International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3406

(09/2022)

SERIES Q: SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

Signalling requirements and protocols for the NGN – Service and session control protocols

Signalling requirements for telemetry of virtual broadband network services

Recommendation ITU-T Q.3406

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3709
General	Q.3000–Q.3029
Network signalling and control functional architecture	Q.3030–Q.3099
Network data organization within the NGN	Q.3100–Q.3129
Bearer control signalling	Q.3130–Q.3179
Signalling and control requirements and protocols to support attachment in NGN environments	Q.3200–Q.3249
Resource control protocols	Q.3300–Q.3369
Service and session control protocols	**Q.3400–Q.3499**
Service and session control protocols – supplementary services	Q.3600–Q.3616
Service and session control protocols – supplementary services based on SIP-IMS	Q.3617–Q.3639
VoLTE/ViLTE network signalling	Q.3640–Q.3655
NGN applications	Q.3700–Q.3709
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR SDN	Q.3710–Q.3899
TESTING SPECIFICATIONS	Q.3900–Q.4099
PROTOCOLS AND SIGNALLING FOR PEER-TO-PEER COMMUNICATIONS	Q.4100–Q.4139
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2020	Q.5000–Q.5049
COMBATING COUNTERFEITING AND STOLEN ICT DEVICES	Q.5050–Q.5069

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Q.3406

Signalling requirements for telemetry of virtual broadband network services

Summary

Recommendation ITU-T Q.3406 specifies the signalling requirements for telemetry of virtual broadband network services, by architecturally adding the dedicated functional component and the corresponding interfaces in the network functions virtualization (NFV) framework.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T Q.3406	2022-09-29	11	11.1002/1000/15044

Keywords

Signalling requirements, telemetry, virtual broadband network services.

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Q.3406

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 term:

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 where an open application model (OAM) in the virtualized environment cannot be met by 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 a 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 change. The conventional OAM technologies which are developed off-line by a specific vendor and installed/uninstalled manually take too much time to catch up with the pace of a 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 a proprietary data model for limited objects and cannot meet this requirement. The telemetry having the 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 the NFV framework. Therefore, it is needed to specify the NFV based telemetry architecture and the signalling 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 below.

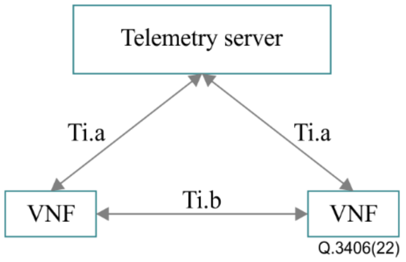


Figure 7-1 – The interface Ti.x reference model for the telemetry of virtual broadband network services

The telemetry server is responsible for data collection and storage.

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

1) Interface Ti.a

Interface Ti.a is between the telemetry server and the virtualized network function (VNF). It collects OAM data from the VNFs.

2) Interface Ti.b

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

The VNFs could reside in the same protocol domain or different domains. Usually, the inter-domain communication occurs in the service function chaining service, since there are a large number of legacy network functions in the network which cannot support the SFC protocol. Correspondingly, the messages exchanged through Ti.b are different based on the locations of the 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 are located in different domains, there must be a network proxy located between the two VNFs (see Figure 7-2).

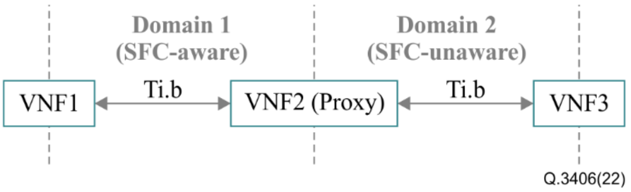


Figure 7-2 – The reference model for Ti.b in the inter-domain scenario

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

For the interface Ti.b located in domain 2 between VNF2 (Proxy) and VNF3, the messages exchanged through it are 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 the related operations are triggered by the signalling 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 the related operations are decided by proxy which is the IP service initiator within the VNF2-VNF3 pair.

8 Signalling procedures for Ti.x

8.1 Signalling procedure for Ti.a

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

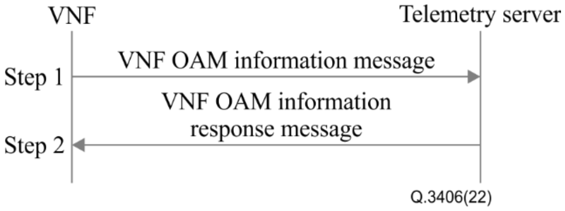

VNF
Telemetry server
Step 1
VNF OAM information message
VNF OAM information response message
Step 2
Q.3406(22)

Figure 8-1 – The general telemetry signalling procedure through interface Ti.a

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

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

One kind of VNF, the 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 the hybrid way, there are also "centralized way" and "distributed way" to push the OAM information to the telemetry server. Appendix I analyses the advantages and disadvantages of these three ways.

