International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.5023

(08/2021)

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

Signalling requirements and protocols for IMT-2020 – Protocols for IMT-2020

Protocol for managing intelligent network slicing with AI-assisted analysis in IMT-2020 networks

Recommendation ITU-T Q.5023

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
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
Signalling requirements and architecture of IMT-2020	Q.5000–Q.5019
Protocols for IMT-2020	**Q.5020–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.5023

Protocol for managing intelligent network slicing with AI-assisted analysis in IMT-2020 networks

Summary

Recommendation ITU-T Q.5023 specifies the protocol for managing intelligent network slicing with AI-assisted network analysis function in International Mobile Telecommunications (IMT)-2020 networks. It describes the architectural concept of intelligent network slicing application programming interfaces (APIs) and management systems, reference points among relevant functional elements, signalling flows over each reference point, and message formats with detailed information.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.5023	2021-08-29	11	11.1002/1000/14767

Keywords

AI-assisted, API management, IMT-2020, network slice.

* 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.5023

Protocol for managing intelligent network slicing with AI-assisted analysis in IMT-2020 networks

1 Scope

This Recommendation specifies the protocol for managing intelligent network slicing with AI-assisted network analysis function in IMT-2020 networks. It describes the architectural concept of intelligent network slicing application programming interface (APIs) and management system, reference points among relevant functional elements, signalling flows over each reference point, and message formats with detail information.

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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 IMT-2020 [b-ITU-T Y.3100]: (Based on [b-ITU-R M.2083) Systems, system components, and related technologies that provide far more enhanced capabilities than those described in [b-ITU-R M.1645].

3.1.2 management [b-ITU-T Y.3100]: In the context of IMT-2020, the processes aiming at fulfilment, assurance, and billing of services, network functions, and resources in both physical and virtual infrastructure including compute, storage, and network resources.

3.1.3 network function [b-ITU-T Y.3100]: In the context of IMT-2020, a processing function in a network.

3.1.4 network slice [b-ITU-T Y.3100]: A logical network that provides specific network capabilities and network characteristics.

3.1.5 third party (3rd party) [b-ITU-T Y.3100]: In the context of IMT-2020, with respect to a given network operator and network end-users, an entity which consumes network capabilities and/or provides applications and/or services.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 data analysis function (DAF): A network function that can collect, analyse, and provide data from/to International Mobile Telecommunications 2020 (IMT-2020) core network functions, network management and third-party applications.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

DAF Data Analysis Functions

IE Information Element

IMT International Mobile Telecommunications

MOS Mean Opinion Score

NF Network Function

PCF Policy Control Function

QoE Quality of Experience

SLA Service Level Agreement

5 Conventions

In this Recommendation:

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

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "can optionally" indicate an optional requirement that is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

The letter "M" indicates the element is mandatory. The letter "O" indicates the element is optional. The letter "C" indicates the element is conditional.

6 Overview

Intelligent network slicing with AI-assisted functions is capable of allocating limited resources to meet the service level agreement (SLA) of slicing users in real time dynamically. It is necessary to develop an intelligent network slicing API framework which makes the IMT-2020 network more efficient and flexible. The framework includes common aspects and some functional APIs which provide AI-assisted functions.

7 API architecture and definition

Figure 7-1 shows the architectural concept of intelligent network slicing APIs and management system which includes IMT-2020 network, network management, data analysis function (DAF) and API management function. It also shows the relationship between the data analysis function with the IMT-2020 core network and related network functions.

Data analysis function provides functionalities to collect data, data analysis, mean opinion score (MOS) training and QoE (Quality of Experience) calculation, which will assist in meeting the requirements of network slicing users.

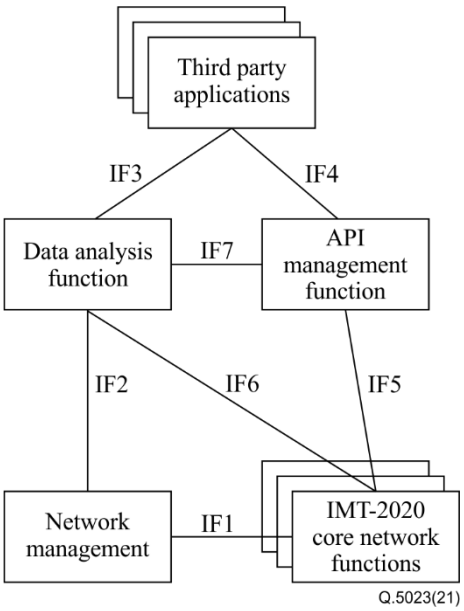

Figure 7-1 – Architectural concept of intelligent network slicing API system

The 3rd party applications can provide service or application related data to the data analysis function by using Application_Data_Collection service.

The API management function is mainly responsible for the management and orchestration of intelligent network slicing APIs, such as Application_Data_Collection API.

The IF1 reference point exists between the network management and the IMT-2020 core network functions (NFs). It supports the management and orchestration of NFs, such as performance related data reporting and NFs configuration policies distribution.

The IF2 reference point exists between the data analysis function and the network management. Data of the network slices monitored by the network management could be sent to the data analysis function by IF2, and the network data analysis results are notified to the network management based on subscription.

The IF3 reference point is the northbound interface that exists between the data analysis function and the third-party applications. It supports slice service-related data collection, and data analysis results exposed to the third-party applications.

The IF4 reference point is the northbound interface that exists between the API management function and third-party applications. It supports discovery, modification, deletion, and other management functions of API provided by 3rd party applications.

The IF5 reference point exists between the API management and NFs. It supports the management of NF capability exposure related APIs.

The IF6 reference point exists between the data analysis function and NFs. It supports the network slice data collection and analysis results offer to IMT-2020 core networks.

The IF7 reference point exists between the API management function and the data analysis function. It supports the management of data analysis exposure related API.

8 Signalling flow

This clause describes the signalling flow procedures in data collection and analysis, MOS training, QoE calculation, etc.

8.1 Data collection flow

This clause describes the signalling flow of data collection which is fulfilled by the data analysis function.

The data collection procedures can be initiated by the data analysis function, 3rd party applications and IMT-2020 core network functions.

8.1.1 DAF triggered periodic data collection flow

Figures 8-1 to 8-3 describe the DAF triggered periodic data collection flow.

