETSI GS NFV-PER 001 (V1.1.2) (2014-12): "Network Functions Virtualisation (NFV); NFV Performance & Portability Best Practises".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

path: data communications feature of the system describing the sequence and identity of system components visited by packets, where the components of the path may be either logical or physical

NOTE: Examples of physical components include a physical switch or a network interface of a host, and an example of a logical component is a virtual network switch. Paths may be unidirectional or bi-directional. Paths may be further characterized as data plane or control plane when serving these classes of traffic, and as packet payload-agnostic or payload processing (as in the case of transcoding, compression, or encryption).

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ACL	Access Control List
API	Application Programming Interface
BGP	Broder Gateway Protocol
BMWG	Benchmarking Methodology Working Group
CLI	Command Line Interface
EVPN	Ethernet Virtual Private Network
FUT	Function Under Test
GENEVE	Generic Network Virtualization Encapsulation
GR	Group Report
GRE	Generic Routing Encapsulation
GS	Group specification
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ISG	Industry Specification Group
KVM	Kernel-based Virtual Machine
LTS	Long-Term Stability
MAC	Media Access Control
MB	Mega Bytes
NB	North Bound
NETCONF	Network Configuration Protocol

NOTE: See IETF RFC 6241 [i.2].

NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
NIC	Network Interface Circuit
NS	Network Service
NSD	Network Service Description
NSH	Network Service Header
PCE	Path Computation Element
PCEP	PCE Communication Protocol

NOTE: See IETF RFC 5440 [i.9].

PNF	Physical Network Function
ODL	OpenDayLight
ONOS	Open Network Operating System
OSC	Operating System Container
OSS/BSS	Operation Support System/Business Support System
OSX	Apple Operating System for Mac
OVS	Open vSwitch

RPC	Remote Procedure Call
RTT	Round-Trip Time
SB	South Bound
SDN	Software Defined Network
SFC	Service Function Chains
SUT	System Under Test
VIM	Virtual Infrastructure Manager
VLOOP-VNF	Loopback Virtual Network Function
VM	Virtual Machine
VNF	Virtual Network Function
VNFC	VNF Component
VNFFG	VNF Forwarding Graph
VNFM	VNF Manager
VSPERF	OPNFV vSwitch Performance project
VXLAN	Virtual eXtensible Local Area Network

NOTE: See IETF RFC 7348 [i.14].

4 Test Plan and Approach

This clause outlines the first steps toward conducting a test of path instantiation and path performance.

The plan assumes that many selections of fundamental infrastructure have been made, such as the hardware platforms for compute, memory and storage, and hardware networking aspects such as switches, link technology and speed, and physical Network Interface Circuit (NIC) on each host. The configuration of these devices is a critical factor in their performance, and their parameters should be documented along with the tested technology-specific parameters (item 3 below). In principle, this allows evaluation of hardware alternatives, but this aspect is not emphasized beyond this point (consistent with the scope).

The plan also assumes that testing or benchmarking of individual components will be accessed or conducted in advance, as an aid to the selection of alternatives. After conducting tests according to this plan, it may be useful to re-examine component-level testing with the same or similar stimuli introduced in the path testing if the results are surprising or inconsistent, especially when the current instantiation differs from the benchmarked instantiation in an earlier test or different platform.

In the context of path testing, the System Under Test (SUT) consists of one or more Functions Under Test (FUT) and the network connecting the various FUT to establish the path itself.

The organization wishing to compare various path-implementation alternatives (candidates) and employing the guidance of the present document would build test cases as follows:

1) Determine the set of Functions Under Test (FUT) and the network connectivity that constitutes the path, including the physical arrangement of switches and hosts in each NFVI (and when there are more than one, the links between NFVI), the selected virtualization-layer, the availability of virtual functions and virtual switches, and the arrangement and configuration of SDN controller(s) along with their application-level and resource-level interfaces. The System Under Test (SUT) comprises all these components.

2) Determine the list of candidate data-plane and control-plane protocols and design of overlay networks (such as those given in clause 5).

