International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4113

(09/2016)

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

Internet of things and smart cities and communities – Requirements and use cases

Requirements of the network for the Internet of things

Recommendation ITU-T Y.4113

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND 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.4113

Requirements of the network for the Internet of things

Summary

Recommendation ITU-T Y.4113 describes the requirements of the network for the Internet of things (IoT) that enhance the common requirements of the IoT identified in Recommendation ITU-T Y.4100/Y.2066. The requirements focus on the transport functions of the network, but also cover service support functions.

The requirements described in this Recommendation are common requirements for core network, access network and IoT area network.

There are a lot of use cases of the IoT with heterogeneous characteristics. Considering the current status of deployments in the IoT market, this Recommendation focuses on the requirements of the network for the IoT with smart meters and sensors as devices. Other use cases will be covered in the future revisions of this Recommendation.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4113	2016-09-13	20	11.1002/1000/13025

Keywords

Internet of Things, requirements of the network, sensor, smart meter.

* 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.4113

Requirements of the network for the Internet of things

1 Scope

This Recommendation describes the requirements of the network for the Internet of things (IoT). The common requirements of the IoT described in [ITU-T Y.4100] are high-level; thus this Recommendation is complementary to [ITU-T Y.4100] in term of specific requirements of the network for the IoT.

Because an increasing number of devices with heterogeneous characteristics will be connected to the network via varying access technologies depending on the specific deployment environment, it is important to consider the requirements of the network that are applicable to those various use cases of the IoT, and avoid case-by-case studies for each specific use case. This approach is expected to encourage IoT development.

There are many use cases of the IoT with heterogeneous characteristics. Considering the current status of the deployments in the IoT market, this Recommendation focuses on the network for the IoT with smart meters and sensors as device for the IoT. Other use cases will be covered in future revisions of this Recommendation.

The scope of this Recommendation includes:

- general description of the network for the IoT, addressing respectively:
  - basic model of the network for the IoT;
  - general characteristics of smart meters and sensors;
  - general issues of the network for the IoT.
- requirements of the network for the IoT, addressing respectively:
  - general requirements;
  - core network requirements;
  - IoT area network requirements.

Examples of use cases with smart meters and sensors are described in Appendix I.

Several access network and IoT area network technologies for the network supporting the IoT are identified in Appendix II.

NOTE – The technologies listed in Appendix II are not meant to be exhaustive.

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.4100] Recommendation ITU-T Y.4100/Y.2066 (2014), *Common requirements of the Internet of things*.

[ITU-T Y.4101] Recommendation ITU-T Y.4101/Y.2067 (2014), *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 access network [b-ITU-T Q.1742.11]: A network that connects access technologies (such as a radio access network) to the core network.

3.1.2 core network [b-ITU-T Y.101]: A portion of the delivery system composed of networks, systems equipment and infrastructures, connecting the service providers to the access network.

3.1.3 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.

3.1.4 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.

3.1.5 thing [ITU-T Y.4000]: With regard to the Internet of things, this is an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 IoT area network: A network of devices for the IoT and gateways interconnected through local connections.

NOTE – This definition is based on "Overview of the Internet of things" [ITU-T Y.4000], where clause 6.2 states "devices can communicate with other devices using direct communication through a local network (i.e., a network providing local connectivity between devices and between devices and a gateway, such as an ad-hoc network)".

3.2.2 sensor: (Based on the definition given in [b-ITU-T Y.2221]) An electronic device that senses a physical condition or chemical compound and delivers an electronic signal proportional to the observed characteristic.

NOTE – Examples of usage of sensors include temperature monitoring, gas-leak alert, traffic congestion prediction, earthquake early warning, etc.

3.2.3 smart meter: With regard to the Internet of things, a device for monitoring, measurement recording and control of utility usage.

NOTE – Examples of utilities include electricity, gas and water.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

2G Second Generation wireless telephony technology

3G	Third Generation wireless telephony technology
ADSL	Asymmetric Digital Subscriber Line
API	Application Programming Interface
DSL	Digital Subscriber Line
FTTx	Fiber To The x
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
LAN	Local Area Network
LPWA	Low Power Wide Area
LTE	Long Term Evolution
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
PSTN	Public Switched Telephone Network
SDSL	Symmetric Digital Subscriber Line
ULE	Ultra Low Energy
xDSL	x Digital Subscriber Line

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. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 General description of the network for the IoT

This clause introduces a basic model of the network for the IoT, general characteristics of smart meters and sensors, and general issues of the network for the IoT.