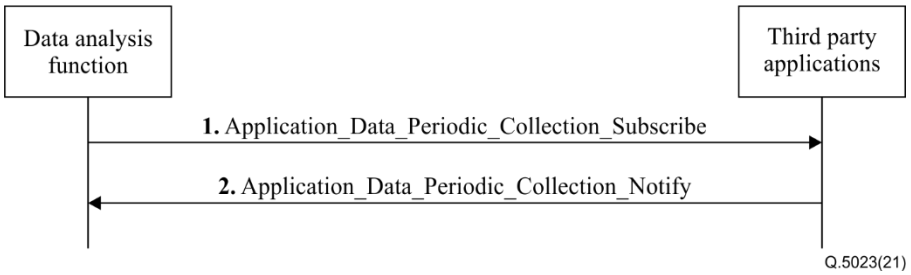

Figure 8-1 – Signalling flow for subscribing periodic data collection from 3rd party applications

1. Data analysis function subscribes the application service data from 3rd party applications by invoking Application_Data_Periodic_Collection_Subscribe service to create a new subscription and modify an existing subscription. It includes UE level sample data, application information and user information.
2. The 3rd party applications notify the data analysis function by invoking Application_Data_Periodic_Collection_Notify service operation. It includes user experience data and related information.

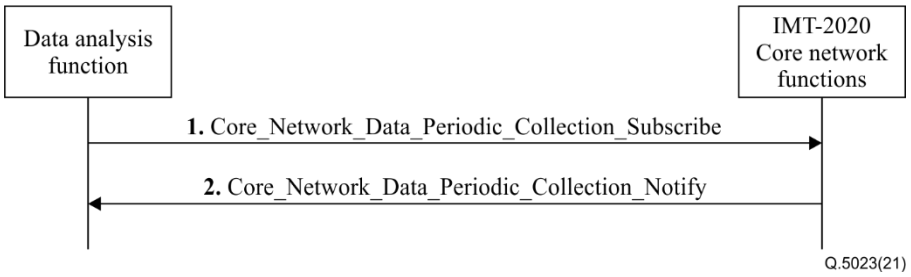

Figure 8-2 – Signalling flow for subscribing periodic data collection from IMT-2020 core network

1. Data analysis function subscribes to the network function service data from IMT-2020 core network functions by invoking Core_Network_Data_Periodic_Collection_Subscribe service to create a new subscription and modify an existing subscription. It includes NF level performance measurement data and network level KPI data.
2. The core network functions notify the data analysis function by invoking the Core_Network_Data_Periodic_Collection_Notify service operation.

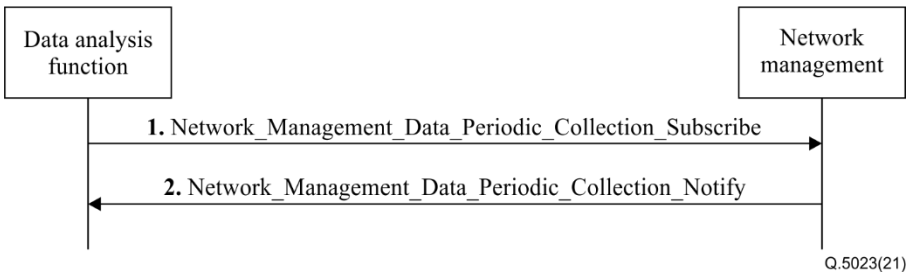

Figure 8-3 – Signalling flow for subscribing periodic data collection from network management

1. Data analysis function subscribes the service data from network management by invoking Network_Management_Data_Periodic_Collection_Subscribe service to create a new subscription and modify an existing subscription. It includes sample data, NF level performance measurement data, network coverage area, number of subscribers, fault supervision data, resource usage data and network level KPI data.
2. The network management notify the data analysis function by invoking Network_Management_Data_Periodic_Collection_Notify service operation.

8.1.2 DAF triggered data collection flow

Figures 8-4 to 8-6 describe the DAF triggered data collection flow.

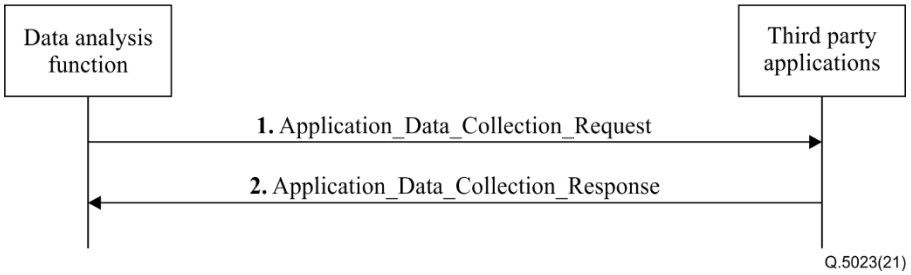

Figure 8-4 –DAF triggered signalling flow for data collection from 3rd party applications

1. Data analysis function requests for application service data from 3rd party applications by invoking Application_Data_Collection_Request. It includes UE level sample data, application information and user information.
2. The 3rd party applications send a response to the data analysis function by invoking Application_Data_Collection_Response. It includes user experience data and related information.

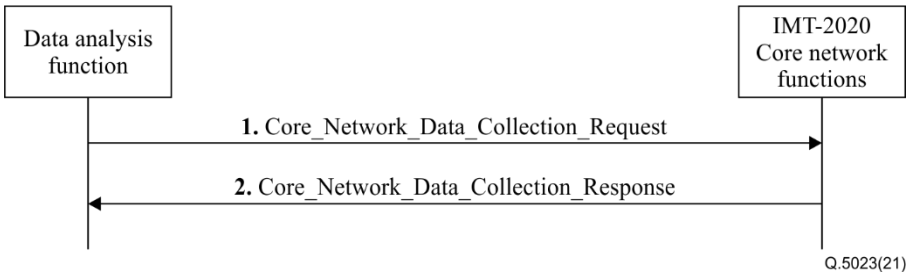

Figure 8-5 – DAF triggered signalling flow for data collection from IMT-2020 core network

1. Data analysis function requests for network function service data from IMT-2020 core network functions by invoking Core_Network_Data_Collection_Request. It includes NF level performance measurement data and network level KPI data, like data bandwidth, data

rate, latency data, data latency measurement period, data latency jitter measurement frequency, data latency retrieving times and other KPI information.

