International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3916

(12/2019)

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

Testing specifications – Testing specifications for next generation networks

Signalling requirements and architecture for the Internet service quality monitoring system

Recommendation ITU-T Q.3916

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
Testing specifications for next generation networks	**Q.3900–Q.3999**
Testing specifications for SIP-IMS	Q.4000–Q.4039
Testing specifications for Cloud computing	Q.4040–Q.4059
Testing specifications for IMT-2020 and IoT	Q.4060–Q.4099
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.3916

Signalling requirements and architecture for the Internet service quality monitoring system

Summary

The quality of service (QoS) of Internet services (e.g., web and over the top (OTT) video) has become a concern of the Internet service provider (ISP) and the Internet content provider (ICP). To evaluate the QoS in this regard, Recommendation ITU-T Q.3916 defines the architecture and signalling requirements of the Internet service quality monitoring (SQM) system. Components, interfaces and interactions among components of the SQM system are described in detail in this Recommendation.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.3916	2019-12-14	11	11.1002/1000/14145

Keywords

Architecture, Internet services, probe, quality of service, QoS, signalling requirement.

* 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, 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 TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Q.3916

Signalling requirements and architecture for the Internet service quality monitoring system

1 Scope

This Recommendation specifies the signalling requirements of the Internet service quality monitoring system. In particular, it specifies the system's components, architecture, interface, signalling requirements, etc.

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.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 quality of service [b-ITU-T E.800]: Totality of characteristics of a telecommunications service that bear on its ability to satisfy stated and implied needs of the user of the service.

3.1.2 SOAP [b-W3C SOAP 1]: The formal set of conventions governing the format and processing rules of a SOAP message. These conventions include the interactions among SOAP nodes generating and accepting SOAP messages for the purpose of exchanging information along a SOAP message path.

3.1.3 probe [b-ITU-T Y.1545.1]: An end-point test tool which uses probing packets to collect measurements.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 monitoring centre: The central control system, which manages probes, monitoring tasks, data analytics, etc.

3.2.2 user agent: A kind of service, which connects the monitoring centre remotely in order to conduct operations on the monitoring centre.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3G 3rd Generation of Mobile Communications Technology

4G 4th Generation of Mobile Communications Technology

DNS	Domain Name Server
FTP	File Transfer Protocol
SFTP	FTP over SSH
HDFS	Hadoop Distributed File System
HGU	Home Gateway Unit
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ICP	Internet Content Provider
IP	Internet Protocol
ISP	Internet Service Provider
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
KQI	Key Quality Indicator
NAT	Network Address Translation
NGN	Next Generation Network
NTP	Network Time Protocol
OTT	Over The Top
POP3	Post Office Protocol version 3
QoS	Quality of Service
RTT	Round Trip Time
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SQM	Internet Service Quality Monitoring System
TCP	Transmission Control Protocol
XML	Extendable Markup Language

5 Conventions

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

The keywords "**is prohibited from**" indicate a requirement which 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 which 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 the specification.

In this Recommendation, 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.

6 Introduction to the Internet service quality monitoring system

The Internet service quality monitoring (SQM) system, as shown in Figure 6-1, is able to measure both the QoS of the Internet service and the network quality like the packet loss rate, the round trip time (RTT), the bandwidth, etc. It mainly consists of probes and the monitoring centre. A probe can access to the Internet by connection to routers in the network or the home gateway unit (HGU). To measure the quality of service (QoS) of the Internet service, the probe mimics a person to use the Internet service, computes and records the data of the QoS, and sends them to the monitoring centre. Using the web service as an example, the probe disguises as a browser and initiates the task of browsing web pages. During the interaction with the domain name server (DNS) and web servers, the probe records the time of departure packets and arrival packets and then figures out the key quality indicator (KQI) that is used to measure the QoS of the web service. The testing data are sent to the monitoring centre in order to display them to users. The monitoring centre is also responsible for task assignment to probes. The network quality detection can also be conducted by probes. Overall, the SQM system can monitor the QoS of the Internet services for 7*24 hours. It helps to discover service faults in time and evaluate the Internet service.

