International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4418

(06/2018)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet of things and smart cities and communities – Frameworks, architectures and protocols

Gateway functional architecture for Internet of things applications

Recommendation ITU-T Y.4418

ITU International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	**Y.4400–Y.4549**
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.4418

Gateway functional architecture for Internet of things applications

Summary

Recommendation ITU-T Y.4418 provides the gateway functional architecture for Internet of things (IoT) applications, including gateway functional entities, relevant reference points and logical flows.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4418	2018-06-29	20	11.1002/1000/13640

Keywords

Functional architecture, gateway, Internet of things (IoT)

---

* 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 Y.4418

Gateway functional architecture for Internet of things applications

1 Scope

This Recommendation provides the gateway functional architecture for Internet of things (IoT) applications. The scope of this Recommendation also includes:

– the gateway functional entities for IoT applications;

– the gateway reference points for IoT applications;

– typical logical flows.

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.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.

[ITU-T Y.4101] Recommendation ITU-T Y.4101/Y.2067 (2017), *Common requirements and capabilities of a gateway for Internet of things applications*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 device [ITU-T Y.4000]: With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing.

3.1.2 gateway [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.

3.1.3 Internet of things (IoT) [ITU-T Y.4000]: 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.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of application, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CoAP	Constrained Application Protocol
DM	Device Management
GPRS	General Packet Radio Service
GW	Gateway
HTTP	Hypertext Transfer Protocol
IoT	Internet of Things
LTE	Long-Term Evolution
MAC	Media Access Control
PHY	Physical layer
QoS	Quality of Service
WCDMA	Wideband Code Division Multiple Access

5 Conventions

In this Recommendation:

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

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" and "may" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are 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.

6 Introduction

IoT devices need to interact with IoT applications through communication networks to provide different kinds of service to end users. In many cases, devices cannot connect to communication networks directly. Therefore, gateways support the interconnection of such devices with communication networks [ITU-T Y.4101]. Correspondingly, gateway capabilities belong to the device layer in the IoT reference model (see [ITU-T Y.4000]). Its capabilities include applications, device management (DM), communication management, data storage, data processing, data dispatching, interface abstraction, device adaptation and network adaptation [ITU-T Y.4101]. Figure 1 shows the typical gateway deployment scenario for IoT applications [ITU-T Y.4101].

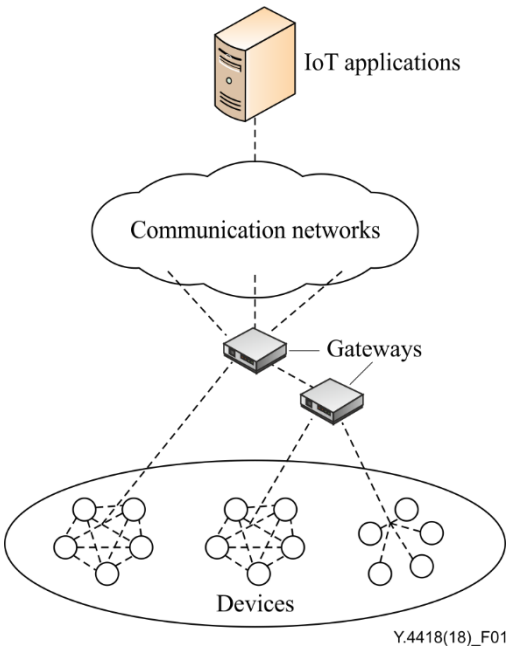

Figure 1 – Typical gateway deployment scenario for IoT applications [ITU-T Y.4101]

There are a lot of use cases where IoT system can play important roles, from lightweight cases that just collect raw data remotely and generate a full view of business in the cloud, to heavyweight cases like smart city applications that require more complicated application logic processing. In different cases, gateways have different capabilities.

In some cases, gateways just act as a message relay between IoT devices and an IoT application. They are only responsible for message-forwarding, protocol translation, if necessary, and some support capabilities, such as DM and security management. There is no specific application logic in the gateways. For instance, in one case, the gateway communicates with the IoT application through the hypertext transfer protocol (HTTP), and all devices managed by the gateway support the constrained application protocol (CoAP). In this case, the gateway is responsible for message forwarding and protocol translation between the CoAP and HTTP. In other cases where the IoT application supports the CoAP, it is sufficient for the gateway to forward CoAP messages only. This kind of gateway is called a message-forwarding gateway.

However, in many cases, it is far from sufficient for gateways only to perform message forwarding and protocol translation. Gateways often need to run specific application logic to fulfil user requirements. For instance, in one case, a gateway needs to collect data from devices, analyse data and send notifications to IoT applications only if pre-defined conditions are met. In another case, a gateway needs to collect data from one device and trigger another device to perform some action, if pre-defined conditions are met. These cases can be considered as the examples of so-called edge computing. Edge computing makes it possible to provide real-time services by executing application logic at the network edge, and reduces the stress on both the network and cloud side. A gateway is a suitable means for providing such edge computing capabilities.