2. The core network functions send a response to the data analysis function by invoking Core_Network_Data_Collection_Response. For example, DAF can evaluate the data latency jitter based on latency data, data latency measurement period, data latency jitter measurement frequency, data latency retrieving times and provide it to policy control function (PCF).

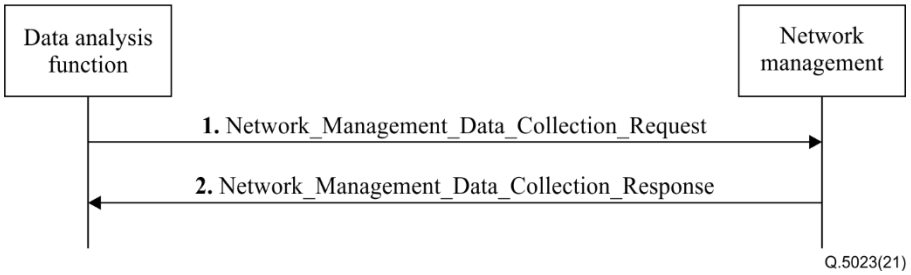

Figure 8-6 – DAF triggered signalling flow for data collection from network management

1. Data analysis function requests for service data from network management by invoking Network_Management_Data_Collection_Request.

2. The network management sends a response to data analysis function by invoking Network_Management_Data_Collection_Response. It includes sample data, NF level performance measurement data, network coverage area, number of subscribers, fault supervision data, resource usage data and network level KPI data.

8.1.3 3rd party application triggered service data report flow

Figures 8-7 and 8-8 describe the 3rd party application triggered service data report flow.

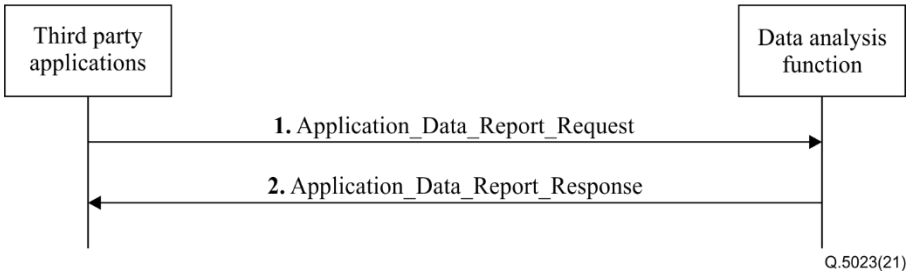

Figure 8-7 – 3rd party application triggered data report signalling flow

1. 3rd party applications send a request to the data analysis function to report 3rd party application service data. It includes UE level sample data and user experience data.

2. Data analysis function sends a response to 3rd party application by invoking Application_Data_Report_Response to indicate receiving of application service data.

8.1.4 Core network functions triggered service data report flow

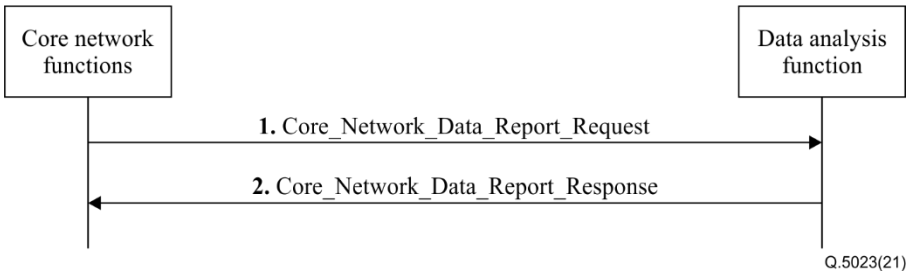

Figure 8-8 – Core network functions triggered data report signalling flow

1. Core network functions send a request to data analysis function to report network data. It includes NF level performance measurement data and network level KPI data, e.g., data bandwidth, data rate, data latency jitter and other KPI information.
2. Data analysis function sends a response to the core network functions by invoking the Core_Network_Data_Report_Response to indicate receiving of core network function data.

8.1.5 Network management triggered network data report flow

The network management triggered network data report flow is described in Figure 8-9.

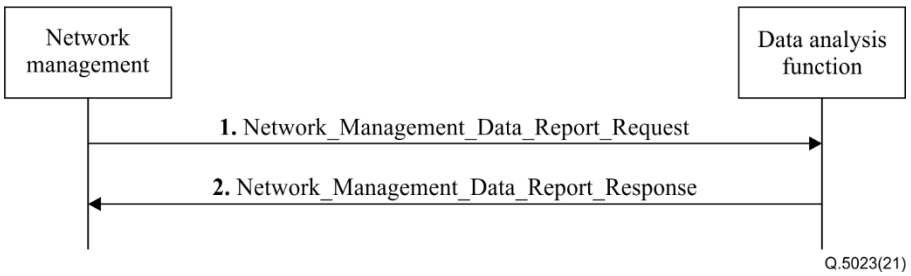

Figure 8-9 – Network management triggered network data report flow

1. Network management sends a request to data analysis function to report network data. It includes sample data, NF level performance measurement data, number of subscribers, network coverage area, fault supervision data, resource usage data and network level KPI data.
2. Data analysis function sends a response to network management by invoking Network_Management_Data_Report_Response to indicate receiving of network management data.

8.2 MOS training flow

8.2.1 MOS query flow

The MOS query flow is described in Figure 8-10.

