INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION
STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

**SG11-TD224-R1/GEN**

**STUDY GROUP 11**

**Original: English**

**Question(s):** 4/11 Geneva, 6-15 July 2022

**TD**

**Source:** Editors

**Title:** Consent – draft new Recommendation ITU-T Q.3406 (ex Q.telemetry-VBNS) “Signalling requirements for telemetry of virtual broadband network services” (Geneva, 6-15 July 2022)

**Contact:** Cancan Huang
China Telecom
P.R China
Tel: +862038639366
E-mail: huangcanc@chinatelecom.cn

**Contact:** Ying Cheng
China Unicom
P.R.China
Tel: +861066259394
E-mail:chengying10@chinaunicom.cn

**Abstract:** This document is the output of draft new Recommendation ITU-T Q.3406 (ex Q.telemetry-VBNS) “Signalling requirements for telemetry of virtual broadband network services”. It includes the discussion results in the Q4/11 e-meeting held on 6-15 July 2022.

The following table shows discussion results for input documents.

| Document Number | Source | Title | Meeting results |
|---|---|---|---|
| T22-SG11-C-0033 | China Telecom,<br>China Unicom | Chapter 7 and chapter 8 modification of Q.telemetry-VBNS | Agreed with modification |

# Draft new Recommendation ITU-T Q.3406 (ex Q.telemetry-VBNS)

## Signalling requirements for telemetry of virtual broadband network services

### Summary

This Recommendation specifies the signalling requirements for telemetry of virtual broadband network services, by architecturally adding the dedicated functional component and the corresponding interfaces in NFV framework.

### Keywords

telemetry; virtual broadband network services; signalling requirements

## Table of Contents

# Draft new Recommendation ITU-T Q.3406 (ex Q.telemetry-VBNS)

# Signalling requirements for telemetry of virtual broadband network services

## 1 Scope

The scope of this Recommendation consists of:

– Overview for telemetry of virtual broadband network services;

– Interface Ti.x reference model;

– Signalling procedures for interfaces Ti.x;

– Signalling requirements for interfaces Ti.x.

## 2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.3321] Recommendation ITU-T Y.3321 (2015), Requirements and capability framework for NICE implementation making use of software-defined networking technologies.

## 3 Definitions

### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 service function chain** [b-ITU-T Y-Sup.41]: A chain that defines an ordered set of abstract service functions and ordering constraints that must be applied to packets and/or frames and/or flows selected as a result of classification and/or policy.

**3.1.2 virtualized network function** [ITU-T Y.3321]: A network function whose functional software is decoupled from hardware, and runs on virtual machine(s).

### 3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 **telemetry server**: The centralized server which is responsible for controlling the telemetry services.

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

| | |
|---|---|
| ISDOEV | Integrated Service and Device OAM Evaluation Value |

| | |
|---|---|
| OIAF | OAM Information Acquisition Function |
| OISF | OAM Information Sending Function |
| SFC | Service Function Chain |
| SFF | Service Function Forwarder |
| VNF | Virtualized Network Function |

## 5 Convention

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

In the body of this document and its appendixes, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

{A}: indicates that the parameter A is mandatory;

*: indicates that the parameter may be multiple items.

## 6 Overview

For virtual broadband network services, there are several requirements for OAM in the virtualized environment which cannot be met by the traditional OAM tools.

(1) High data-collection frequency

The conventional OAM technologies, such as SNMP, cannot meet the real-time data collection requirement, especially for the virtual resource, due to its low-frequency pull-based mechanism. The telemetry with push-based mechanism can satisfy the requirement.

(2) Real-time probe deployment

The probe's updating and deploying pace should be in resonance with the pace of virtual service resource changing. The conventional OAM technologies which are developed off-line by specific vendor and installed/uninstalled manually take too much time to catch up with the pace of virtual resource change. By contrast, the telemetry with an open and programmable interface can deploy and activate the probes without the vendors' limitations.

(3) Model-based Integration

Many applications need to collect data from multiple sources (e.g., from distributed nodes or from different network layers). Too many models and formats of data bring difficulties to consolidate the data from multiple sources. Therefore, it is necessary to define the uniformed data model to integrate all the data from different sources. The traditional OAM technologies have proprietary data model for limited objects and obviously cannot meet this requirement. The telemetry with standard model of data can satisfy this requirement.

To conclude, telemetry technologies are playing a very important role in managing virtual broadband network services and are usually implemented in NFV framework. Therefore, it is needed to specify the NFV based telemetry architecture and the signaling requirements for virtual broadband network services.

## 7 The interface Ti.x reference model

The interface Ti.x reference model for the telemetry of virtual broadband network services is shown as below.

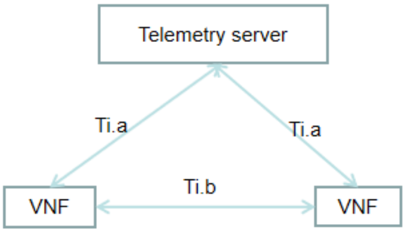


**Figure 7-1 The interface Ti.x reference model for the telemetry of virtual broadband network services**

The telemetry server is responsible for data collection and storage.

The telemetry server collects data through open and programmable interface Ti.a with push-mode.

(1) Interface Ti.a

Interface Ti.a is between telemetry server and VNF. It collects OAM data from VNFs.

(2) Interface Ti.b

Interface Ti.b is between different VNFs. It transfers data packets which carry the OAM request information and collected OAM information between VNFs.

The VNFs could resides in the same protocol domain or different domains.Usually, the inter-domain communication happened in service function chaining service, since there are large number of legacy network functions in the network which cannot support SFC protocol. Correspondingly, the messages exchanged through Ti.b are different based on the locations of VNF pairs.

A) If the VNFs pair is located in the same domain, the interface Ti.b permits the information exchange between different VNFs.

B) If the VNFs pair is located in different domains, there must be a network proxy located between the two VNFs (See Figure 7-2) .

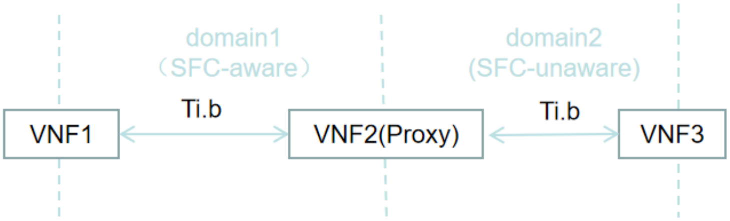


**Figure 7-2 The reference model for Ti.b in inter-domain scenario**

For the interface Ti.b between VNF1 and Proxy(VNF2) in domain 1, the messages exchanged through it is always encapsulated in dedicated packets headers used in domain 1 (e.g., NSH of SFC).;

For the interface Ti.b located in domain 2 between Proxy(VNF2) and VNF3,the messages exchanged through it is always encapsulated in dedicated packets headers used in domain 2 (e.g., IP network);

From the interface Ti.b's perspective, the header selection for message encapsulation and related operation are triggered by the signaling initiator within the pair. For example, for the interface Ti.b in domain 1, the header selection and related operation are decided by VNF1 which is the SFC service initiator within the VNF1-VNF2 pair. Equivalently, for the interface Ti.b in domain 2, the header selection and related operations are decided by proxy which is the IP service initiator within the VNF2-VNF3 pair.