8.2 Signalling procedure for Ti.b in an intra-domain telemetry

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

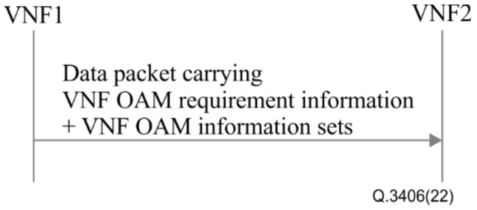


Figure 8-2 – The general telemetry signalling procedure through Ti.b in an SFC aware domain

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

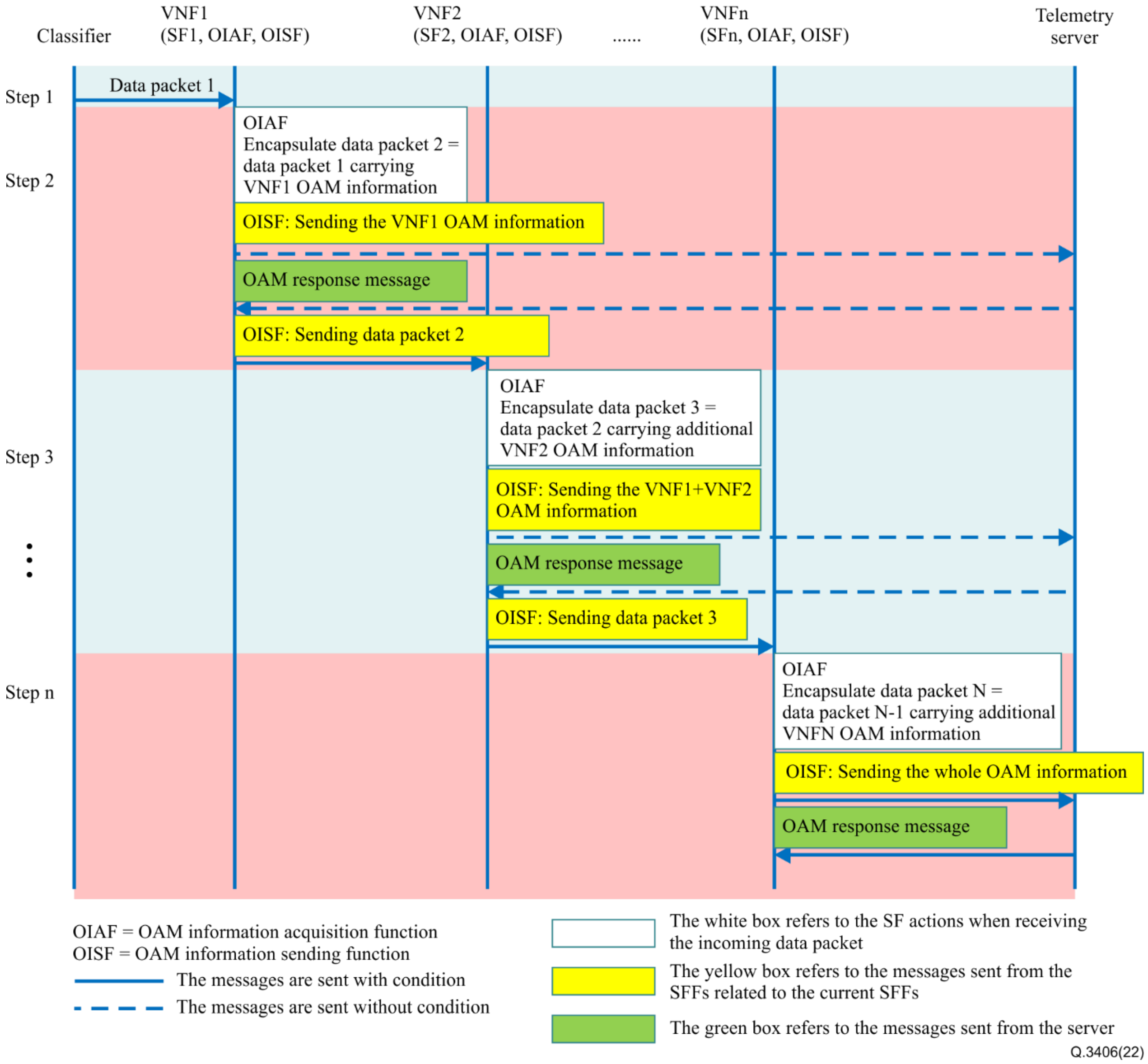

Classifier
VNF1 (SF1, OIAF, OISF)
VNF2 (SF2, OIAF, OISF)
......
VNFn (SFn, OIAF, OISF)
Telemetry server
Step 1
Data packet 1
Step 2
OIAF
Encapsulate data packet 2 = data packet 1 carrying VNF1 OAM information
OISF: Sending the VNF1 OAM information
OAM response message
OISF: Sending data packet 2
Step 3
OIAF
Encapsulate data packet 3 = data packet 2 carrying additional VNF2 OAM information
OISF: Sending the VNF1+VNF2 OAM information
OAM response message
OISF: Sending data packet 3
Step n
OIAF
Encapsulate data packet N = data packet N-1 carrying additional VNFN 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
Q.3406(22)

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

Step 1: The classifier encapsulates the data packet in the NSH header to form the original packet 1 and sends it to VNF1(SF1, OIAF, OISF).

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 the telemetry server needs to collect from the SFs and the OAM evaluation parameter information. The programming instructions include but are not limited to:

1) The required OAM information:

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

b) the threshold information of each category.