6.1 Basic model of the network for the IoT

The basic model of the network for the IoT consists of three parts as shown in Figure.1: core network, access network and IoT area network.

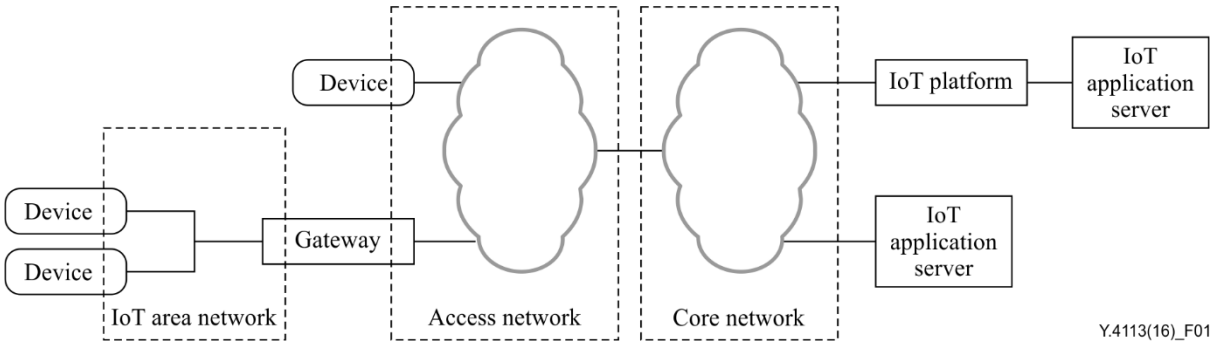

Figure 1 – Basic model of the network for the IoT

The device is a piece of equipment with mandatory capabilities of communication, and optional capabilities of sensing, actuation, data capture, data storage and data processing with regard to the IoT [ITU-T Y.4000].

The gateway is a unit with regard to the IoT which interconnects the devices with the core network. It performs the necessary translation between the protocols used in the core network and those used by devices [ITU-T Y.4101].

The core network is a portion of the delivery system composed of networks, equipment and infrastructures, and connects the service provider domain with the access network.

The access network connects the devices for the IoT and gateways to the core network. It can be implemented using different technologies such as fibre optics and radio access technologies.

The IoT area network is a network of devices for the IoT and gateways that are interconnected. Connectivity is realized through local connections, typically using short-range communication technologies.

The IoT platform is a technical infrastructure that provides integration of generic and specific capabilities [ITU-T Y.4000]. These capabilities, in conjunction with capabilities of the core network, may be exposed to one or more IoT application servers. The core network provides communication functionalities to support the data transfer to devices and gateways via access network. Some of those functionalities can be used by service providers.

The IoT application server runs applications, and communicates with devices, gateways and IoT platform via the core network (or directly in case of communicate with the IoT platform) directly in order to deliver application services.

6.2 General characteristics of smart meters and sensors as devices for the IoT

The general characteristics of smart meters and sensors as devices for the IoT are described in this clause.

6.2.1 Small size data communication

Typical data handled by smart meters and sensors concern environmental information, usage of energy resources and status of communication availability of smart meters and sensors.

Since most of these data are text based, not video or image based, the typical data handled by smart meters and sensors are, in general, of small size.

6.2.2 Periodic data communication

One popular usage of smart meters and sensors is for environmental data measurements. Environmental data are in many use cases measured at fixed times and it is natural to send measured data at those same times; thus, periodic data communication is expected to occur.

Another aspect of consider is the long lifetime of smart meters and sensors. Once these devices are deployed, they are expected to work for 10 years or more. Therefore, status monitoring of smart meters and sensors, i.e., checking they are working correctly, is needed. In some implementations, status monitoring data transmissions occur due to a pre-defined value of data transmission interval although this interval may vary depending on the specific implementations.

NOTE – Appendix I.1 shows related use cases with smart meters.

6.2.3 Huge number of deployed devices

The number of deployed smart meters and sensors is expected to be huge. The decreasing cost of these devices and the increasing number of related applications are both factors leading to the increasing scale of such deployments.

