

ITU-T

Y.4101/Y.2067

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(10/2017)

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 –
Requirements and use cases

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

Next Generation Networks – Frameworks and functional
architecture models

Common requirements and capabilities of a gateway for Internet of things applications

Recommendation ITU-T Y.4101/Y.2067

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.4101/Y.2067

Common requirements and capabilities of a gateway for Internet of things applications

Summary

Recommendation ITU-T Y.4101/Y.2067 provides the common requirements and capabilities of a gateway for Internet of things (IoT) applications. The common requirements and capabilities provided are intended to be generally applicable in gateway application scenarios.

NOTE – Recommendation ITU-T Y.4101/Y.2067 focuses on the gateway as equipment interconnecting devices with communication networks.

History

| Edition | Recommendation | Approval | Study Group | Unique ID* |
|---------|---------------------|------------|-------------|---|
| 1.0 | ITU-T Y.4101/Y.2067 | 2014-06-06 | 13 | 11.1002/1000/12170 |
| 2.0 | ITU-T Y.4101/Y.2067 | 2017-10-29 | 20 | 11.1002/1000/13384 |

Keywords

Capabilities, gateways, IoT applications, requirements.

* 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/>.

© ITU 2017

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

| | | Page |
|---|---|------|
| 1 | Scope..... | 1 |
| 2 | References..... | 1 |
| 3 | Definitions | 1 |
| | 3.1 Terms defined elsewhere | 1 |
| | 3.2 Terms defined in this Recommendation..... | 2 |
| 4 | Abbreviations and acronyms | 2 |
| 5 | Conventions | 2 |
| 6 | Introduction to gateways for IoT applications..... | 3 |
| 7 | General characteristics of a gateway for IoT applications..... | 4 |
| | 7.1 Connection to communication networks | 4 |
| | 7.2 Device access..... | 4 |
| | 7.3 Protocol translation..... | 4 |
| | 7.4 Interaction and support of applications | 4 |
| | 7.5 Adaptability | 4 |
| | 7.6 Management functions support | 4 |
| | 7.7 Security functions support | 4 |
| 8 | Common requirements of a gateway for IoT applications | 5 |
| | 8.1 General gateway requirements | 5 |
| | 8.2 Adaptation-related requirements | 5 |
| | 8.3 Support capabilities-related requirements | 6 |
| | 8.4 Application-related requirements | 8 |
| | 8.5 Security- and management-related requirements | 9 |
| 9 | Common capabilities of a gateway for IoT applications..... | 9 |
| | 9.1 Reference technical framework and typical high-level flows of a gateway for IoT applications | 9 |
| | 9.2 Details of common capabilities of a gateway for IoT applications | 11 |
| | Appendix I – Use cases of a gateway for IoT applications..... | 14 |
| | I.1 Gateway in home services | 14 |
| | I.2 Gateway in automotive telematics..... | 15 |
| | I.3 Gateway in online collaborative whiteboard..... | 16 |
| | Bibliography..... | 18 |

Recommendation ITU-T Y.4101/Y.2067

Common requirements and capabilities of a gateway for Internet of things applications

1 Scope

This Recommendation provides the common requirements and capabilities of a gateway for Internet of things (IoT) applications. The common requirements and capabilities provided are intended to be generally applicable in gateway application scenarios.

The scope of this Recommendation includes:

- general characteristics of a gateway for IoT applications;
- common requirements of a gateway for IoT applications;
- common capabilities of a gateway for IoT applications.

Use cases of a gateway for IoT applications are provided in appendices.

NOTE – This Recommendation focuses on the gateway as equipment interconnecting devices with communication networks.

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.4111] Recommendation ITU-T Y.4111/Y.2076 (2016), *Semantics based requirements and framework of the Internet of things*.
- [ITU-T Y.4114] Recommendation ITU-T Y.4114 (2017), *Specific requirements and capabilities of the Internet of things for big data*

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 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 applications, 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

This Recommendation defines the following term:

3.2.1 gateway: 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.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

| | |
|--------|---|
| 3G | Third Generation |
| 4G | Fourth Generation |
| CAN | Controller Area Network |
| CRM | Customer Relationship Management |
| ECU | Electronic Control Unit |
| GPRS | General Packet Radio Service |
| GPS | Global Positioning System |
| IoT | Internet of Things |
| IP | Internet Protocol |
| LTE | Long Term Evolution |
| MAC | Media Access Control |
| MSISDN | Mobile Station International ISDN/PSTN Number |
| NGN | Next Generation Network |
| PHY | Physical layer |
| QoS | Quality of Service |
| SMS | Short Message Service |
| TCP | Transmission Control Protocol |
| TV | Television |
| URI | Uniform Resource Identifier |
| WCDMA | Wideband Code Division Multiple Access |
| Wi-Fi | Wireless Fidelity |
| xPON | x Passive Optical Network |

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 to gateways for IoT applications

In IoT applications, information in either the physical or information world is collected by devices and is received through communication networks. Some devices cannot connect to communication networks directly. Gateways support the interconnection of such devices with communication networks.