3) Determine the complete set of configuration parameters required for repeatable results, and the range of configuration settings which the test runs will use to evaluate and compare the candidates.

4) Determine the test device configurations (test stimuli), as well as the metrics and benchmarks the test devices will collect (including intermediate metrics of the path instantiation process and segments of the end-to-end path), in addition to resource utilization reading/logging from the functions under test where appropriate.

5) Arrange to instantiate each combination of parameters, variables, protocols, function arrangements, and verify their operation.

6) Execute the resulting test cases and measure the selected metrics, and record the results.

7) Prepare a clear report of the results, sufficiently detailed to allow repeating the tests at a future date. This will usually include scripts prepared to automate the configuration, instantiation, and testing of the SUT.

When preferred combinations and implementations emerge in the analysis, the testing organization should ensure that the needed management capabilities are consistent with the NFV framework, or suggest how the framework might be modified to accommodate such implementations. The steps to evaluate management capabilities fall under the scope of interoperability testing and are beyond the present document's scope.

5 Taxonomy of Options for SUT

This clause organizes the options for the SUT in several categories, and provides examples of each category for clarity. The categories include Application-Control Interfaces and Protocols, SDN Controller type, Controller Arrangement with controller-controller protocols where necessary, Orchestration interfaces and protocols (direct to the SDN Controller), Resource Control interface(s) and protocols.

Figure 5 of ETSI GS NFV-EVE 005 [i.1] provides an illustration of the SDN controller interfaces, and provides terminology and organization to discuss the many options possible in the SUT.

Function Placement: Each of the functions described in figure 5 of ETSI GS NFV-EVE 005 [i.1] has Placement options in two categories - within the abstract NFV Reference Framework and within the Physical (and logical) resources of the SUT. Both the Framework and Physical placement will have performance implications in one or more of the metrics measured when testing path instantiation and path performance.

SDN Application Type: A control application could take several forms. One is Intent-based networking, where the desired network and VNF connectivity are expressed in a prescriptive manner (and many details are communicated in an abstract way). Another uses an exact description of packet-forwarding path outcome. The controller(s) may apply policies and acquired knowledge of network resources to fulfil the prescribed intent or exact description.

Application-Control interfaces: Sometimes called the "north-bound" (NB) interface of an SDN controller, this interface provides for communication between an SDN Application and the controller(s). Examples of this interface include RESTful APIs, Remote Procedure Call (RPC) interfaces, protocols such as NETCONF [i.2], inter-process communication, and others. The use of clear or secure protocols represents an additional option on this interface. The use of clear or secure protocols represents an additional option on any interface.

SDN Controller type: There are many different types of SDN Controllers available today, each with its own design strengths and features. ONOS [i.3], OpenDayLight® [i.4], OpenContrail [i.5], and FloodLight® [i.6] are a few of the active open-source controller projects. The SDN Controller and the VIM (such as OpenStack [i.7] Nova and Neutron) may both have a role in path setup.

Controller Arrangement and protocols: In some SUT designs, multiple controller entities may share the role of the SDN controller function, as indicated in figure 5 of ETSI GS NFV-EVE 005 [i.1]. The controllers are sometimes described as acting in a cluster, where one controller is the leader and others are followers, each having a partial view of the network resources and the paths under control. The protocols used between controllers (sometimes referred to as the east-west interface) may be provided by BGP IETF RFC 4271 [i.8] or other gateway protocols, plus alternatives such as the Path Computation Element (PCE) Communication Protocol (PCEP) [i.9] or OpenFlow [i.10].

Orchestration interfaces and protocols: This interface may be indirect or direct to the SDN Controller, and may re-use some of the protocols already listed, or other protocols and options yet to emerge.

Resource Control interface(s) and protocols: Sometimes called the SDN Controller Southbound (SB) interface, it provides communication between the controller(s) and the network functions under control, such as hardware switches and virtual switches. A commonly used protocol on this interface is Openflow [i.10], but others approaches are in development, such as the P4 language for programming the network dataplane [i.11]. The use of clear or secure protocols represents an additional set of options on this interface, when combined with the different choices of cypher-suites and acceleration technologies ETSI GS NFV-INF 003 [i.12].

