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: Scalable Service Chaining Technology for Flexible Use of Network Functions

- Network Operators/ Service Providers:
  NTT   Contact: Konomi Mochizuki (mochizuki.konomi@lab.ntt.co.jp)
                                                  Shunsuke Homma (homma.shunsuke@lab.ntt.co.jp)
                                                  Hiroshi Waki (waki.hiroshi@lab.ntt.co.jp)

- Manufacturer A: ALAXALA Networks   Contact: Shinsuke Suzuki (suz@alaxala.net)
                                                  Toshiyuki Kubo (toshiyuki.kubo@alaxala.com)
                                                  Yuki Yamashita (yuki.yamashita@alaxala.com)

- Manufacturer B: Hitachi   Contact: Junnosuke Wakai (junnosuke.wakai.gq@hitachi.com)
                                                  Ryoji Furuhashi (ryoji.furuhashi.pd@hitachi.com)
                                                  Michitaka Okuno (michitaka.okuno.nc@hitachi.com)

- Manufacturer C: Cisco Systems   Contact: Satoshi Ogata (sogata@cisco.com)
                                                  Hiroyuki Sugano (hsugano@cisco.com)
                                                  Yoshiki Yamada (yoyamada@cisco.com)

- Manufacturer D: NEC   Contact: Junichi Yano (j-yano@ce.jp.nec.com)
                                                  Hiroshi Dempo (dem@ah.jp.nec.com)

- Manufacturer E: Alcatel-Lucent   Contact: Roy Aoki (roy.aoki@alcatel-lucent.com)

A.1.2 PoC Project Goals

- PoC Project Goal #1: The PoC will verify that Service Function Chaining (SFC) is effective to implement the VNF Forwarding Graph. Also, by using functions for SFC provided by several vendors, we will verify the interoperability of SFC. Here, SFC is currently being standardized in IETF, as a method to perform packet forwarding for service chaining using SFC encapsulation.

- PoC Project Goal #2: This PoC will verify that flexible use of the network function is possible by using VNF Forwarding Graph with SFC.

A.1.3 PoC Demonstration

- Venue for the demonstration of the PoC: NTT Musashino R&D Center (Tokyo, Japan)

A.1.4 Publication

- What would be the publication channel(s) for the PoC.   Public demonstrations at NTT R&D Forum 2015

- What would be the planned publication date(s)?   February 19-20, 2015

- URLs where applicable: The abstract of our PoC may be shown at URL:
  http://labevent.ecl.ntt.co.jp/forum2015/e/index.html

A.1.5　PoC Project Timeline

- What is the PoC start date?　　　　　　　　December 3, 2014 (Already underway)

- (First) Demonstration target date　　　　　February 19, 2015

- PoC Report target date　　　　　　　　　March 31, 2015

- When is the PoC considered completed?　　March 31, 2015

A.2　　NFV PoC Technical Details

A.2.1　PoC Overview

In this PoC, we demonstrate that the Network Forwarding Path of the VNF Forwarding Graph can be formed using SFC. SFC is one of the packet forwarding methods for service chaining, and standardization of SFC is underway in IETF SFC WG. The PoC related service chaining, PoC#2: Service Chaining for NW Function Selection in Carrier Networks, demonstrated the concept of service chaining. In contrast, this PoC demonstrates the packet forwarding method to implement the VNF Forwarding Graph using a new method that is currently being standardized in IETF (reference: Service Function Chaining (SFC) Architecture, draft-ietf-sfc-architecture-04). From this point, using the term in SFC, network function is referred to as Service Function (SF).