Figure 1 shows a typical deployment scenario of gateways for IoT applications.

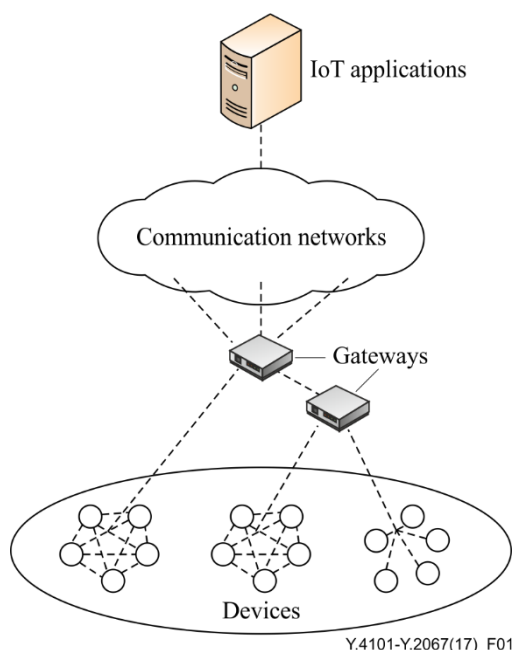


Figure 1 – Typical deployment scenario of gateways for IoT applications

As shown in Figure 1, different kinds of devices can connect to communication networks through one or multiple gateways. The connectivity between devices and gateway(s) can be based on different kinds of wired or wireless technologies, such as a controller area network (CAN) bus [b-ISO 11898-1], ZigBee [b-IEEE 802.15.4], Bluetooth [b-IEEE 802.15.1] or Wi-Fi [b-IEEE 802.11].

The communication networks can be realized via existing networks, such as those based on the transmission control protocol/Internet protocol (TCP/IP) or evolving networks, such as next generation networks (NGNs) [b-ITU-T Y.2001]. A gateway that connects to these networks should support the appropriate communication technologies.

IoT applications implement application logic according to application requirements. The applications can not only be based on proprietary application platforms, but also be built upon common service or application support platforms providing generic enabling capabilities, such as authentication, device management, charging and accounting [ITU-T Y.4000].

The gateway connects to IoT applications through the communication networks.

7 General characteristics of a gateway for IoT applications

7.1 Connection to communication networks

The gateway has the general characteristic of connecting to communication networks. Devices can connect to communication networks through such a gateway. In some cases, for example in configurations with multiple gateways, one or more gateways are connected to other gateways (as shown in Figure 1) and not directly to communication networks.

The gateway supports different kinds of communication technology to connect to different communication networks.

7.2 Device access

The gateway has the general characteristic of supporting access of devices. The devices can connect to each other or to the communication networks by accessing gateways. The gateway supports different kinds of device access technology.

7.3 Protocol translation

The gateway has the general characteristic of protocol translation. The gateway supports the protocol translation between devices and communication networks. In some cases, a gateway translates the protocols among different devices that are connected to the gateway itself.

7.4 Interaction and support of applications

The gateway has the general characteristic of providing interaction with, and support of, applications, including common application logic interaction and support of data caching, data semantic mediation and data analytics [ITU-T Y.4111], [ITU-T Y.4114].

This enables, for example, reduction of end-to-end operation time for time-critical applications and separation of common capabilities from application dedicated logic for reducing application development time.

7.5 Adaptability

The gateway has the general characteristic of adaptability. It is expected that the gateway has standardized interfaces and semantic mediation support. The gateway can be deployed in different application environments by adaptation according to functional components and related protocols.

7.6 Management functions support

The gateway has the general characteristic of supporting management functions, including device management, network management, service management and protocol management.

7.7 Security functions support

The gateway has the general characteristic of supporting security functions. The gateway provides security mechanisms to support the security requirements of applications.

NOTE – Common security mechanisms used in a gateway include those for device authentication, data encryption, confidentiality and security policy management.

8 Common requirements of a gateway for IoT applications

8.1 General gateway requirements

– Scalability

There may be a huge number of devices accessing a gateway.

The gateway is required to be scalable in terms of the number of connected devices and to support interconnection with other gateways to increase the global scalability of the gateways.

– Addressing

The gateway is required to support various addressing schemes, e.g., IP and non-IP addressing schemes, including public and private addressing for IP schemes.

– Openness to functional extensions

The gateway is required to provide standard interfaces to support functional extensions of the gateway, e.g., for deployment in diversified application environments.

– Quality of service

The gateway usually plays a key role in the IoT application scenarios where quality of service (QoS) support is essential.

The QoS-related requirements of the gateway are as follows:

- 1) the gateway is required to support traffic control policy and QoS differentiation according to the categories of traffic;
- 2) the gateway is required to provide mechanisms for performance measurement and management.

– Communication aspects

The gateway is deployed between devices and communication networks and can use different communication technologies [e.g., third generation (3G), fourth generation (4G), x passive optical network (xPON), ZigBee, wireless fidelity (Wi-Fi) and Ethernet] to transfer data.