There are two modes for gateways to provide such capabilities.

In some cases, a gateway is designed for only one specific IoT application. The gateway can process some IoT application logic locally. This kind of gateway is called a local-processing gateway.

In other cases, a gateway provides a common interface to many IoT applications instead of one only. Such a gateway manages IoT devices as resources. The resources of the gateway can be discovered and accessed to create new IoT applications. Different IoT applications interact with devices through a gateway resource-oriented interface. This kind of gateway is called a resource-openness gateway.

In summary, in addition to common capabilities, such as DM and security management, different gateways provide different capabilities depending on the case.

7 Gateway functional architecture for IoT applications

Figure 2 shows a full view of the gateway functional architecture for IoT applications, which covers the functions of the three typical gateway types discussed in clause 6. In the functional architecture, the application support functional entity is the core, which includes message-forwarding, local processing and recourse openness capabilities. At least one of these three capabilities is provided in one gateway according to different IoT application scenarios. Besides the core functional entity, other functional entities in the functional architecture are often used.

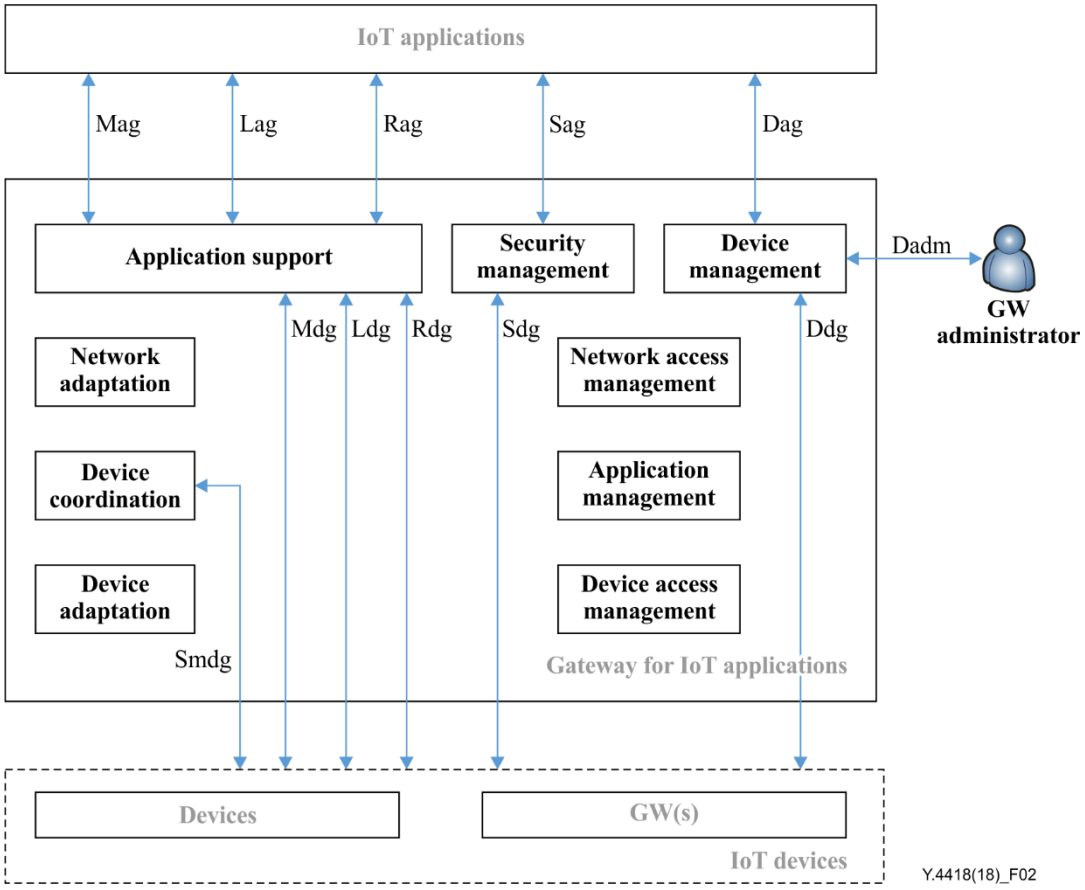

Figure 2 – Gateway functional architecture for IoT applications

The application support functional entity provides functions such as messages forwarding, local processing of application and resource openness with proper access control.

The network adaptation functional entity provides an adaptation function to different network technologies.

The device coordination functional entity provides functions such as interface abstraction, service discovery and service monitoring.

The device adaptation functional entity provides a connectivity adaptation function for the different types of device or other gateways that connect to the gateway.

The security management functional entity provides functions such as authentication and authorization, key management, as well as privacy protection.

The DM functional entity provides device-managing functions for devices connected to the gateway, other gateway(s) connected to the gateway and the gateway itself.

The network access management functional entity provides communication management functions between the gateway and IoT applications.

The application management functional entity provides core functional entity management functions, such as application deployment, application monitoring and application control, especially if several applications are running in one gateway.

The device access management functional entity provides communication management functions between devices and the gateway.

