International Telecommunication Union

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# Q.3745

(04/2020)

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

Signalling requirements and protocols for SDN – Network signalling and signalling requirements for services

# Protocol for time constraint Internet of things-based applications over software-defined networking

Recommendation ITU-T Q.3745

ITU-T

International
Telecommunication
Union

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 |
| Resource control protocols | Q.3710–Q.3739 |
| **Network signalling and signalling requirements for services** | **Q.3740–Q.3779** |
| TESTING SPECIFICATIONS | Q.3900–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.3745

# Protocol for time constraint Internet of things-based applications over software-defined networking

## Summary

Traffic generated by smart devices is becoming a significant part of the Internet. Smart devices require mobility and guaranteed quality of service (QoS) that needs to be managed. Potentially, software-defined networking- (SDN-) and network function virtualization- (NFV-) based technologies (IMT-2020) will be used for managing all types of services and therefore, SDN is to be tasked to manage these kinds of demands as well.

A significant number of the available Internet services require the exact value of network parameters such as latency, jitter, round trip time (RTT) and bandwidth. Using SDN capabilities for managing network parameters, will give a possibility to implement new services such as a tactile Internet, augmented reality, e-health applications.

In this regard, the protocol is proposed to ensure the transfer of the network performance requirements requested by an IoT server for IoT applications in SDN- and NFV-based networks in International Mobile Telecommunications-2020 (IMT-2020). This protocol is to be used for interconnection between the IoT server and the orchestrator application layer (management application (MA)).

## History

| Edition | Recommendation | Approval | Study Group | Unique ID* |
|---|---|---|---|---|
| 1.0 | ITU-T Q.3745 | 2020-04-29 | 11 | 11.1002/1000/14244 |

## Keywords

IoT, NFV, SDN.

* 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

Page

# Recommendation ITU-T Q.3745

# Protocol for time constraint Internet of things-based applications over software-defined networking

## 1 Scope

This Recommendation describes the protocol for providing network performance requirements requested by an IoT server for IoT applications in software-defined networking- (SDN-) and network function virtualization- (NFV-) based networks in International Mobile Telecommunications-2020 (IMT-2020). This protocol defines a set of application-level interface conventions between the IoT server and the orchestrator application layer (management application (MA)). High-level architecture, functions and message formats are addressed in this Recommendation.

## 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-R M.2083-0] Recommendation ITU-R M.2083-0 (2015), *IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*.

## 3 Definitions

### 3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

**3.1.1 application** [b-ITU-T Y.2091]: A structured set of capabilities, which provide value-added functionality supported by one or more services, which may be supported by an API interface.

**3.1.2 device** [b-ITU-T Y.2060]: With regard to the Internet of things, this a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing.

**3.1.3 future network (FN)** [b-ITU-T Y.3001]: A network able to provide services, capabilities, and facilities difficult to provide using existing network technologies. A future network is either:

a) a new component network or an enhanced version of an existing one, or

b) a heterogeneous collection of new component networks or of new and existing component networks that is operated as a single network.

**3.1.4 gateway** [b-ITU-T Y.4101]: A unit in the Internet of things which interconnects the devices with the communication networks. It performs the necessary translation between the protocols used in the communication networks and those used by devices.

**3.1.5 Internet of things (IoT)** [b-ITU-T Y.2060]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

**3.1.6 software-defined networking** [b-ITU-T Y.3300]: A set of technologies that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner.

**3.1.7 thing** [b-ITU-T Y.2060]: With regard to the Internet of things, this is an object of the physical world (physical things) or the information world (virtual thing), which is capable of being identified and integrated into communication networks.

### 3.2 Terms defined in this Recommendation

None.

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

| | |
|---|---|
| AAA | Authentication, Authorization, Accounting |
| API | Application Programming Interface |
| BLS | Battery Level Status |
| BSS | Business Support System |
| b2b | business to business |
| CoAP | Constrained Application Protocol |
| DPI | Deep Packet Inspection |
| e2e | end to end |
| FN | Future Network |
| HTTP | Hypertext Transfer Protocol |
| IMS | Internet protocol Multimedia Subsystem |
| IMT-2020 | International Mobile Telecommunications-2020 |
| IoT | Internet of Things |
| JSON | JavaScript Object Notation |
| LAN | Local Area Network |
| MA | Management Application |
| MQTT | Message Queue Telemetry Transport |
| NFV | Network Function Virtualization |
| NGN | Next Generation Network |
| OSS | Operation Support System |
| QoS | Quality of Service |
| REST | Representational State Transfer |
| RTT | Round Trip Time |
| SDN | Software-Defined Networking |
| VM | Virtual Machine |
| WAN | Wide Area Network |

## 5 Conventions

None.