The communication-related requirements of the gateway are as follows:

- 1) the gateway is required to support communication bridging between devices and communication networks;
- 2) the gateway is required to support communications with at least one application;
- 3) the gateway is recommended to support multiple communication technologies to interact with communication networks and devices, and to be able to enhance the capabilities of the communication interfaces, if the support of additional communication technologies is required – in such a case, the gateway is required to be able to select the communication technologies according to the specific service requirements.

8.2 Adaptation-related requirements

– Protocol diversity support

The gateway needs to communicate with devices and applications that may support different protocols. The gateway should be able to load new protocols according to communication requirements.

The protocol-related requirements of the gateway are as follows:

- 1) the gateway is required to support protocol translation between different protocols as necessary when communicating with devices and applications;
- 2) the gateway is recommended to support dynamic protocol loading;
- 3) the gateway is recommended to support protocol semantic description [ITU-T Y.4111].

– **Uniformity of interactions**

The gateway is recommended to support uniform interaction with different devices and applications.

The requirements of the gateway related to uniformity of interactions are as follows:

- 1) The gateway is recommended to support uniform operations through standardized protocols on devices which use different communication technologies.
- 2) The gateway is recommended to support uniform interaction through standardized protocols with different applications.
- 3) The gateway is recommended to support uniform interaction with applications or devices through semantic mediation in case of heterogeneous protocols.

8.3 Support capabilities-related requirements

– **Device and service discovery**

When devices are connected to a gateway, the gateway needs to discover them. In addition, the gateway needs to discover new services that are published by applications.

The device and service discovery requirements of the gateway are as follows:

- 1) the gateway is required to support mechanisms for device discovery when a device connects to the gateway for the first time or in the case of gateway restart;
- 2) the gateway is required to support mechanisms for service discovery when new services are published by applications.

NOTE – Service discovery may include advertisement by the gateway and solicitation of the gateway. Effective mechanisms depend on application implementation aspects. Semantic discovery mechanisms [ITU-T Y.4111] may be used if devices and services can provide semantic description information.

– **Device management**

There are a great number of devices that are connected to a gateway and most of them have capability constraints. The gateway manages devices based on policies or instructions received from applications.

The device management requirements of the gateway are as follows:

- 1) the gateway is required to support management of device-related information, e.g., device identification, device configuration;
- 2) the gateway is required to support monitoring of device status for usage by applications or itself;
- 3) the gateway is required to support firmware and software update of devices;
- 4) the gateway is required to support device management on behalf of applications upon request;
- 5) the gateway is recommended to support fault management of devices based on policies;
- 6) the gateway is recommended to support performance management of devices based on policies.

– **Service management**

Devices which are connected to a gateway may use different communication technologies such as IP and non-IP based wireless technologies. According to these communication technologies, different types of service discovery protocols may be used in devices. The gateway requires some service management capabilities, including the schemes for the discovery of the services offered by devices (e.g., a sound speaker in a Bluetooth-enabled device, sound player in a Wi-Fi enabled device), for the collection of information related to

the services, for monitoring service status in devices and for realizing interoperability between the different service discovery protocols used in devices.

The service management requirements of the gateway are as follows:

- 1) the gateway is required to support the collection of service-related information (e.g., service identification, service configuration, service semantic description information when supported) through service discovery schemes;
- 2) the gateway is recommended to support the advertisement of service-related information collected through service discovery schemes;
- 3) the gateway is required to support the monitoring of the service status in devices;
- 4) the gateway is required to support the interworking between the various service discovery protocols used in devices;
- 5) the gateway is required to support service management on behalf of device applications upon application request.

– **Device identifier management**

Multiple types of device identifiers may be used in IoT applications, e.g., IP address, mobile station international ISDN/PSTN number (MSISDN), uniform resource identifier (URI) and data elements. A device may have single or multiple identifiers that are managed by the gateway.

The device identifier requirements of the gateway are as follows:

- 1) the gateway is required to support identifier mapping capability between different types of device identifiers;
- 2) the gateway is recommended to support identifier combination capability, e.g., the combination of device identifier with gateway identifier;

NOTE – The combined identifiers may be provided to applications as globally unique identifiers, while the gateway resolves the combined identifiers to address the different devices.

- 3) the gateway is recommended to support the assignment of temporary communication identifiers to the devices connected to the gateway itself.

– **Storage**

A gateway has two methods to store data. The first is temporary storage: in this case, the data that are temporarily stored need to be removed according to pre-defined policies, e.g., service logic, maximum data storage volume. The second data storage method is permanent storage: in this case, the data that are permanently stored are important for successful service operations and for correct gateway and device operations.

For data safety and security, the data stored in gateways and applications should be kept consistent.

The storage requirements of the gateway are as follows:

- 1) the gateway is required to support local storage, including temporary and permanent storage;
- 2) the gateway is recommended to support capabilities for ensuring data consistency between the gateway and applications.

NOTE – Applications are expected to support capabilities for ensuring data consistency with gateways.