In the functional architecture, the gateway is connected with IoT applications, devices and other gateway(s) through reference points, as follows.

Reference points between the gateway and IoT applications:

– Mag reference point: reference point between the gateway and IoT applications in support of message-forwarding functions;
– Lag reference point: reference point between the gateway and IoT applications in support of local processing functions;
– Rag reference point: reference point between the gateway and IoT applications in support of resource openness functions;
– Sag reference point: reference point between the gateway and IoT applications in support of security management functions;
– Dag reference point: reference point between the gateway and IoT applications in support of DM functions.

Reference points between the gateway and IoT devices:

NOTE – IoT devices here include the devices and gateway(s) connected to the gateway.

– Smdg reference point: reference point between the gateway and IoT devices in support of service discovery related functions;
– Mdg reference point: reference point between the gateway and IoT devices in support of message-forwarding functions;
– Ldg reference point: reference point between the gateway and IoT devices in support of local processing functions;
– Rdg reference point: reference point between the gateway and IoT devices in support of resource openness functions;
– Sdg reference point: reference point between the gateway and IoT devices in support of security management functions;
– Ddg reference point: reference point between the gateway and IoT devices in support of DM functions.

Reference point between the gateway and the gateway administrator:

– Dadm reference point: reference point between the gateway and gateway administrator in support of DM functions.

8 Gateway functional entities for IoT applications

8.1 Application support functional entity

The application support functional entity is responsible for provision of capabilities including message forwarding, local processing and resource openness.

The functionalities of the message-forwarding capability support:

– message forwarding among the devices and communication networks;
– message forwarding among different devices or gateways that are connected to the gateway;
– message forwarding according to the sequential order of device data;
– adjustment of the sequential order of device data based on policies;
– a protocol translation function between different protocols as necessary when communicating with devices and applications.

The functionalities of the local processing capability support:

– local processing of applications, including aggregating data from devices and applications, analysing data, data format transformation between different data formats as required by devices and applications, encapsulating data based on application protocols, semantic mediation for data from devices and applications, collection or generation of device-related metadata as applicable, etc.
– local processing and execution interacting with remote IoT applications.

The functions of resource openness capability can be divided to different groups as described in clauses 8.1.1 to 8.1.7.

8.1.1 Resource discovery

The functions of resource discovery include supporting resources managed by devices to be found and identified by the gateway, resource registration and deregistration, resource identifier management, collection of information about resources and abstracting them into the resource repository according to the resource profile.

8.1.2 Resource monitoring

The functions of resource monitoring include checking and maintaining the consistency of the status of resources between the devices and the resource repository.

8.1.3 Resource access

The functions of resource access include getting information about resources in the resource repository or directly from devices with proper access control, and accessing resources managed by devices in order to perform some operations with proper access control.

8.1.4 Resource dispatch

The functions of resource dispatch include dispatching notifications to corresponding IoT applications according to the subscription rules registered by the IoT applications in advance. The content of notifications can include a status change of resources, a snapshot of resources to which IoT applications have subscribed, etc.

8.1.5 Resource profile management

The functions of resource profile management include creating, updating and deleting profiles of resources. Information in the resource profile includes, but is not limited to, resource name, resource type (e.g. home automation, vehicle or agriculture) and the data structure of the resource. Resources from devices should be abstracted according to the resource profile.

8.1.6 Application access management

The functions of application access management include access control rule management, and subscription and notification management of IoT applications to resources, including subscription and unsubscription of resources.

8.1.7 Resource repository

The functions of resource repository include storage of information about the resources managed by the gateway.

8.2 Network adaptation functional entity

The functionalities of network adaptation functional entity support:

– adaptation to different communication technologies, including physical layer/media access control (PHY/MAC) layer adaptation between the gateway and the access portion of the communication networks;

– communication network connection establishment and connection termination between the gateway and IoT applications;

– data transfer between the gateway and IoT applications.

There can be multiple network adaptation functional entities in one gateway to support different kinds of communication network (since one network adaptation functional entity is usually dedicated to only one type of communication network).

8.3 Device coordination functional entity

The functionalities of device coordination functional entity support:

– provision of an abstract interface supporting basic operations (such as reading data from a device) to interact with devices and applications;

– interface mapping between abstract interface and specific interfaces supported by devices and applications, which enables the interaction between devices and the gateway, and between different types of devices – the capabilities of interface mapping include interface syntax mapping and interface semantic mapping;

– interface abstraction for new device interfaces when new types of devices connect to the gateway;

– automatic discovery of services enabled in devices (e.g., via semantic service discovery mechanisms when applicable);

– collection of information about services and monitoring service status in devices.

– provision of information related to services enabled in devices (such as service type, service status, service discovery protocol and service semantic description information) to other devices connected to the gateway.

There can be multiple device coordination functional entities in one gateway to support different types of devices managed by gateway.

8.4 Device adaptation functional entity

The functionalities of device adaptation functional entity support:

– connectivity adaptation to different types of devices or other gateways that connect to the gateway;

– device connection establishment and connection termination;

– data transfer between the gateway and IoT devices.