## 6 Overview

The IoT, according to clause 3.1.5, is a global infrastructure that consists of different technologies and solutions. New IoT-based services, which are coming to existing networks and FNs, bring new requirements from and opportunities for infrastructure. One type of IoT-based services is time constraint applications, which are sensitive to delay and jitter parameters. FNs should be based on SDN and NFV technologies to meet new network infrastructure requirements.

In this regard, a new protocol for realization time constraint IoT-based applications over SDN is proposed. The protocol ensures conventions and message formats for transfer of network performance requirements requested by an IoT server for IoT applications to the orchestrator application layer.

## 7 The high-level architecture and general descriptions of elements interaction

FNs, according to clause 3.1.3, are those able to provide different kinds of service that are difficult to supply using existing network technologies. One of the limiting factors is the quality of service (QoS) required for new services. However, the heterogeneity in basic telecommunication FN elements should not affect QoS. Responsibility for ensuring the required QoS falls on the infrastructure of the IMT-2020 networks, which according to [ITU-R M.2083-0], should be based on SDN and NFV, which in turn help to ensure high-level network scaling and flexibility in management, allowing delivery of new services.

As such, the use of SDN and NFV allows for the dynamic management of connections following the "on-demand" model. This Recommendation presents a protocol for providing network performance requirements requested for IoT applications, taking into account NFV and SDN architecture. Figure 1 shows infrastructure based on SDN/NFV concepts, taking into consideration various access technologies and possible integration with multi-service next generation network/Internet protocol multimedia subsystem (NGN/IMS) networks.