Figure 1 illustrates the basic concept of SFC. A Classifier is placed at the starting point of the chain and it determines the service to be applied to the flow. Here, "service" refers to the type of SFs and the order in which the flow passes through them. Then, the Classifier attaches an SFC header identifying the service to the packet. A Service Function Forwarder (SFF) placed in the network refers to the SFC header and determines the SF as a destination. An SFC Proxy is placed between the SFF and the SFC-unaware SF. Since the existing legacy SF is not compatible with the SFC encapsulation, the SFC proxy is necessary for removing the SFC header just before the packet reaches the SF and is necessary for reattaching the SFC header just after the packet is output from the SF. The SFC proxy may be implemented in the physical server or may be implemented as a software application. SFC Controller manages the Classifier and SFF, and updates these tables. In the functional blocks of NFV, SFC Controller may be included in the Virtualised Infrastructure Manager (VIM).

In SFC, since the number of entries in the table held by the SFF is only the number of combinations of service, this method is superior in terms of scalability. In addition, SFC allows separation of the SF management from the network management, and enables the management of total network to be simpler. By simply rewriting the SFC header of the flow in the Classifier, it is possible to change the applied service. In this case, no special setting change is required in the existing network layer, and the SFF may forward the packet to the appropriate devices or VNFs on the basis of the newly attached SFC header. In this PoC, we demonstrate the change in the chain route that occurs by replacing the SFC header, and we show the flexible use of the SFs.

Figure 2 shows the network environment in this PoC. Edge Routers serve as a Classifier for the upstream traffic, and the Gateway Router serves as a Classifier for the downstream traffic. Four functions for SFC (Classifier, SFF, SFC Proxy, and SFC Controller) are implemented by several companies as follows, and we verify the interoperability.

Classifier: ALAXALA Networks, Hitachi, Cisco Systems, NEC, and Alcatel-Lucent

SFF: NTT, ALAXALA Networks, Hitachi, Cisco Systems, and NEC

SFC Proxy: NTT, ALAXALA Networks, Hitachi, Cisco Systems, and NEC

SFC Controller: NTT

In this demonstration, the Network Service Header (NSH) is used as the SFC header. The NSH is one of the SFC header formats that have been proposed in IETF. The examples of SFs used are Traffic Monitor (TM), Traffic