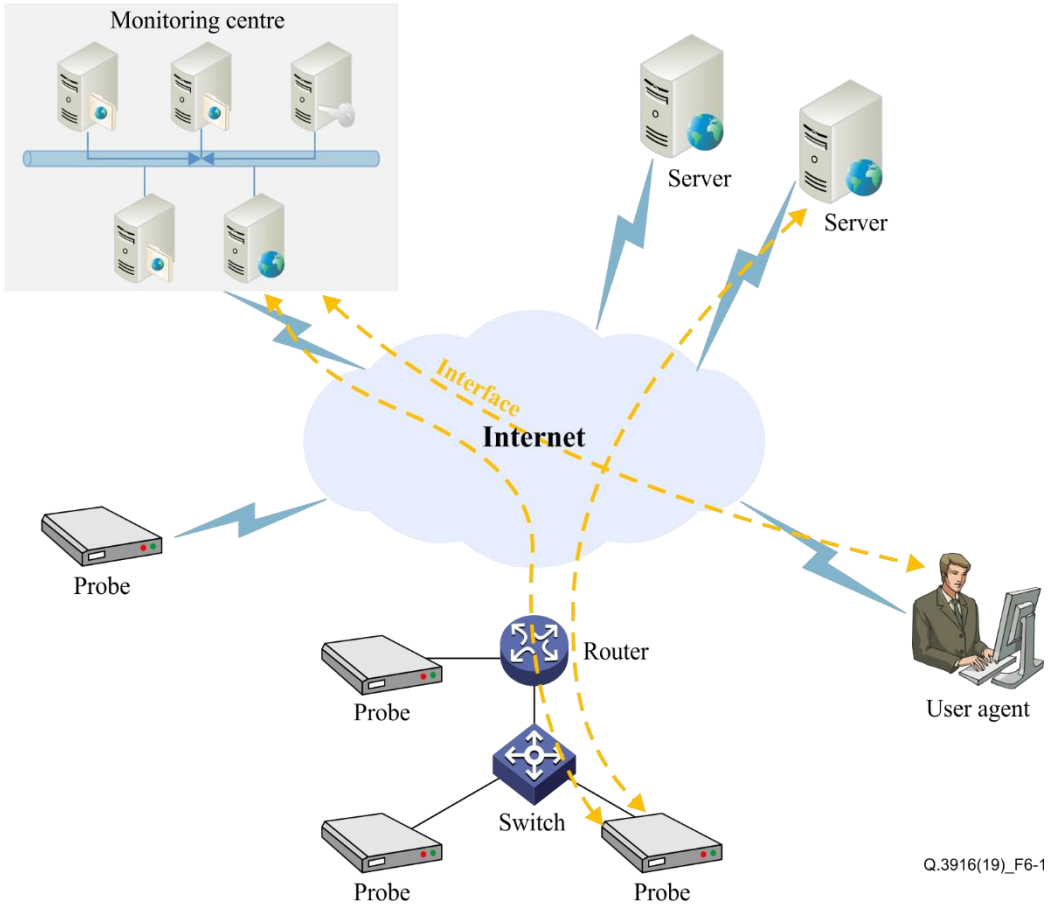

Figure 6-1 – An illustration of the SQM system

7 System architecture

7.1 Overview

The SQM system is mainly comprised of probes, the monitoring centre and the user agent. Probes, deployed as nodes in different network layers and at various locations, mimic human behaviours of accessing Internet services, gather QoS data for Internet services, and report the data to the monitoring centre. The monitoring centre manages all probes and testing tasks on probes, collects QoS data from probes and performs data cleaning, analytics, storage, etc. The user agent allows users to retrieve the QoS data of Internet services in the forms of tables, figures or the original data and to manage probes and testing tasks through the monitoring centre.

The implementation of probes could be the dedicated hardware or pure software installed in ordinary computers in terms of diversified requirements of access scenarios and performance. The monitoring centre, as the control centre of SQM system, is recommended to deploy in clouds including the public cloud or the private cloud. The user agent could be a browser or an application on a mobile terminal and a computer.