There can be multiple device adaptation functional entities in one gateway to support devices belonging to different kinds of network (since one device adaptation functional entity is usually dedicated to only one type of local network).

8.5 Security management functional entity

The functionalities of security management functional entity support:

– functions of access control, which includes authentication and authorization – authentication capability includes mutual authentication between the gateway and IoT applications, as well as mutual or one-way authentication between the gateway and IoT devices;

– functions of key management, which includes key generation, key distribution, key update and key destruction;

– security policies according to different security levels;

– data encryption and decryption based on security policies;

– privacy policy enforcement.

8.6 Device management functional entity

The functionalities of a DM functional entity support:

– capabilities including configuration management, performance management, fault management, security management, DM protocol engine, accounting management and service exposure.

– device identifier management, including creating, updating, deleting and retrieving device identifiers and managing identifier mapping;

– the grouping of IoT devices based on device attributes (such as device type and device location);

NOTE – IoT devices here include the devices and gateway(s) connected to the gateway.

– gateway self-management and remote maintenance;

– gateway configuration according to multiple configuration modes, e.g., remote and local configuration, automatic and manual configuration, and dynamic configuration based on policies.

8.7 Network access management functional entity

The functionalities of network access management functional entity support:

– network profile management;

– selection of the communication network according to the communication technologies supported by the gateway [e.g., general packet radio service (GPRS), wideband code division multiple access (WCDMA) and long-term evolution (LTE)];

– data transfer quality of service (QoS) policies between the gateway and IoT applications;

– monitoring of the network connection status between the gateway and IoT applications;

– traffic control according to communication QoS requirements (e.g., communication delay and packet loss).

Support network connection performance measurement and analysis.

8.8 Application management functional entity

The functionalities of application management functional entity support:

– the management of multiple IoT applications in the gateway;

– status monitoring of applications running in the gateway;

– control of application, such as rebooting, if necessary.

8.9 Device access management functional entity

The functionalities of device access management functional entity support:

– device connection profile management;

– device connection status monitoring;

– data transfer QoS policies:

– communication based on device grouping.

9 Gateway reference points

Gateway reference points are identified in clauses 9.1 to 9.3.

9.1 Reference points between the gateway and IoT applications

9.1.1 Reference point Mag

The Mag reference point supports communication between the gateway and IoT applications. It enables the gateway to forward messages to IoT applications from IoT devices and to receive messages from IoT applications so that the messages can be forwarded to IoT devices by the gateway.

9.1.2 Reference point Lag

The Lag reference point supports communication between the gateway and IoT applications. It enables the gateway to interact with IoT applications for local processing, such as data aggregation from devices and applications according to the instructions of the IoT applications.

9.1.3 Reference point Rag

The Rag reference point supports communication between the gateway and IoT applications. It enables the gateway to interact with IoT applications in order to provide resource openness functions, such as resource subscription and dispatching notifications to IoT applications in response to the subscription of IoT applications as needed.

9.1.4 Reference point Sag

The Sag reference point supports communication between the gateway and IoT applications. It enables the gateway to interact with IoT applications in order to provide security management functions as needed, such as authentication, authorization and key management.

9.1.5 Reference point Dag

The Dag reference point supports communication between the gateway and IoT applications. It enables the gateway to interact with IoT applications in order to provide DM functions as needed, such as configuration management, performance management and fault management.

9.2 Reference points between gateway and IoT devices

NOTE – IoT devices here include the devices and gateway(s) connected to the gateway.

9.2.1 Reference point Smdg

The Smdg reference point supports communication between the gateway and IoT devices. It enables the gateway to interact with IoT devices in order to provide functions such as service discovery, collection of information about services in devices and provision of information related to services enabled in devices to other devices connected to the gateway.

9.2.2 Reference point Mdg

The Mdg reference point supports communication between the gateway and IoT devices. It enables the gateway to forward messages to IoT devices from IoT applications, and to receive messages from IoT devices, so that the messages can be forwarded to IoT applications by the gateway.

9.2.3 Reference point Ldg

The Ldg reference point supports communication between the gateway and IoT devices. It enables the gateway to interact with IoT devices to accomplish local application functions in the gateway, such as aggregating data from IoT devices and applications.

9.2.4 Reference point Rdg

The Rdg reference point supports communication between the gateway and IoT devices. It enables the gateway to interact with IoT devices in order to provide resource openness functions as needed, such as resource discovery, accessing resources from IoT devices and executing operations on IoT devices in accordance with requests from IoT applications under access control.

9.2.5 Reference point Sdg

The Sdg reference point supports communication between the gateway and IoT devices. It enables the gateway to interact with IoT devices in order to provide security management functions as needed, such as authentication, authorization and key management.

9.2.6 Reference point Ddg

The Ddg reference point supports communication between the gateway and IoT devices. It enables the gateway to interact with IoT devices in order to provide DM functions as needed, such as configuration management, performance management and fault management.

