# A.1 NFV ISG PoC Proposal

## A.1.1 PoC Team Members

Include additional manufacturers, operators or labs should additional roles apply.

PoC Project Name: network function acceleration with resource orchestration

Network Operators/ Service Providers: BT Contact: Milind Bhagwat (milind.2.bhagwat@bt.com)

Network Operators/ Service Providers: China Telecom Contact: Yunpeng Xie (xieyp@ctbri.com.cn)

Manufacturer A: Huawei Contact: Jinwei Xia (xiajinwei@huawei.com)

Manufacturer B: Intel Contact: Abdel Rabi (abdel.rabi@intel.com)

Manufacturer C: Cavium Contact: Kin-Yip Liu (Kin-Yip.Liu@cavium.com)

## A.1.2 PoC Project Goals

PoC # 21 successfully demonstrates the usage of hardware acceleration in the NFV infrastructure can provide higher performances for the network and compute intensive functions compa­red to the same functions without acceleration. However, the accelerators are statically pre-configured to these requesting functions without dynamic resource allocation mechanism involvement. This succeeding PoC further incorporates the usage of management API to involve MANO in the acceleration resources management for the requesting functions.

The PoC will take over the Service Function Chaining (SFC) acceleration which was expected in PoC#21 but was cancelled finally.

The PoC will also demonstrate how to utilize a set of abstracted interfaces to meet VNF portability requirements. Moreover, a universal API that is self-adaptive to different network functions will be demonstrated as well.

The project goals are the following:

* PoC Project Goal #1: Demonstrate the dynamic acceleration resource management used in NFV hardware acceleration environment.
* PoC Project Goal #2: Demonstrate the service chain acceleration based on the VNF Forwarding Graphs use case.
* PoC Project Goal #3: Demonstrate the APIs used to decouple the VNF software with underlying accelerators to meet VNF portability.

## A.1.3 PoC Demonstration

* Venue for the demonstration of the PoC: 1, Lab in Huawei UK Institute which provides the doors open day for public; 2, Another exact venue to be confirmed but targeting NFV World Congress 2017

## A.1.5 PoC Project Timeline

* What is the PoC start date? 21st Nov 2016
* Demonstration target date:
* Scenario 1 21st March 2017
* Scenario 2 21st June 2017
* Scenario 3 21st Sep 2017
* PoC Report target date 15th Oct 2017
* When is the PoC considered completed?
* Stage 1: when the scenario 1 is demonstrated and a stage report for it is made available
* Stage 2: when the scenario 2 is demonstrated and a stage report for it is made available
* Stage 3: when the scenario 3 is demonstrated and a comprehensive NFV ISG POC report for it is made available

# A.2 NFV PoC Technical Details

## A.2.1 PoC Overview

This PoC focuses on the hardware acceleration in the NFV Infrastructure with dynamic acceleration resources management, demonstrating the benefits of using management API to enable MANO to manage acceleration resources for the requesting virtual network functions.

Furthermore, this PoC demonstrates the VNF portability achievement using a set of common APIs or a universal API between VNF and NFV Infrastructure.

Figure 1 indicates the PoC project and its building blocks:

Figure 1: PoC project and its building blocks

In this PoC, MANO is added to demonstrate how the acceleration resources are managed, allocated and released to the VNFs during the life cycle of the VNFs and accelerators. In addition, the accelerators will periodically (or on demand) report their latest status to the MANO.

Figure 2 indicates the basic workflows of VNF acceleration with MANO system involvement.

Figure 2: Basic workflows of VNF acceleration with MANO system

We reuse and extend the open source code developed in Openstack to realize management aspect of the PoC. In addition, the accelerators are high-end enough to support reprogramming and hence allow MANO to adjust its resources to different VNFs based on their different acceleration requirements.

Figure 3 indicates the mapping of PoC functional entities on the ETSI NFV Architecture.

Figure 3: PoC functional entities mapping on the ETSI NFV architecture

## A.2.2 PoC Scenarios

The high level scenario(s) that will be demonstrated are:

**Scenario 1 - vIPSec session setup acceleration using look-aside accelerator**

The IPSec protocol suite compasses two phases – cryptograph exchange and traffic encryption. The first phase occurs during the user authentication and IPSec session setup process, which involves complex CPU calculation and consumes significant CPU resources, and therefore has a performance impact on the session setup rate. The second phase involves the encryption and verification of traffic running through the IPSec tunnel, which involves a large amount of packets processing per second, and therefore has a performance impact on the overall throughput performance.

This scenario aims to accelerate the first phase, i.e., vIPSec cryptograph exchange.

The scenario is using a look aside accelerator card to accelerate the session setup operation. The look aside accelerator card receives the acceleration command from IPSec VNF and then returns the operation results.

Figure 4 indicates the logical test setup of vIPSec session setup acceleration.