# 8 Signaling procedures for Ti.x

## 8.1 Signaling procedure for Ti.a

Figure 8-1 describes the general signalling procedure between VNF and telemetry server. The information exchange is based on push-mode that the VNF actively pushes the OAM information of itself to the telemetry server. When telemetry server receives the VNF OAM information, it sends an acknowledgement information back to the VNF. Then VNF checks if the information which telemetry server received is correct.

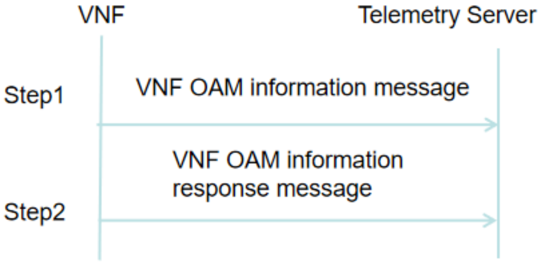


**Figure 8-1 The general telemetry signaling procedure through interface Ti.a**

Step 1: The VNF sends VNF OAM information message to telemetry server.

Step 2: The telemetry server responds to the VNF to acknowledge that the information is received.

One kind of VNF, service function chain, is not a dedicated VNF but an ordered set of VNFs.(e.g. CGN, Firewall, DPI, etc.). In this situation, the "hybrid way" which is depicted in Figure I-1 is used for pushing SFC's OAM information to the telemetry server.

NOTE - Other than hybrid way, there are also "centralized way" and "distributed way" to push the OAM information to telemetry server. Appendix I analyzes the advantages and disadvantages of these three ways.

## 8.2 Signaling procedure for Ti.b in intra-domain telemetry

To fulfill the telemetry, the signaling procedure of the interface Ti.b between VNF1 and VNF2 are depicted in Figure 8-2. In SFC aware domain, the VNF1 is a service function, the VNF2 could be a service function or a SFC proxy within the SFC aware domain.

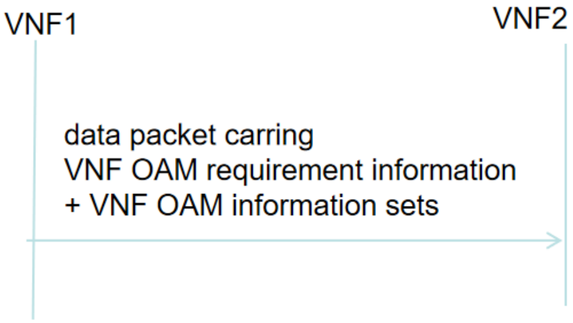


**Figure 8-2 the general telemetry signaling procedure through Ti.b in SFC aware domain**

Figure 8-3 describes the signaling procedure of intra-domain telemetry for SFC service, which is one of the most complicated service scenario. The signaling procedures of intra-domain telemetry for other network services are similar or simpler than SFC scenario and consequently not described in this Recommendation.

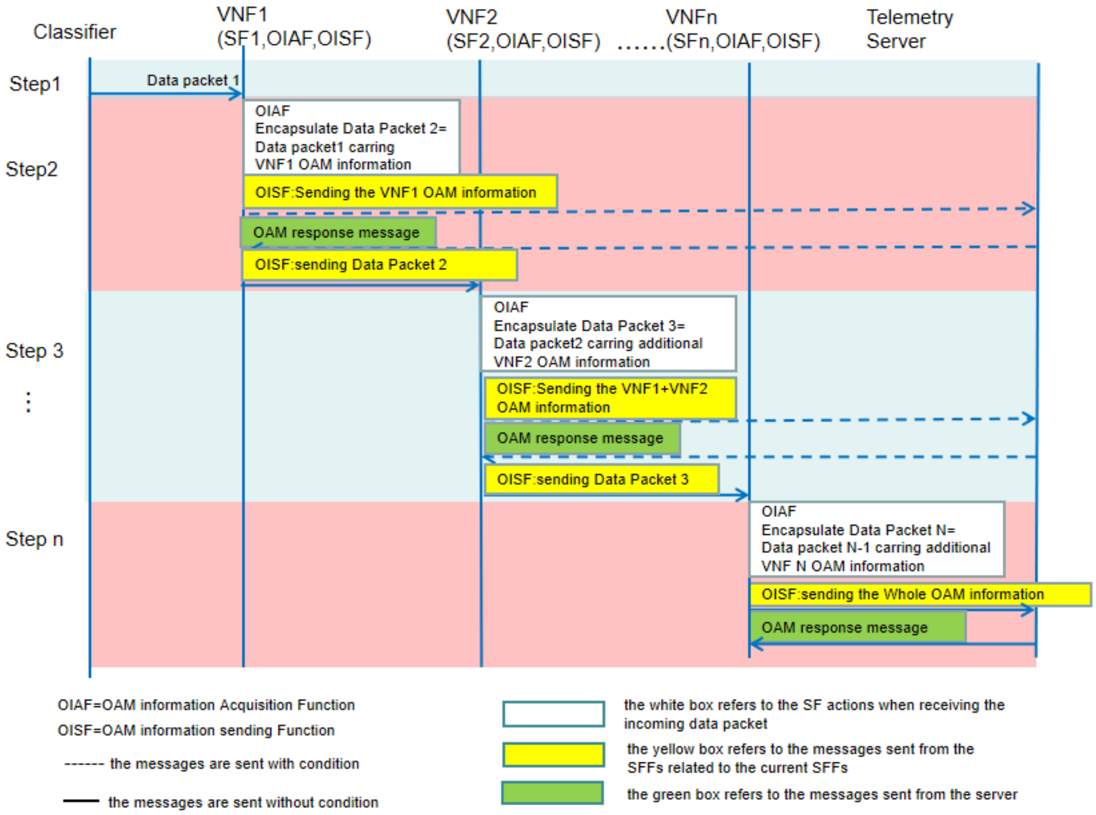

Classifier
VNF1 (SF1,OIAF,OISF)
VNF2 (SF2,OIAF,OISF)
……(SFn,OIAF,OISF)
VNFn
Telemetry Server
Step1
Step2
Step 3
⋮
Step n
Data packet 1
OIAF
Encapsulate Data Packet 2= Data packet1 carring VNF1 OAM information
OISF:Sending the VNF1 OAM information
OAM response message
OISF:sending Data Packet 2
OIAF
Encapsulate Data Packet 3= Data packet2 carring additional VNF2 OAM information
OISF:Sending the VNF1+VNF2 OAM information
OAM response message
OISF:sending Data Packet 3
OIAF
Encapsulate Data Packet N= Data packet N-1 carring additional VNF N OAM information
OISF:sending the Whole OAM information
OAM response message
OIAF=OAM information Acquisition Function
OISF=OAM information sending Function
------ the messages are sent with condition
the messages are sent without condition
the white box refers to the SF actions when receiving the incoming data packet
the yellow box refers to the messages sent from the SFFs related to the current SFFs
the green box refers to the messages sent from the server

**Figure 8-3 The signalling procedure of intra-domain telemetry for SFC service**

**Step1:** The classifier encapsulates the data packet in NSH header to form the original packet 1 and send it to VNF1(SF1).