– **Device grouping**

Devices may be grouped by type, location, etc. For example, all devices in the same room can constitute a group. Likewise, the devices of the same type behind a gateway can constitute a group. A gateway can operate devices efficiently based on groups. The gateway

is required to support group operations for devices, including operations to create, update, read and delete groups of devices.

– **Data collection and aggregation**

A gateway collects data from devices and transfers the data to applications. A gateway may have multiple modes of capturing and aggregating data based on policies.

The data collection and aggregation requirements of the gateway are as follows:

- 1) the gateway is required to support data collection from devices based on policies, e.g., real time collection or time schedule-based collection;
- 2) the gateway is recommended to support aggregation of data from devices;
- 3) the gateway is recommended to support compression mechanisms for data from devices (e.g., for redundancy elimination);
- 4) the gateway is recommended to collect device-related metadata or to generate them by itself as applicable.

NOTE 1 – Device-related metadata may include the data providing information about device semantic descriptions, device data provenance and device data model.

NOTE 2 – Data collection requirements of the gateway that are specific for big data can be found in [ITU-T Y.4114].

– **Data dispatching and delivery**

For a large number of devices behind a gateway, the gateway can efficiently dispatch and transfer data between devices and applications based on policies.

The data dispatching and delivery requirements of the gateway are as follows:

- 1) the gateway is required to support mechanisms to dispatch data based on policies;
- 2) the gateway is recommended to support mechanisms to pre-process data based on policies before dispatching them;
- 3) the gateway is required to support data delivery based on QoS requirements of applications;
- 4) the gateway is required to support data delivery based on device group identification if devices are grouped.

8.4 Application-related requirements

– **Application logic integration**

The gateway is recommended to support application logic integration.

NOTE 1 – By supporting application logic integration, the gateway can process application-related functions locally and independently from remote facilities.

The gateway is recommended to interact with the appropriate application (platform) for application logic integration.

– **Data analytics**

The gateway is recommended to provide data analytics for support of specific application requirements (e.g., time-critical applications).

NOTE 2 – By supporting data analytics, the gateway can locally analyse data from devices and applications, as needed, before transferring data to applications and thus reduce the total operation time. Application domain examples include automatic driving and industrial control in smart manufacturing.

8.5 Security- and management-related requirements

– Security and confidentiality

For the security of applications, a gateway must control access to devices and to itself, and must protect data security and confidentiality for itself and devices.

The security and confidentiality requirements of the gateway are as follows-

- 1) The gateway is required to support identification of access to the connected devices.
- 2) The gateway is required to support authentication with devices. Based on application requirements and device capabilities, the gateway is required to support mutual or one-way authentication with devices.
- 3) The gateway is required to support mutual authentication with applications.
- 4) The gateway is required to support the security of the data that are stored in devices and the gateway, or transferred between the gateway and devices, or transferred between the gateway and applications – the gateway is required to support the security of these data based on security levels.
- 5) The gateway is required to support mechanisms to protect confidentiality for devices and the gateway.

– Self-management and remote maintenance

The gateway is required to support self-management and remote maintenance.

The self-management and remote maintenance requirements of the gateway are as follows:

- 1) The gateway is required to support self-diagnosis and self-repair as well as remote maintenance.
- 2) The gateway is required to support firmware and software update.
- 3) The gateway is required to support auto configuration or configuration by applications. The gateway is required to support multiple configuration modes, e.g., remote and local configuration, automatic and manual configuration, and dynamic configuration based on policies.

9 Common capabilities of a gateway for IoT applications

9.1 Reference technical framework and typical high-level flows of a gateway for IoT applications

9.1.1 Reference technical framework

The reference technical framework of a gateway for IoT applications is composed of the following capability groups:

- applications group;
- support capabilities group;
- adaptation capabilities group;
- security and management capabilities group.

The applications group provides support for interacting with remote applications and for local processing of application logic. It supports the deployment of multiple IoT applications of different kinds and used in different domains (e.g., power metering in smart home domain, monitoring of the elderly in the e-health domain). This group may utilize the capabilities provided by the support capabilities group.

The support capabilities group provides common capabilities for the gateway to interact with devices and applications. This group includes the following capabilities.

- Device management, which provides capabilities for managing devices and communicates device profiles to the gateway itself and to applications.
- Communication management, which provides capabilities for establishing and managing communication with devices and applications. It includes capabilities for the support of the communication QoS requirements (e.g., communication delay, packet loss).
- Data storage, which provides capabilities for permanent and temporary storage of data, including data collected from devices, gateway configuration data and data from applications.
- Data processing, which provides capabilities for processing data, including analysing data, transforming data formats, enabling semantic mediation, encapsulating data based on application protocols and aggregating data from devices.
- Data dispatching, which provides capabilities for pre-processing data from applications based on policies and for optimizing data distribution.
- Service management, which manages the services of devices connected to the gateway providing the service management capabilities.

The adaptation capabilities group provides capabilities for communicating with devices and applications, and hiding the differences between devices and applications. This group includes the following capabilities.