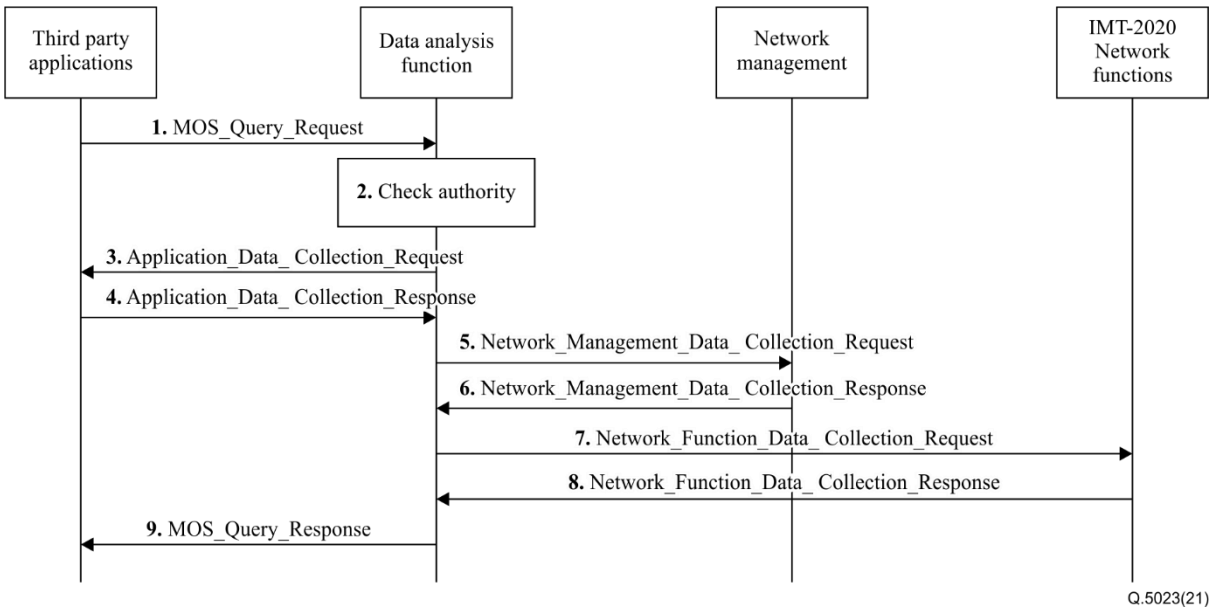

Figure 8-10 – MOS query flow

1. The 3rd party applications send a request to query MOS of specific UEs or applications by invoking MOS_Query_Request. It includes UE ID or application ID.
2. Data analysis function checks authorization information to make sure whether the 3rd party application is authorized to access the MOS.
3. Data analysis function collects 3rd party application data from 3rd party applications by invoking Application_Data_Periodic_Collection_Subscribe or Application_Data_Collection_Request.
4. The 3rd party application sends data collection response to data analysis function.
5. Data analysis function collects network management data from network management by invoking Network_Management_Data_Periodic_Collection_Subscribe or Network_Management_Data_Collection_Request.
6. Network management sends data collection response to the data analysis function.
7. Data analysis function collects core network function data from IMT-2020 network functions by invoking Core_Network_Data_Collection_Request.
8. IMT-2020 network functions send data collection response to data analysis function.
9. DAF trains MOS based on the UE ID, application information and training algorithm. Data analysis function sends MOS of UE/application to the 3rd party application.

8.2.2 MOS modification flow

The MOS modification flow is described in Figure 8-11.

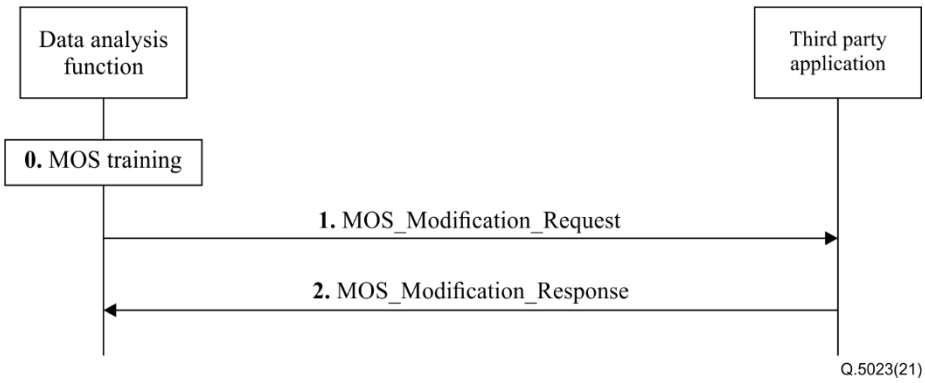

Figure 8-11 – MOS modification flow

0. DAF trains MOS of the network slicing based on the UE ID, application service data, network function data collected from core network function, 3rd party application and network management and training algorithm.
1. DAF sends updated MOS by invoking MOS_Modification_Request. DAF trains MOS and updates it regularly based on the time required by the 3rd party application.
2. The 3rd party application responds to DAF by invoking MOS_Modification_Response, which indicates whether updated MOS is successfully received. The 3rd party application adjusts requirements based on the updated MOS.

8.3 QoE calculation flow

The QoE calculation flow is described in clauses 8.3.1 to 8.3.4 and Figures 8-12 to 8-15.

8.3.1 Network management subscribe QoE flow

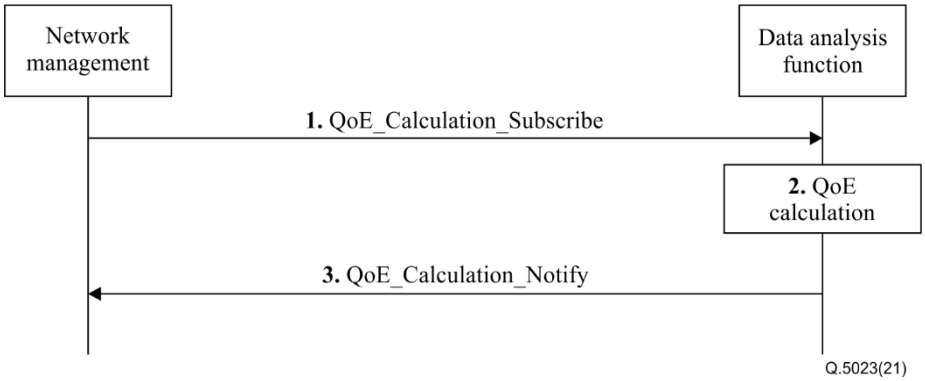

Figure 8-12 – Network management subscribe QoE flow

1. Network management subscribes QoE information notification by invoking QoE_Calculation_Subscribe. It includes network slicing ID which network management requires QoE to justify the resource of slicing to ensure service level agreement (SLA), customer satisfaction and time interval.
2. DAF calculates QoE of the network slicing based on the user data, application service data, network function data collected from core network function, 3rd party application, network management and MOS training by DAF.
3. DAF sends updated QoE regularly by invoking QoE_Calculation_Notify.