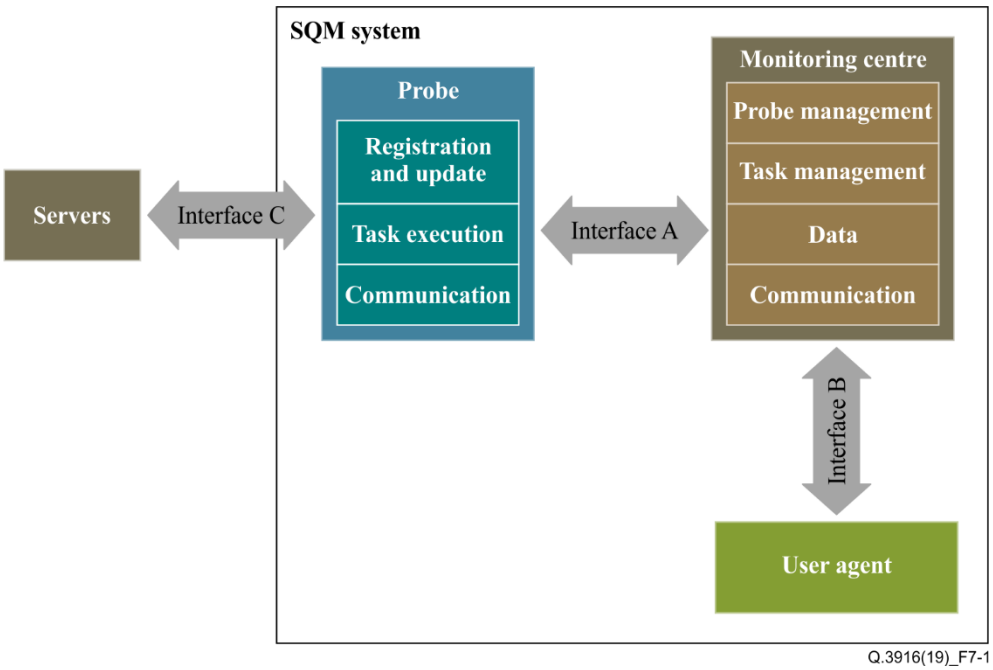

Figure 7-1 – The architecture of the SQM system

7.2 Monitoring centre

The monitoring centre is the control centre of SQM system and connects probes and the user agent. Therefore, it manages probes and tasks on probes and displays testing results to users.

The monitoring centre mainly consists of four modules, that is, the probe management module, the task management module, the data and analytic and display module and the communication module. These four modules fulfil functions of the monitoring centre that is described as follows:

1) The probe management module

This module achieves management functions related to probes such as the probe registration, the probe keep-alive, and the probe software update. After a probe is configured for use, it is required to perform registration in the monitoring centre and is then displayed in the monitoring centre. If there is a testing task, the monitoring centre can choose probes to perform it. All living probes are required to keep alive on the monitoring centre whether there is a task running on it or not. If the software of

probes is updated, the monitoring centre is required to send the software of a new version to probes and command probes install the new version.

2) The task management module

This module is mainly related to the management of testing tasks on probes. The monitoring centre is required to be able to start, pause and stop a task on probes. To start a task, the monitoring centre sends the task and its profile to probes. The profile of the task is required to have the task name, the Internet service and KQIs, the starting time, the stopping time, and the execution mode (e.g., once or a cycle). The monitoring centre is required to be able to pause or stop testing tasks. After receiving the command from the monitoring centre, probes must pause or stop the testing task immediately. On the other hand, the monitoring centre is required to be able to collect testing results from probes. After completion of testing tasks, probes should send testing results to the monitoring centre. Specifically, besides the value of KQIs, configuration information, such as probe ID, starting time and execution mode is also contained.

3) The data and analytics and display module

The monitoring centre is required to be able to store data, analyse data, display results (e.g., tables or figures). After collection of testing data from probes, the monitoring centre stores them in places such as in database or hadoop distributed file system (HDFS). It is recommended that the storage space in the monitoring centre should support data storage for one or more years. Simple analysis on data includes specified search, data comparison, statistics, etc. For example, the monitoring centre could yield the ranking for well-known websites based on their KQIs. Complex analysis involves utilization of various algorithms such as machine learning and deep learning algorithms. It is recommended that the data monitoring centre should support the above analysis methods. Tables and figures, which are easily understandable to users, should be supported by the monitoring centre to visualize data. Other forms of displaying data are encouraged.