NOTE 1 – The OAM information identification and programming instructions are included in the NSH header of the packet.

NOTE 2 – The OAM information identification is the label to tell the SF that the data packet carries not only the customer data but also the OAM information along the path.

NOTE 3 – The programming instructions describes the required OAM information which telemetry server needs to collect from the SFs and the OAM evaluation parameter information. The programming instructions include but not limited to:

1) The required OAM information:

a) the classification information of different categories generated by using programming manner.

b) the threshold information of each category.

NOTE – the threshold information may include a set of thresholds of the OAM performance parameters.

c) The relationship information among different OAM categories.

d) The operation for the OAM classification information mentioned above.

NOTE – This required OAM information is applied to both device and service.

2) The OAM evaluation parameter information:

a) The weight of the OAM information of device.

b) The threshold defined for service SLA.

c) The weight of service SLA.

d) The threshold of integrated service and device OAM information.

**Step2：** When the first intermediate SF node (SF1) receives the original data packet 1,

Step2.1: It checks the NSH header and finds the OAM information identification.

NOTE – According to the OAM information identification, SF1 launches the OAM information acquisition Function(OIAF) to select and collect the required OAM information from SF.

Step2.2: It runs the OIAF to collect the SF1's OAM information according to the descriptions of the instructions in the NSH header.

NOTE – The OIAF mechanism and detailed example are described in Annex A.

Step2.3: It runs the OAM information sending function (OISF) to send the OAM information to the telemetry server through different methods depending on integrated service and device OAM evaluation value (ISDOEV) which is calculated based on service OAM information, device OAM information and the OAM evaluation parameter information.

The method is described as below, when the calculated ISDOEV is smaller than the threshold of integrated service and device OAM information.

Step2.3.1: It adds the SF1 OAM information including both of device and service OAM information, which is part of the whole OAM information, to the data packet 1 to form data packet 2.

NOTE – The whole OAM information is composed by multiple VNFs' OAM information which are located in front of the current VNF.

Step2.3.2: The SFF which the SF belongs to transfers the packet 2 to the destination SF.

The method is described as below, when the calculated ISDOEV is larger than or equal to the threshold of integrated service and device OAM information.

Step 2.3.3: the SF sends the dedicated OAM packet carrying OAM information of itself including both of device and service OAM information to the telemetry server.

NOTE – The OISF mechanism is described in Annex B.

**Step3：** When the second SF node SF2 receives the data packet 2,

Step3.1: It checks the NSH header and finds the OAM information identification.

Step3.2: It then runs the OIAF to collect the SF2's OAM information according to the descriptions of the instructions in the NSH header.

Step3.3: Finally it adds the SF2 OAM information which is part of the whole OAM information to form data packet 3. Now the OAM information in packet 3 includes the OAM information for VNF1(SF1)+VNF2(SF2).

Step3.4: The SFF which the SF belongs to transfers the packet 3 to the destination SF.

Step3.5: In dedicated conditions which is calculated by the OISF, the SF sends the dedicated packet carrying OAM information of itself or OAM information collection of the former SFs which is carried in packet 2 to the telemetry server through the related SFF.

**Step n:** When the n-th SF receives the data packet n. If it is the intermediate SF, it repeats the steps 1~n-1. If it is the destination SF, it takes the actions as follows:

Step n.1: It checks the NSH header and finds the OAM information identification.

Step n.2: It then collects the OAM information of itself according to the description of the instructions in the NSH header.

Step n.3: Finally it adds the OAM information of itself which is part of the whole OAM information to the data packet n to form data packet n+1. Now the OAM information in packet n+1 includes the OAM information for VNF1+VNF2+VNF3+...+VNFn.

Step n.4: It sends the packet which carries the whole OAM information to the telemetry server.

Step n.5: When the telemetry server receives the packet, it checks the NSH header. It reads out the OAM information according to the OAM information identification. This OAM information could be the dedicated OAM information from specific intermediate SF, or part/whole of the OAM information of the chain collected from subset or full set of the SFs in the chain from the intermediate or destination SF.

Step n.6: The telemetry server sends back a response message to the SF who sends the OAM information to the server through SFF to acknowledge that the pushed information was already received.

### 8.3 Signalling procedure for Ti.b in inter-domain telemetry

To fulfill the telemetry, the signaling procedure of the interface Ti.b between VNF1 and VNF2 are depicted in Figure 8-4. In SFC unaware domain, the VNF1 could be a SFC proxy and the VNF2 could be a SFC unaware network function.

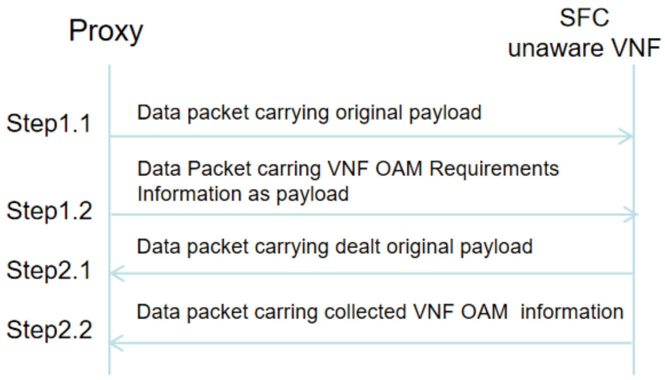

Proxy
SFC
unaware VNF
Step1.1
Data packet carrying original payload
Data Packet carring VNF OAM Requirements
Information as payload
Step1.2
Data packet carrying dealt original payload
Step2.1
Data packet carring collected VNF OAM information
Step2.2

**Figure 8-4 The general telemetry signaling procedure through Ti.b in SFC unaware-domain**

Interface Ti.b is responsible for exchanging the data packets encapsulated with the dedicated protocol used in the SFC unaware domain. This data packet could carry two kinds of payloads.

(1) Original customer data payload

This payload is resolved from the SFC packet by proxy and it is sent from proxy to the SFC unaware VNF. Correspondingly the dealt original customer payload is sent from the SFC unaware VNF to the proxy after the VNF deals with customer data.