9.3 Reference point between the gateway and gateway administrator

9.3.1 Reference point Dadm

The Dadm reference point supports communication between the gateway and gateway administrator. It enables the gateway to be managed by local gateway administrator(s), e.g., for configuration management and fault management.

10 Logical flows

This clause describes the main gateway logical flows, which include typical scenarios, such as message forwarding, local processing and resource openness.

NOTE – IoT device(s) here include the device(s) and gateway(s) connected to the gateway.

10.1 Typical logical flows of message-forwarding scenarios

Figure 3 shows the logical flows describing the message-forwarding procedure. Three typical message-forwarding scenarios are listed, including:

1) from IoT device(s) to IoT application through the gateway;
2) from IoT application to IoT device(s) through the gateway;
3) among IoT devices through the gateway.

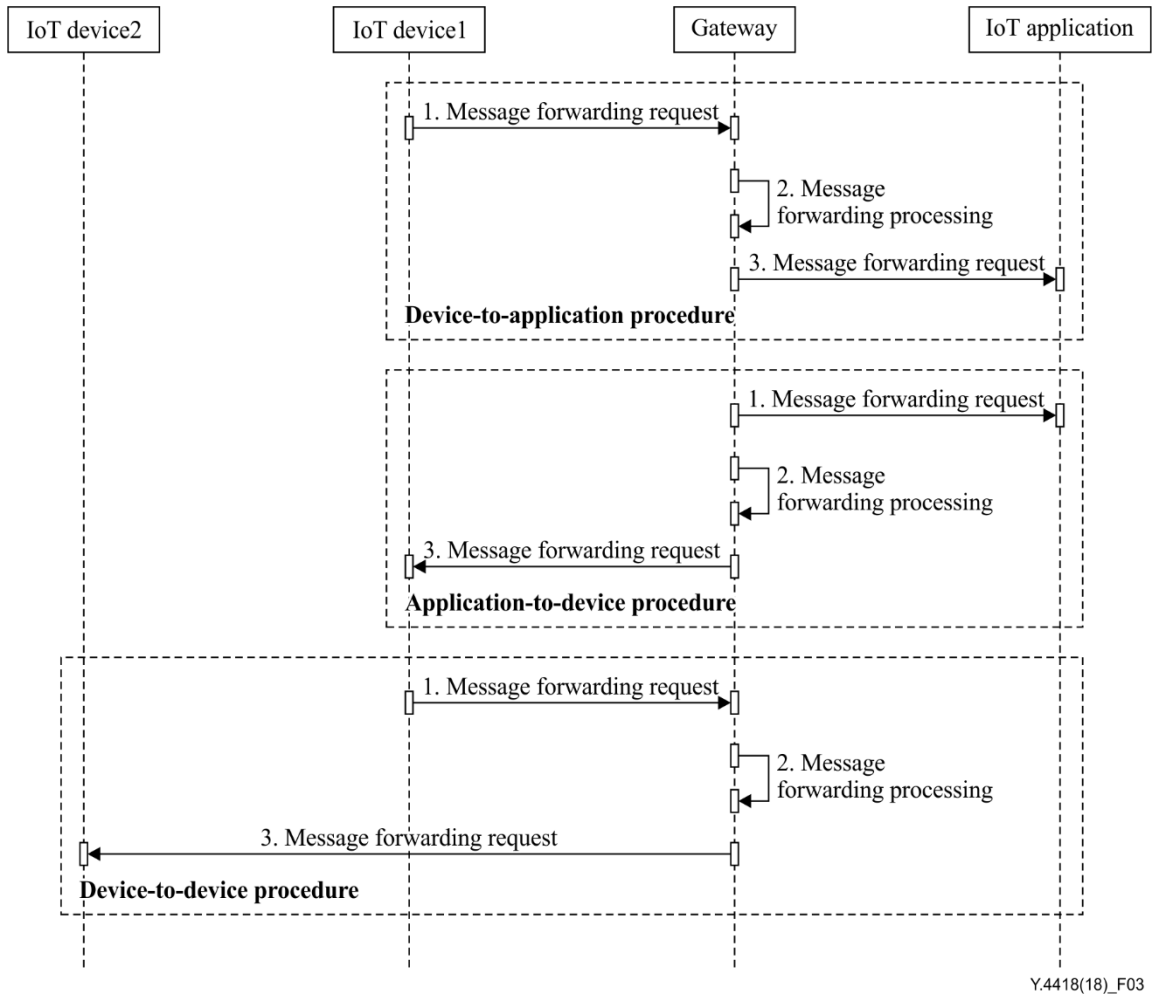

Figure 3 – Logical flows of message-forwarding scenarios

The main steps are outlined in clauses 10.1.1 to 10.1.3.

NOTE – Access verification is needed before message forwarding. Access verification includes authentication and authorization between the gateway and IoT applications, and between the gateway and IoT devices.