4) The communication module

The communication module is responsible for the communication of the monitoring centre, which is indicated by the interface in Figure 7-1. Basically, it is recommended that the communication module should support Transmission Control Protocol/Internet Protocol (TCP/IP). Furthermore, the web service, which is performed by transmitting the simple object access protocol (SOAP) data defined by the extendable markup language (XML) over the Hypertext Transfer Protocol (HTTP), is recommended too since it is open and independent of the specified development language and platform. The communication module is required to support authentication protocol, which is used for probe registration in the monitoring centre. In addition, sometimes the data stored in the monitoring centre may be accessed heavily, for example, for data backup. The communication module could support transmission of a great volume of data.

7.3 Probe

Probes are the actual entities who perform the test of QoS for Internet services. They get commands from the monitoring centre to perform the on-demand test or planned test. To include influential factors that are related to the QoS of Internet service as much as possible, probes are deployed near the user side in the network. Therefore, diverse interfaces such as 3G/4G/Ethernet are recommended to be supported by probes.

A probe is comprised of three modules, which are the registration and update module, the task execution module and the communication module. Functions of the probes reflected by the above modules are described as follows:

1) The registration and update module

When probes are switched on, they are required to register in the monitoring centre actively. Note that probes launch the process of the registration. Since the IP address of a probe could be private due to a local network or a network address translation (NAT) server, probes are sometimes unreachable from the monitoring centre. The registration message of a probe is required to contain the probe ID, the probe IP address, the software version and hardware model, and authentication information. After successful registration, probes are available and visible on the monitoring centre.

Probes are required to periodically report that they are alive to the monitoring centre whether there are testing tasks on them or not. Likewise, probes actively send keep-alive messages to the monitoring centre. The period of keep-alive message is set on the monitoring centre and is sent to probes as configuration parameters. If the monitoring centre has not received the keep-alive messages for several periods from a probe, it assumes that the probe is inactive or that the network is out of service. Therefore, the monitoring centre will not distribute any task for that probe.

Update refers to software upgrade or patch installation. If there is a new version of software, the monitoring centre will notify it to probes. Probes then get the new software, install it and perform restart.

2) The task execution module

After getting tasks and corresponding profiles from the monitoring centre, probes set the testing tasks according to profiles and perform them at the specified timing. Task execution mimics the process as much as possible when a person uses the Internet service. For example, the domain name resolution is the first step when a webpage is browsed by a person. Consequently, resolution of the domain name should be contained in the testing task. As a result, the testing result contains necessary KQIs that evaluate QoS of the Internet service. Moreover, the task execution module is required to support performing the task once or many times. It is required to support the web-browsing service, the OTT video service, and the bandwidth testing service at least. During the task execution, the testing results are stored on probes temporarily.

3) The communication module

The communication module is responsible for communication between the probe and the server of the Internet service and communication between the probe and the monitoring centre.

To support testing various services, the communication modules are required to support protocols of TCP/IP, HTTP, HTTPs, SMTP, POP3, FTP and SFTP. Both IPv4 and IPv6 are required to be supported. In addition, a large number of simultaneous connections between the probe and servers of the Internet service (e.g., TCP connections) is recommended to be supported by the communication module, which is used for performance test or pressure test.

All of the probe registration, the keep-alive report, the software update, the task distribution and the testing results feedback require communication between the probe and the monitoring centre. As mentioned before, the web service is recommended for the communication. If the IP address of the probe is private, the probe shall actively contact the monitoring centre. Finally, an authentication protocol is required to be supported by the communication module.

7.4 User agent

The user agent is used by the system operators to control the monitoring centre remotely, to view testing results, to inspect probes, etc. Therefore, it could be developed as an application on a mobile phone or a laptop. Optionally, a browser (e.g., IE and Firefox) could also be the user agent. The browser acts as the entrance to all functions on the monitoring centre.

8 Interface requirement

8.1 Overview

As illustrated in Figure 7-1, there are three interfaces in SQM system, i.e., the interface between a probe and the monitoring centre (Interface A), the interface between the user agent and the monitoring centre (Interface B), and the interface between a probe and servers of Internet services (Interface C). Interface A is used for interactions between probes and the monitoring centre, such as the probe registration. It is crucial to define the functions of this interface especially when probes and the monitoring centre derives from different manufactures. Therefore, interface A will be introduced in detail in this clause. Interface B is used for operators to login the monitoring centre with the user agent. Since the user agent is usually a browser and all functions are performed in the monitoring centre, there is no special requirement for interface B. Likewise, interface C is used by probes to test QoS of Internet services so interactions comply with standard protocols such as HTTP or SMTP. Therefore, interface B and C are not discussed in detail.