NOTE 1 – Smart meters may be used for smart grids and for applications using environmental data collection. Houses, offices and commercial facilities are typical places where smart meters are deployed.

NOTE 2 – Sensors may be used for public infrastructure (buildings, roads, trains, etc.). In addition, embedded sensors in smart phones, wearable devices and other devices are also in use.

6.3 General issues of the network for the IoT

The large deployment of smart meters, sensors and related applications in the field may impose new challenges on the network due to the unique features of these devices. The following clauses describe general issues of the network due to the characteristics described in clause 6.2.

6.3.1 Packet loss and higher latency due to simultaneous data transmission

Numerous IoT deployments concern devices, like smart meters, transmitting data containing readings at specific timings.

A group of devices may upload their data at the same time (e.g., when a trigger event for data transmission occurs on these devices at the same time, or when simultaneous processing of these data by the remote application server is required). In such a case, the network may face the problem of simultaneous data transmissions (e.g., increasing the possibility of collisions of the random access channel) which may lead to packet loss and/or higher latency for these data transmissions.

NOTE – Obviously, packet loss and higher latency are particularly relevant in case of a large number of simultaneous data transmissions.

6.3.2 Unreliability of short-range radio communications in the IoT area network

Some critical applications may need particular consideration in terms of reliability. In the case of smart meters connected to an IoT area network using short-range radio communications, transmissions may not be reliable due to the instability of the short-range radio connections. There may be substantial loss of data in the data collection in this situation. If, for example, the collected data are intended to be used for monitoring of total power consumption and control of generation of electricity, the error-prone IoT system would not contribute to an improvement in level of the electricity system.

6.3.3 Network overload due to large amount of traffic to be processed

With the increasing deployment of smart meters and sensors, the number of IoT area networks connected to the core network also increases accordingly. In such a case, even if the IoT area network has sufficient resources to process data from smart meters and sensors, issues in the core network may arise. One of the causes for such issue is that the amount of data received from IoT area networks may be too great to be processed in the core network. This may cause overload problems of the resources of the core network in term of links and network entities.

Those issues may also arise in the access network. Even if the IoT area network operates without specific issues, congestion may be caused in the access network. One of the causes for such

congestion is that the amount of data received from these IoT area networks may be too great to be processed in the specific area of the access network connecting these IoT area networks to the core network.

7 Requirements of the network for the IoT

This clause describes the requirements of the network for the IoT, distinguished in general requirements, core network requirements and IoT area network requirements. The requirements of the access network for the IoT are not specified.

Considering requirements for the IoT, technologies that may be applicable for use in the access network and IoT area network are provided in Appendix II.

7.1 General requirements

This clause describes general requirements of the network for the IoT with smart meters and sensors which are potentially related to all three parts of the networks.

NOTE – Each clause also identifies rational for the respective requirements, although this rational is not meant to be exhaustive.

7.1.1 Support of a variety of devices for the IoT

Based on requirement C9 of [ITU-T Y.4100], the following general requirement is derived for this Recommendation:

– the network is recommended to accommodate a variety of devices including devices with constrained capabilities.

NOTE – Some devices such as environmental sensors have constrained capabilities with limited power, memory and processing resources in order to be ultra-low cost. The network should accommodate devices with constrained capabilities.

7.1.2 Scalability

Based on clauses 6.2.3 and 6.3.3 of this Recommendation, the following general requirement is derived for this Recommendation:

– the network is required to be scalable.

NOTE – Decreasing cost of devices and increasing number of application demands are the main factors driving the increased number of deployed devices. The decreasing cost of devices allows new use cases, which are not profitable at higher device cost, to be deployed commercially. There is a clear trend that the number of deployed devices continues to increase. Therefore, the network ultimately needs to support a large number of devices.

7.2 Core network requirements

This clause describes the requirements for the core network.

7.2.1 Status monitoring

Based on clauses 6.3.2 and 6.3.3 of this Recommendation, the following core network requirements are derived for this Recommendation:

– the core network is recommended to support status monitoring for gateways, devices and IoT area networks;

– the core network is recommended to support status information request to gateways and/or devices according to the network management policies.

The monitored status information includes, among other things: load status of gateways and devices, IoT data traffic routes, gateway and IoT area network topologies, and failure detection for critical devices and gateways which maintain IoT area network topologies. The network can request this

information on-demand based on policies so that the network can leverage the latest information (independently from the status information autonomously provided to the network by devices and gateways).