*Figure 4: IPSec session setup look-aside acceleration*

**Scenario 2 - vIPSec Traffic acceleration on accelerator NIC**

The scenario is using an in-line accelerator card to accelerate the IPSec traffic procedure. It means that traffic encryption and decryption are processed by the accelerator card. IPSec session setup is performed by the host processor. For traffic receive direction, the accelerator card receives IPSec encrypted data from the network, and executes the IPSec traffic processing. The IPSec traffic processing includes SA (security association) lookup, various checks like anti-replay check, and decryption of the data. The accelerator card then transmits the decrypted data to the host CPU. For traffic transmit direction, the host CPU sends unencrypted data to the accelerator card, which performs IPSec encryption and sends the encrypted data out to the network. In addition, the accelerator NIC provides SR-IOV VFs (virtual functions) for individual VMs (virtual machines) running on the server for direct management like configuration of security associations and keys, as well as communicating data directly between the VMs and the accelerator NIC.

Figure 5 indicates the logical test setup of vIPSec traffic acceleration.

*Figure 5: IPSec traffic in-line acceleration*

**Scenario 3 - vBNG data plane offloading to accelerator NIC**

Network intensive function is one kind of function which usually process a large of number of packets and bytes per second whereas involve some static and relatively small CPU code, such as L3 Forwarding, VxLAN and QoS.

This scenario aims to demonstrate network intensive acceleration using virtual Broadband Network Gateway (vBNG) as VNF. vBNG is a popular network function that includes a set of typical network intensive function components, such as L3 Forwarding, VxLAN, QoS etc. This PoC keeps vBNG’s control plane block on X86 and offload its data plane block on accelerator NIC. The control plane will use an abstract forwarding model to instruct the accelerator NIC to process the data plane, for example, adding/updating/deleting entries to the match + action tables and setting the order of these tables maintained on the accelerator NIC. The forwarding graph of vBNG is used here to ensure all traffic goes through the accelerator NIC.

Figure 6 indicates the logical test setup of vBNG offloading acceleration.

*Figure 6: vBNG offloading acceleration*

**Scenario 4 - vCPE acceleration**

Scenario 4 focuses on service-function-chained vCPE applications for both customer site and NFVI data centre scenarios. A number of telcos are deploying vCPE solution for their customers. Typically, vCPE solutions include multiple vCPE VNFs, e.g. vFirewall, vRouter, etc. In addition, it is essential to be able to preserve the CPU cycles of the server for processing the vCPE VNFs, as opposed to infrastructure processing like vSwitching (e.g. OVS [OVS]) and service function chaining (e.g. NSH protocol processing [NSH]). For the customer site scenario, the vCPE systemtypically supports all the targeted VNFs on the same system. Even for the NFVI data centre scenario, where vCPE applications are processed in a central office or cloud data centre, it is still desirable to support as many service-function-chained VNFs as possible or as much subscriber traffic as possible on the same server. This is because if the service-function-chained VNFs are processed on the same server, the overall latencies are improved. With more of the CPU cycles of the server freed up for processing VNFs, the server can support more VNFs for better latencies and more traffic for better compute density. In this PoC scenario, we will explore potential optimisations for performing VNF service chains by offloading service function chaining and vSwitching, i.e. OVS+NSH to an accelerator NIC.

Figure 7 shows the non-accelerated traffic flow. Specifically, traffic coming into the server is classified into the relevant service chain, and goes through OVS+NSH processing to be vSwitched to the first VNF, vFirewall in the diagram. After going through vFirewall processing, the packet traffic goes through OVS+NSH again, and is then vSwitched to the second VNF on the chain, vRouter in the diagram. After going through vRouter, the packet traffic goes through OVS+NSH one more time. This time, OVS+NSH figures that there is no more VNF in the service chain which is running on the same server. As such, the packet traffic is transmitted out of the server. In this example, the total processing on the server includes going through OVS+NSH processing 3 times, plus the VNF processing of vFirewall and vRouter.

*Figure 7: non-accelerated service-function-chained vCPE*

Figure 8 shows the accelerated traffic flow. In this scenario, OVS+NSH processing is offloaded to an accelerator NIC. The accelerator NIC receives the packet traffic for the server, and processes OVS+NSH as well. The OVS+NSH processing results in forwarding the packet traffic to the first VNF, vFirewall in the diagram, directly using SR-IOV interface to bypass the hypervisor. After going through vFirewall, the packet traffic goes to the accelerator NIC for OVS+NSH processing, and is then forwarded to the second VNF, vRouter in the diagram, directly using SR-IOV interface. After going through vRouter, the packet traffic goes to the accelerator NIC for OVS+NSH processing. Given that there is no more VNF on the service chain, the packet traffic is then directly sent out from the accelerator NIC. In comparison with the non-accelerated flow, the 3x OVS+NSH processing overhead is offloaded from the server by using an accelerator NIC for OVS+NSH offload. The equivalent processing bandwidth for 3x OVS+NSH can be utilized to support more VNF processing on this server.