8.2 Interface A

The main functions of interface A are the probe registration, the keep-alive heartbeat, the task management, the data submission, the status report and the software update, as shown in Figure 8-1.

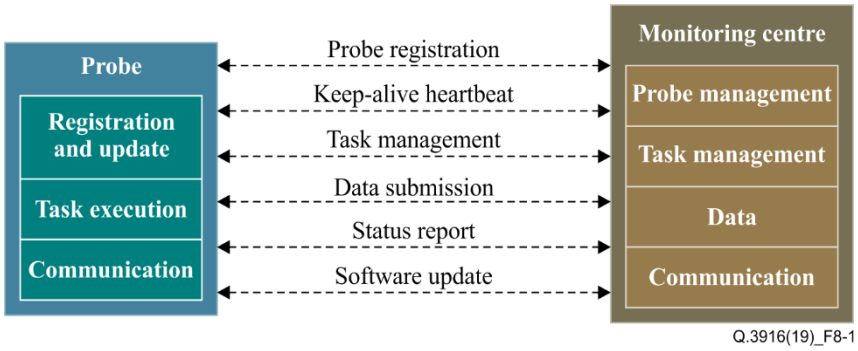

Figure 8-1 – Functions of Interface A

Each function of interface A is introduced in detail as follows:

1) Probe registration

The probe registration refers to probes that register themselves in the monitoring centre automatically when they are switched on. Probes transmit basic information to the monitoring centre and the monitoring centre authenticates the probes. The basic required information include probe's ID, IP address, software version, and hardware model.

2) Keep-alive heartbeat

The keep-alive heartbeat is to keep connection between a probe and the monitoring centre, which is fulfilled by periodic exchange of messages between them. In addition to report of a living probe, the heartbeat messages are also used for notification of new configurations, new tasks or new software on the monitoring centre.

3) Task management

Task management chiefly includes task distribution, task update and execution control. In the task distribution and task update, the monitoring centre firstly chooses probes that perform the task, and then distributes the task and corresponding profile to these probes. The execution control refers to pause or termination of the tasks on probes.

4) Data submission

Data submission is used for probes to submit testing results and corresponding testing parameters to the monitoring centre. The testing results primarily include KQIs of Internet service. The testing parameters should include the probe's ID, Internet service, execution mode, etc.

5) Status report

The status report is used for probes to report execution status as well as an alarm in case of abnormal situations. The execution status could include the information of the CPU, memory, disk, and port. The warning could support alarms of the CPU, memory, disk and unknown errors. On the other hand, it at least includes warning type, warning level, and description.

6) Software update

The software update is used for the monitoring centre to notify probes of new software and transmit the software file.

9 Signalling requirement

9.1 Overview

As mentioned earlier, probes interact with the monitoring centre for probe registration, keep-alive heartbeat, task management, data submission, status report and software update. This clause defines the signalling requirements for probes.

All the message interactions between probes and the monitoring centre are chiefly in the request and response mode. It is recommended that the interaction between probes and the monitoring centre should be implemented by web service. Hence, signalling messages are transmitted with SOAP, namely it is formatted by XML and carried by HTTP. Furthermore, all messages contain a message header and a message body, as described in Figure 9-1. The message header specifies the message type, the message length and the message ID. The message ID is generated by the sender and kept the same in the response message if there is one. The message body specifies message contents.

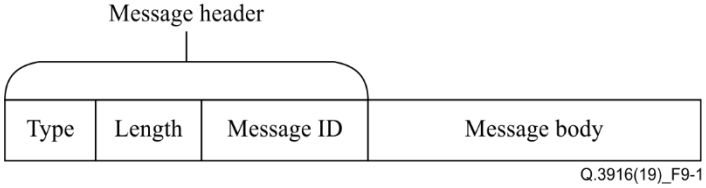

Figure 9-1 – Message composition

9.2 Signalling for probe registration

9.2.1 Message type

The messages for probe registration, i.e., the registration request message and the registration response message, are illustrated in Figure 9-2. The registration request message contains necessary information such as IP address and software version and is transmitted to the monitoring centre for registration. The registration response message from the monitoring centre is the feedback showing success or failure of the registration.