(2) VNF OAM requirement information

This payload is in the form of executive programming codes and it is sent from proxy to the SFC unaware VNF.This payload could be carried in the same data packet as the original customer data payload. Also, it could be carried in a dedicated data packet different from the data packet carrying the original customer data payload. Correspondingly the collected OAM information of the SFC unaware VNF is sent from the VNF to the proxy after the VNF collects the related OAM information of itself.

Figure 8-5 describes the signaling procedure of inter-domain telemetry for SFC which is one of the most complicated service scenario. The signaling procedures of inter-domain telemetry for other network services are similar to SFC scenario and consequently not described in this Recommendation.

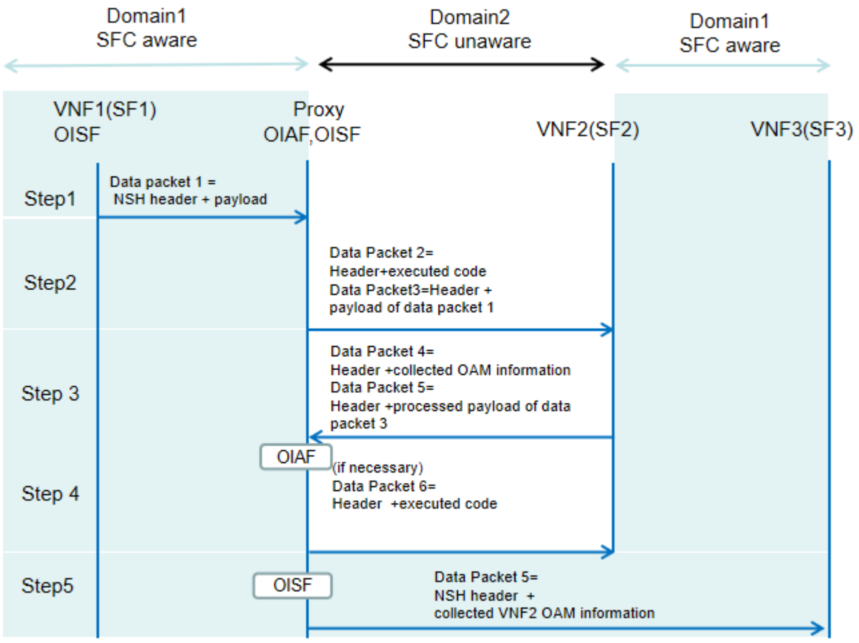


**Figure 8-5 Signalling procedure of inter-domain telemetry for SFC service**

NOTE – The related inter-SFC domain OAM information collection is described in Annex C.

**Step1:** The VNF1 encapsulates the data packet in NSH header to form the original packet 1 and send it to SFC proxy.

NOTE –This NSH header includes the same parameters as the NSH header described in step1 of clause 8.2.

**Step2:** When the proxy receives the packet 1, it takes the actions as follows. It resolves the packet 1 into two parts: the header and the payload. For the header part, the proxy takes the actions with step 2.1.For the payload, the proxy takes the actions with step2.2.

**For the header part:**

Step2.1:

Step2.1.1: It launches the OIAF to figure out the OAM information that should be collected from the SFC unaware SF2(e.g. the OAM category 1) from the header part.

Step2.1.2: It programs the required OAM information to a bulk of executable codes.

Step2.1.3: It encapsulates the required OAM information in the form of executable codes with the protocols used to exchange messages between the SFC proxy and SFC unaware SF (in SFC unaware domain) to form data packet 2.

Step2.1.4: It sends these data packet 2 to SF2(in SFC unaware domain).

**For the payload part:**

Step2.2:

Step2.2.1: The proxy encapsulates the original payload with the protocols used to exchange messages between the SFC proxy and SFC unaware SF (in SFC unaware domain) to form data packet 3.

Step2.2.2: The proxy sends data packet 3 to SF2(in SFC unaware domain).

**Step3:** When the SF2 receives the data packets, it takes the actions as follows.

Step3.1: It resolves the payload from the packets.

Step3.1.1: If the payload is resolved from packet 2. It runs the executable codes to collect the OAM information from itself and form the payload 4.

Step3.1.2: If the payload is resolved from packet 3. It deals with the payload to form payload 5.

Step3.2: SF2 encapsulates the payload mentioned above with the protocol header used in the SFC unaware domain to generate the packet (payload 4 to packet 4, payload 5 to packet 5).

Step3.3: SF2 sends the packet 4 and 5 to the proxy.

Step4: When the proxy receives the data packets 4 and 5, it takes the actions as follows.

Step4.1: It resolves the payload from the packets.

Step4.2:

Step4.2.1: For payload 4, it launches the OIAF to figure out if there is other OAM information that should be collected from SF2 or not. If it is necessary, it repeats Step2~3.If it is not necessary, jump to the Step 4.3.

Step4.2.2: For payload 5, jump to the Step 4.3

Step4.3: It encapsulates the payloads with the NSH header and transfers the packets to the SFF located in SFC aware domain or the telemetry server.

## 9 Signalling requirements for Ti.x

### 9.1 Overview

The signalling messages are exchanged over the interface Ti by extending the NSH header. The signalling messages may be extensible markup language (XML)-based messages over (or carried by) transmission control protocol (TCP), user datagram protocol (UDP), stream control transmission protocol (SCTP), transport layer security (TLS), etc. All of the messages consist of the message header and the message body.

The message format is described in Figure 9-1.

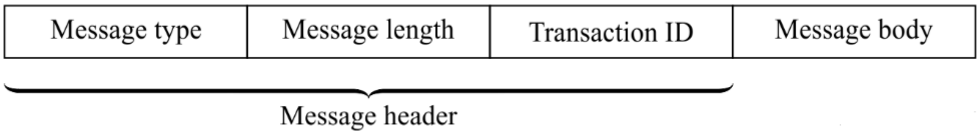


**Figure 9-1 – Message composition**

The message header field contains the following information:

– Message type: uniquely specifies the type of message;

– Message length: specifies the length of the message body;

– Message transaction ID: generated by the sender of the message. If there is a response message for the request message, the transaction IDs of the request and response messages are the same.

The message body field contains the message contents.

The interface Ti.x are divided into three types Ti.a, Ti.b for intra-domain message exchanging and Ti.b for inter-domain message exchanging. The signaling requirements for inter-domain message exchanging through Ti.b is out of the scope of this recommendation.

### 9.2 Signalling requirements for Ti.a

The VNF OAM information message is defined as VNFI message.

The VNFI message, indicated by the message type in the message header field, is sent by the VNF to the telemetry server.

Message format:

```
<VNFI-Message> ::= < Message Header >
                  * {VNF-Type}
                  * {VNF-Instance-ID}
                  * {VNF-Session-Number}
                  * {VNF-OAM-Information}
```

Meanings and explanations:

The detailed information indicates but not limited to:

(a) VNF-Type uniquely specifies the VNF function.