NOTE 4 – 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 5 – 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 the device.

b) The threshold defined for service SLA.

c) The weight of the service SLA.

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

Step 2: When the first intermediate SF node (SF1) receives the original data packet 1.

Step 2.1: It checks the NSH header and finds the OAM information identification.

NOTE 6 – According to the OAM information identification, SF1 launches the OAM information acquisition function (OIAF) to select and collect the required OAM information from SF.

Step 2.2: It runs the OIAF to collect the SF1's OAM information according to the descriptions of the instructions in the NSH header.

NOTE 7 – The OIAF mechanism and detailed example are described in Annex A.

Step 2.3: It runs the OAM information sending function (OISF) to send the OAM information to the telemetry server through different methods depending on the integrated service and device OAM evaluation value (ISDOEV) which is calculated based on the service OAM information, device OAM information and the OAM evaluation parameter information.

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

Step 2.3.1: It adds the SF1 OAM information including both the device and service OAM information, which is part of the whole OAM information, to data packet 1 to form data packet 2.

NOTE 8 – The whole OAM information is composed of multiple VNFs' OAM information which is located in front of the current VNF.

Step 2.3.2: The service function forwarder (SFF) to which the SF belongs to transfers the packet 2 to the destination SF.

The method is described 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 the OAM information of itself including both device and service OAM information to the telemetry server.

NOTE 9 – The OISF mechanism is described in Annex B.

Step 3: When the second SF node SF2 receives the data packet 2.

Step 3.1: It checks the NSH header and finds the OAM information identification.

Step 3.2: It then runs the OIAF to collect the SF2's OAM information according to the descriptions of the instructions in the NSH header.

Step 3.3: 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).

Step 3.4: The SFF to which the SF belongs to transfers the packet 3 to the destination SF.

Step 3.5: In dedicated conditions which are calculated by the OISF, the SF sends the dedicated packet carrying the 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 a specific intermediate SF, or part/whole of the OAM information of the chain collected from the subset or full set of the SFs in the chain from the intermediate or the 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 the SFF to acknowledge that the pushed information was already received.

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

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

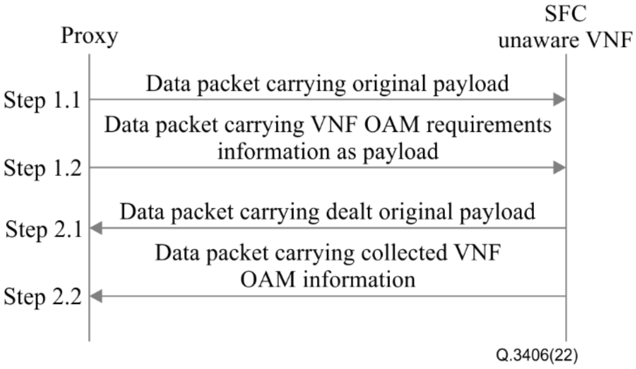

Proxy
SFC unaware VNF
Step 1.1
Data packet carrying original payload
Data packet carrying VNF OAM requirements information as payload
Step 1.2
Data packet carrying dealt original payload
Step 2.1
Data packet carrying collected VNF OAM information
Step 2.2
Q.3406(22)

Figure 8-4 – The general telemetry signalling 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 the 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 the 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 signalling procedure of the inter-domain telemetry for SFC which is one of the most complicated service scenarios. The signalling procedures of the inter-domain telemetry for other network services are similar to the SFC scenario and consequently not described in this Recommendation.