- Interface abstraction, which provides an abstract interface supporting basic operations (such as reading data from a device) to interact with devices and applications, and also provides mapping capability from an abstract interface to specific interfaces supported by devices and applications.
- Device adaptation, which provides connectivity for the different types of devices or other gateways that connect to the gateway.
- Network adaptation, which provides adaptation to different network technologies, including physical layer/media access control (PHY/MAC) layer adaptation between the gateway and the (access portion of the) communication networks.

The security and management capabilities group provides capabilities for supporting security and management of the gateway itself.

Figure 2 shows the reference technical framework of a gateway for IoT applications.

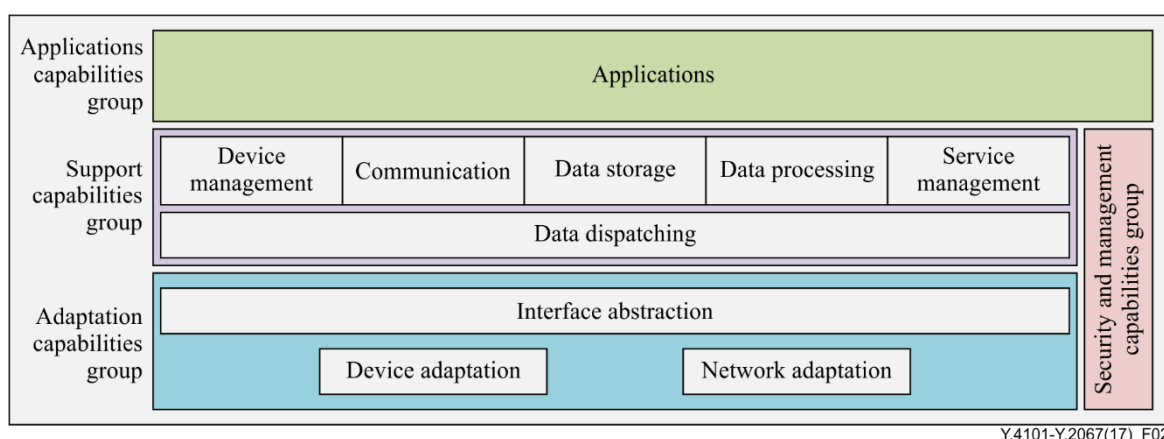


Figure 2 – Reference technical framework of a gateway for IoT applications

9.1.2 Typical high-level flows

In IoT applications, a gateway can receive data from IoT applications and then send the data to devices and it can receive data from devices and then send the data to IoT applications. In this regard, the

typical high-level flows with respect to the capability groups identified in the gateway reference technical framework are as follows.

- Data are received from IoT applications and sent to devices: the gateway receives data from IoT applications through the adaptation capabilities group that provides network adaptation and interface abstraction. The gateway does the necessary application logic processing via the applications capabilities group and sends data to devices through the adaptation capabilities group that provides interface abstraction and device adaptation. These processes are accomplished in collaboration with the support capabilities group and the security and management capabilities group.
- Data are received from devices and sent to IoT applications: the gateway receives data from devices through the adaptation capabilities group that provides device adaptation and interface abstraction. The gateway does the necessary application logic processing via the applications capabilities group and sends data to IoT applications through the adaptation capabilities group that provides interface abstraction and network adaptation. These processes are accomplished in collaboration with the support capabilities group and the security and management capabilities group.

9.2 Details of common capabilities of a gateway for IoT applications

9.2.1 Applications group

The functionalities of the applications group are as follows.

- The applications group supports deployment of specific IoT application logic in the gateway via a standard open interface. Via such application logic, the gateway can process some IoT application-related functions locally.
- The applications group supports resource openness with proper access control via a standard open interface, so that the resources of the gateway can be discovered and accessed. The gateway is required to support functions for resource openness, including resource abstraction, resource identifier management, and resource registration and deregistration.

9.2.2 Support capabilities group

9.2.2.1 Data dispatching

The functionalities of data dispatching are as follows:

- to support capability of dispatching data to devices according to the sequential order of the device data.
- to support capability of dispatching data from devices to applications as appropriate.
- to support capability of adjusting the sequential order of the device data based on policies.

9.2.2.2 Device management

The functionalities of device management are as follows:

- to support capability of providing collection and monitoring of device status;
- to support capability of providing device-related information to applications;
- to support capability for device firmware and software update;
- to support device configuration, according to configuration profiles (downloaded from applications, or stored in the gateway) or configuration commands (received from applications);
- to support device diagnosis and automatic reparation;
- to support capability of creating, updating, deleting and retrieving device identifiers and managing identifier mapping;

- to support device discovery;
- to support capability of grouping devices based on device attributes (such as device type, device location, etc.).

9.2.2.3 Data processing

The functionalities of data processing are as follows:

- to support capability of data format transformation between different data formats as required by devices and applications;
- to support capability of aggregating data from devices and applications;
- to support capability of semantic mediation for data from devices and applications;
- to support capability of data analytics for local decision making or control at the gateway level;
- to support capability of collection or generation of device-related metadata as applicable.