Analyzer (TA), Firewall (FW), Deep Packet Inspection (DPI), Video Optimizer (VO), and WAN accelerator (WAC).
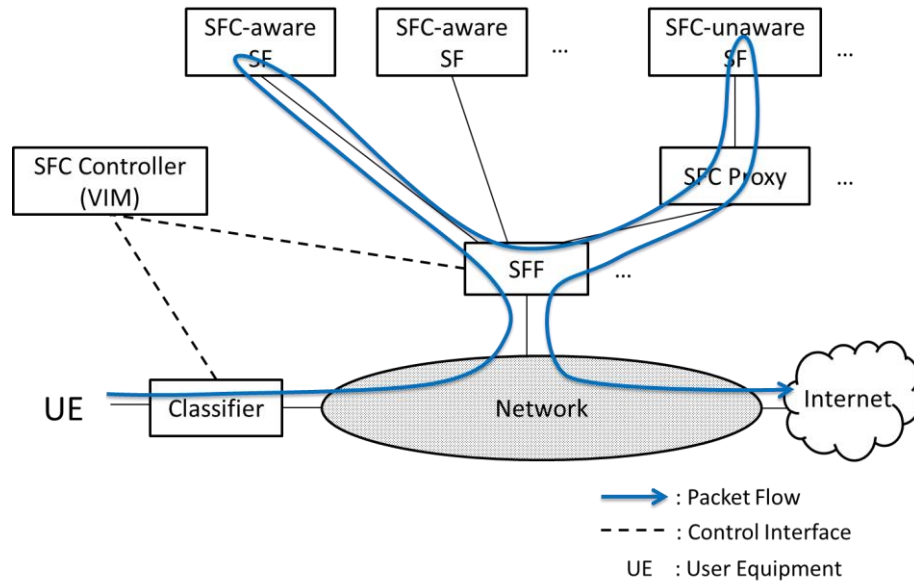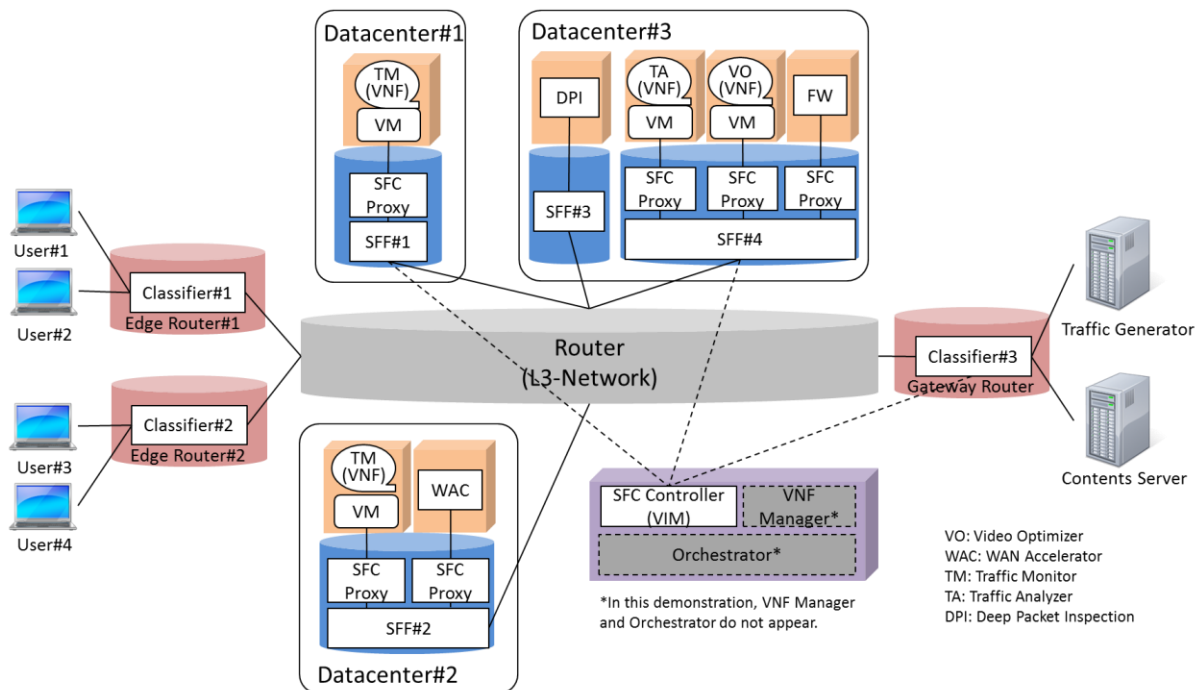

Figure 1. Service chaining with SFC.

Figure 2. Network environment of our PoC.