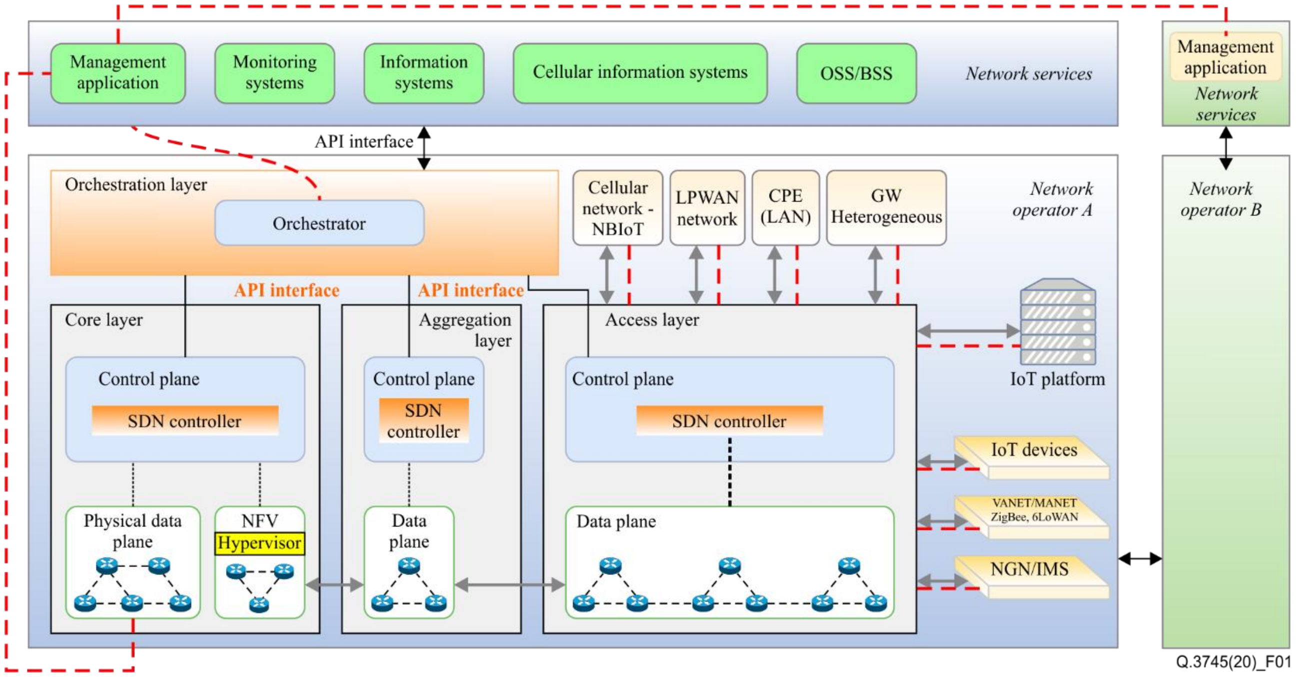


**Figure 1 – Infrastructure of a telecommunication network with QoS management system**

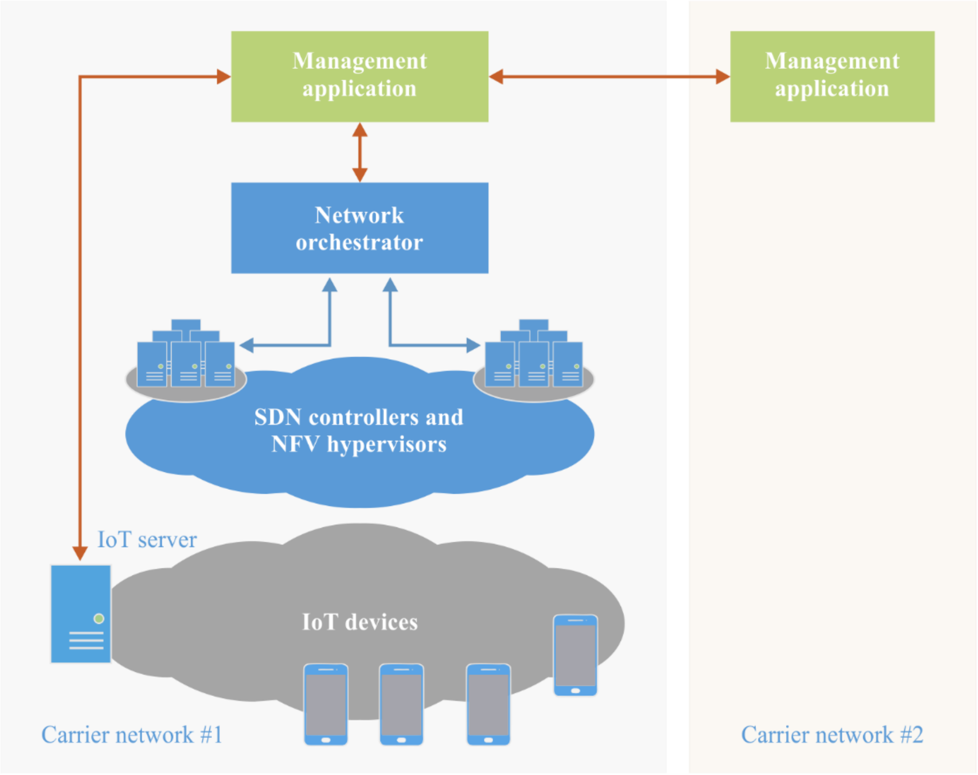
Figure 1 presents a telecommunication network logically broken down into several segments: access layer; aggregation layer; network core layer; and operator service layer. Such a breakdown is common for most operators (e.g., telecommunication networks on the territory of the Russian Federation). Each segment (access, aggregation and core) is controlled by an SDN controller. It is also possible to have virtual segments on networks, each of which may perform one or more network functions. To ensure interaction between the segments, a network orchestrator is required that will in turn, via the southern interface, manage the controllers and interact with the hypervisors of the network's virtual segments and also directly with virtual machines (VMs) performing one network function or another. The red dotted line in Figure 1 represents the interaction between basic elements of the system ensuring QoS. The system includes the basic elements 1) to 3).

1) MA. The task of this element is to support the protocol for providing network performance requirements requested, including the processing of requests for the provision of QoS from service users, interaction with the network orchestrator and networks of third-party operators to ensure end-to-end (e2e) QoS.

2) IoT device. A user device comprising a hardware and software system offering the support of application protocols for the request of necessary QoS and IoT server parameters.

3) IoT server. Software or hardware and software system(s) provide(s) an implementation of application protocols for interaction with the MA to request the necessary QoS level for the network segment between IoT server and device, for the provision of services in IMT-2020 networks.

Figure 2 presents the direct interaction between elements 1) to 3) in this framework.