(b) VNF-instance-ID uniquely specifies the VNF instance ID.

(c) VNF-session-number uniquely specifies the session number of a specific VNF.

(d) VNF-OAM-information uniquely specifies the OAM information collected from this VNF.

The VNF OAM information acknowledge message is defined as VNFIA message.

The VNFIA message, indicated by the message type in the message header field, is sent by the telemetry server to the VNF.

Message format:

```
<VNFIA-Message> ::= < Message Header >
                         *{VNF-Type}
                         *{VNF-Instance-ID}
                         *{VNF-Session-Number}
```

Meanings and explanations:

The detailed information indicates but not limited to:

(a) VNF-Type uniquely specifies the VNF function.

(b) VNF-Instance-ID uniquely specifies the VNF instance ID.

(c) VNF-Session-Number uniquely specifies the session number of a specific VNF.

### 9.3 Signalling Requirements for Ti.b in intra-domain telemetry

The VNF information collection message is defined as VNFC message.

The VNFC message, indicated by the message type in the message header field, it is sent from the one VNF to another.

Message format:

```
<VNFC-Message> ::= < Message Header >
                 {OAM-Information-Identification}
                 {V-Delay}
                 {T-Delay}
                 {W-Delay}
                 {V-Thr}
                 {T-Thr}
                 {W-Thr}
                 {V-Loss}
                 {T-Loss}
                 {W-Loss}
                 {CatName}
                 {T-CatName}
                 {W-CatName}
                 {R-CatName}
                 {Operation}
                 {T-IDSI}
```

Meanings and explanations:

The detailed information indicates but not limited to:

– OAM-Information-Identification uniquely specifies that this is the packet for collecting OAM information from the devices according to the next field “programming instructions”.

The required service OAM information and evaluation parameters are described below which is used by OISF to choose the appropriate method to send the OAM information to the telemetry server. The value of the parameters are defined by the administrator(human being or machine). It includes but not limited to:

a) V-Delay uniquely specifies the value of end-to-end delay which should be collected.

b) T-Delay uniquely specifies the value of end-to-end delay threshold of the service SLA.

c) W-Delay uniquely specifies the value of weight of end-to-end delay of the service SLA.

d) `V-Thr` uniquely specifies the value of end-to-end throughput which should be collected.

e) `T-Thr` uniquely specifies the value of end-to-end throughput threshold of the service SLA.

f) `W-Thr` uniquely specifies the value of weight of end-to-end throughput of the service SLA.

g) `V-Loss` uniquely specifies the value of end-to-end loss which should be collected.

h) `T-Loss` uniquely specifies the value of end-to-end loss threshold of the service SLA.

i) `W-Loss` uniquely specifies the value of weight of end-to-end loss of the service SLA.

The required device OAM information and evaluation parameters uniquely specifies the device OAM information which is used by OISF to choose the appropriate method to send the OAM information to the telemetry server. It includes but not limited to:

a) `CatName` uniquely specifies the category name of one specific category of OAM information that should be collected from device.

NOTE – the OAM parameters related to the specific OAM category could be carried in the programming instructions in the header or stored in each VNF in advance based on the common agreement of mapping between category and OAM parameters.

b) `T-CatName` uniquely specifies the threshold of the specific OAM category mentioned above.

c) `W-CatName` uniquely specifies the weight of the specific OAM category mentioned above.

d) `R-CatName` uniquely specifies the relationship between the different categories or category group.

e) `Operation` uniquely specifies operation for the OAM classification information.

d) `T-IDSI` uniquely specifies threshold of integrated device and service OAM information, which is provided by administrator (human being or machine).

# Annex A

## The mechanism and an example of OAM information acquisition function (OIAF)

(This annex forms an integral part of this Recommendation.)

### 1. Background

In the consideration of mass mount of OAM information, to carry all the OAM information in the data packets is impractical. It is necessary to classifier the OAM information and collect the OAM information according to the categories.

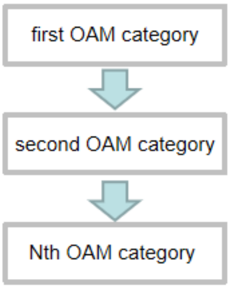


**Figure A.1 – A typical relationship among different OAM categories**

As shown in Figure A.1, the logical relationship among different OAM categories is hierarchical. The value change of the OAM parameter of the lower layer category always causes the value change of OAM parameters of the upper layer category. Using this laying model, it is capable to hierarchically trace and locate the reasons of abnormal OAM information.

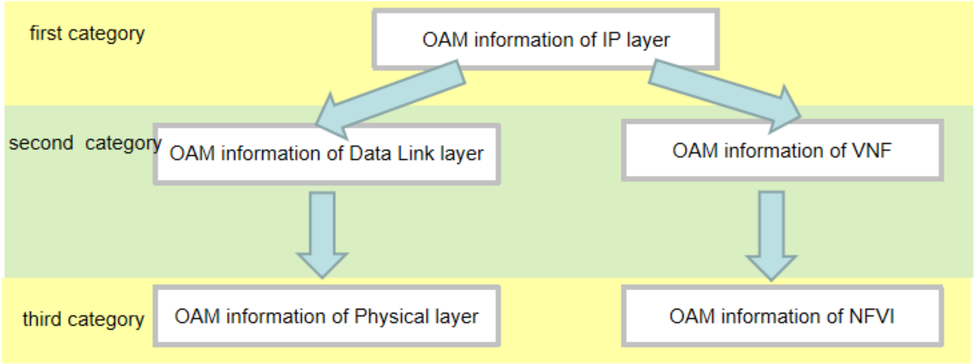

first category
OAM information of IP layer
second category
OAM information of Data Link layer
OAM information of VNF
third category
OAM information of Physical layer
OAM information of NFVI

**Figure A.2 – Relationship example among different OAM categories**

For example, as shown in Figure A.2, a detailed example of relationship of the OAM category, the information of IP layer is the first category. When the OAM information of IP layer is abnormal(for example, exceed the threshold), the second category OAM information should be collected. If the OAM information of second category is normal, it is possible to figure out the failure of IP layer itself which leads to the abnormal OAM data.