In Figure 3, the elements of this PoC are mapped to NFV architectural framework. TM, TA and VO are provided as VNF. WAC, DPI, and FW are provided as physical network functions. These SFs are distributed across multiple NFVI. Classifiers, SFFs and SFC Proxies are mapped to NFVI, because they provide connectivity between NFVI which spans across several locations. SFC Controller is mapped to one of the functions of VIM. SFC Controller controls the identification rules of Classifiers and the routing table of SFs centrally. Therefore, SDN controller may be used as SFC Controller. In this PoC, VNF Manager and Orchestrator do not be used, but SFC Controller will need cooperation with VNF Manager. For example, when new VNF is added, the route tables in SFFs require to be changed. In this case, VNF Manager notifies SFC Controller of the addition of NFV, and then SFC Controller sets a new route table in each SFF.
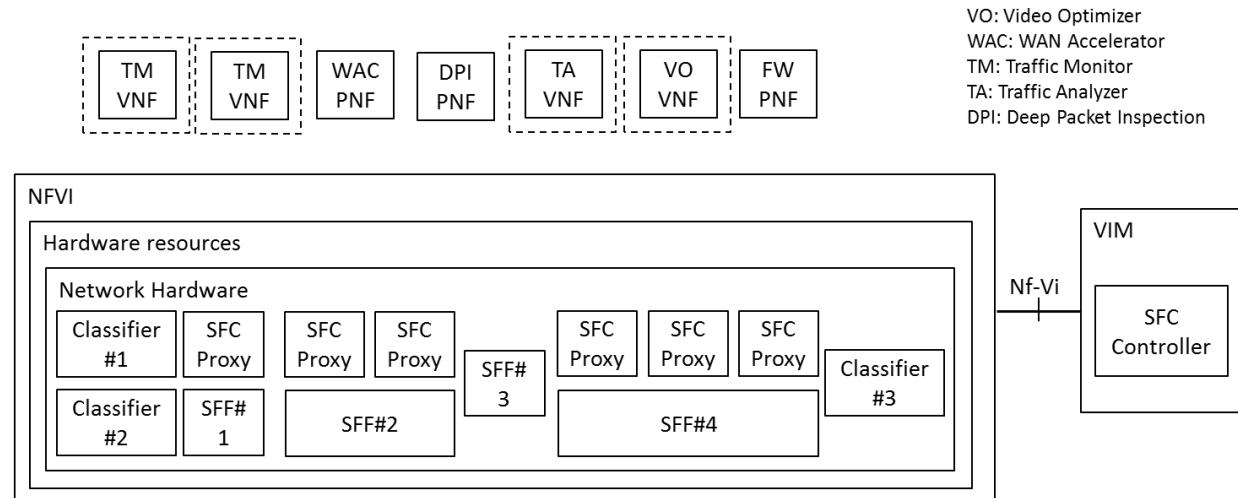
VO: Video Optimizer
WAC: WAN Accelerator
TM: Traffic Monitor
TA: Traffic Analyzer
DPI: Deep Packet Inspection

Figure 3. PoC architecture mapped to NFV architectural framework

A.2.2   PoC Scenarios

- Scenario 1 - Change of chain by replacement of SFC header

In this scenario, we show that it is possible to change the chain simply by replacing the SFC header, using a security service as an example. Figure 4 shows an overview of this scenario. In the initial state, the chain passing through only the TM is set to download traffic to User #1. When the operator detects an abnormality in the TM, the operator instructs the SFC Controller to change the chain. Then, the SFC Controller instructs the Gateway Router to change the chain for download traffic to User #1. As a result, the traffic passes through the TA. When the attack traffic is identified by the TA, the SFC Controller instructs the Gateway Router to change the chain for the attack traffic again. The attack traffic passes through the FW and is blocked. With SFC, it is possible to change the chain by only changing the configuration in the Classifier, and to perform stepwise analysis.
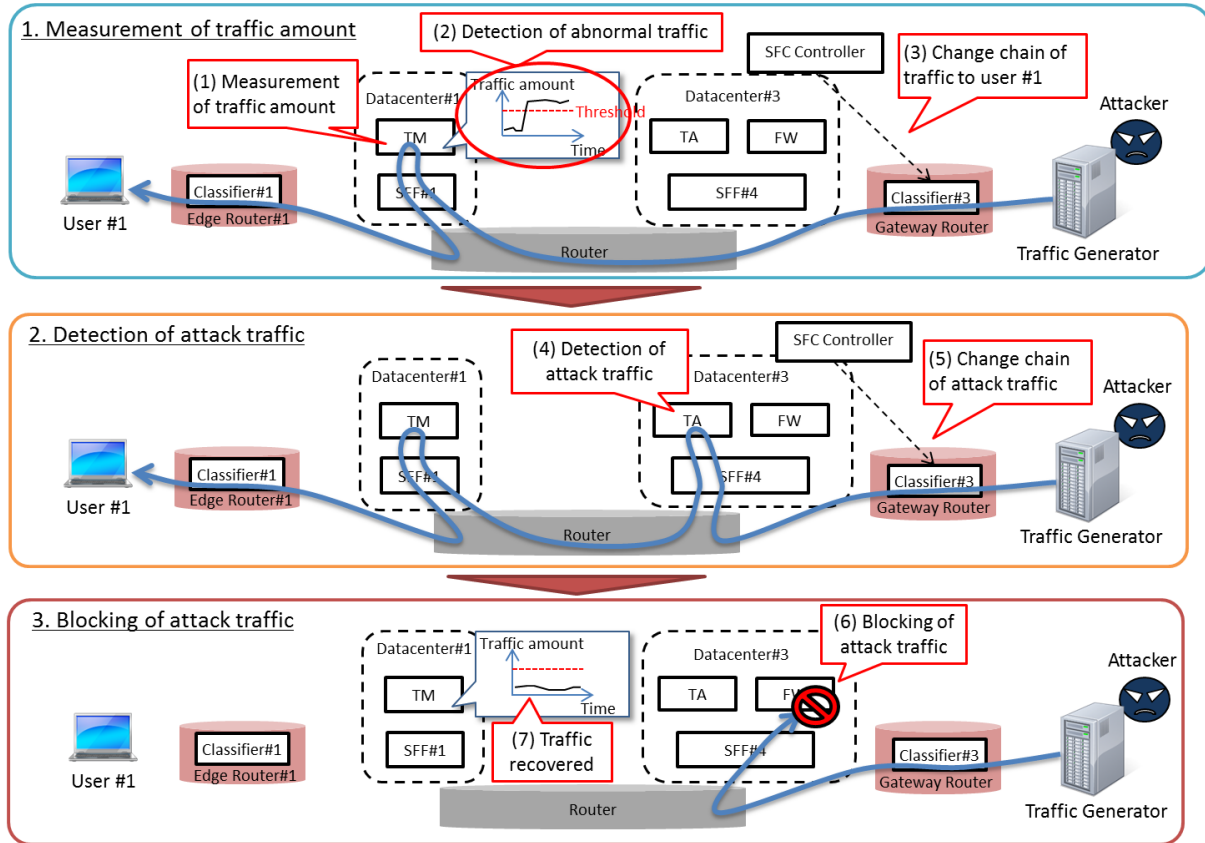
Figure 4. Scenario 1.