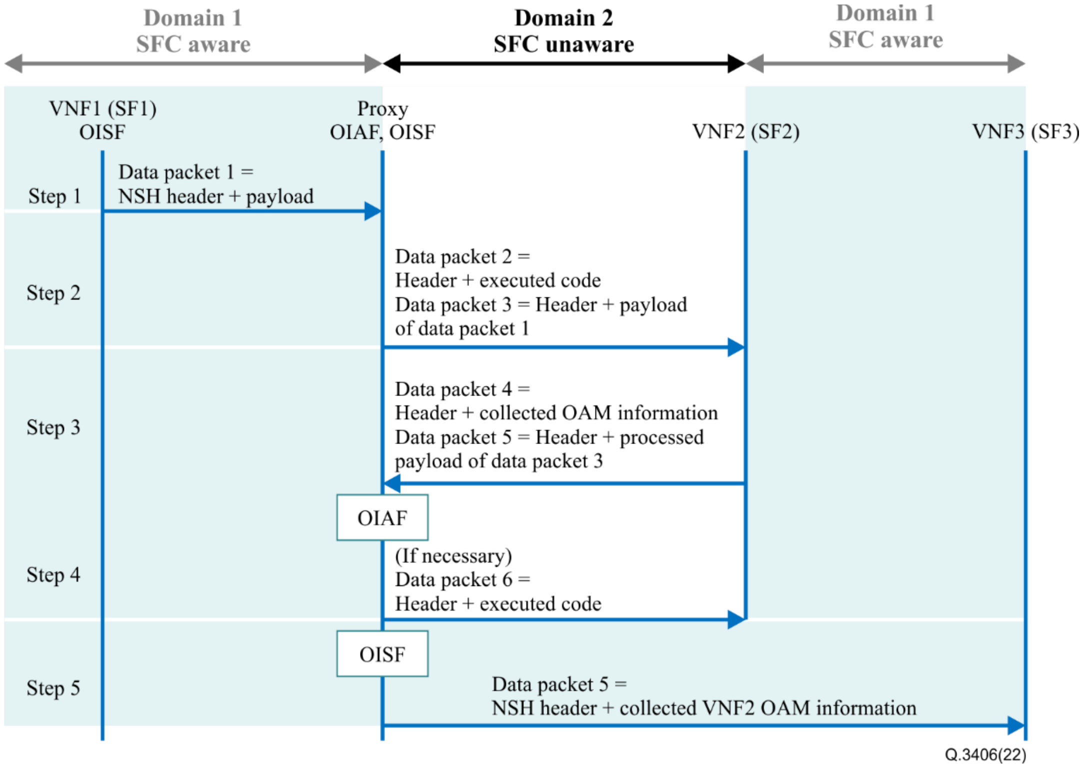


Figure 8-5 – Signalling procedure of the inter-domain telemetry for an SFC service

NOTE 1 – The related inter-SFC domain OAM information collection is described in Annex C.

Step 1: The VNF1 encapsulates the data packet in the NSH header to form the original packet 1 and sends it to the SFC proxy.

NOTE 2 – This NSH header includes the same parameters as the NSH header described in step 1 of clause 8.2.

Step 2: When the proxy receives packet 1, it takes the actions as follows. It resolves 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 step 2.2.

For the header part:

Step 2.1:

Step 2.1.1: 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.

Step 2.1.2: It programs the required OAM information to a bulk of executable codes.

Step 2.1.3: 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 the SFC unaware domain) to form data packet 2.

Step 2.1.4: It sends these data packet 2 to SF2 (in the SFC unaware domain).

For the payload part:

Step 2.2:

Step 2.2.1: The proxy encapsulates the original payload with the protocols used to exchange messages between the SFC proxy and the SFC unaware SF (in the SFC unaware domain) to form data packet 3.

Step 2.2.2: The proxy sends data packet 3 to SF2 (in the SFC unaware domain).

Step 3: When the SF2 receives the data packets, it takes the actions as follows.

Step 3.1: It resolves the payload from the packets.

Step 3.1.1: 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.

Step 3.1.2: If the payload is resolved from packet 3. It deals with the payload to form payload 5.

Step 3.2: 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).

Step 3.3: SF2 sends the packet 4 and packet 5 to the proxy.

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

Step 4.1: It resolves the payload from the packets.

Step 4.2:

Step 4.2.1: For payload 4, it launches the OIAF to figure out if there is other OAM information that should be collected from the SF2 or not. If it is necessary, it repeats Steps 2~3. If it is not necessary, jump to the Step 4.3.

Step 4.2.2: For payload 5, jump to Step 4.3.

Step 4.3: It encapsulates the payloads with the NSH header and transfers the packets to the SFF located in the 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) the transmission control protocol (TCP), user datagram protocol (UDP), stream control transmission protocol (SCTP), transport layer security (TLS), etc. All the messages consist of the message header and the message body.

The message format is described in Figure 9-1.

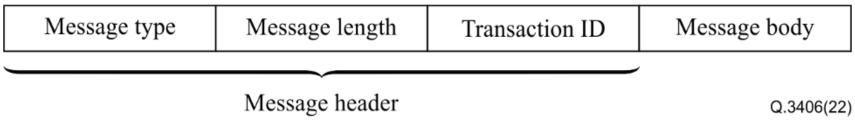


Figure 9-1 – Message composition

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 signalling 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 a 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 is 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 a 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 is 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 the intra-domain telemetry

The VNF information collection message is defined as a VNFC message.

The VNFC message, indicated by the message type in the message header field, is sent from 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 is 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 the OISF to choose the appropriate method to send the OAM information to the telemetry server. The value of the parameters is defined by the administrator (human being or machine). It includes but is not limited to:

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

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

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

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

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

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

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

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

i) `W-Loss` uniquely specifies the value of the weight of the 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 the OISF to choose the appropriate method to send the OAM information to the telemetry server. It includes but is not limited to:

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

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

d) `T-IDSI` uniquely specifies the threshold of the integrated device and service OAM information, which is provided by the 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.)

A.1 Background

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

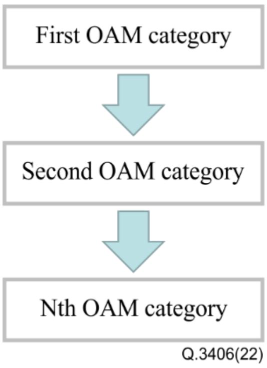


Figure A.1 – A typical relationship among different OAM categories

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 in the OAM parameters of the upper layer category. Using this laying model, it is capable to hierarchically trace and locate the reasons for abnormal OAM information.