8.3.2 DAF update QoE flow

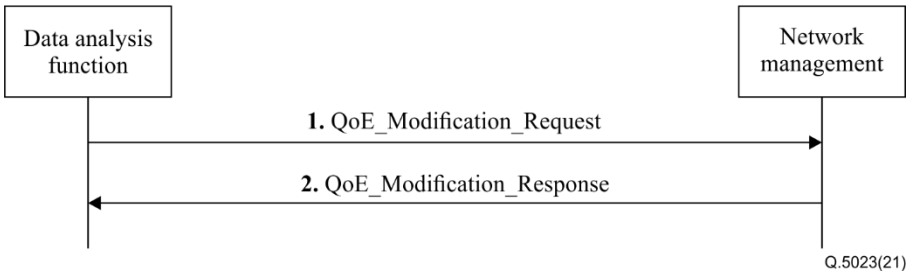

Figure 8-13 – Network management modification QoE flow

1. DAF calculates QoE of network slicing which network management requires based on the user data, application service data and network function data collected from core network function, 3rd party application, network management and MOS training by DAF. DAF sends the updated QoE by invoking QoE_Modification_Request. DAF calculates QoE and updates it regularly based on the time required by network management.
2. Network management sends the response to DAF by invoking QoE_Modification_Response. Network management adjusts the resource of the network slicing based on the updated QoE to ensure service level agreement.

8.3.3 Network management query QoE of UE/application/network slice flow

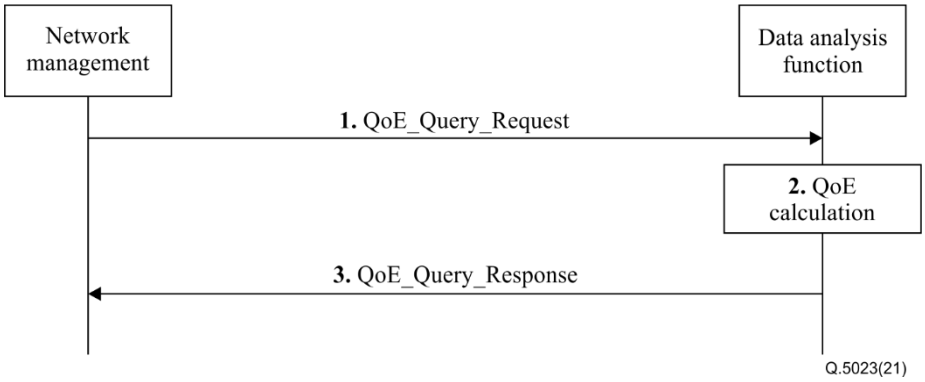

Figure 8-14 – Network management subscribe QoE flow

1. The network management sends QoE_Query_Request to DAF to query QoE information. It includes network slicing ID which network management requires QoE to justify the resource of slicing to ensure service level agreement and time interval.
2. DAF calculates QoE of network slicing which network management requires based on the user data, application service data, network function data collected from core network function, 3rd party application, network management and MOS training by DAF.
3. DAF sends QoE to network management by invoking QoE_Query_Response.

8.3.4 DAF triggered alert of QoE flow

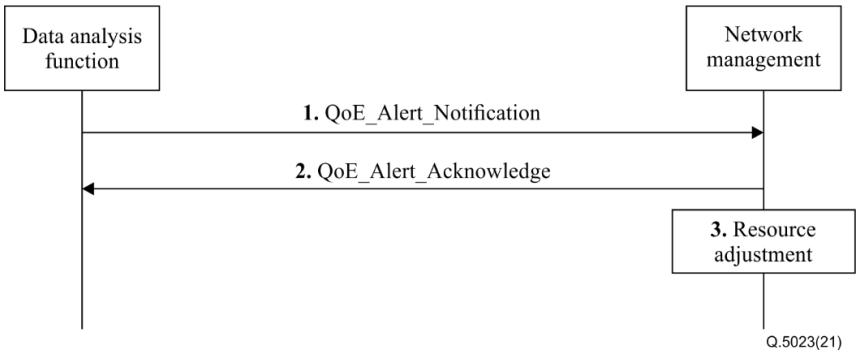

Figure 8-15 – Network management subscribe QoE flow

0. Network management has subscribed periodic QoE query to DAF.
1. DAF calculates QoE based on the user data, application service data, network function data collected from core network function, 3rd party application, network management and MOS training by DAF regularly. DAF compares current QoE with the QoE requirements. DAF sends QoE_Alert_Notification to network management if the current QoE does not meet the network slicing service requirements.
2. Network management sends QoE_Alert_Acknowledge to DAF.
3. Network management adjusts the resource of network slicing to meet the service requirements.

9 Message format

This clause describes the message formats, including message name, information of message carrying, and type of message, etc.

9.1 Application_Data_Periodic_Collection

This message is sent to 3rd party applications to subscribe for application data. 3rd party applications will report user experience data and related information over IF3.

Table 9-1 describes in detail information of Application_Data_Periodic_Collection_Subscribe:

Table 9-1 – Application_Data_Periodic_Collection_Subscribe

Information element	Status	Data type	Cardinality	Description
3rd party application identity information	C	string	1..N	Identity information of the 3rd party application of which DAF requires data. If DAF subscribe data at the application level, this information element (IE) shall be present.
Name of the 3rd party application vendor	O	string	1..N	The name of the 3rd party application vendor.
UE ID	C	string	1..N	UE ID of which DAF requires data. DAF subscribe data of users of the 3rd party application if both 3rd party application identity information and UE ID are present. At least one of these two IE shall be present.
Sample data	O	string	1..N	This IE indicates sample data for user experience training.
Periodic	M	string	1	Periodic user experience data report.

Table 9-2 describes in detail information of Application_Data_Periodic_Collection_Notify:

Table 9-2 – Application_Data_Periodic_Collection_Notify

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of the data collection subscribe. 200 OK 400 Input parameter error 500 Server internal error
User experience data	M	string	1..N	N/A	User experience data of a user of 3rd party application.
3rd party application identity information	O	string	1	N/A	Identity information of the 3rd party application of the user experience data. This IE shall be present if user experience data is collected at the application level.
UE ID	O	string	1..N	N/A	UE ID of user experience data. This IE shall be present if user experience data is collected in the UE level.
Time information	M	string	1..N	N/A	Time information of the user experience data which is collected.

9.2 Core_Network_Data_Periodic_Collection

This message is sent to core network functions to subscribe for network data. Core network functions will report NF level performance measurement data and network level KPI data over IF6.