Q.3745(20)_F02

**Figure 2 – Interaction of elements in ensuring QoS in IMT-2020 networks**

Interaction occurs between the following elements of the framework:

- Internet thing and IoT server (the server on which the thing is registered);
- IoT server and MA – interaction occurs along a protected telecommunication channel to ensure security;

- IoT server and other IoT server (if it is necessary to ensure the connection between devices, which are registered on different servers);
- MA for the orchestrator of one network with that of another network operator.

The organization of the MA element, working with the orchestrator via an application programming interface (API), helps to ensure the transparent performance of services throughout the operator-supervised network (in the case of one orchestrator). The operator's other information systems are at this level, including those performing operation support system /business support system (OSS/BSS) functionality, monitoring, data analysis, etc., enabling this functionality to be easily integrated during framework implementation.

## 7.1 Functions of entities

### 7.1.1 Functions of IoT server

An IoT server is a server that can be represented in software or hardware-software form. The IoT server implements the following main functions.

- Interaction with IoT device. The interaction utilizes one of the IoT protocols (e.g., hypertext transfer protocol (HTTP) 2.0, constrained application protocol (CoAP) and message queue telemetry transport (MQTT)).
- Implementation of authentication, authorization, accounting (AAA) functionality for registered IoT devices.
- Interaction with the MA. Interaction with another IoT server. These interactions require communication between IoT devices, with the participation of IoT server(s).

### 7.1.2 Functions of management application

An MA is a server that can be represented in both software and hardware-software form.

The main functions of an MA follow.

- Checking the ability to interact with the IoT server. The service operator to ensure the quality of the services provided, concludes an agreement with the network operator; as a result, the network operator enters the IP addresses of the service operator into the registry. This registry is used by the network operator when checking at the stage of a request for interaction from the IoT server(s). Also at this stage, the number of services provided by the network operator to the service operator (e.g., restrictions of network performance parameters) is determined.
- Interaction with the IoT server. This interaction occurs through the MA API using a specific application-level protocol. The software interface implements a set of functions, the reachability of some of which is determined by the initially established ability to interact with the IoT server during the initial verification process. The main functions are: accepting service requests for a specific device or group of devices from the IoT server, as well as signalling with the IoT server in the process of maintaining the IoT device(s) and providing the appropriate quality.
- Interaction with the network orchestrator. This interaction occurs via the orchestrator API.

An MA-MA interaction is possible if it is necessary to establish a connection either with an IoT server located on a network controlled by another orchestrator (the same or another network operator, e.g., international roaming), or when establishing an IoT device – IoT device connection, given the fact that one of the devices is in the network, controlled by another orchestrator.

NOTE – If an IoT device identifier has a unified identification system, it is also possible to provide lifelong Internet access for a device that generates telemetry traffic, and this device is automatically linked to a specific IoT server. Payment for communication is part of the cost of the device, and the calculation is made for the period of the lifecycle of each device. At the same time, the interaction between different operators is governed by the terms of the contract.

## 7.2 Interconnection framework

### 7.2.1 Main framework interconnection diagram

The interaction between framework elements (network devices) is shown in Figure 3.