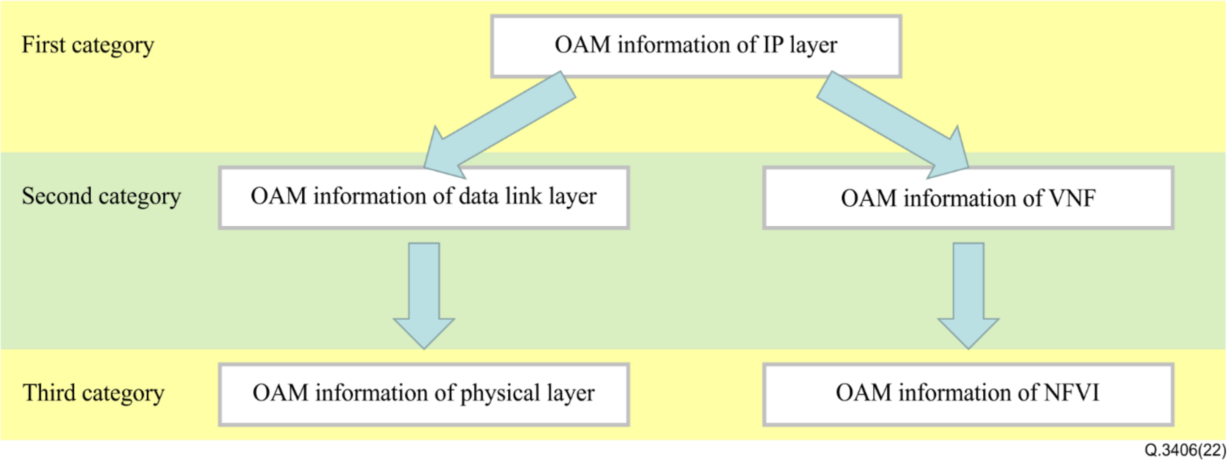


Figure A.2 – Relationship example among different OAM categories

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

A.2 Mechanism

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

Step1: It reads out the OAM categories names, the threshold of each OAM category, the 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 stored 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 stored in the SF by default. The operations of the OAM information collection based on the OAM categories' thresholds and their relationship is demonstrated in Figure A.3 given below:

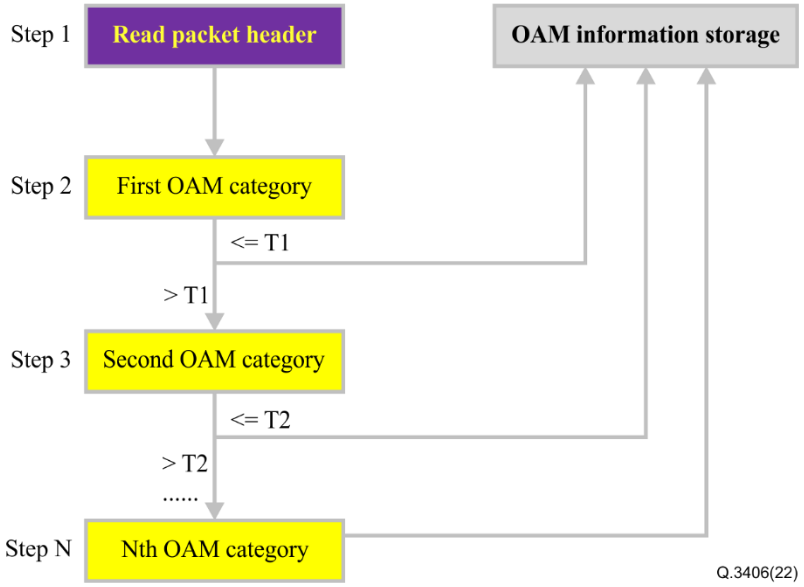


Figure A.3 – The operations based on the OAM classification information

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

Step 3: OIAF not only collects the first category's OAM information but it also collects the second category's OAM information related to the first category and then stores them. If the OAM value is above the second category's threshold T2:

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

Annex B

The mechanism of the 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 the 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 the SFC.

The mechanism of the OISF is responsible for figuring out the current condition based on the current integrated OAM information both from the device and the service and chooses 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 the device

   The OAM information of the device reflects the resource consumption of the specific device in total and can barely reflect the dedicated resource allocation for specific services running on the device. Thus, the OAM information of the device can only approximately deduce the rough status of the various network services.

2) The OAM information of service

   Traditionally, the OAM information of service can be collected using dedicated OAM packets. Nowadays, the OAM information of service can be collected using the telemetry way. However, both of these two methods have the same shortcoming, i.e., the OAM information will be lost when the packet that 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 for sending the OAM information which can satisfy the requirements below:

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

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

OISF is designed to meet these two requirements by using the parameters carried out 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 needs to be collected from the SF. One is the 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`

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

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

- OAM classification information includes but is not limited to:
  `CatName,T-CatName,W-CatName`
- OAM category relationship information includes:
  `R-CatName`
- Operations based on the OAM classification information includes:
  `Operation`

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

When the packets arrive 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.

Step 1: Collects the service OAM values, for example, the `V-delay`, `V-Thr`, `V-loss`;

Step 2: 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`

Step 3: 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`

Step 4: 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

Step 1: Collects the device OAM information according to the device OAM classification information, OAM category relationship information, and the operations based on the OAM classification information and prepare the collected device OAM information.