10.1.1 Message forwarding from IoT device to IoT application through the gateway

Step 1: An IoT device sends a message-forwarding request to the gateway through the reference point Mdg. The request includes information such as the identifier of the source IoT device, the identifier of the destination IoT application and the payload of the message.

Step 2: Upon receiving the request, the gateway is responsible for message-forwarding processing, such as verifying the destination IoT application and undertaking protocol translation, if needed.

NOTE – In the message-forwarding mode, after sending a message-forwarding request, the sender may not expect an acknowledgment of receipt, but a response can also be supported if needed.

Step 3: The gateway forwards the message to the IoT application through the reference point Mag.

10.1.2 Message forwarding from IoT application to IoT device through the gateway

Step 1: An IoT application sends a message-forwarding request to the gateway through the reference point Mag. The request includes information such as the identifier of the source IoT application, the identifier of the destination IoT device and the payload of the message.

Step 2: Upon receiving the request, the gateway is responsible for message-forwarding processing, such as verifying the destination IoT device and undertaking protocol translation, if needed.

NOTE – In the message-forwarding mode, after sending a message-forwarding request, the sender may not expect an acknowledgment of receipt, but a response can also be supported if needed.

Step 3: The gateway forwards the message to the IoT device through the reference point Mdg.

10.1.3 Message forwarding between IoT devices through the gateway

Step 1: An IoT device sends a message-forwarding request to the gateway through the reference point Mdg. The request includes information such as the identifier of the source IoT device, the identifier of the destination IoT device and the payload of the message.

Step 2: Upon receiving the request, the gateway is responsible for message-forwarding processing, such as verifying the destination IoT device and undertaking protocol translation, if needed.

NOTE – In the message-forwarding mode, after sending a message-forwarding request, the sender may not expect an acknowledgment of receipt, but a response can also be supported if needed.

Step 3: The gateway forwards the message to the destination IoT device through the reference point Mdg.

10.2 Typical logical flows of local processing scenarios

Figure 4 shows the logical flows describing how the gateway interacts with IoT devices and IoT applications for local processing of applications. Three typical local processing scenarios are listed, namely:

1) between IoT device(s) and the gateway;
2) notification to IoT application(s);
3) operation of IoT device(s) (originated from the IoT application side).