Table 9-3 describes in detail information of Core_Network_Data_Periodic_Collection_Subscribe:

Table 9-3 – Core_Network_Data_Periodic_Collection_Subscribe

Information element	Status	Data type	Cardinality	Description
Network function information	M	string	1..N	Identity information of the core network function which offers storage, network, computing resource and other information.
Network KPI	M	string	1..N	Indicates the KPI information DAF request to subscribe. KPI is the key information of the network instance to which users belong to. It includes data bandwidth, latency, data rate and other KPI information.

Table 9-3 – Core_Network_Data_Periodic_Collection_Subscribe

Information element	Status	Data type	Cardinality	Description
UE ID	O	string	1..N	UE ID of which DAF requires data.
Sample data	O	string	1..N	This IE indicates sample data for network experience training for users.
Periodic	M	string	1	Periodic data report of network experience training for user's report.

Table 9-4 describes in detail information of Core_Network_Data_Periodic_Collection_Notify:

Table 9-4 – Core_Network_Data_Periodic_Collection_Notify

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of the core network data collection subscribe. 200 OK 400 Input parameter error 500 Server internal error
Network function information	M	string	1..N	N/A	Identity information of the core network function which offer storage, network, computing resource and other information.
Network KPI data	O	string	1..N	N/A	Identify KPI information of network instance which users belong to. It includes data bandwidth, latency, data rate and other KPI information.
UE ID	O	string	1..N	N/A	UE ID of which core network offer data.
Time information	M	string	1..N	N/A	Time information of the user experience data which is collected.

9.3 Network_Management_Data_Periodic_Collection

This message is sent to network management to subscribe for network management data. Network management will report network data and related information over IF2.

Table 9-5 describes in detail information of Network_Management_Data_Periodic_Collection_Subscribe:

Table 9-5 – Network_Management_Data_Periodic_Collection_Subscribe

Information element	Status	Data type	Cardinality	Description
UE ID	M	string	1..N	UE ID of which DAF requires training data.
Network function information	M	string	1..N	Identity information of the core network function which offer storage, network, computing resource and other information.
Network KPI	M	string	1..N	Indicates the KPI information DAF requests to subscribe. KPI is the key information of network instance to which users belong to. It includes data bandwidth, latency, data rate and other KPI information.
Periodic	M	string	1	Periodic user experience data report.
Network coverage area	M	string	1	Indicates coverage of the network slicing.
Number of subscribers	M	num	1	Indicates the number of subscribers of a network slicing/3rd party application.
Fault supervision	O	string	1	Indicates the number and list of network fault events.
Resource usage	M	string	1	Percent or absolute value of the used resource, including but not limited to computing, network, storage resource

Table 9-6 describes in detail information of Network_Management_Data_Periodic_Collection_Notify:

Table 9-6 – Network_Management_Data_Periodic_Collection_Notify

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of the data collection request. 200 OK 400 Input parameter error 500 Internal server error
Sample data	M	string	1..N	N/A	This IE indicates sample data for network experience training for users.
Time information	M	string	1..N	N/A	Time information of the network management data is collected.

9.4 Application_Data_Collection

This message is sent to 3rd party applications to request application data. 3rd party applications will report user experience data and related information over IF3.

Table 9-7 describes in detail information of Application_Data_Collection_Request:

Table 9-7 – Application_Data_Collection_Request

Information element	Status	Data type	Cardinality	Description
3rd party application identity information	C	string	1..N	Identity information of the 3rd party application of which DAF requires data. If DAF subscribes data at the application level, this IE shall be present.
Name of the 3rd party application vendor	O	string	1..N	The name of the 3rd party application vendor.
UE ID	O	string	1..N	UE ID of which DAF requires data. DAF requests data of users of the 3rd party application if both 3rd party application identity information and UE ID are present. At least one of these two IE shall be present.
Sample data	O	string	1..N	This IE indicates sample data for network experience training for users.

Table 9-8 describes in detail information of Application_Data_Collection_Response:

Table 9-8 – Application_Data_Collection_Response

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of the data collection request. 200 OK 400 Input parameter error 500 Server internal error
User experience data	M	string	1..N	N/A	User experience data of user of 3rd party application.
3rd party application identity information	O	string	1	N/A	Identity information of the 3rd party application of the user experience data. This IE shall be present if user experience data is collected in the application level.
UE ID	O	string	1..N	N/A	UE ID of user experience data. This IE shall be present if user experience data is collected in UE level.
Time information	M	string	1..N	N/A	Time information of the user experience data which is collected.

9.5 Core_Network_Data_Collection

This message is sent to core network functions to request for network data. Core network functions will report NF level performance measurement data and network level KPI data over IF6.

Table 9-9 describes in detail information of Core_Network_Data_Collection_Request:

Table 9-9 – Core_Network_Data_Collection_Request

Information element	Status	Data type	Cardinality	Description
Network function information	M	string	1..N	Identifies which network function that DAF requests for information, like storage, network, computing resource and other information.
Network KPI	M	string	1..N	Indicates the KPI information DAF requests to subscribe. KPI is the key information of network instance to which users belong to. It includes data bandwidth, latency, data rate, data latency jitter and other KPI information.
UE ID	O	string	1..N	UE ID of which DAF requires data.
Sample data	O	string	1..N	This IE indicates sample data for network experience training for users.

Table 9-10 describes in detail information of Core_Network_Data_Collection_Response:

Table 9-10 – Core_Network_Data_Collection_Response

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of the core network data collection request. 200 OK 400 Input parameter error 500 Server internal error
Network function information	M	string	1..N	N/A	Identity information of the core network function which offer storage, network, computing resource and other information.
Network KPI data	O	string	1..N	N/A	Identifies the KPI information of network instance to which users belong to. It includes data bandwidth, latency, data rate and other KPI information.
UE ID	O	string	1..N	N/A	UE ID of which core network offer data.
Time information	M	string	1..N	N/A	Time information of network experience training for users.

9.6 Network_Management_Data_Collection

This message is sent to network management to request for network data. Network management will report sample data, NF level performance measurement data and network level KPI data over IF2.