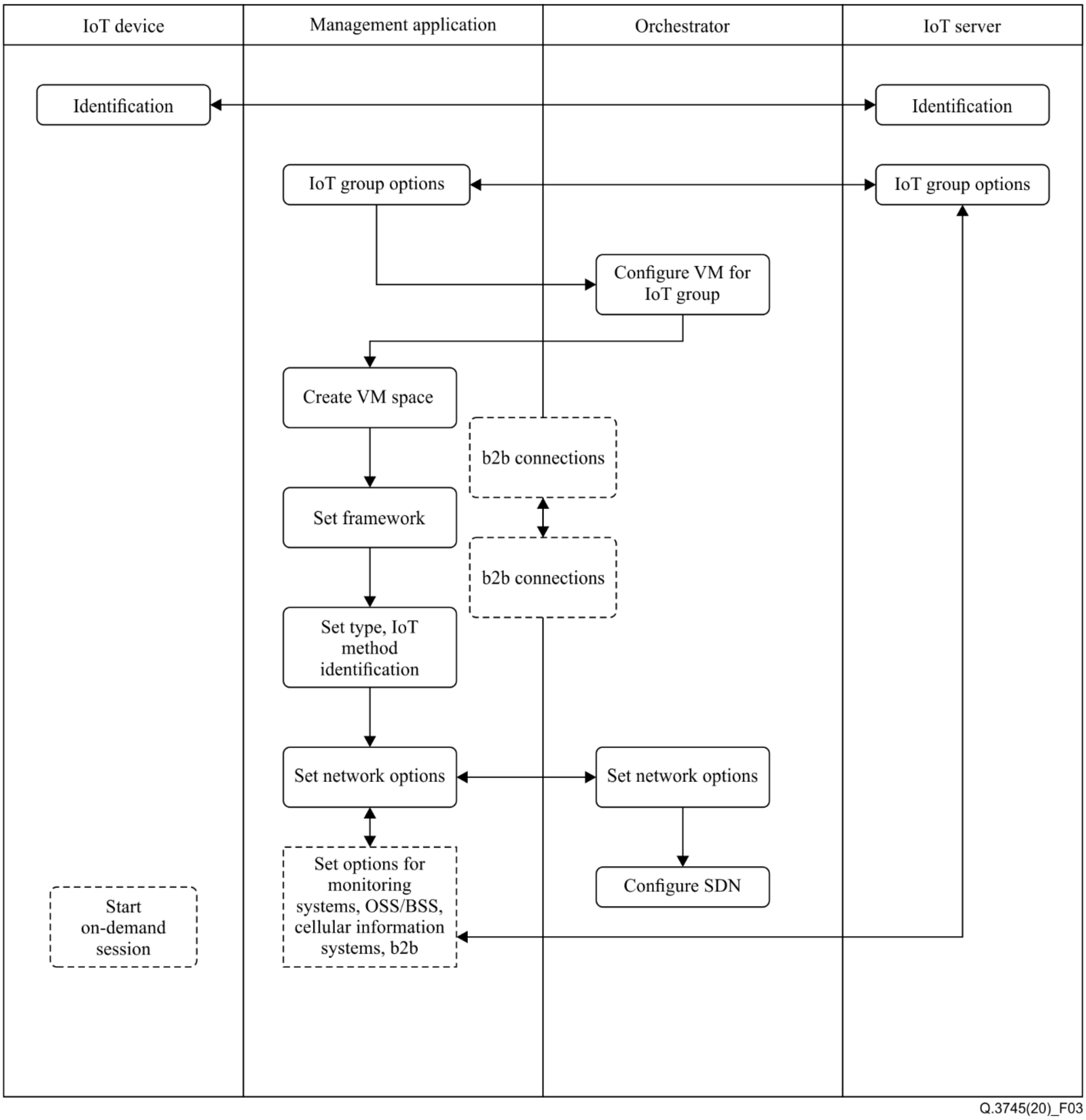


**Figure 3 – Diagram of interaction in ensuring e2e QoS in IMT-2020 networks**

Figure 3 addresses the logic of the interaction of elements in ensuring a given level of QoS in IMT-2020 networks.

A description of interactions reflected in Figure 3 follows.

1) Identification process. The process involves a set of actions aimed at fulfilling AAA. This process occurs only between the IoT device (virtual or physical) and a third-party IoT server. Authentication involves the allocation of the computing resources of the server in accordance with information previously entered into the database, helping to match the device to a specific user, with the IoT device undergoing the authentication procedure using its own unique identifier. The authorization process helps to determine the number of services

available to the Internet thing or object in question. It is also worth remembering that in certain cases, the thing can perform a set of functions that share commonalities in their tasks for the type of thing in question. For example, a thing might be a tactile Internet device and also perform one or more medical functions. Given the variety in types of Internet things, it is possible to separate (classify) them into groups. In the accounting process, the computing resources allocated to the Internet thing are accounted for on the IoT server. In addition, any process failures are logged, and, in certain cases, billing procedures are carried out on the part of the service operator (owner of the IoT server). It is worth noting that this process might involve other functions, but in each case, the set of functions is determined by the service provider (owner of the IoT server).

2) IoT group options. Options include the IoT server's formation and subsequent transmission of parameters of an IoT group or adding an Internet thing with data at the required QoS to this group, data transfer protocol used (MQTT, CoAP, etc.), security level (determining whether further encryption of communication channel is required) of the network segment concerned.

3) Configure VM for IoT group. Upon completion of the operations above, a request is made to the network orchestrator in accordance with data obtained in the IoT group options process, after which the orchestrator configures the VM space for a specific group of IoT devices or adds or removes specific devices to or from the group.