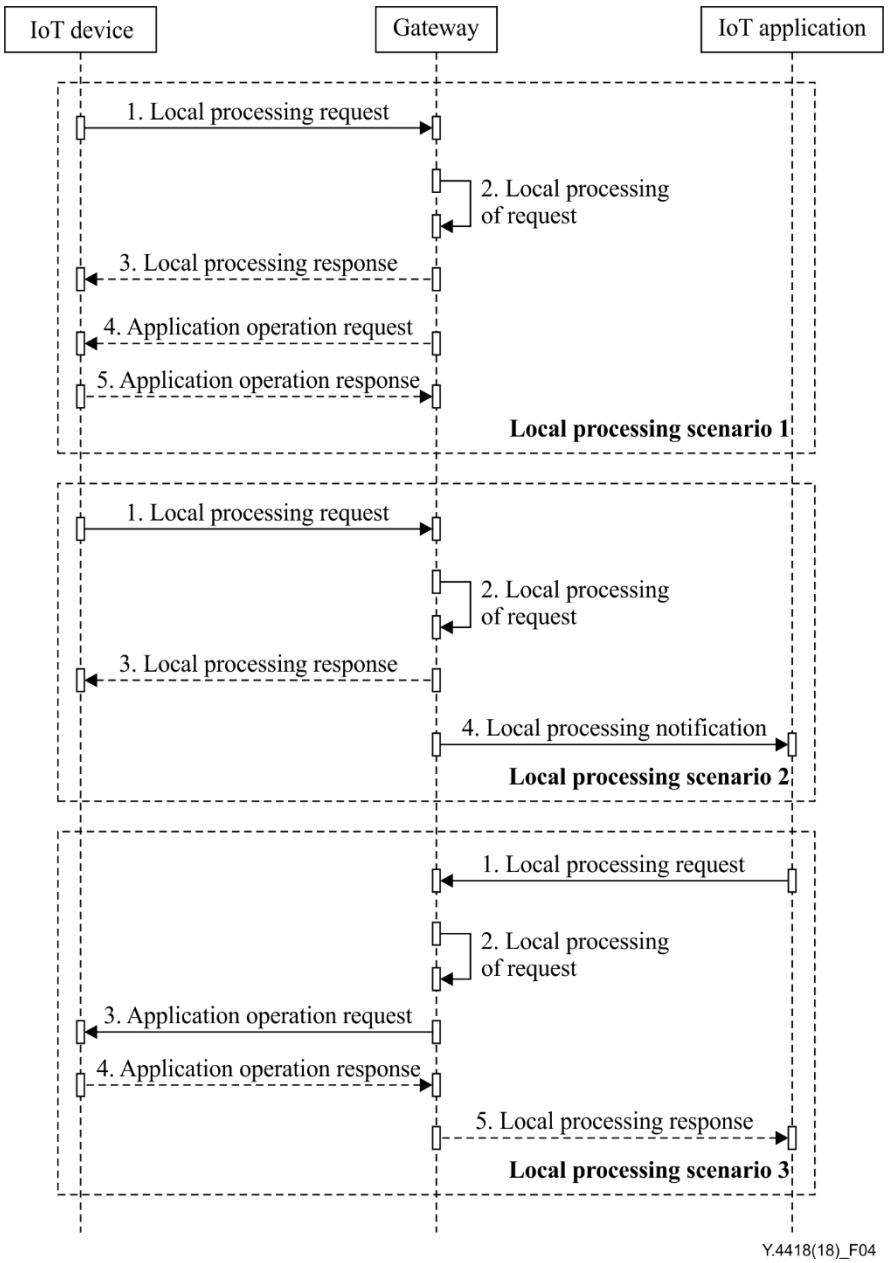

Figure 4 – Logical flows of local processing scenarios

The main steps are outlined in clauses 10.2.1 to 10.2.3.

NOTE – The gateway is responsible for authentication and authorization between the gateway and IoT applications, and between the gateway and IoT devices. The authentication and authorization procedure is supported before or after the local processing request according to the specific scenarios.

10.2.1 Local processing between IoT device(s) and the gateway

Step 1: An IoT device sends a local processing request to the gateway through the reference point Ldg. The content of the request depends on the specific requirements of the application, such as uploading the data from devices periodically or reporting abnormal status.

Step 2: Upon receiving the request, the gateway is responsible for processing the request locally, such as data aggregation or data analysis.

Step 3 (optional): The gateway sends a local processing response to the IoT device through the reference point Ldg.

NOTE 1 – The gateway supports receiving a request without sending a response in accordance with specific requirements.

NOTE 2 – After finishing the local processing of an application, the gateway may need to interact with the IoT device to perform some operations according to specific scenarios.

Step 4 (optional): The gateway sends an application operation request to the IoT device to control the application through the reference point Ldg.

NOTE 3 – Dispatch of a DM message to control the device (such as turn off the device because of an abnormal status) through the reference point Ddg is also supported.

Step 5 (optional): The IoT device executes the operation according to the application operation request and feeds back the result through the reference point Ldg.

NOTE 4 – The gateway may not expect a response from the IoT device(s), but a response can also be supported if needed.

10.2.2 Local processing notification to IoT application(s)

Step 1: An IoT device sends a local processing request to the gateway through the reference point Ldg. The content of the request depends on the specific requirement of the application, such as uploading the data from devices periodically or reporting abnormal status.

Step 2: Upon receiving the request, the gateway is responsible for processing the request locally, such as data aggregation or data analysis.

Step 3 (optional): The gateway sends a local processing response to the IoT device through the reference point Ldg.

NOTE 1 – The gateway supports receiving a request without sending a response in accordance with the specific requirements.

Step 4: If the pre-configured event is triggered, the gateway sends an application notification message to the IoT application(s) through the reference point Lag.

NOTE 2 – The gateway may not expect a response from the IoT application(s), but a response can also be supported if needed.

10.2.3 Local processing operation of IoT device(s) (originated from the IoT application side)

Step 1: An IoT application sends a local processing request to the gateway through the reference point Lag. The content of the request depends on the specific requirement of the application, such as instructions on triggering a pre-configured event.

Step 2: Upon receiving the request, the gateway is responsible for processing the request locally, such as analysing the instructions from the IoT application and executing the corresponding operations.

Step 3: The gateway sends an application operation request to IoT device(s) to control the application through the reference point Ldg.

NOTE 1 – Dispatch of a DM message to control the device (such as turn off the device because of an abnormal status) through the reference point Ddg is also supported.

Step 4 (optional): The IoT device executes the operation according to the application operation request and feeds back the result through the reference point Ldg.

NOTE 2 – The gateway may not expect a response from the IoT device(s), but a response can also be supported if needed.

Step 5 (optional): The gateway sends a local processing response to the IoT application through the reference point Lag.

NOTE 3 –The gateway supports receiving a request without sending a response, or to send a response immediately after receiving the request in accordance with the specific requirements.

10.3 Typical logical flows of resource openness scenarios

10.3.1 Subscription and notification of resource

Figure 5 shows the logical flow describing how the gateway interacts with an IoT application and IoT devices in the subscription and notification of resource scenario.