Table 9-11 describes in detail information of Network_Management_Data_Collection_Request:

Table 9-11 – Network_Management_Data_Collection_Request

Information element	Status	Data type	Cardinality	Description
UE ID	M	string	1..N	UE ID of which DAF requires training data.
Sample data	M	string	1..N	This IE indicates sample data for network management.
Network function information	M	string	1..N	Identifies which network function that DAF requests for information, like storage, network, computing resource and other information.
Network KPI	M	string	1..N	Indicates the KPI information DAF requests to subscribe. KPI is the key information of network instance to which users belong to. It includes data bandwidth, latency, data rate and other KPI information.
Network coverage area	M	string	1	Indicates coverage of the network slicing which DAF requests.
Number of subscribers	M	num	1	Indicates the number of subscribers of a network slicing/3rd party application that DAF requests.
Fault supervision	O	string	1	Indicates the number and list of network fault events of network slicing which DAF requests.
Resource usage	M	string	1	Percent or absolute value of used resource which DAF requests, including but not limited to computing, network, storage resource

Table 9-12 describes in detail information of Network_Management_Data_Collection_Response:

Table 9-12 – Network_Management_Data_Collection_Response

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of the network data collection request. 200 OK 400 Input parameter error 500 Internal server error
User experience data	M	string	1..N	N/A	User experience data of user which DAF requests.
Network function information	M	string	1..N	N/A	Identity information of the core network function which offer storage, network, computing resource and other information.
Network KPI data	M	string	1..N	N/A	Identifies the KPI information of network instance to which users belong to. It includes data bandwidth, latency, data rate and other KPI information.
Network coverage area	M	string	1	N/A	Indicates coverage of the network slicing.
Number of subscribers	M	num	1	N/A	Indicates the number of subscribers of a network slicing/3rd party application.
Fault supervision	O	string	1	N/A	Indicates the number and list of network fault events.
Resource usage	M	string	1	N/A	Percent or absolute value of used resource, including but not limited to computing, network, storage resource
Time information	M	string	1..N	N/A	Time information of network management data which is collected.

9.7 Application_Data_Report

This message is sent to the data analysis function to report application data from 3rd party applications. Data analysis function will send a response to 3rd party application over IF3.

Table 9-13 describes in detail information of Application_Data_Report_Request:

Table 9-13 – Application_Data_Report_Request

Information element	Status	Data type	Cardinality	Description
User experience data	M	string	1..N	User experience data of user of 3rd party application.
3rd party application identity information	O	string	1	Identity information of the 3rd party application of the user experience data. This IE shall be present if user experience data is collected in application level.
UE ID	O	string	1..N	UE ID of user experience data. This IE shall be present if user experience data is collected in UE level.
Time information	M	string	1..N	Time information of the user experience data is collected.

Table 9-14 describes in detail information of Application_Data_Report_Response:

Table 9-14 – Application_Data_Report_Response

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of the data report request. 200 OK 400 Input parameter error 500 Server internal error

9.8 Core_Network_Data_Report

This message is sent to the data analysis function to report for network data from core network functions, including NF level performance measurement data and network level KPI data. Data analysis function will send a response to core network functions over IF6.

Table 9-15 describes in detail information of Core_Network_Data_Report_Request:

Table 9-15 – Core_Network_Data_Report_Request

Information element	Status	Data type	Cardinality	Description
Network function information	M	string	1..N	Identity information of the core network function which offers storage, network, computing resource and other information.
Network KPI data	M	string	1..N	Identifies the KPI information of network instance to which users belong to. It includes data bandwidth, latency data, data rate, data latency measurement

Table 9-15 – Core_Network_Data_Report_Request

Information element	Status	Data type	Cardinality	Description
				period, data latency jitter measurement frequency, data latency retrieving times and other KPI information.
UE ID	O	string	1..N	UE ID of which DAF requires data.
Time information	M	string	1..N	Time information of the user experience data which is collected.

Table 9-16 describes in detail information of Core_Network_Data_Report_Response:

Table 9-16 – Core_Network_Data_Report_Response

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of the core network data collection request. 200 OK 400 Input parameter error 500 Server internal error

9.9 Network_Management_Data_Report

This message is sent to the data analysis function to report the network management data from network management, including sample data, NF level performance measurement data and network level KPI data. Data analysis function will send a response to network management over IF2.

Table 9-17 describes in detail information of Network_Management_Data_Report_Request:

Table 9-17 – Network_Management_Data_Report_Request

Information element	Status	Data type	Cardinality	Description
User experience data	M	string	1..N	User experience data of user which DAF requests or subscribes.
Network function information	M	string	1..N	Identity information of the core network function which offer storage, network, computing resource and other information.
Network KPI data	M	string	1..N	Identifies the KPI information of network instance to which users belong to. It includes data bandwidth, latency, data rate and other KPI information.

Table 9-17 – Network_Management_Data_Report_Request

Information element	Status	Data type	Cardinality	Description
Network coverage area	M	string	1	Indicates coverage of the network slicing which DAF requests.
Number of subscribers	M	num	1	Indicates the number of subscribers of a network slicing/3rd party application which DAF requests.
Fault supervision	O	string	1	Indicates the number and list of network fault events of network slicing which DAF requests.
Resource usage	M	string	1	Percent or absolute value of used resource which DAF requests, including but not limited to computing, network, storage resource
Time information	M	string	1..N	Time information of the user experience data is collected.

Table 9-18 describes in detail information of Network_Management_Data_Report_Response:

Table 9-18 – Network_Management_Data_Report_Response

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of the network data report request. 200 OK 400 Input parameter error 500 Internal server error

9.10 MOS_Query

This message is sent to the data analysis function to request MOS information of UEs or application. The data analysis function sends the MOS information to the 3rd party application over IF3.

Table 9-19 describes in detail information of MOS_Query_Request:

Table 9-19 – MOS_Query_Request

Information element	Status	Data type	Cardinality	Description
3rd party application identity information	M	string	1	Identity information which 3rd party application requires MOS information.
Name of the 3rd party application vendor	O	string	1..N	The name of the 3rd party application vendor.

Table 9-19 – MOS_Query_Request

Information element	Status	Data type	Cardinality	Description
UE ID	M	string	1..N	UE ID of which 3rd party application request MOS.
Period	O	string	1	MOS information notification can be periodic. Time interval indicates the time interval of MOS notification. The default value is only one time.