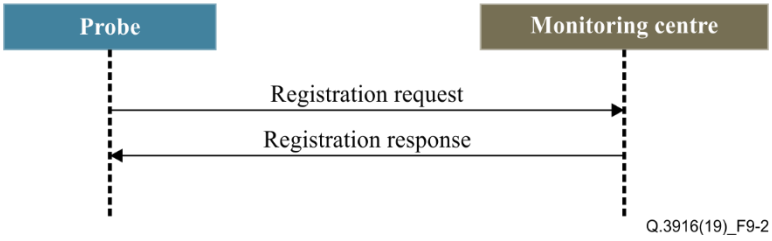

Figure 9-2 – Signalling procedure for probe registration

9.2.2 Registration request message

The registration request message contains fields of probe name, IP address, software version, etc. All fields and corresponding descriptions are shown in Table 9-1.

Table 9-1 – Registration request message format

Field	Type	Description
IP address	String	An IP address of a probe
Software version	String	Software version, e.g., 3.3.0
Probe name	String	A readable string to identify a probe
Serial number	String	The globally unique number for a probe
Authentication	String	Authentication code for validation of probes
Task status	Int	0: tasks are paused; 1: tasks are running
Heartbeat interval	Long	An interval for heartbeat messages
NTP address	String	An IP address of a NTP server
Network interface	String	Names of network interfaces of probes
Network interface IP	String	An IP address for each network interface
Network interface MAC	String	A MAC address for each network interface

9.2.3 Registration response message

The registration response message contains two fields, i.e., the response code and description. Descriptions of the two fields are shown in Table 9-2.

Table 9-2 – Registration response message format

Field	Type	Description
Response code	Int	0: success; 1: failure
Description	String	More information for the response code, especially for registration failure
Probe ID	Long	Probe ID specified by the monitoring centre if registration is successful

9.3 Signalling for keep-alive heartbeat

9.3.1 Message type

The messages for keep-alive heartbeat are illustrated in Figure 9-3, i.e., the heartbeat request message and the heartbeat response message. The heartbeat request message is transmitted to the monitoring centre for notification of a living probe. The heartbeat response message from the monitoring centre is a confirmation.

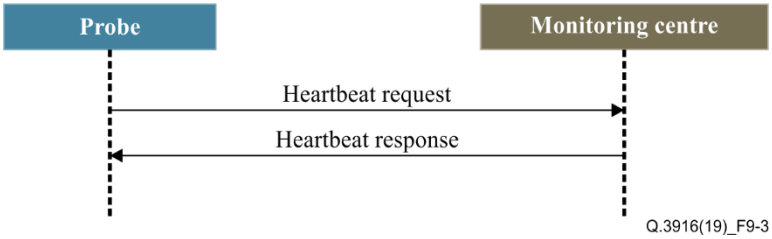

Figure 9-3 – Signalling procedure for keep-alive heartbeat

9.3.2 Heartbeat request message

All fields and corresponding descriptions of the heartbeat request message are shown in Table 9-3.

Table 9-3 – Heartbeat request message format

Field	Type	Description
Probe ID	Long	Probe ID specified by the monitoring centre

9.3.3 Heartbeat response message

All fields and corresponding descriptions of the heartbeat response message are shown in Table 9-4.

Table 9-4 – Heartbeat response message format

Field	Type	Description
Response code	Long	0: success; 1: failure
Description	String	More information for the response code
New task	Int	0: no new task; 1: a new task
New configuration	Int	0: no new configuration; 1: a new configuration
New version	Int	0: no new version of software; 1: a new version of software

9.4 Signalling for task management

9.4.1 Message type

The messages for task management are illustrated in Figure 9-4, i.e., the task request message and the task distribution message. When a probe receives a heartbeat response message with a new task indicator, it will send a task request message to ask the monitoring centre for the new task. The monitoring centre then transmits the new task and its profile to probes.

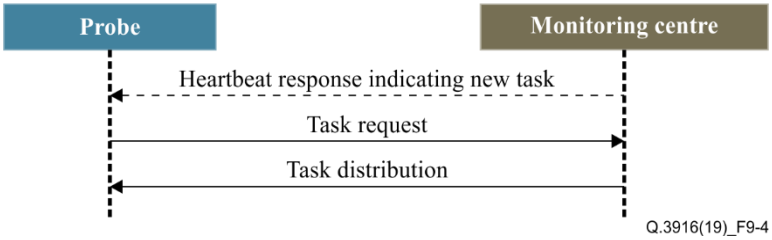

Figure 9-4 – Signalling procedure for task management

9.4.2 Task request message

All fields and corresponding descriptions of the task request message are shown in Table 9-5.