Supporting status monitoring can allow the core network to manage several IoT area networks in a unified manner. There may be several IoT area networks, each with its own resource capacity and connection reliability. For IoT service provisioning, communication between devices and service providers is needed; therefore, the connections between IoT area networks and core network should be as reliable as possible. Traffic volumes from IoT area networks toward the core network may be unbalanced, which may lead to network resource unavailability unless those IoT area networks are managed in a unified manner. Unified network management with status monitoring may be able to reduce resource unavailability due to traffic imbalance.

It is not always required that the core network be involved in status monitoring, however the core network can assist the service providers by exposing monitored information if the core network supports status monitoring.

7.2.2 Data transmission scheduling management

Based on clauses 6.2.2 and 6.3.1 of this Recommendation, the following core network requirement is derived for this Recommendation:

– the core network is recommended to support data transmission scheduling management for gateways, devices and IoT area networks.

The timing of the data transmission from gateways and/or devices is normally dependent on the application implementation by developers and can be configurable by the application user. If no specific considerations are applied with respect the data transmission timing, the impact of many devices transmitting data to the network at the same time may cause traffic congestion. Therefore, the network should exhibit robustness with respect to such situations by supporting mechanisms which manage the timing of data transmission from gateways and/or devices.

In particular, data transmission scheduling management aims to coordinate the data transmission timing within a relevant group of gateways (e.g., a domain based group or an application based group) according to policies and load considerations. In case the devices are connected to the core network without gateways, the network may consider timing coordination among the devices according to the policies.

NOTE – Coordination of the transmission times can be realized via either setting an explicit device transmission time or randomizing the device transmission time within a given interval.

7.2.3 Topology calculation

Based on clauses 6.3.2 and 6.3.3 of this Recommendation, the following core network requirements are derived for this Recommendation:

– the core network is recommended to support an IoT area network topology calculation with consideration of access network selection of devices and gateway by using monitored status information;

– the core network is recommended to support notification actions such as requesting network topology recalculation based on the calculation results to critical devices and gateways those maintain the IoT area network topologies.

In order to avoid congestion caused by unexpectedly heavy traffic for particular network entities, the network is required to manage the topologies of IoT area networks with consideration of access network selection of devices/gateway based on monitored information. The network will then be aware of which network entities unbalanced traffic comes from.

For managing the topology of a given IoT area network, the network calculates an appropriate traffic topology for that particular IoT area network with appropriate access network selection of devices and gateway.

Based on the result of such calculations, the core network requests the devices and/or gateways to re-calculate the network topology.

NOTE – Appendix I.2.1 describes several issues and provides solutions for a use case involving smart meters.

7.2.4 Traffic route calculation

Based on clauses 6.3.2 and 6.3.3 of this Recommendation, the following core network requirements are derived for this Recommendation:

– the core network is recommended to support the calculation of an optimal traffic route within the IoT area network by using monitored status information;

– the core network is recommended to support notification of actions such as requesting traffic route reformulation based on calculation results to critical devices and gateways that maintain the IoT area network topologies.

The traffic route of devices/gateways toward the core network can be calculated by the core network in order to avoid congestion caused by unbalanced traffic. The network calculates a balanced traffic route for the particular IoT area network. The traffic route of devices and gateways can be reformulated based on a request from the network.

Based on the results of such calculations, the core network requests the devices and gateways to recalculate the traffic route.

NOTE – Appendix I.2.2 describes several issues and provides solutions for scenario involving smart meters.

7.2.5 Access granted time

Based on clause 6.3.1 of this Recommendation, the following core network requirements are derived for this Recommendation:

– the core network is recommended to support data communications triggered by devices only during the access granted time interval and the access time duration;

– the core network is recommended to support termination of data communications after expiration of the access time duration of devices.

The core network can avoid congestion by controlling the communication time of the devices and gateways. The conditions are implemented as time values which reflect network side requirements and/or service provider demands, e.g., application specific data requirements with cost effective time choice.

The values of the granted access time interval (e.g., once every 12 hours) and access time duration (e.g., 10 minutes) can be pre-shared between network operators and service providers. These values are defined per device on a per application basis, and configured on both network and device sides.