Table 9-20 describes in detail information of MOS_Query_Response:

Table 9-20 – MOS_Query_Response

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of the MOS query. 200 OK 400 Input parameter error 500 Server internal error
MOS	M	string	1	N/A	MOS of the UEs/application which 3rd party requests for.
3rd party application identity information	C	string	1	N/A	Indicates the 3rd party application which 3rd party requires for MOS. This IE shall be present if the MOS is trained in application level.
UE ID	C	string	1..N	N/A	Indicates the UE which 3rd party requires for MOS. This IE shall be present if the MOS is trained at the user level.
Time information	M	string	1..N	N/A	Time information of the MOS information is trained.

9.11 MOS_modification

This message is sent by the data analysis function to report the updated MOS information over IF3.

Table 9-21 describes in detail information of MOS_Modification_Request:

Table 9-21 – MOS_Modification_Request

Information element	Status	Data type	Cardinality	Description
3rd party application identity information	M	string	1	Identity information which 3rd party application requires MOS information.
Name of the 3rd party application vendor	O	string	1..N	The name of the 3rd party application vendor.
UE ID	M	string	1..N	UE ID of which 3rd party application requests MOS.
Time information	O	string	1	Time information indicates the updated MOS notification time.

Table 9-22 describes in detail information of MOS_Modification_Response:

Table 9-22 – MOS_Modification_Response

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of the updated MOS modification. 200 OK 400 Input parameter error 500 Server internal error

9.12 QoE_Subscription

This message is sent to the data analysis function to subscribe for QoE. DAF will calculate QoE of network slicing based on the user data, application service data, network function data collected from core network function, 3rd party application, network management and MOS training by DAF over IF2.

Table 9-23 describes in detail information of QoE_Calculation_Subscribe:

Table 9-23 – QoE_Calculation_Subscribe

Information element	Status	Data type	Cardinality	Description
Network slicing ID	M	string	1..N	Identity information of the network slicing which network management query about.
QoE threshold	O	string	1..N	QoE threshold of the network slicing. Network management sends a value of QoE to DAF. DAF will monitor QoE and sends an alert notification to network management if QoE is out of the QoE threshold.
Period	M	string	1	Periodic QoE calculation and notification.

Table 9-24 describes in detail information of QoE_Calculation_Notify:

Table 9-24 – QoE_Calculation_Notify

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of QoE calculation subscribe. 200 OK 400 Input parameter error 500 Internal server error
QoE	M	string	1..N	N/A	QoE of the network slicing network management requests.
Network slicing ID	M	string	1..N	N/A	List of network slicing which DAF has authority to collect data and calculate QoE.
Abnormal NS	M	string	1..N	N/A	List of network slicing which DAF does not have authority to collect data and calculate QoE.
Time information	M	string	1..N	N/A	Time information of the QoE which is calculated.
Customer satisfaction	O	num	1..N	N/A	Indicates the satisfaction of network slicing like 3rd party applications. Higher the score, higher the satisfaction.

9.13 QoE_Modification

This message is sent to network management to update QoE over IF2.

Table 9-25 describes in detail information of QoE_Modification_Request:

Table 9-25 – QoE_Modification_Request

Information element	Status	Data type	Cardinality	Description
Network slicing ID	M	string	1..N	Identity information of the network slicing which DAF calculates for QoE.
QoE	M	string	1..N	QoE of the network slicing updated by DAF.
Time information	M	string	1	Time information of the updated QoE.

Table 9-26 describes in detail information of QoE_Modification_Response:

Table 9-26 – QoE_Modification_Response

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of the QoE modification. 200 OK 400 Input parameter error 500 Server internal error

9.14 QoE_Query

This message is sent to the data analysis function to query about QoE. DAF will calculate QoE of network slicing based on the user data, application service data, network function data collected from core network function, 3rd party application, network management and MOS training by DAF over IF2. Network management can query about QoE of network slicing by invoking QoE_Query if the network management does not subscribe to QoE query service.

Table 9-27 describes in detail information of QoE_Query_Request:

Table 9-27 – QoE_Query_Request

Information element	Status	Data type	Cardinality	Description
Network slicing ID	M	string	1..N	Identity information of the network slicing which network management query for.

Table 9-28 describes in detail information of QoE_Query_Response:

Table 9-28 – QoE_Query_Response

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of the QoE query. 200 OK 400 Input parameter error 500 Server internal error
QoE	M	string	1..N	N/A	QoE of the network slicing which network management requests.
Network Slicing ID	M	string	1..N	N/A	List of network slicing which DAF has authority to collect data and calculate QoE.
Abnormal NS	M	string	1..N	N/A	List of network slicing which DAF does not have authority to collect data and calculate QoE.
Time information	M	string	1..N	N/A	Time information of the QoE which is calculated.

9.15 QoE_Alert

This message is sent to the data analysis function to notify abnormal QoE of network slicing over IF2 if calculated QoE is not in the predefined range.

Table 9-29 describes in detail information of QoE_Alert_Notificaiton:

Table 9-29 – QoE_Alert_Notificaiton

Information element	Status	Data type	Cardinality	Description
Network slicing ID	M	string	1..N	Identity information of the network slicing of which QoE is abnormal.
Abnormal QoE	M	string	1..N	Abnormal QoE of the network slicing.
QoE threshold	O	string	1..N	QoE threshold of the network slicing. Network management sends it to DAF during QoE calculation subscribe.
Time information	M	string	1	Time information of the abnormal QoE.

Table 9-30 describes in detail information of QoE_Alert_Acknowledge:

Table 9-30 – QoE_Alert_Acknowledge

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of an alert notification. 200 OK 400 Input parameter error 500 Server internal error
Network slicing ID	M	string	1..N	N/A	Identity information of the network slicing of which QoE is abnormal.

Bibliography

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network.*

[b-ITU-T Y.3101] Recommendation ITU-T Y.3101 (2018), *Requirements of the IMT-2020 network*.

[b-ITU-T Y.3153] Recommendation ITU-T Y.3153 (2019), *Network slice orchestration and management for providing network services to 3rd party in the IMT-2020 network.*

[b-ITU-T Y.3156] Recommendation ITU-T Y.3156 (2020), *Framework of network slicing with AI-assisted analysis in IMT-2020 networks*.

[b-ITU-R M.1645] Report ITU-R M.1645 (2003), *Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000.*

[b-ITU-R M.2083] Report ITU-R M.2083 (2006), *Level of unwanted emissions of mobile-satellite service feeder links operating in the bands 1 390-1 392 MHz (Earth-to-space) and 1 430-1 432 MHz (space-to-Earth).*

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, 2021