Table 9-5 – Task request message format

Field	Type	Description
Probe ID	Long	Probe ID specified by the monitoring centre

9.4.3 Task distribution message

All fields and corresponding descriptions of the task distribution message are shown in Table 9-6.

Table 9-6 – Task distribution message format

Field	Type	Description
Response code	Int	0: success; 1: failure
Description	String	More information for the response code
Task ID	Long	An identification for a task
Task type	String	Internet service, e.g., web, OTT video
Operation	String	Operations that are performed on tasks on probes, such as pause, termination, restart, etc.
Network interface	String	Names of network interfaces of a probe used to perform the task
Destination IP	String	An IP address of an Internet service server
Data submission time	String	Time to submit testing data
Starting time	String	Time to start the task
Ending time	String	Time to end the task
Execution interval	String	An interval for task execution

9.5 Signalling for data submission

9.5.1 Message type

The messages for data submission are illustrated in Figure 9-5. The messages are the data submission message and the submission response message. Probes submit the testing result and configuration data formatted in XML to the monitoring centre with the data submission message. Since the testing result may be too big, several data submission messages could be transmitted consecutively. After getting each data submission message, the monitoring centre replies with the submission response message to confirm the reception and inform probes whether the testing results are satisfactory.

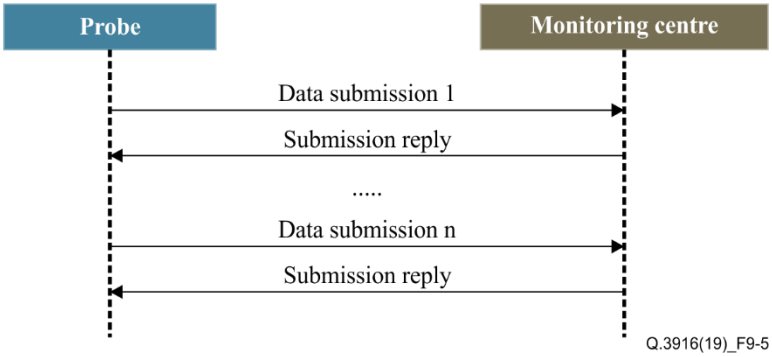

Figure 9-5 – Signalling procedure for data submission

9.5.2 Data submission message

All fields and corresponding descriptions of the data submission message are shown in Table 9-7.

Table 9-7 – Data submission message format

Field	Type	Description
Probe ID	Long	Probe ID specified by the monitoring centre
Task ID	Long	An identification for a task
Task type	String	Internet service, e.g., web, OTT video
Network interface	String	Names of network interfaces of a probe used to perform the task
Destination IP	String	An IP address of an Internet service server
Testing times	Long	Times that the task runs for
Attribute: value	String	An attribute related to a specific task and Internet service and its value

9.5.3 Submission response message

The submission response message contains three fields, which are a response code, description and the probe ID. Descriptions of the three fields are shown in Table 9-8.

Table 9-8 – Submission response message format

Field	Type	Description
Response code	Long	0: success; 1: failure
Description	String	More information for the response code
Probe ID	Long	Probe ID specified by the monitoring centre

9.6 Signalling for status report

9.6.1 Message type

The messages for status report, i.e., the status report message and the report response message, are illustrated in Figure 9-6. In a normal situation, probes send a status report message to inform the monitoring centre about the running status. In an abnormal situation, probes send a status message containing alarm information to the monitoring centre.

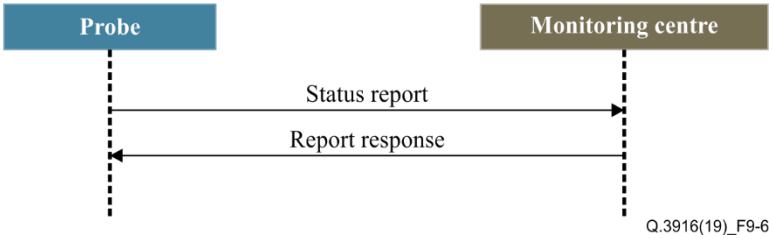

Figure 9-6 – Signalling procedure for status report

9.6.2 Status report message

All fields and corresponding descriptions of the status report message are shown in Table 9-8.