4) Create VM space. Virtual space is created for a group of IoT devices according to specific service criteria (various IoT service operators, QoS, financial regulation or billing, deep packet inspection (DPI) requirements, etc.) or addition of new registered IoT devices to an existing group.

5) Set framework procedure. This procedure involves the entry and configuration of QoS parameters for the IoT group. At this stage, it is possible that there are further processes (set type, IoT method identification) that are essential for inter-operator connections.

6) Set options for monitoring systems, OSS/BSS, cellular information systems, business to business (b2b). Where necessary, these processes are aimed at integration with monitoring, OSS/BSS and other systems required for the operator's provision of services to the client. Figure 3 also shows a return link between processes, which implies the complete monitoring of the provision of services and information gathering on information systems not only of the operator, but also the IoT server. In the event of an anomaly, whereby the network, as a system, is lacking in resources and will not be able to provide the required QoS, the system will be obliged to interrupt the provision of services, based on priorities, type of IoT application and the agreement between the network operator and service operator (owner of IoT server), as well as informing the server of the error code. The return link to the IoT server helps with not only the mutual analysis and information gathering of systems, but also the outlook for increasing the number of Internet objects in each of the sectors and their type, which, as a result, will help to optimize planning of communication networks, IoT service operators, etc.

## 8 Protocol format

This clause defines the data requirements that are transferred between functional elements at various stages of interaction, displayed in clauses 7.1 and 7.2, including the format of the transmitted messages between the functional elements of the IoT server and MA.

This clause displays the requirements for the parameters to be transmitted and the message format.

### 8.1 Interconnection between IoT device and IoT server

The purpose and description of the interaction processes at this stage are given in clause 7.2.1. At the moment, there are a large number of open and commercial server solutions (also known as clouds or platforms) for building and providing IoT services. At the same time, most (especially commercial) solutions have their own peculiarities in the implementation of IoT device – IoT server interaction processes, namely, the choice of interaction protocols, architecture and the underlying software principles. Concurrently, it is also worth considering several IoT technologies, where a different protocol stack is used (e.g., sensor networks), which are connected via a gateway. Thus, taking into account the multi-vendor requirements, the differences in the stacks of protocols at this stage of interaction determine the number of parameters that must be transferred from the IoT device (or gateway) to the IoT server. The functions of the IoT server element are defined in clause 7.1.1.

Parameters include:

- identifier of things;
- type of device:
  - a) physical (code in the message – "001"),
  - b) virtual (code in the message – "010"),
  - c) gateway (code in the message – "011");
- QoS requirements:
  - a) minimum number of hops,
  - b) range of round trip time (RTT),
  - c) maximum lost packets;
- battery level status (BLS);
- requirements for additional connection encryption.

### 8.2 Interconnection between IoT server and management application

The purpose and description of the interaction processes at this stage are given in clause 7.2.1. At this stage, there is an interaction between the IoT server elements and the MA. The functions of the MA element are specified in clause 7.1.2. At the moment, the northbound interface of SDN controllers, orchestrators is based on the representational state transfer (REST) architecture of distributed element interaction. The message format, in this case, is the structure of the transmitted data, defined in JavaScript object notation (JSON) format.

The interaction should include the following types of requests:

- up message – this type of message is generated from the IoT server to MA;
- way down message – this type of message is generated from the MA to the IoT server.
- equal message – this type of message can be generated by both elements (MA, IoT server).

The types of messages (according to actions) are:

- create (create a new group of things; also used on first connection) – refers to an up message;
- update (intended for modification parameters about iot devices) – refers to an up message;
- delete (delete IoT device from the group or delete group) – refers to an up message;
- status (update information about the actual group's data) – refers to an "equal message".

### 8.2.1 Format of messages

Each format contains a part of data expansion. Extensions in the message are for developers.