9.2.2.4 Data storage

The functionalities of data storage are as follows:

- to support access rights (e.g., read, write) to data that are stored in the gateway for security and confidentiality purposes;
- to support capability of data caching for data from devices and applications;
- to support data synchronization between the gateway and applications, e.g., upload of collected data from devices to applications, download of configuration management data from applications to the gateway.

9.2.2.5 Communication management

The functionalities of communication management are as follows:

- to support capability of establishing and managing communications between the gateway and applications;
- to support selection of the access network (to connect with the communication networks) according to the communication technologies supported by the gateway [e.g., General Packet Radio Service (GPRS), Wideband Code Division Multiple Access (WCDMA), Long Term Evolution (LTE)];
- to support capability of data transferring from applications and devices based on QoS-enabled policies, e.g., priority of data transferring from devices in different network environments;
- to support capability of communication based on device grouping.

9.2.2.6 Service management

The functionalities of service management are as follows:

- to support capability of automatic discovery of services enabled in devices (e.g., via semantic service discovery mechanisms when applicable);
- to support capabilities of collecting information of services and monitoring service status in devices;
- to support capability of providing 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.

9.2.3 Adaptation capabilities group

9.2.3.1 Interface abstraction

The functionalities of interface abstraction are as follows.

- To support interface mapping between abstract interface and specific interfaces supported by devices and applications. 1-to- N and N -to-1 mappings are supported for interface abstraction. This includes interface mapping for new device interfaces when new types of devices connect to the gateway.

NOTE – If applicable, data semantic mediation mechanisms may be used to convert data between abstract interface and specific interfaces.

9.2.3.2 Device adaptation

The functionalities of device adaptation are as follows:

- to support capability of connectivity for the different types of devices or other gateways that connect to the gateway.

9.2.3.3 Network adaptation

The functionalities of network adaptation are as follows:

- to support capability for connecting to various types of communication networks according to the appropriate communication technologies, including for PHY/MAC layer adaptation between the gateway and the access portion of the communication networks;
- to support capability for dynamic loading of communication protocols.

9.2.4 Security and management capabilities group

The functionalities of security and management capabilities group are as follows:

- to support mutual authentication between the gateway and applications;
- to support mutual or one-way authentication between the gateway and devices;
- to support security policies according to different security levels;
- to support key lifecycle management including key generation, key distribution, key update and key destruction;
- to support data encryption and decryption based on security policies;
- to support confidentiality of the data of the gateway and devices;
- to support gateway self-management and remote maintenance;
- to support gateway firmware and software update;
- to support gateway configuration according to multiple configuration modes, e.g., remote and local configuration, automatic and manual configuration, and dynamic configuration based on policies.

Appendix I

Use cases of a gateway for IoT applications

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

I.1 Gateway in home services

A gateway in home services can connect to electrical equipment and safety equipment through local networks and can connect to remote application servers through communication networks. The electrical equipment and safety equipment can be controlled remotely by the gateway. Figure I.1 shows a use case of a gateway in home services.

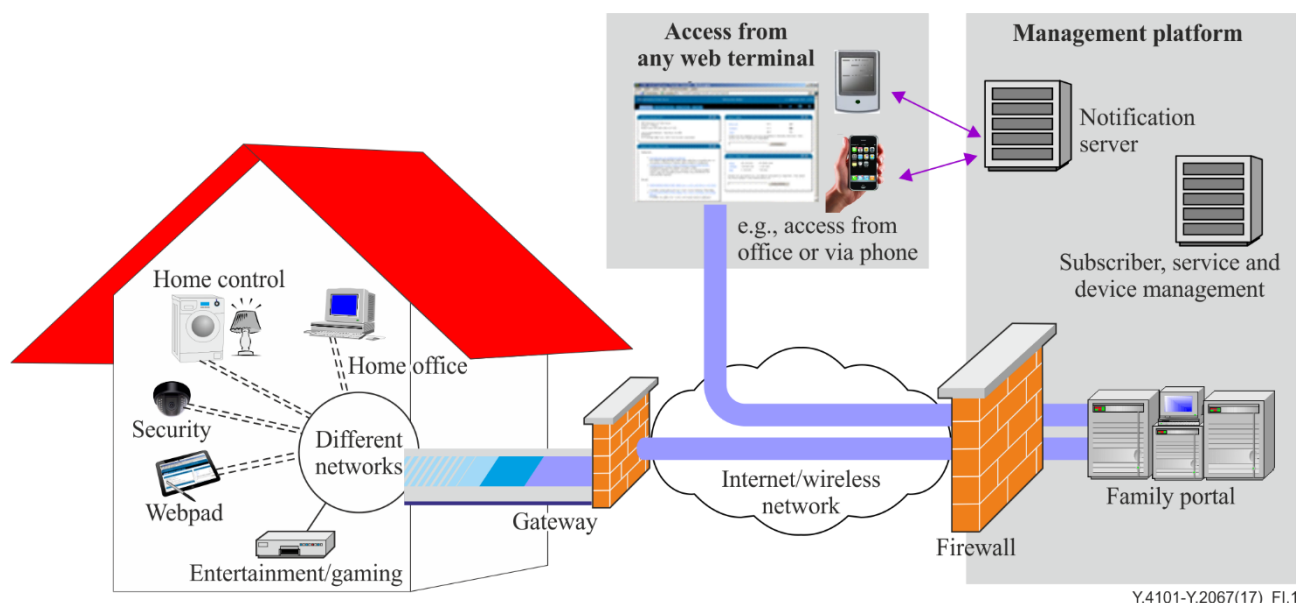


Figure I.1 – Use case of a gateway in home services

Home monitoring and management applications include:

- monitoring of home security remotely (i.e., remote monitoring through web cameras via the TV, laptop or smartphone);
- control of appliances (e.g., turn lights on/off, sprinklers, garage door, security alarm, thermostat, pool heater) remotely via a device with a web browser;
- scheduling of appliances (e.g., scheduling of lighting, water heater, alarm system and heating) via automatically created profiles;
- monitoring of home or office service appliances (e.g., printer, projector, scanner, speaker and game console) remotely via a device with a web browser;
- service management of appliances (i.e., providing the service information related to service on/off of printer, projector and scanner).

In these scenarios, as shown in Figure I.1, the gateway has a very important role.

The home owner can configure the gateway to control each of the connected devices and monitor their service status. Control functions may be implemented through pre-set rules (time-of-day, threshold or alarm driven, etc.) or implemented through commands delivered via a short message service (SMS) message.

Even though the connected devices may be heterogeneous, the gateway can collect information about devices and available services by using service discovery (e.g., advertisement and solicitation schemes) for interoperability between them, and aggregate the collected data of multiple sensors and the service profile of the connected devices. The gateway allows combination of data and profiles in order to provide advanced services.

For example, in home security scenarios, the gateway usually integrates the inputs coming from different sensors and provides the home owner with a user interface to configure the home security system.

I.2 Gateway in automotive telematics

Automotive telematics deals with wireless communications of information and applications between a vehicle or its occupants and external entities. Such communications allow authorized entities, such as automakers, emergency services and service centres, to interact with a vehicle and its driver, enabling enhanced safety and support services. In its most advanced modes, automotive telematics also allows motorists to safely expand mobile computing capabilities directly into their vehicles and benefit from Internet-based services.

The applications of automotive telematics can be divided into four categories:

- driver safety and security applications;
- customer relationship management (CRM) applications for automakers and dealers;
- personal applications and services;
- business applications and services.

Figure I.2 shows a typical use case of a gateway in automotive telematics.

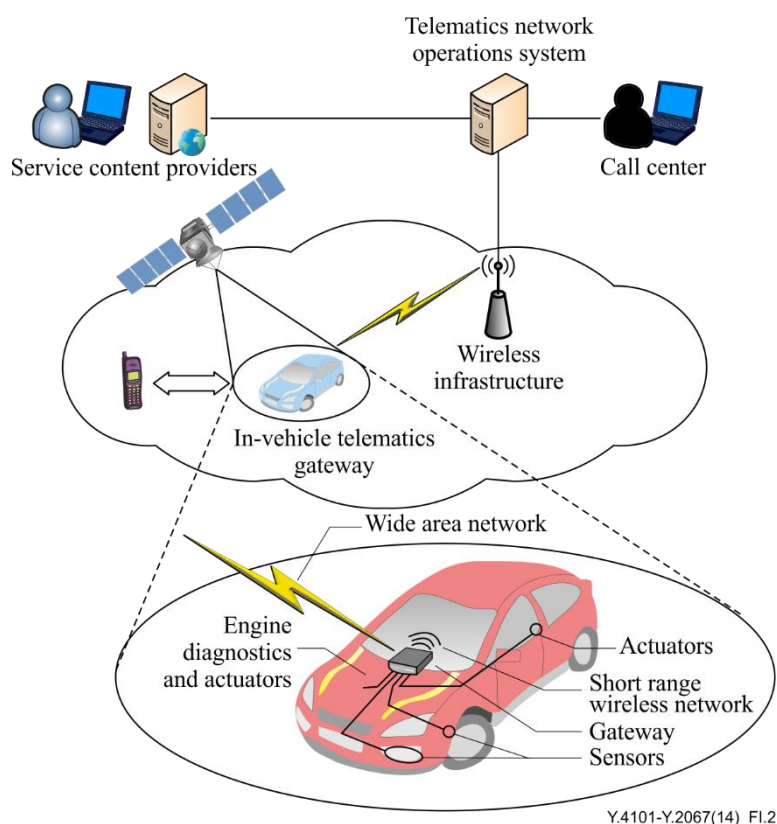


Figure I.2 – Use case of a gateway in automotive telematics

In automotive telematics, the gateway is the key entity. It is the embedded in-vehicle gateway that communicates with the automobile electronic control units (ECUs) and the global positioning system (GPS) satellite and accesses the telematics services over the wireless infrastructure.