Table 9-8 – Status report message format

Field	Type	Description
Probe ID	Long	Probe ID specified by the monitoring centre
Status type	Int	0: a status report; 1: a warning report
Source	String	Source of the status or warning
Occurring time	String	Time that the status or warning happens
Attribute: value	String	An attribute of the status, warning or source and its value
Alarm level	Int	0: non alarm; 1: tips; 2: minor; 3: general; 4: bad; 5: severe
Description	String	More information about the status or alarm

9.6.3 Report response message

All fields and corresponding descriptions of the report response message are shown in Table 9-9.

Table 9-9 – Report response message format

Field	Type	Description
Response code	Int	0: success; 1: failure
Description	String	More information for the response code
Probe ID	Long	Probe ID specified by the monitoring centre

9.7 Signalling for software update

9.7.1 Message type

The messages for software update are illustrated in Figure 9-6. The messages are the update request message, the file list message, the file request message and the file download message. When receiving the heartbeat message indicating a new version from the monitoring centre, probes send the update request message to ask for updating its software. The monitoring centre replies with the file list message to show files for the new software. Then, the probes work out which files they have and which files they need to download from the monitoring centre, and send the file request message to ask for necessary files. Finally, the monitoring centre replies with the requested files with the file download message.

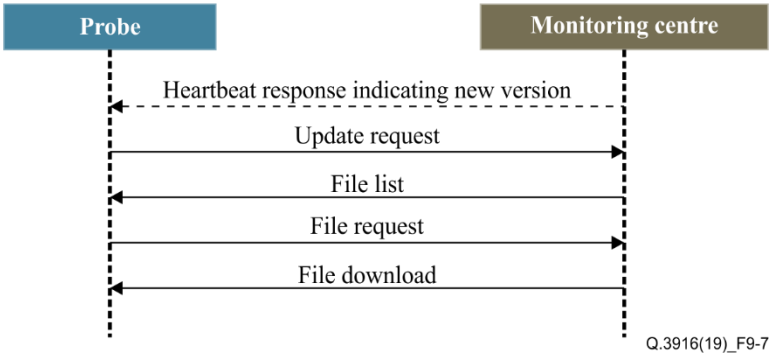

Figure 9-7 – Signalling procedure for software update

9.7.2 Update request message

All fields and corresponding descriptions of the update request message are shown in Table 9-10.

Table 9-10 – Update request message format

Field	Type	Description
Probe ID	String	Probe ID specified by the monitoring centre
Requested version	String	The software version that probes ask for
Hardware model	String	Hardware information of probes
Software version	String	Software information of probes

9.7.3 File list message

All fields and corresponding descriptions of the file list message are shown in Table 9-11.

Table 9-11 – File list message format

Field	Type	Description
Probe ID	String	Probe ID specified by the monitoring centre
Response code	Int	0: success; 1: failure
Description	String	More information for the response code
Updated files	String	Files that probes need to update
Created files	String	Files that probes need to create
Deleted files	String	Files that probes need to delete

9.7.4 File request message and file download message

According to the file list message, probes choose files to request from the monitoring centre. It is recommended to request and download files with HTTP.

10 Security considerations

Overall, it is recommended to adopt the security requirements contained in [ITU-T Y.2701] which provides network-based security for end user communications across multiple-network administrative domains. Although probes, the monitoring centre and the user agent are not common network elements of the next generation network (NGN), they are highly involved in administrative domains, such as the deployment of probes in different layers of the network. As a result, it is recommended that they all comply with the security requirements in [ITU-T Y.2701]. In addition, it is encouraged to take additional measures to protect the SQM system.

Bibliography

[b-ITU-T E.800] Recommendation ITU-T E.800 (2008), *Definitions of terms related to quality of service.*

[b-ITU-T Y.1545.1] Recommendation ITU-T Y.1545.1 (2017), *Framework for monitoring the quality of service of IP network services.*

[b-W3C SOAP 1] W3C Recommendation (2007), SOAP Version 1.2 Part 1: Messaging Framework (Second Edition).

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, 2020