Step 2: Figure out the device OAM ratio using the equation:

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

Step 3: Figure out the weighted device OAM ratio using the equation:

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

Step 4: 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 the integrated service and device OAM information,

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

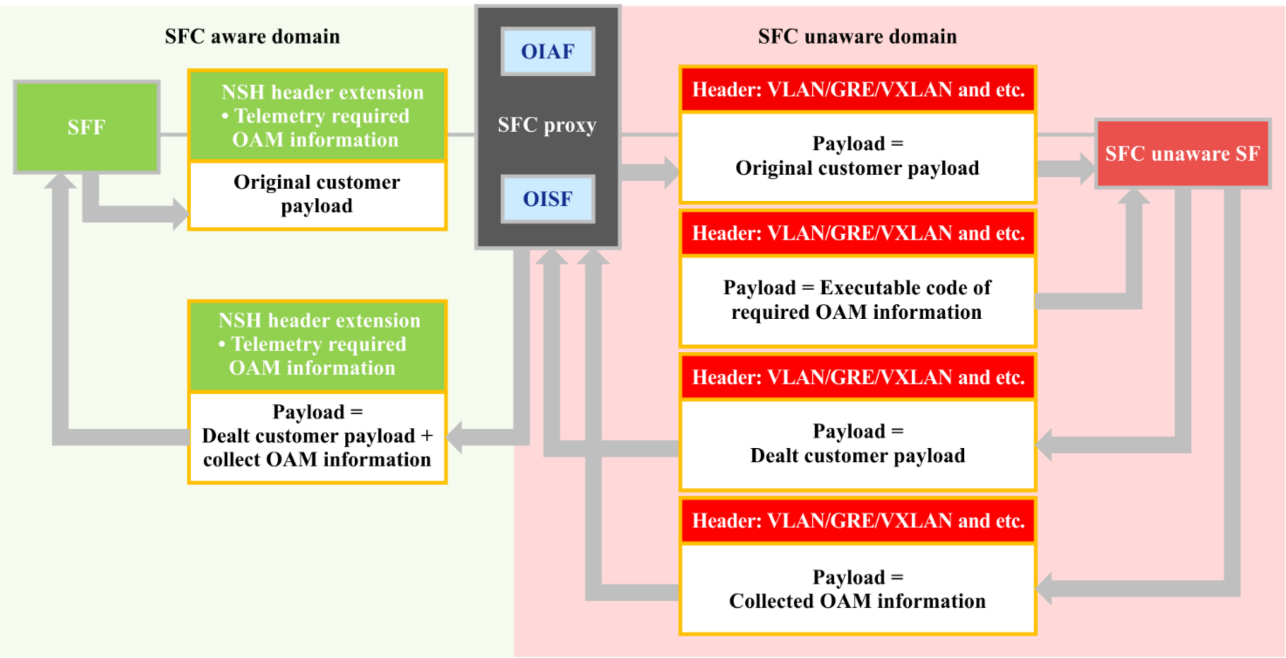
If the integrated evaluation value < T-IDSI, the OISF encapsulates the OAM information in the data packet and sends this packet to the destination of the SFP.

Annex C

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

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

The service function chain (SFC) is composed of several service functions. Some of the service functions are historic legacy devices, no matter whether they are virtual or not, that are not capable of supporting the SFC related protocols. This kind of SF is called SFC unaware SF and within the non-SFC domain. Relevantly, the SF which supports the SFC related protocols is called SFC aware SF and is within the SFC domain. When a service function chain steers the packets to an SFC unaware SF, an SFC proxy is inevitably used to translate and exchange the messages between the two domains (see [b-IETF RFC 7665]). 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 the local attachment circuit. The SF deals with the payload and then returns the new payload to the SFC proxy. The SFC proxy encapsulates the new payload with the NSH header and sends it back to the SFF.



Q.3406(22)

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

In this Recommendation, the required OAM information is carried in the extended NSH header and consequently can only be recognized by an SFC aware device (example: SFC aware SF, SFC proxy, SFF, etc.). It cannot be recognized by an SFC unaware SF. So, the OAM information of an 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.

Step 1: The SFC proxy resolves the OAM required information from the extended NSH header. Meanwhile, it decapsulates the customer's original payload from the packets.

Step 2: The SFC proxy launches the OIAF function to figure out the OAM information that should be collected from the SFC unaware SF.

Step 3: 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.

Step 4: The SFC proxy encapsulates this customer's original payload with the protocols used to exchange messages between the SFC proxy and SFC unaware SF. This packet is called packet 2.

Step 5: When the SFC unaware SF receives the packet 1, it resolves the payload from the packet and runs the dedicated piece of executable code within the payload to collect the OAM information.

Step 6: The SFC unaware SF encapsulates this payload of collected OAM information with the protocols used to exchange messages between the SFC proxy and the SFC unaware SF (SFC unaware domain) and send the packet to the SFC proxy.

Step 7: 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.

Step 8: The SFC unaware SF encapsulates this payload of dealt customer data payload with the protocols used to exchange messages between the SFC proxy and the SFC unaware SF (SFC unaware domain) and sends the packet to the SFC proxy.

Step 9: The SFC proxy receives the packets and isolates the headers and payloads. The payload is the customer data payload or the collected OAM information payload.

Step 10: The OIAF function within the SFC proxy evaluates the collected OAM information and makes the decision whether to collect the other category of OAM information from the SFC unaware SF or not.