### 2. **Mechanism**

The SF reads the NSH header of the incoming packet. The OAM information identification provides the hint that SF need to launch the OIAF to collect the OAM information of itself according to the programming instructions carried in the header. The procedure of OIAF is as below:

Step1: It reads out the OAM categories names, the threshold of each OAM category, relationship of these categories and the related operations from the instructions;

Step2~StepN are the operations based on the OAM category information mentioned above. These operations could be written in the instructions carried in the header or locally storied in the SF previously. The OIAF will follow the operations written in the header in advance. If there is no operation written in the header, the OIAF will follow the operations storied in the SF by default. The operations of OAM information collection based on the OAM categories' thresholds and their relationship demonstrated in Figure A.3 is as below:

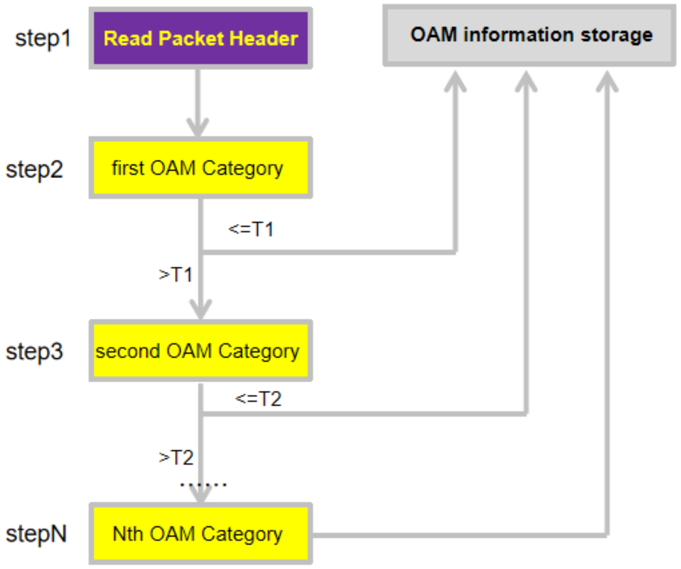


**Figure A.3 – The operations based on OAM classification information**

Step 2: For the first category of OAM information, if the related OAM value is below or equal to its threshold T1, the OIAF only collects the related OAM information of first category and then stores it. If the OAM value is above the first category's threshold T1:

Step3: OIAF not only collects the first category's OAM information but also collects the second category OAM information related to the first category and then stores then. If the OAM value is above the second category's threshold T2:

......

Step N: OIAF repeats the steps mentioned above until the value of OAM parameter is below the threshold of Nth category or the Nth category is the last category within the relationship.

# Annex B

## The mechanism of OAM information sending function (OISF)

(This annex forms an integral part of this Recommendation.)

The hybrid way is used to send the OAM information to telemetry server according to Appendix I. It means that in some conditions the OAM information is sent to the telemetry server from the current intermediate VNF and, in other conditions, the OAM information is sent to the telemetry server from the tail VNF of SFC.

The mechanism of OISF is responsible for figuring out the current condition based on the current integrated OAM information both from device and service and choose the appropriate way to send the OAM information to the telemetry server based on the matching results of the current conditions and situation.

The OAM information can be roughly divided into two types: the device OAM information and service OAM information.

(1) The OAM information of device

The OAM information of device reflects resource consumption of the specific device in total and could barely reflects the dedicated resource allocation for specific service running on this device. So OAM information of device could only approximately deduce the rough status of various network services.

(2) The OAM information of service

Traditionally, the OAM information of service could be collected using dedicated OAM packets. Nowadays, the OAM information of service could be collected using telemetry way. However, both of these two methods have the same shortcoming that the OAM information will be lost when the packet who carries it is lost encountering network congestion or failure.

Consequently, the current methods of collecting OAM information of device and service cannot meet the requirements for efficiency and effectiveness. It is necessary to develop an upgraded method to sending the OAM information which can satisfies the requirements as below:

(1) It is required that combined statuses of device and services are reflected;

(2) It is required that combined statuses of device and service could be sent to the telemetry server in time in any situation especially when network congestion or failure occurred.

OISF is designed to meet these two requirements by using the parameters carried in the extended NSH header (also see clause 9.2).

To figure out the current statuses of both device and service, there are two kinds of information that need to be collected from SF. One is required OAM information and the other is the OAM evaluation parameter. These two kinds of information are applied to both device and service.

(1) The representing required OAM information of service and its related OAM evaluation parameters are presented in Table B-1.

**Table B-1 The representing required OAM information of service and its related OAM evaluation parameters**

| QoS parameter | Required OAM information of service | Related OAM evaluation parameters | |
|---|---|---|---|
| | | SLA threshold | SLA weight |
| End-to-end delay | `V-Delay` | `T-Delay` | `W-Delay` |

| | | | |
|---|---|---|---|
| End-to-end throughput | V-Thr | T-Thr | W-Thr |
| End-to-end loss | V-Loss | T-Loss | W-Loss |

(2) The required OAM information of device and its related OAM evaluation parameters include but not limited to:

- OAM classification information includes but not limited to:

  CatName,T-CatName,W-CatName

- OAM category relationship information includes:

  R-CatName

- Operations based on OAM classification information includes:

  Operation

(3) The threshold of integrated service and device OAM information: T-IDSI

When the packets arrives at the intermediate node (e.g.,VNF2 in Figure 8-3), it acts as below:

(1) Reading the parameters mentioned above from the extended NSH header;

(2) Figuring out the service OAM evaluation value.

Step1: Collects the service OAM values, for example the V-delay,V-Thr, V-loss;

Step2: Figure out the service OAM ratio using the equation:

Service OAM ratio= collected service OAM value/ SLA threshold T. For example:

End-to-end delay ratio=V-delay/T-delay,

End-to-end throughput ratio= V-thr/T-thr,

End-to-end loss ratio=V-loss/T-loss,

Step3: Figure out the weighted service OAM ratio using the equation:

Weighted Service OAM ratio=Service OAM ratio*related SLA Weight, For example:

Weighted End-to-end delay ratio=End-to-end delay ratio*W-Delay,

Weighted End-to-end throughput ratio=End-to-end throughput ratio*W-Thr,

Weighted End-to-end Loss ratio=End-to-end Loss ratio*W-Loss,

Step4: Figure out the weighted service OAM evaluation value using the equation:

Weighted Service OAM evaluation ratio = Weighted Service OAM ratio 1 * Weighted Service OAM ratio 2 *Weighted Service OAM ratio3 * .....Weighted Service OAM ratio n

(3) Figure out the device OAM evaluation value

Step1: Collects the device OAM information according to the device OAM classification information, OAM category relationship information and the operations based on OAM classification information and prepare the collected device OAM information.

Step2: Figure out the device OAM ratio using the equation:

Device OAM ratio= (collected Device OAM value of CatName)/T-CatName.

Step3: Figure out the weighted device OAM ratio using the equation:

Weighted device OAM ratio=Device OAM ratio*W-CatName

Step4: Figure out the integrated device OAM evaluation value using the equation:

Weighted Device OAM evaluation ratio = Weighted category 1 ratio *Weighted category 2 ratio *Weighted category 3 ratio * ......Weighted category N ratio

(4) Figure out the integrated evaluation value using the equation:

Integrated evaluation value=Weighted service OAM evaluation ratio*Weighted device OAM evaluation ratio

(5) Compare the integrated evaluation value threshold of integrated service and device OAM information,

If Integrated evaluation value>=T-IDSI, the OISF encapsulates the OAM information in dedicated OAM packet and sends this packet to the telemetry server from the current device;

If Integrated evaluation value<T-IDSI, the OISF encapsulates the OAM information in data packet and sends this packet to the destination of the SFP.