*Figure 8: accelerated service-function-chained vCPE*

**Demo layout for scenario 1 & 2 & 3 & 4**

The demo layout consists of two servers providing vIPSec, vBNG and vCPE software from Huawei and Cavium (server 1is standard COTS and server 2 is accelerated, it aims to justify MANO’s role for choosing the appropriate server to meet the VNF resource requirements), one normal NIC (*Huawei 82559*), two accelerator NICs (*Altera Stratix V and Cavium LiquidIO NIC*), one normal switch (*Huawei Cloud Engine 6850*), one server providing Openstack management, one tester (Ixia), one user client, one ISP server and one GUI used to indicate the performance of VNF and resource status of accelerator NICs as shown in Figure 9.

Figure 9: PoC layout

First, we will take a baseline test with software-only solution running on the standard server 1. Next, we will test accelerated solutions provided by vendors and compare their performance to the baseline value on the server 2.

## A.2.3 Mapping to NFV ISG Work

Describe how this PoC relates to the NFV ISG work:

1. Specify below the most relevantNFV ISG end-to-end concept from the NFV Use Cases [2], Requirements [3], and Architectural Framework functional blocks or reference points [4] addressed by the different PoC scenarios:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Use Case** | **Requirement** | **E2E Arch** | **Comments** |
| **Scenario 1&2&3** |  | *Perf.3* |  | *Accelerator collects the performance related information regarding the usage of acceleration resources by VNF;* |
| **Scenario 1&2&3** |  | *Perf.4* |  | *Accelerator collects the performance related information regarding the resource usage at the accelerator level;* |
| **Scenario 4** | Use Case #4  Use Case #2 |  |  | Service chaining aspects of the VNF Forwarding Graph  Virtualization of the CPE use case. |
|  |  |  |  |  |

1. If this PoC intends to solve or validate any challenge or ongoing work in NFV ISG Work Items, complete the table below:

|  |  |  |
| --- | --- | --- |
|  | **Work Items** | **Comments** |
| **Scenario 1** | *NFV-IFA 002ed221* | *This scenario is intended to validate and/or complete the VNF Interface* |
| **Scenario 2** | *NFV-IFA 018* | *This scenario is intended to validate and/or complete the Network Acceleration Interface* |
| **Scenario 1&2&3** | *NFV-IFA 019* | *This scenario is intended to validate and/or complete the Acceleration Resource Management Interface* |
|  | TST NWI on Metrics if approved |  |

## A.2.4 PoC Success Criteria

This PoC will be considered successful when these scenarios have been successfully implemented and demonstrated.

Functional Success Criteria:

* Be able to accelerate vIPSec cryptograph operation on the accelerator NIC.
* Be able to perform vBNG data plane offloading on the accelerator NIC. The vBNG control plane running on the server control the traffic running on the accelerator NIC via a set of common APIs or a universal API.
* Be able to perform vCPE acceleration on the accelerator NIC. The traffic forwarding and service function chain of vCPE are offloaded on the accelerator NIC.
* MANO system is able to find and allocate acceleration resource to the requesting VNFs based on their acceleration requirements.

Performance Success Criteria:

* Measuring the performance in terms of IPSec session setup rate (session/sec) for the vIPSec cryptograph with and without function acceleration, comparing the measure results and justifying the performance improvement via acceleration.
* Measuring the performance in terms of throughput (bps) for the vBNG and vCPE traffic with and without function acceleration, comparing the measure results and justifying the performance improvement via acceleration.
* Measuring the efficiency in terms of CPU usage percent for the vIPSec, vBNG and vCPE with and without function acceleration, comparing the measure results and justifying the power/space/cost saving via acceleration.

## A.2.5 Expected PoC Contribution

One of the intended goals of the NFV PoC activity is to support the various groups within the NFV ISG. The PoC Team is therefore expected to submit contributions relevant to the NFV ISG work items as a result of their PoC Project.

List of contributions towards specific NFV ISG WIs expected to result from the PoC Project:

PoC Project Contribution #1: IPSec, VxLAN, QoS API contributions for NFV acceleration data model WI(s) in NFV stage 3

#### References

[OVS] Open vSwitch <http://openvswitch.org/>

[NSH] Network Service Header <https://tools.ietf.org/html/draft-ietf-sfc-nsh-10>

IFA001 – Acceleration Overview & use Cases

IFA002 – VNF acceleration interface specifications

IFA003 – vSwitch requirements

IFA004 – Acceleration Management Aspects

IFA018 –Network Acceleration Interface

IFA019 –Resource Management Acceleration