Step 11: If it is necessary to collect other OAM information from the SFC unaware SF, the SFC proxy will repeat Step 3 ~ Step 9.

Step 12: 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 the 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 an 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.

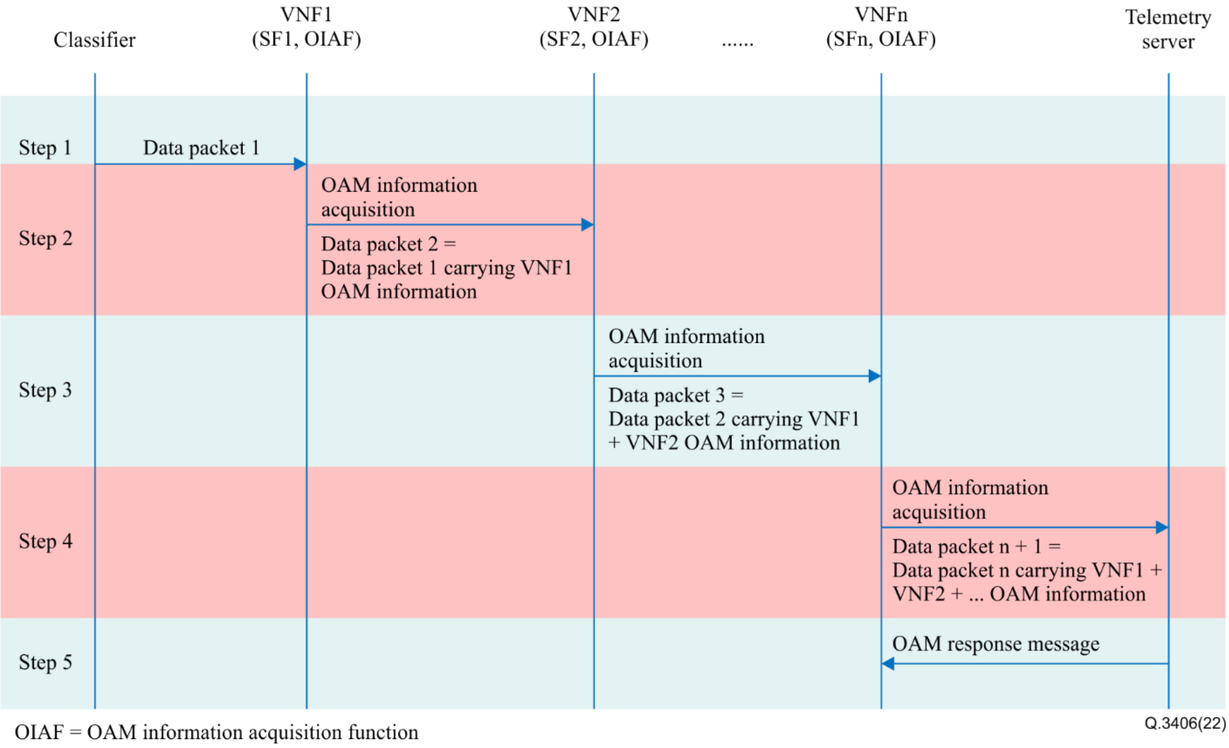


Figure I.1 – The procedure of the centralized way

– **The distributed way**

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

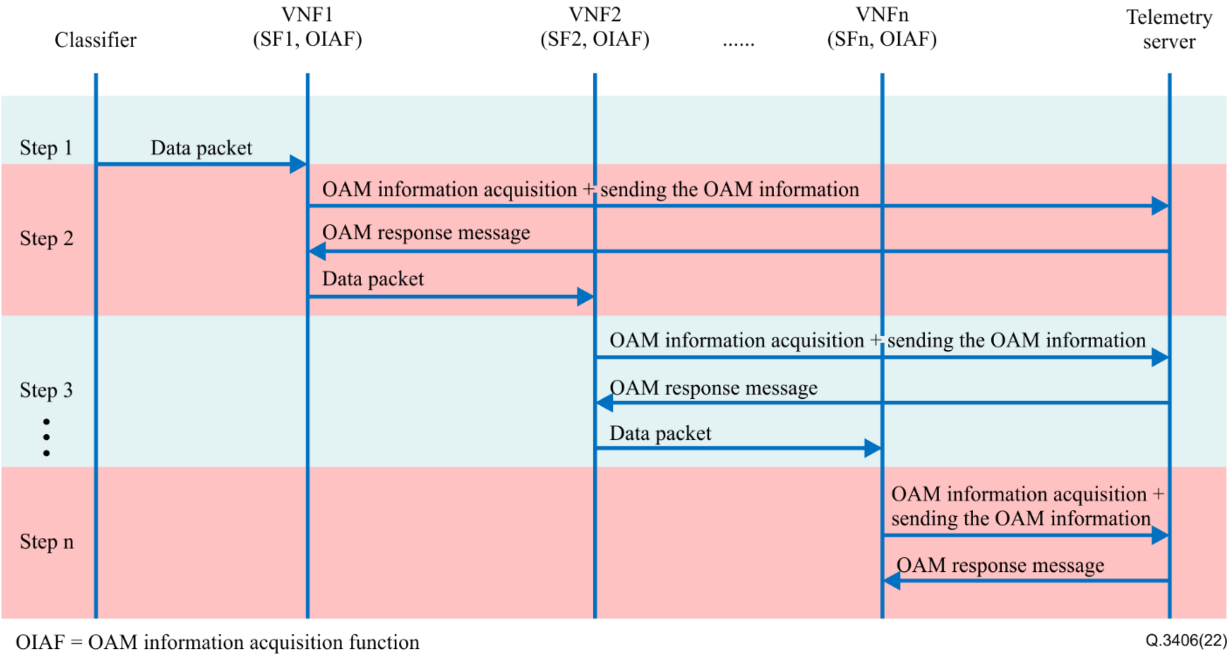

Classifier
VNF1 (SF1, OIAF)
VNF2 (SF2, OIAF)
......
VNFn (SFn, OIAF)
Telemetry server
Step 1
Data packet
Step 2
OAM information acquisition + sending the OAM information
OAM response message
Data packet
Step 3
OAM information acquisition + sending the OAM information
OAM response message
Data packet
Step n
OAM information acquisition + sending the OAM information
OAM response message
OIAF = OAM information acquisition function
Q.3406(22)

Figure I.2 – The procedure of the distributed way

– **The hybrid way**

The hybrid way is a combination of the centralized way and distributed way.