NOTE 1 – The requirements described in this clause do not affect the communications triggered by service providers, i.e., service providers are allowed to trigger IoT communications with devices at any timing if necessary.

NOTE 2 – Appendix I.1 shows related use cases involving smart meters.

7.2.6 Device recognition

Based on requirements C1 to C10 of [ITU-T Y.4100], the following core network requirements are derived for this Recommendation:

– the core network is recommended to recognize the connected device as a device for the IoT, or not; in case of an IoT device, whether or not it is a smart meter or sensor;

NOTE – Recognition is the process of differentiation of the connected device based on the knowledge of the network. However, the details of how to recognize whether a device is for the IoT and is a smart meter or sensor is out of scope of this Recommendation.

– the core network is recommended to recognize the network functionalities for support of the set of services required for devices for the IoT and, specifically, for smart meters and sensors;

– the core network is recommended to support activation/de-activation by the user of the network functionalities to support the set of services required for smart meters and sensors.

If the network is able to recognize a connected device as a device for the IoT, and then additionally as a smart meter or sensor, the network is then able to recognize the network functionalities which can fulfil the requirements of the network for the IoT (including those described in clause 7).

Not only IoT devices, but other devices as well, e.g., smartphones, may be connected to the core network. In such core network deployments, various network functionalities should be implemented to support services required for the IoT devices, specifically for smart meters and sensors, and services required for other devices. Some functionalities are specifically designed and dedicated for IoT services, but some others are not. The core network should be able to recognize which functionalities are applicable to the services required for the IoT devices, specifically smart meters and sensors, in order that it can deliver IoT services with the appropriate functionalities based on the specific connected devices.

7.2.7 Group management

Based on clause 6.2.3 of this Recommendation and requirement A2 of [ITU-T Y.4100], the following core network requirements are derived for this Recommendation:

– the core network is recommended to support IoT groups;

– the core network is required to support join and leave of devices and gateways to/from an IoT group if group management is supported;

– the core network is required to support the capability of data transmission to an IoT group if group management is supported.

Group management [ITU-T Y.4100] is applied to devices and/or gateways. An IoT group may be constructed based on the service provider's preferences, e.g., on an application domain basis, or on a location basis. A device and/or gateway may belong to more than one IoT group if the policies of the different IoT groups are not conflicting. The core network is required to support the capability of data transmission to an IoT group by appropriate technologies, e.g., multicast.

7.2.8 API

In this clause, the requirements of application programming interface (API) exposure by the core network to the service provider domain are described.

7.2.8.1 Network status information exposure

Based on requirement A1 of [ITU-T Y.4100], the following core network requirement is derived for this Recommendation:

– the core network is recommended to support the exposure of the network status information to the IoT platform through an API.

NOTE – An IoT platform is able to use the network status information provided by the network through APIs for the efficient scheduling of IoT data backhaul transmission from gateways and devices, e.g., by arranging data collection time period and collection sequence.

7.2.9 Access technology interface selection support

Based on clauses 6.3.2 and 6.3.3 of this Recommendation, the following core network requirement is derived for this Recommendation:

– the core network is recommended to support specific access network technology selection requests to devices and/or gateways.

Devices or gateways are connected to the core network through the access network; see Figure 1. Even if the IoT area network and access network have sufficient capabilities and resources to process data from devices, the core network may be congested. For example, a gateway may have two interfaces toward the core network, one via long term evolution (LTE) access technology [b-GPP TS 36.300] and another via Wi-Fi access technology [b-IEEE 802.11]. In case where the LTE access technology is having issues while the Wi-Fi access technology is operating with sufficient resources, it is more efficient for the gateway to select the Wi-Fi access. If the core network has knowledge of the situation through network status information monitoring, the core network can request that devices or gateways select a suitable access network interface.

7.2.10 Multi technology access network connection support

Based on clauses 6.3.2 and 6.3.3 of this Recommendation, the following core network requirement is derived for this Recommendation:

– the core network is required to support the connectivity with different kinds of access network technologies.

There are use cases where a gateway connecting to the core network has multiple interfaces with different access technologies. For example, one interface can be a cellular based interface and another cab be a fixed line based interface. Another use case is one of a gateway with two independent access network interfaces connected to the core network, one being a cellular based access network, and another being a fixed line access network.

7.3 IoT area network requirements

In this clause, the requirements for the IoT area network are described.