- Scenario 2 - Reclassification based on the result of processing on the applications

In this scenario, we show the chain branching according to the DPI analysis result, using a content delivery service as an example. Figure 5 illustrates this scenario. If a SF is applied to certain traffic that is identified by DPI, reclassification is performed in the DPI. Since the cost will increase if DPI handles all traffic, the Edge Router or the Gateway Router in which all traffic passes performs discrimination of applied functions based on user's service plan. In this scenario, these routers determine whether or not to pass traffic through the WAC. DPI reclassifies the traffic based on the traffic type. In this scenario, DPI determines whether or not to pass traffic through the VO. The traffic of users who subscribe to the optimization service passes through the WAC, and only the video traffic of these users passes through the VO.
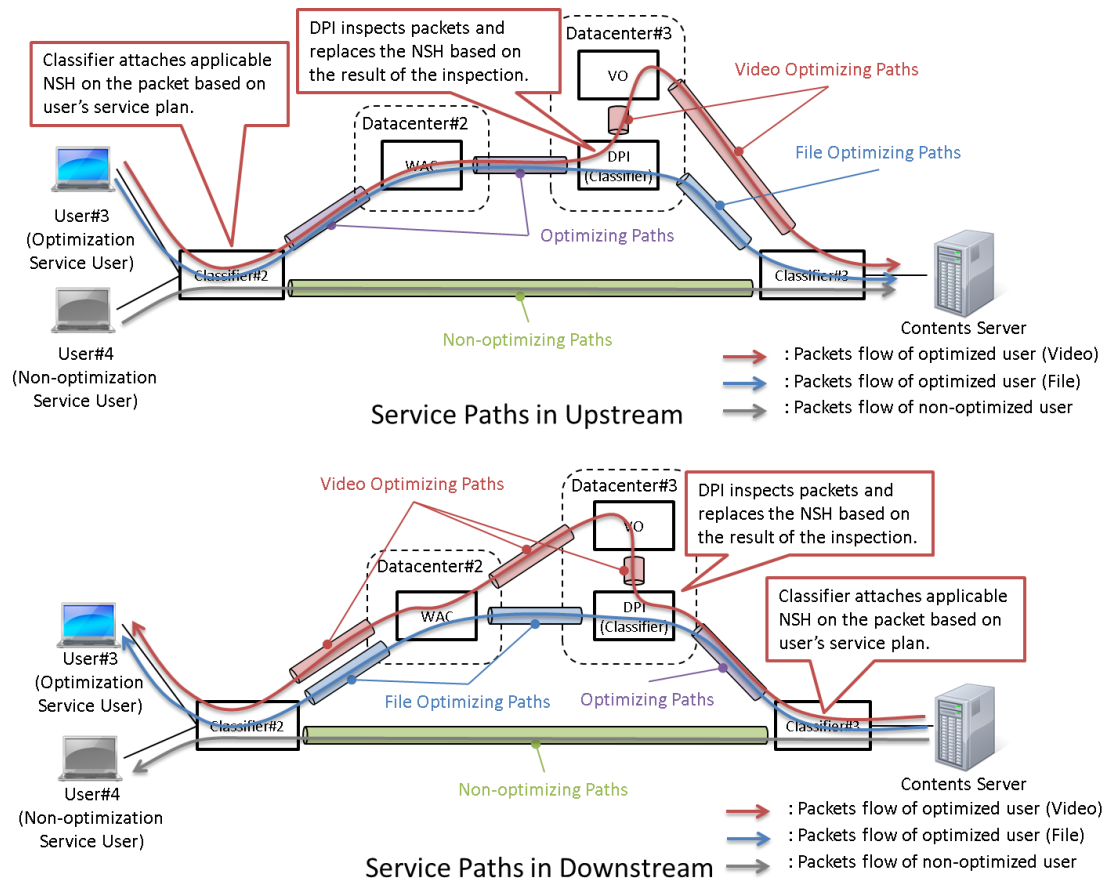
Figure 5. Scenario 2.

- Scenario 3 – Redundancy of chain

In this scenario, we demonstrate how to achieve redundancy in the service (or chain) unit in preparation for a large-scale failure after a serious disaster. Figure 6 shows an image of this scenario. The SFC Controller monitors the health of each SFF. When any SFF is down, the SFC Controller issues instructions to switch the path (replace the SFC header) just before the failed SFF. Thus, switching to a redundant chain is achieved.
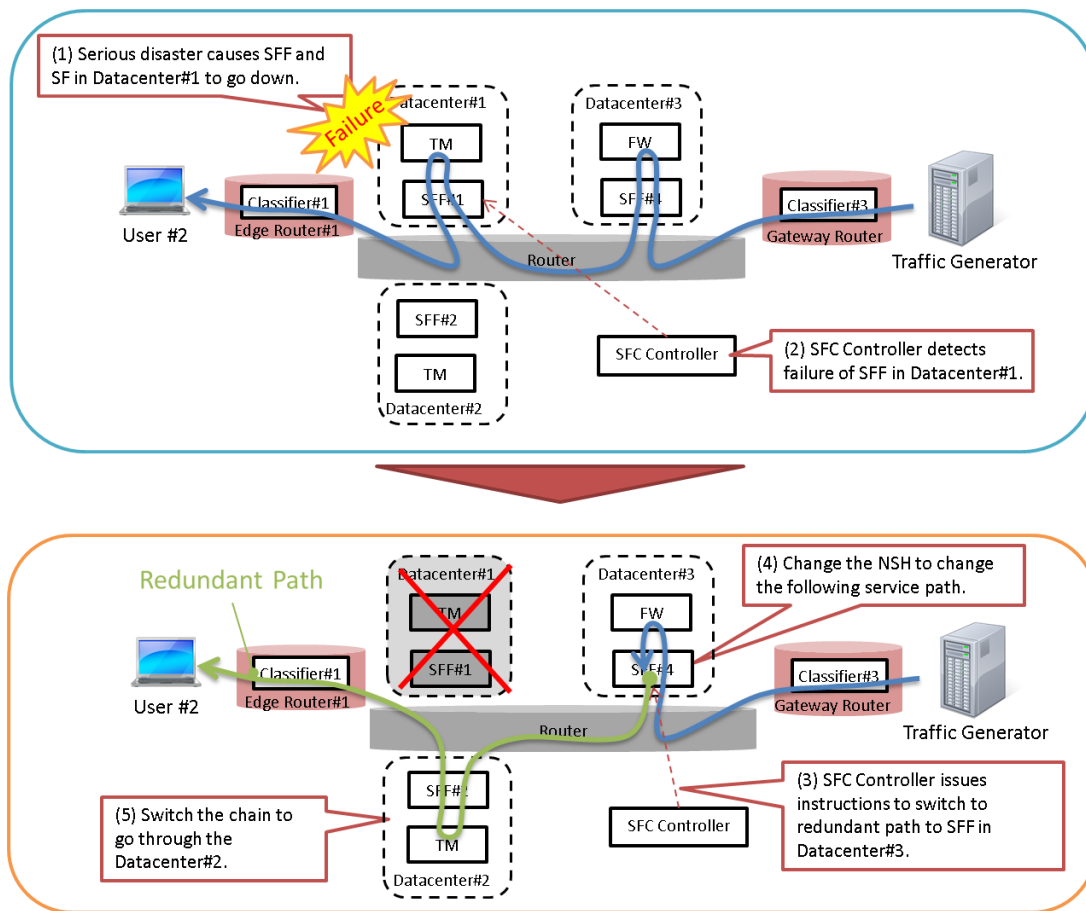
Figure 6. Scenario 3.