In driver safety and security applications, the gateway can monitor the various sensors in the vehicle and, in the event of a crash, sends the details (e.g., intensity and location information) to the service centre, if the crash notification service is provided. For stolen vehicle tracking, anti-theft alarm notification and remote door service, the in-vehicle gateway can be triggered to periodically send precise location information to the service centre or can be triggered automatically by the anti-theft sensors in the vehicle. In this way, the service centre can track the vehicle. Furthermore, even when the in-vehicle gateway cannot send any information about the crash and stolen vehicle tracking because of disconnection from outside networks (e.g., satellite), the in-vehicle gateway can still detect other temporary methods for networking (e.g., Internet-sharing of cell phones) by using service discovery schemes and can then redirect data to the service centre.

In diagnostics services, the gateway in the vehicle can perform a detailed scan when triggered remotely or when some key thresholds are crossed (e.g., distance travelled or time elapsed since last diagnostic scan).

I.3 Gateway in online collaborative whiteboard

An online collaborative whiteboard is an application for web-based visual collaboration.

The online collaborative whiteboard application allows distributed project participants to collaborate on developing and managing software projects. For example, an online collaborative whiteboard allows participants, via the network, to share web documents (e.g., web pages) and spreadsheets, exchange ideas, write and edit annotations, ask questions, post tasks and web applications, and other collaboration tasks with other participants.

The data (e.g., web pages, web applications, spreadsheets) transferred through the network by different devices (e.g., pad, mobile phone, laptop) are handled by the gateway for display on the online collaborative whiteboard. First, the gateway discovers a supporting collaborative whiteboard service and connects devices to it. The gateway in an online collaborative whiteboard acts as the data aggregation point for real-time management and visualization. The data can be regarded as a resource for collaborative work services, such as brainstorming, virtual meeting, remote learning and remote training. Figure I.3 shows a use case of a gateway in an online collaborative whiteboard.

Via the gateway in an online collaborative whiteboard, the participants of the distributed project, who use different devices, can, for example, upload background images and web documents and draw on top of them. All participants connected to the whiteboard can see the various changes in real time.

The gateway in an online collaborative whiteboard represents a typical use case of integration of application functionalities into the gateway. In this use case, the gateway can process some application functions locally without communicating with remote application servers.

The features provided by the local application functionalities of the gateway in online collaborative whiteboard include:

- a fast web document viewer;
- a browser-based application;
- automatic synchronization between project participants;
- recording and displaying of edited web documents;
- writing, inserting and replacing annotations;
- deletion of web documents and web applications;
- connection with the participants of the distributed project via the network.

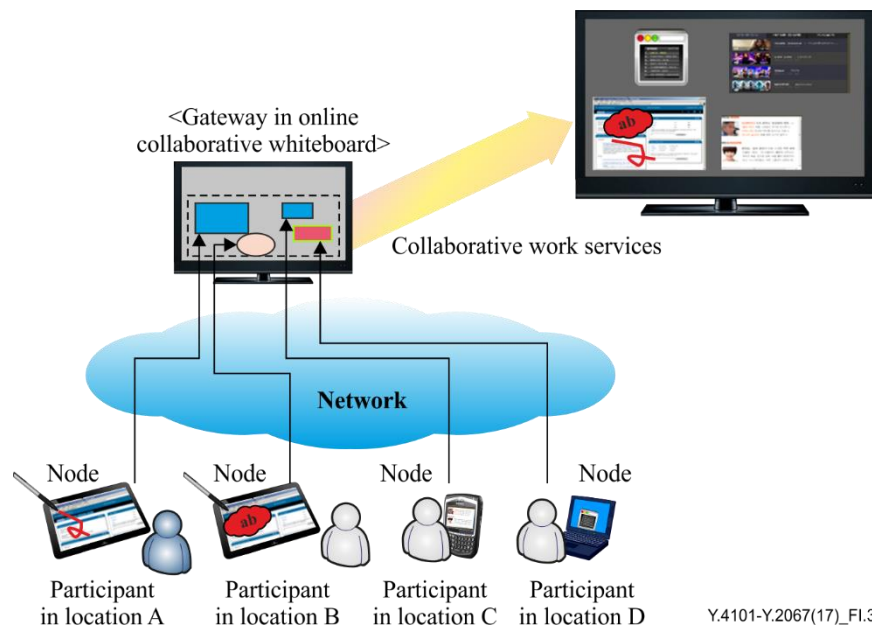


Figure I.3 – Use case of a gateway in an online collaborative whiteboard

Bibliography

- [b-ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.
- [b-IEEE 802.11] IEEE Std 802.11-2016, *IEEE Standard for Information technology – Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.
- [b-IEEE 802.15.1] ANSI/IEEE Std 802.15.1-2005, *IEEE Standard for information technology – Local and metropolitan area networks – Specific requirements – Part 15.1a: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPAN)*.
- [b-IEEE 802.15.4] IEEE Std 802.15.4-2015, *IEEE Standard for low-rate wireless networks*.
- [b-ISO 11898-1] ISO 11898-1:2015, *Road vehicles – Controller area network (CAN) – Part 1: Data link layer and physical signalling*.

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.

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 |