7.3.1 Reliability

Based on clauses 6.3.2 of this Recommendation and requirement N3 of [ITU-T Y.4100], the following IoT area network requirements are derived for this Recommendation:

– the IoT area network is recommended to offer reliable data transmission;

– a necessary measure to ensure high reliability of data transmission in the IoT area network is required in order to achieve end-to-end reliability.

In a large number of IoT system implementations, the IoT area network utilizes short-range radio technologies. Such short-range radio technologies have higher packet and connection loss rates as compared with technologies used in the core network or the access network; therefore, they are not reliable in terms of data communications. In order to achieve high availability of data communications, high reliability should be ensured in the IoT area network.

For core network and access network, there are several well-known measures for reliability and availability, for example mean time between failures (MTBF) and mean time to repair (MTTR). However, the IoT area network requires dedicated measures because of the infrequent data communications, as described in clause 6.2.2.

7.3.2 Reaction to requests and notifications from the core network

Based on clauses 7.2.1, 7.2.2, 7.2.3 and 7.2.4, the following IoT area network requirement is derived:

– the IoT area network is recommended to react to requests and notifications from the core network, specifically concerning status information, topology recalculation, topology information and traffic route information.

The core network may send status information requests, topology recalculation requests and traffic recalculation requests to the IoT area network, or may notify topology or traffic route information. The IoT area network should react to these requests or notifications based on the IoT area network policies.

Appendix I

Examples of use cases of smart meters and sensors

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

I.1 Smart meters and sensors

This clause describes typical use cases and potential issues with the smart meters and sensors deployed as devices for the IoT. The use cases described in this clause may not be applicable to other devices.

I.1.1 Communications between smart meters and network

Figure I.1 shows typical data transmission from deployed smart meters in an IoT area network to the core network. There are two use cases; the first is the direct connection between smart meter and network, and the second is smart meter connection via a gateway. Data are transmitted towards the core network within periodic time interval, e.g., one transmission per hour.

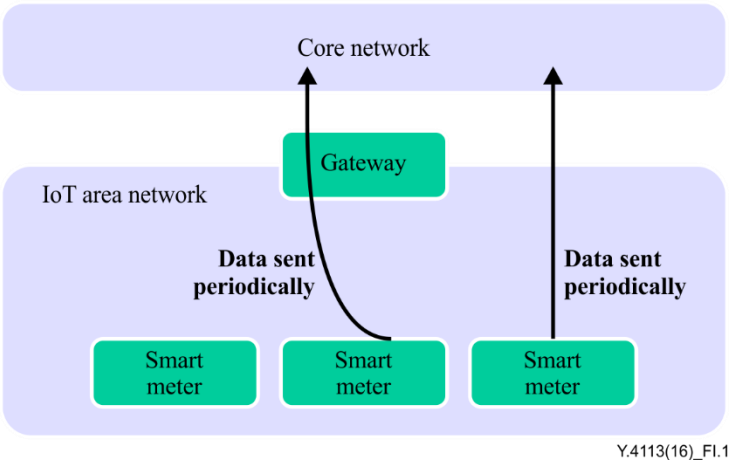

Figure I.1 – Typical data transmission from deployed smart meters in IoT area network to the core network

Figure I.2 shows an example of data transmission within a dedicated time slot. Because of the increasing number of deployed smart meters, data transmission from a large number of smart meters may occur at the same time. This may cause congestion situations in the core network. In order to avoid such congestion, a dedicated time slot for each smart meter can be assigned in order to randomize each data transmission. In Figure I.2, a dedicated time slot (e.g., every 00:15-00:25) is assigned to smart meter A) for data transmission. A different dedicated time slot (e.g., every 00:35-00:45) is assigned to smart meter B) for data transmission. Transmissions are allowed only during the assigned dedicated time slot.