A.2.3 Mapping to NFV ISG Work

Describe how this PoC relates to the NFV ISG work:

1) Specify below the most relevant NFV ISG end-to-end concept from the NFV Use Cases , Requirements , and Architectural Framework functional blocks or reference points addressed by the different PoC scenarios:

	Use Case	Requirement	E2E Arch	Comments
Scenario 1	*UC#4* *UC#2*	*Gen.4*	*Service, VNF and Infrastructure Description* *VIM* *Nf-Vi*	*Implementation of service chaining method by VNF Forwarding Graph.* *Realize the switch of Forwarding Graph.*
Scenario 2	*UC#4* *UC#2*	*Gen.4*	*Service, VNF and Infrastructure Description*	*Implementation of service chaining method by VNF Forwarding Graph.* *Realize bifurcation of Forwarding*

			VIM Nf-Vi	Graph..
Scenario 3	*UC#4*	*Res.4*	*Nf-Vi*	*Realize continuity of Forwarding Graph.in failure.*

A.2.4   PoC Success Criteria

In this PoC, the criteria for success are realizing the VNF forwarding graph with the service chaining technology using SFC and verifying that the flow goes through the appropriate SFs in the multi-vendor environment. Other criteria for success are confirming the flexible use of SFs by switching the chain based on an SFC header change, branching the chain based on the processing result of the application, and failure switch-over with chain redundancy.

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: SFC Controller for VNF Forwarding Graph   NFV WI EVE005

This PoC will contribute to NFV WI EVE005. If VNF Forwarding Graph is formed by SFC, SFC Controller may be implemented in SDN Controller. In this case, we will provide the behavior of SDN Controller and the information managed by SDN Controller. One of the information managed by SDN Controller is the routing table held in SFF which is one of the elements of NFVI. This routing table includes the next-hop address corresponding to a SFC header.

- PoC Project Contribution #2: Fail-over of Forwarding Graph   NFV WI REL002

This PoC will contribute to NFV WI REL002. When the failure of VNF occurs, reliability of the VNFs on the Forwarding Graph will be ensured by switching over of the Forwarding Graph. In case that SFC is used for Forwarding Graph, SFC Controller in VIM instructs to SFF to change the routing table. This PoC will demonstrate the procedure of the fail-over of Forwarding Graph.