In the distributed way, many messages are exchanged between the VNFs and the telemetry servers and this consumes too many network resources. For the centralized way, only two messages are enough to acknowledge the telemetry server of the OAM information. However, if there is a network failure on one of the SF's on the path, the packet will not be possible to reach the destination and all the OAM information of the SFs will not be acknowledged to the telemetry server.

The hybrid way solves these problems by giving the 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 can satisfy the requirements of not only consuming less network resources as possible but also sending the information efficiently.

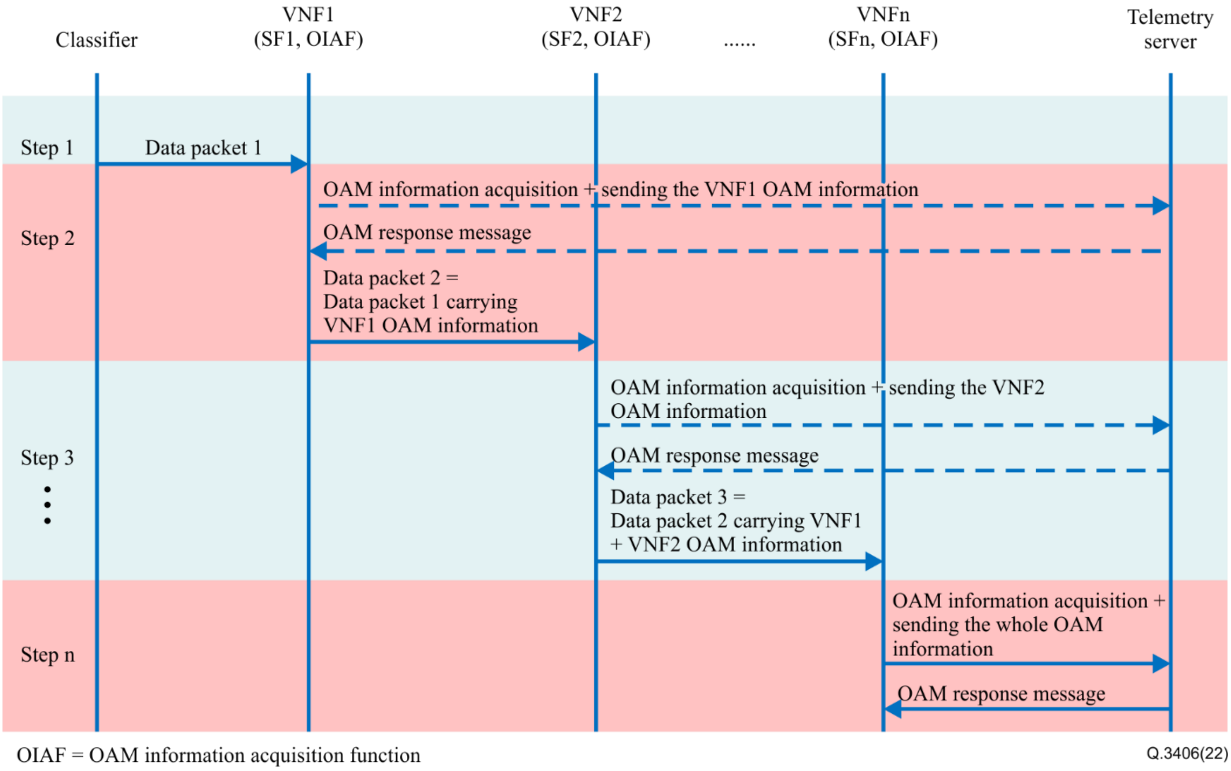


Figure I.3 – The procedure of the hybrid way

Bibliography

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

[b-IETF RFC 7665] IETF RFC 7665 (2015), *Service Function Chaining (SFC) Architecture*. https://www.rfc-editor.org/rfc/rfc7665.html

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling, and associated measurements and tests**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2022