# Annex C

## The mechanism of  OAM information collection for inter-SFC domain

(This annex forms an integral part of this Recommendation.)

The SFC is composed of several service functions. Some of the service functions are historic legacy device, no matter they are virtual or not, that are not capable to support the SFC related protocols. This kind of SF is called SFC unaware SF and within the non-SFC domain. Relevantly, the SF which supports SFC related protocols is called SFC aware SF and within the SFC domain. When a service function chain steers the packets to a SFC unaware SF, a SFC proxy is inevitably to translate and exchange the messages between the two domains (see RFC7665 ). The SFC proxy decapsulates the SFC packet into two parts: NSH header and the payload. Then the SFC proxy sends the payload to the SFC unaware SF through local attachment circuit. The SF deals with the payload and then returns the new payload to the SFC proxy. The SFC proxy encapsulate the new payload with the NSH header and send it back to the SFF.

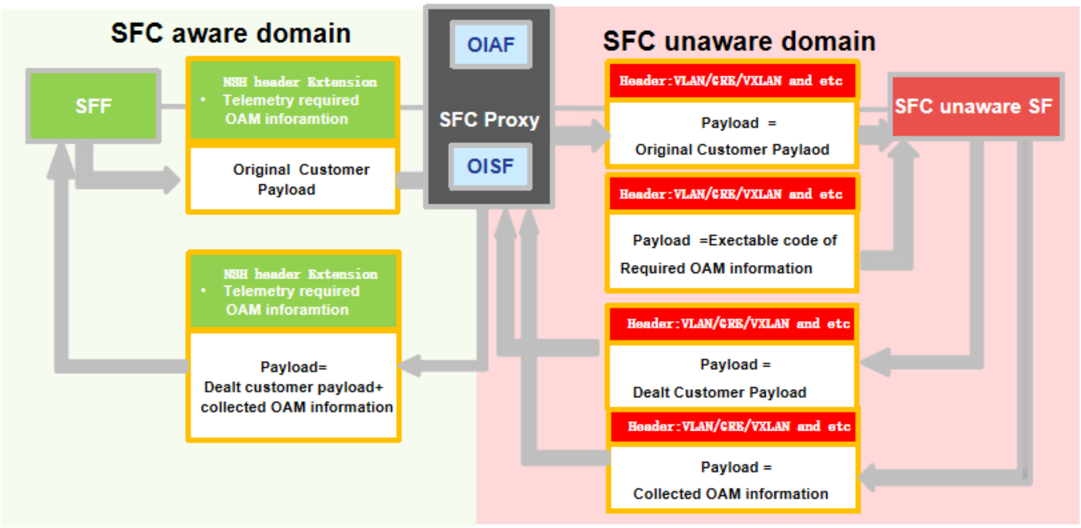

SFC aware domain
SFF
NSH header Extension
• Telemetry required OAM inforamtion
Original Customer Payload
OIAF
SFC Proxy
OISF
SFC unaware domain
Header:VLAN/GRE/VXLAN and etc
Payload = Original Customer Paylaod
SFC unaware SF
Header:VLAN/GRE/VXLAN and etc
Payload =Exectable code of Required OAM information
NSH header Extension
• Telemetry required OAM inforamtion
Payload= Dealt customer payload+ collected OAM information
Header:VLAN/GRE/VXLAN and etc
Payload = Dealt Customer Payload
Header:VLAN/GRE/VXLAN and etc
Payload = Collected OAM information

**Figure C.1 –  The signaling procedure of  OAM information collection for inter-SFC domain**

In this Recommendation, the required OAM information are carried in the extended NSH header and consequently can only be recognized by SFC aware device (eg. SFC aware SF, SFC proxy, SFF and etc). It cannot be recognized by SFC unaware SF. So, the OAM information of SFC unaware SF will be missed during the collection and consequently the collected SFC information is not complete and has no valuable reference.

To solve this problem, the following actions should be taken.

Step1: The SFC proxy resolves the OAM required information from the extended NSH header. Meanwhile,it decapsulates the customer original payload from the packets.

Step2: The SFC proxy launches the OIAF function to figure out the OAM information that should be collected from the SFC unaware SF.

Step3: The SFC proxy programs the required OAM information resolved from the extended NSH header into a piece of executable code as a payload and encapsulates this payload with the protocols used to exchange messages between the SFC proxy and SFC unaware SF. This packet is named as packet 1.

Step4: The SFC proxy encapsulates this customer original payload with the protocols used to exchange messages between the SFC proxy and SFC unaware SF. This packet in called packet 2.

Step5: When the SFC unaware SF receives the packets 1, it resolves the payload from the packet and run the dedicated piece of executable code within the payload to collect the OAM information;

Step6: The SFC unaware SF encapsulates this payload of collected the OAM information with the protocols used to exchange messages between the SFC proxy and SFC unaware SF (SFC unaware domain) and send the packet to the SFC proxy.

Step7: When the SFC unaware SF receives the packets 2, it resolves the payload from the packet and deals with the payload to collect the OAM information;

Step8: The SFC unaware SF encapsulates this payload of dealt customer data payload with the protocols used to exchange messages between the SFC proxy and SFC unaware SF (SFC unaware domain) and send the packet to the SFC proxy.

Step9: The SFC proxy receives the packets and isolates the headers and payloads.The payload is customer data payload or the collected OAM information payload.

Step11: The OIAF function within the SFC proxy evaluates the collected OAM information and make the decision whether to collect the other category of OAM information from the SFC unaware SF or not.

Step10: If it is necessary to collect other OAM information from the SFC unaware SF, the SFC proxy will repeat Step 3 ~Step9.

Step11: If it is not necessary to collect other OAM information from the SFC unaware SF, the SFC proxy will launch the OISF function to send packet to the SFF.