Path Provisioning Models: The Resource Control Protocol may use a proactive or reactive provisioning model (or a combination of both). In the reactive model, flows are created asynchronously when packets arrive at the SDN Resource (switch) and the (first packet in the) flow's disposition is determined through a protocol exchange with the SDN Controller. A proactive model installs the necessary flows in tables at the SDN Resource (switch) before the flows arrive, a process which is usually conducted by the Controller under direction of an SDN Application over the Application-Control Interface.

SDN Resources: Although this plan assumes that many selections of fundamental infrastructure have been made, such as which switches will be implemented in hardware and which as virtual functions, the properties of these functions represent options which should be examined. Hardware networking options such as link technology and speed and physical Network Interface Circuit (NIC) on each host may be variable, along with the range of processing options presented by the resources/switches.

Virtual Network Functions: The path will include VNFs, and the type of VNF employed will determine the type of path testing possible and the applicability of the results. For example, a test VNF that simply returns traffic to the next link of the path/service chain/forwarding graph is one possibility and an open-source VLOOP-VNF is available to simplify performance testing [i.13]. Testing strategies may prefer to employ actual VNFs from the catalogue available to the testing organization, in which case the performance testing should measure the specifics of the network service composed by the path. VNFs implementing an Access Control List (ACL) are an option (see Annex A), although most forms of security-related testing are relegated to follow-on work.

Overlay Networking Technology: There are many options to conceal the end-to-end network addresses of packets and provide local direction and control by encapsulating the packets with new headers. Examples are VXLAN IETF RFC 7348 [i.14], EVPN IETF RFC 7432 [i.15], GRE IETF RFC 1701 [i.16], and GENEVE [i.17]. The use of clear or secure encapsulations represents an additional option for overlay networks. Network Service Header (NSH) [i.18] can be combined with overlay networks, and carries meta-data that can trigger actions that have an effect on performance, so this is another option.

6 Metrics and Methods of Measurement

This clause identifies and describes the key metrics for NFVI path performance, and describes the methods for measuring these metrics based on externally observable events.

There exist methods to characterize individual components of the path implementation architecture, such as SDN Controller benchmarking and virtual switch benchmarking ([i.19] and [i.26]). This clause assumes that individual components and resources in the SUT have been characterized to the extent desired, and that the traffic volumes generated in the tests described here will take the empirical limits discovered in such testing as inputs. For example, Network Resource Discovery (the map of controlled resources and their connectivity is an SDN Controller Benchmark [i.19].

ETSI GS NFV-INF 010 [i.20] provides performance metrics for instantiation of some components of the SUT, such as Virtual Machines and Virtual Network connectivity, as well as the performance of these components. Because the length of VNF instantiation may dominate the other time intervals defined and measured below, this key metric is defined and measured as a precursor to network-related metrics and measurements. The possibility exists to re-use the VNFC s and VNFs when testing different combinations of network technologies and techniques, and this would save considerable time between measurements. Therefore, **VM Provisioning Latency** defined in ETSI GS NFV-INF 010 [i.20] is a separate metric for the SUT, and was intended to be applicable to both VM and OSC instantiation where applicable. However, this metric is re-named **VNFC Instantiation Time** in the present document, to maintain independence from virtualization technology. See the definition of VNF Instance in ETSI GS NFV 003 [i.21], which includes many aspects that could be described as "provisioning".

Among this metric's key input parameters is the size of the image which is to be instantiated as a VNFC. The image size may be directly proportional to instantiation time in some systems. Other factors include the location of the requested image w.r.t. the VNFC instance, network load and host load.

VNFC Instantiation Time Definition: The time interval from the transmission of the request to instantiate the VNFC (to the VIM), to the time that the (remote) communication with the VNFC can be established (and full normal operation can be subsequently confirmed). The example method for measuring this metric is tabulated below.