OPNFV IPv6 compliance test plan

Release draft (e731623)

OPNFV

August 12, 2016

OPNFV IPV6 COMPLIANCE TEST PLAN

1.1 Introduction

The IPv6 compliance test plan outlines the method for testing IPv6 compliance to the OPNFV platform behaviours and features of IPv6 enabled VNFi platforms.

1.1.1 Scope

In this document, and throughout the test suite, the system under test (SUT) is defined as the combination of the VNFi and VIM as defined by the ETSI NVF ISG (need reference).

1.2 Test suite scope and procedures

The IPv6 compliance test suite will evaluate the ability for a NVFi platform and VIM to provide needed IPv6 features and functionality for use as an IPv6 enabled platform.

An IPv6 enabled platform needs to be able to demonstrate the ability to support for instance; the ability to assign IPv6 addresses using SLAAC or stateful and stateless DHCPv6, the ability to securely send a receive IPv6 traffic to an external network, support for multiple address and dual stack interfaces. For a complete list of the test cases refer to the test case specification [2]_.

As the test suite runs as an external entity the system under test includes both the behaviours and interfaces specified for the test. It is expected that the system under test (SUT) interfaces are compliant with the specifications or references supplied in the test case design [1]_ document. In addition the behaviours exhibited by the platform should comply to the referred standards or behaviours as outlined in the test case design [1]_ document.

1.3 Test suite execution

The test suite expects to interact with a system in an IPv6 enabled and ready state. An IPv6 enabled system can be installed using an IPv6 enabled OPNFV scenario, or if you are not using an OPNFV scenario ensure you have configured your system to use IPv6, in this case also pay specific attention to the details of specific test preconditions captured in the test procedure specification [3]_.

The test suite is designed to be run from an external server, the jump host, with access to the control and network interfaces in order that it interacts with the SUT as an external entity. The test suite will be executed by the test suite operator via scripts to be executed on the jump host, or by leveraging the OPNFV infrastructure to execute an IPv6 compliance test job from the jump host. Test cases may instantiate additional workloads on the SUT as part of the test cases being executed, the system shall be returned to it's original state once the test suite has completed.

.._[1]: http://www.opnfv.org .._[2]: http://www.opnfv.org .._[3]: http://www.opnfv.org

IPV6 TEST DESIGN SPECIFICATION

This document outlines the approach and method for testing IPv6 in the OPNFV compliance test suite. Providing a brief outline of the features to be tested, the methodology for testing, schema's and criteria.

2.1 Features to be tested

The IPv6 compliance test plan outlines the method for testing IPv6 compliance to the OPNFV platform behaviours and features of IPv6 enabled VNFi platforms. The specific features to be tested by the IPv6 compliance test suite is outlined in the following table.

Features / Requirements	Tests available	Test Cases
All topologies work in a multi-tenant environment	No	
IPv6 VM to VM only	No	
IPv6 external L2 VLAN directly attached to a VM	No	

IPv6 subnet routed via L3 agent to an external IPv6 network
  1. Both VLAN and overlay (e.g. GRE, VXLAN) subnet attached to VMs;
  2. Must be able to support multiple L3 agents for a given external network to support scaling (neutron scheduler to assign vRouters to the L3 agents)
	No	

Ability for a NIC to support both IPv4 and IPv6 (dual stack) address.
  1. VM with a single interface associated with a network, which is then associated with two subnets.
  2. VM with two different interfaces associated with two different networks and two different subnets.
	No	

Support IPv6 Address assignment modes.
  1. SLAAC
  2. DHCPv6 Stateless
  3. DHCPv6 Stateful
	No	

Ability to create a port on an IPv6 DHCPv6 Stateful subnet and assign a specific IPv6 address to the port and have it taken out of the DHCP address pool.	No	
Full support for IPv6 matching (i.e., IPv6, ICMPv6, TCP, UDP) in security groups. Ability to control and manage all IPv6 security group capabilities via Neutron/Nova API (REST and CLI) as well as via Horizon.	No	
During network/subnet/router create, there should be an option to allow user to specify the type of address management they would like. This includes all options including those low priority if implemented (e.g., toggle on/off router and address prefix advertisements); It must be supported via Neutron API (REST and CLI) as well as via Horizon	No	
Security groups anti-spoofing: Prevent VM from using a source IPv6/MAC address which is not assigned to the VM	No	
Protect tenant and provider network	No	

2.2 Test approach for IPv6

The most common approach for testing IPv6 capabilities in the test suite is through interaction with the SUT control plane. In this instance the test framework will exercise the NBI provided by the VIM to configure and leverage IPv6 related features in the platform, instantiate workloads, and invoke behaviours in the platform. The suite may also interact directly with the data plane to exercise platform capabilities and further invoke helper functions on the platform for the same purpose.

2.2.1 Test result analysis

All functional tests in the IPv6 test suite will provide a pass/fail result on completion of the test. In addition test logs and relevant additional information will be provided as part of the test log, available on test suite completion.

Some tests in the compliance suite measure such metrics as latency and performance. At this time these tests are intended to provide a feature based pass/fail metric not related to system performance. These tests may however provide detailed results of performance and latency in the 'test report'_ document.

2.3 Test identification

TBD: WE need to identify the test naming scheme we will use in DoveTail in order that we can cross reference to the test projects and maintain our suite effectively. This naming scheme needs to be externally relevant to non-OPNFV consumers and as such some consideration is required on the selection.

2.4 Pass Fail Criteria

This section requires some further work with the test teams to identify how and where we generate, store and provide results.