**Message No. 1. Create a group**

```
{
      “request_type” : “up_message”,
      “action” : ”create”
       “groups” : {
                   { “id_group” : ‘…’,
                     “group-name” : “”,
                      "group": [
                            {
                           "IoT-device_id": “..",
                                   "service_provided": "..",
                           "Type_of_device": "..",
                           "qos_range_min_rtt": “..”,
                           "qos_range_max_rtt": “..”,
                                   “max-lost-packets”: “..”,
                           "battery-level-status": “..”,
                           "additional-encryption": “..”
                            },
                            {
                           "IoT-device_id": “..",
                                   "service_provided": "..",
                           "Type_of_device": "..",
                           "qos_range_min_rtt": “..”,
                           "qos_range_max_rtt": “..”,
                                   “max-lost-packets”: “..”,
                           "battery-level-status": “..”,
                           "additional-encryption": “..”
                                },
                              ]
                     },
                   { “id_group” : “…”,
                     “group-name” : “”,
                      "group": [
                             {
                           "IoT-device_id": “..",
                                   "service_provided": "..",
                           "Type_of_device": "..",
                           "qos_range_min_rtt": “..”,
                           "qos_range_max_rtt": “..”,
                                   “max-lost-packets”: “..”,
                           "battery-level-status": “..”,
                           "additional-encryption": “..”
                                   },
                                ]
                   }
      },
      “vendor_extend” : {..}
}
```

**Message No. 2. Delete group**

```
{
      “request_type” : “up_message”,
      “action” : ”delete”
       “groups” : {
                    { “id_group” : ‘…’,
                      “group-name” : “”
                    },
                    { “id_group” : ‘…’,
                      “group-name” : “”
                    }
                    }
      “vendor_extend” : {..}
}
```

**Message No. 3. Update group**

```
{
      “request_type” : “up_message”,
      “action” : ”update”
       “groups” : {
                    { “id_group” : ‘…’,
                      “group-name” : “”,
                       "group": [
                       {
                      "IoT-device_id": “..",
                             "service_provided": "..",
                      "Type_of_device": "..",
                      "qos_range_min_rtt": “..”,
                      "qos_range_max_rtt": “..”,
                             “max-lost-packets”: “..”,
                      "battery-level-status": “..”,
                      "additional-encryption": “..”
                       },
                       {
                      "IoT-device_id": “..",
                             "service_provided": "..",
                      "Type_of_device": "..",
                      "qos_range_min_rtt": “..”,
                      "qos_range_max_rtt": “..”,
                             “max-lost-packets”: “..”,
                      "battery-level-status": “..”,
                      "additional-encryption": “..”
                          },
                        ]
               },
             { “id_group” : “…”,
               “group-name” : “”,
                “group": [
                       {
                      "IoT-device_id": “..",
                             "service_provided": "..",
                      "Type_of_device": "..",
                      "qos_range_min_rtt": “..”,
                      "qos_range_max_rtt": “..”,
                             “max-lost-packets”: “..”,
                      "battery-level-status": “..”,
                      "additional-encryption": “..”
                             },
                          ]
             }
},
      “vendor_extend” : {..}
}
```

**Message 4. Status**

```
{
      “request_type” : “equal_message”,
      “action” : ”status”
      “src_of_request” : ”…”
      “dst_of_request” : ”…”
      “vendor_extend” : {..}
}
```

# Appendix I

## Use cases

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

A new protocol for providing necessary network performance requirements for time constraint IoT-based applications over SDN is addressed in this Recommendation. The protocol ensures conventions and message formats for transfer of network performance requirements requested by an IoT server for IoT applications to the orchestrator application layer. The protocol is implemented between an IoT server and orchestrator and can be used in the following cases.

- Wide area network (WAN). Interconnection between the operator's network infrastructure (management layer) and that of third parties, which are IoT server providers.
- Local area network (LAN). Interconnection between the management layer of network infrastructure (orchestrator application layer) and a local IoT server, which is the platform for local time constraint IoT-based applications (e.g., LAN of a medical organization).

The use case in Figure I.1 presents a LAN with the implemented protocol for procuring the necessary network performance requirements for IoT (healthcare) applications. In this case, the LAN is based on SDN technologies.