# Appendix I

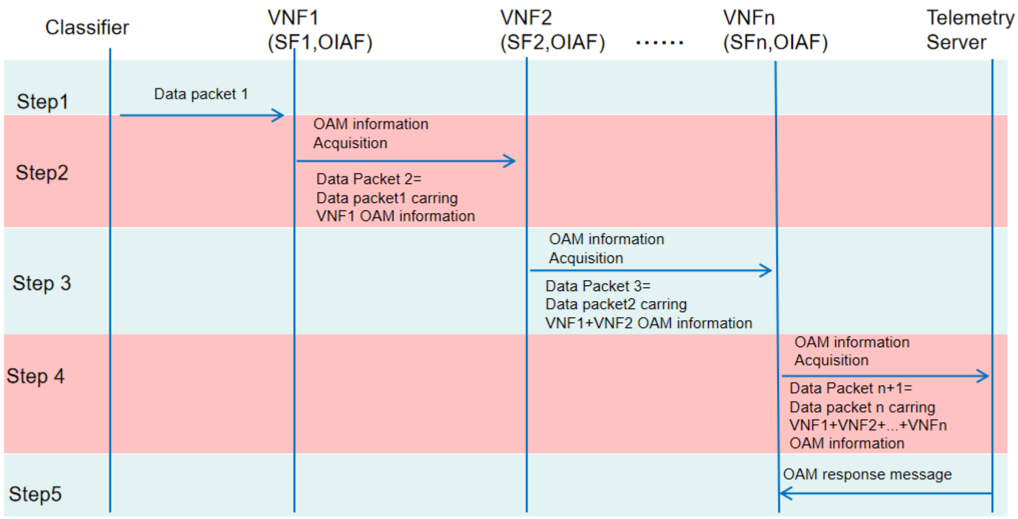
## Three different ways to push the OAM information of VNF to the telemetry server

(This appendix does not form an integral part of this Recommendation.)

This appendix provides analysis of three different ways to push the OAM information of SFC which is carried in data packets to the telemetry server.

### - The centralized way

The destination VNF of the SFC collects all the SFs' OAM information along the way and launches a one-time operation to push the OAM information to the telemetry server.

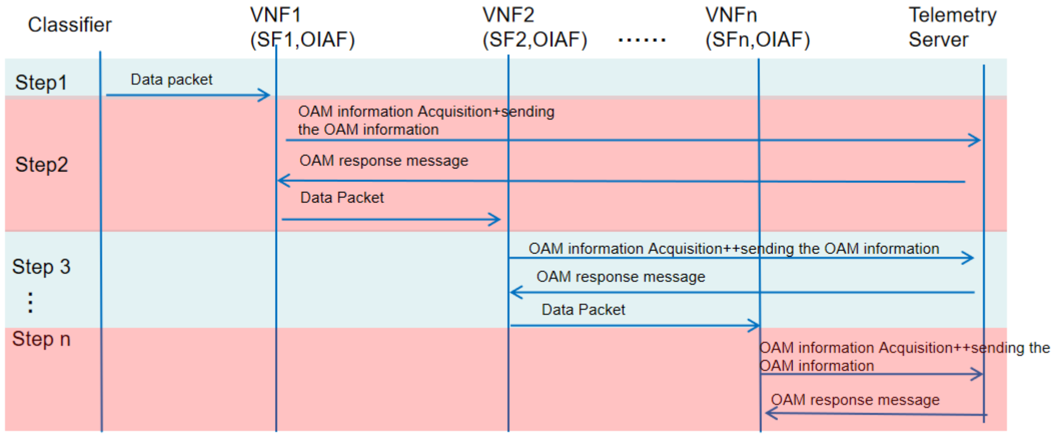

Classifier
VNF1 (SF1,OIAF)
VNF2 (SF2,OIAF)
……
VNFn (SFn,OIAF)
Telemetry Server
Step1
Data packet 1
Step2
OAM information Acquisition
Data Packet 2= Data packet1 carring VNF1 OAM information
Step 3
OAM information Acquisition
Data Packet 3= Data packet2 carring VNF1+VNF2 OAM information
Step 4
OAM information Acquisition
Data Packet n+1= Data packet n carring VNF1+VNF2+...+VNFn OAM information
Step5
OAM response message

OIAF=OAM information Acquisition Function

**Figure I.1 – The procedure of centralized way**

### - The distributed way

Each of the SF within the SFC sends the OAM information of itself to the telemetry server separately.



OIAF=OAM information Acquisition Function

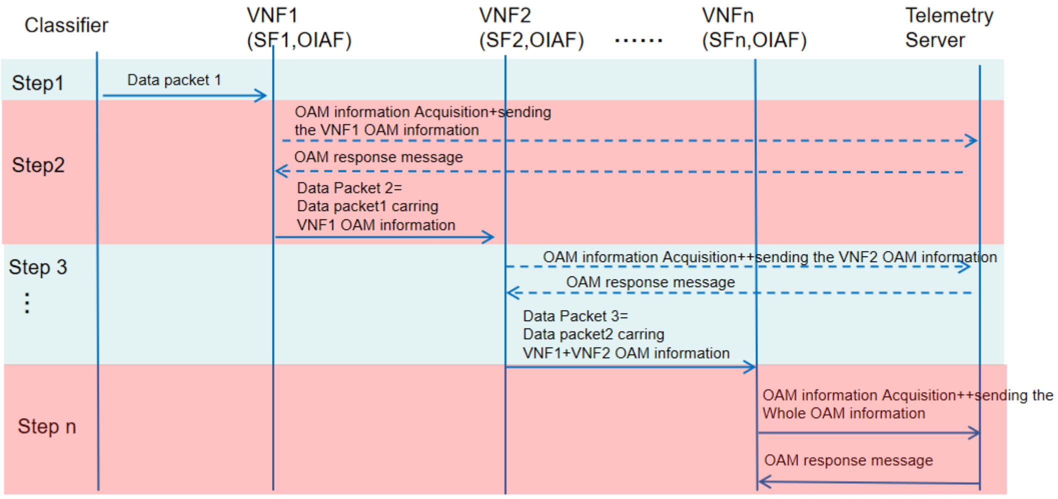
**Figure I.2 – The procedure of distributed way**

### - The hybrid way

This way is the combination of centralized way and distributed way.

For the distributed way, large mount of messages are exchanged between VNFs and telemetry servers and consumes too much network resource. For the centralized way, only two messages are enough to acknowledge the telemetry server the OAM information. However, if there is network failure happened on one of the SF on the path, the packet will not be possible to reach the destination and all the OAM information of SFs will not be acknowledged to the telemetry server.

The hybird way solves these problems by giving current ( intermediate,other than the destination) SF the capability to send the OAM information of itself and the OAM information collections of former SFs to the telemetry server according to different conditions.In this way, the hybrid way could satisfies the requirements of not only consuming the network resources as less as possible but also sending the information with efficiently.


Classifier
VNF1 (SF1,OIAF)
VNF2 (SF2,OIAF)
······
VNFn (SFn,OIAF)
Telemetry Server
Step1
Data packet 1
Step2
OAM information Acquisition+sending the VNF1 OAM information
OAM response message
Data Packet 2= Data packet1 carring VNF1 OAM information
Step 3
⋮
OAM information Acquisition++sending the VNF2 OAM information
OAM response message
Data Packet 3= Data packet2 carring VNF1+VNF2 OAM information
Step n
OAM information Acquisition++sending the Whole OAM information
OAM response message

OIAF=OAM information Acquisition Function

**Figure I.3 – The procedure of of hybrid way**

## Bibliography

[b-ITU-T Y-Sup.41] Supplement 41 to ITU-T Y-series Recommendations (2016), *Deployment models of service function chaining*.

___________________