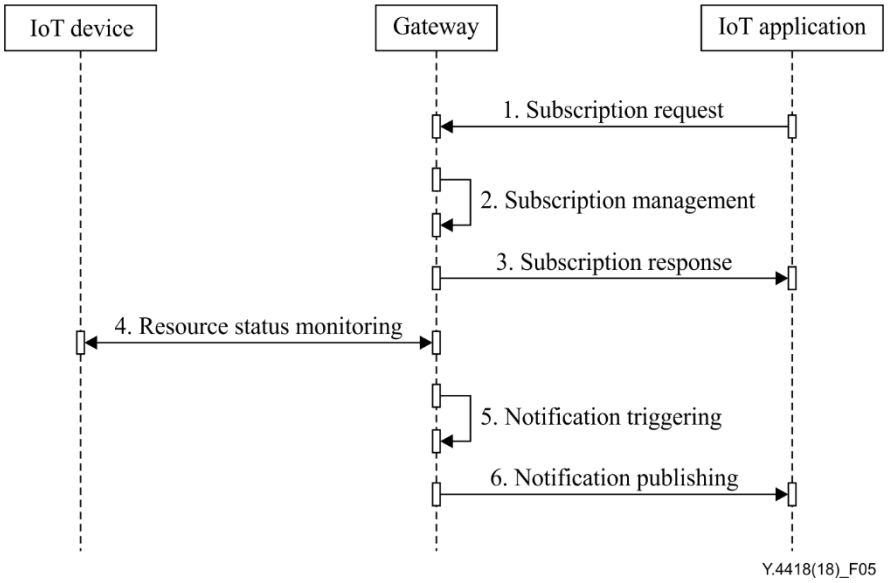

Figure 5 – Logical flow of subscription and notification of resource

The main steps are outlined as follows.

Step 1: An IoT application sends a resource subscription request to the gateway through the reference point Rag. The request includes information such as the identifier of the IoT application, the identifier of the resource or the content of the subscription (e.g., the frequency of the notification or the threshold to trigger the notification).

Step 2: Upon receiving the request, the gateway is responsible for processing the request, such as verifying whether the IoT application has the right to subscribe to the resource or recording the subscription logic if the subscription is successful.

Step 3: The gateway returns a subscription response to indicate the result of the subscription.

Step 4: If the subscription is successful, the gateway monitors the status of the subscribed resource. The monitoring mechanism includes, but is not limited to, polling by the gateway, addressing status changes initialy reported by the IoT device.

Step 5: When the triggering threshold is reached, the gateway triggers the notification.

Step 6: The gateway publishes the notification to the IoT application. The content of the notification depends on the specific requirement of the subscription, such as the status change of resources or the snapshot of resources to which IoT applications have subscribed.

NOTE – The gateway may not expect a response from the IoT application, but a response can also be supported if needed.

10.3.2 Resource access

Figure 6 shows the logical flow describing how the gateway interacts with an IoT application and IoT devices in the resource access scenario.

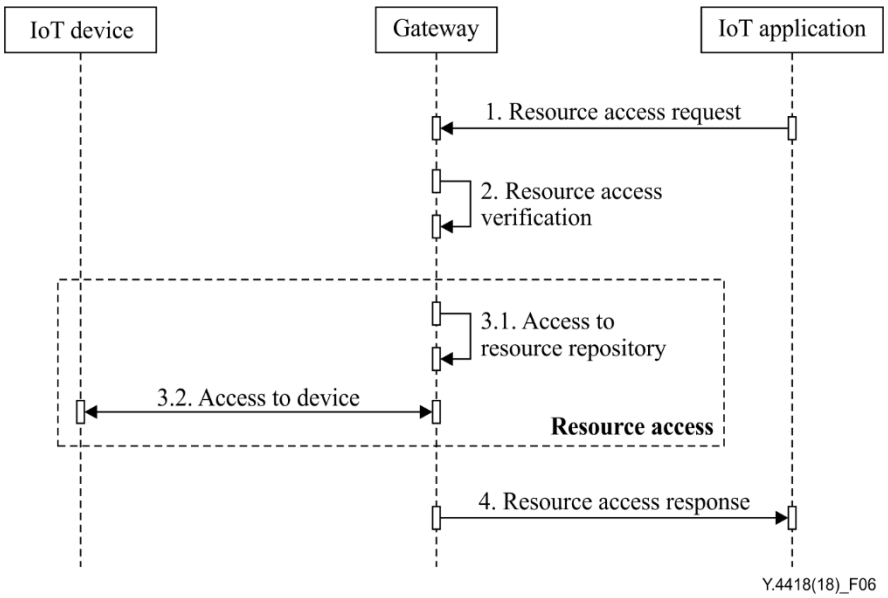

Figure 6 – Logical flow of resource access

The main steps are outlined as follows.

Step 1: An IoT application sends a resource access request to the gateway through the reference point Rag. The request includes information such as the identifier of the IoT application, the identifier of the resource and the purpose of the access (e.g., getting information about the accessed resource or performing an operation on the resource).

Step 2: Upon receiving the request, the gateway is responsible for verifying whether the IoT application has the right to obtain access to the resource and perform the related operation on the resource.

Step 3: If the verification is successful, the gateway allows the IoT application to obtain access to the resource. Two mechanisms are supported according to the specific requirements of the IoT application and implementation of the gateway, including:

Step 3.1: Accessing the resource repository or

Step 3.2: Accessing directly the IoT device.

Step 4: The gateway returns a response to the resource access request, to feed back the requested resources or the results of the requested operation to the resource.

11 Security considerations

The gateway for IoT applications supports provision of security management functions through the security management functional entity (see clause 8.5).

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, 2018