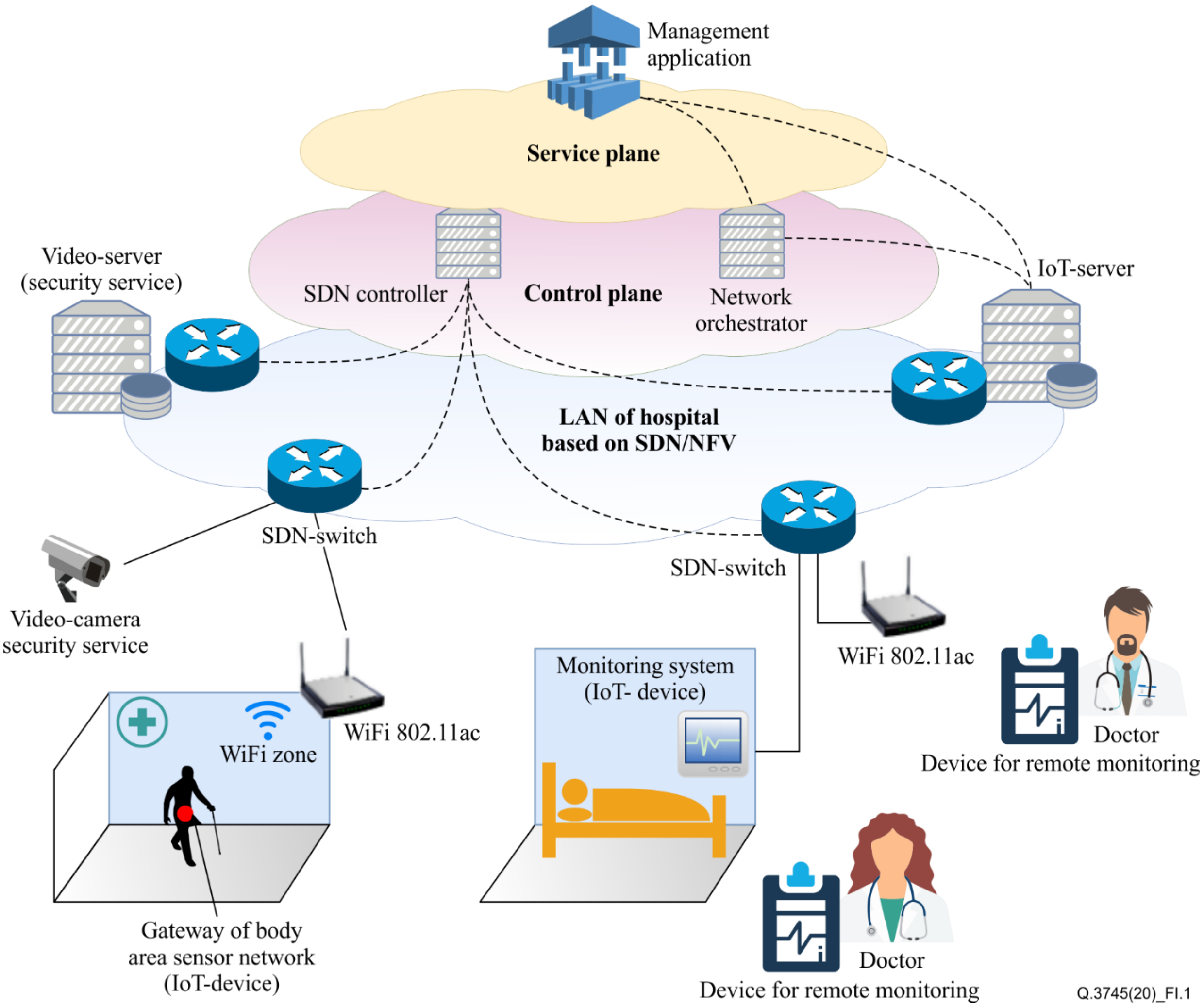


**Figure I.1 –Use case of protocol implementation in a hospital local area network**

In Figure I.1 the following connections are presented:

- solid line – wire connections;
- dotted lines – logical control connections, e.g., between SDN controller and SDN switches.

The protocol proposed in this Recommendation is to be used for interconnection between the IoT server and the orchestrator application layer (MA). According to the use case presented, the protocol provides the opportunity to set special settings for network control with necessary network performance requirements for IoT healthcare applications.

For example, there are two types of service presented in Figure I.1: video streaming (security service); and monitoring of patient health (body area sensor network with gateway and hospital bed monitoring system). In this case, the protocol requires network performance characteristics for operation data transfer to the doctor's remote devices through an IoT server.

# Bibliography

| | |
|---|---|
| [b-ITU-T Y.2060] | Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*. |
| [b-ITU-T Y.2091] | Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks*. |
| [b-ITU-T Y.3001] | Recommendation ITU-T Y.3001 (2011), *Future networks: Objectives and design goals*. |
| [b-ITU-T Y.3300] | Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking*. |
| [b-ITU-T Y.4101] | Recommendation ITU-T Y.4101/Y.2067 (2017), *Common requirements and capabilities of a gateway for Internet of things applications*. |

# 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