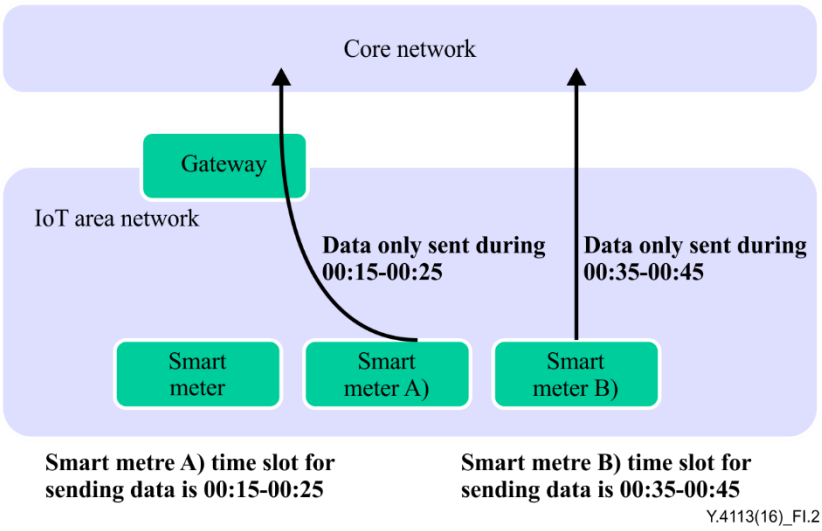

Figure I.2 – Data transmission within assigned dedicated time slot

Figure I.3 shows two cases of data communication initiated by the core network; one is the status information request and the other is the data retransmission request. When the core network realizes that part of the data communication is not completed for some reason, the core network may send a status information request to the smart meters in order to check their device health, or it may send a data retransmission request for data recovery. Even if it is outside the assigned dedicated time slot indicated in Figure I.2, the smart meters can communicate as a reaction upon receiving the request from the core network.

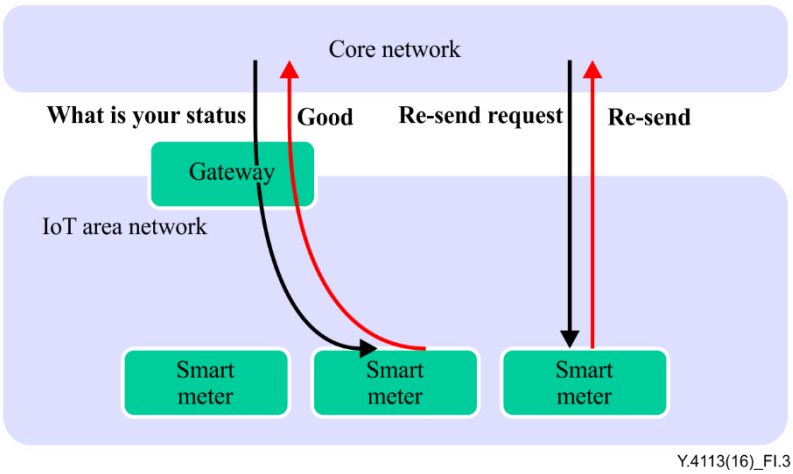

Figure I.3 – Data communication initiated by the core network (status request and re-send request)

Figure I.4 shows the case of data communication initiated by smart meters. Typical data concerns device health information, which is sent periodically. In terms of the device health check, a status report including device status of communication availability may be sent from smart meters toward the core network periodically.

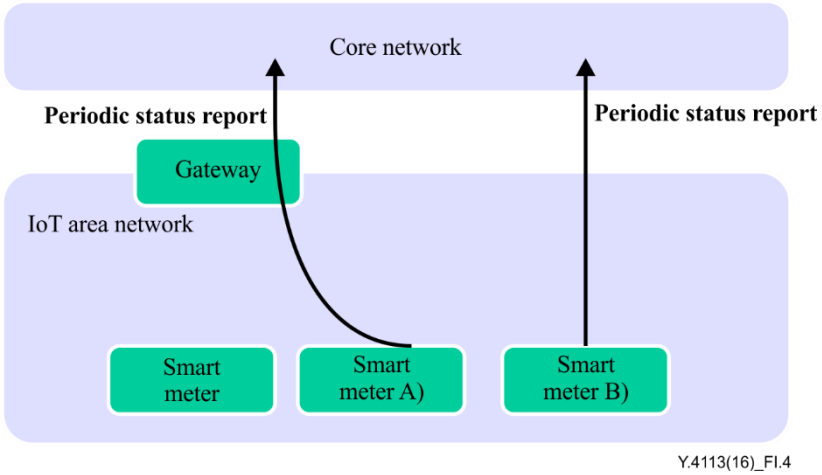

Figure I.4 – Data communication initiated by smart meters

I.1.2 Potential issues

This clause describes potential issues by deploying smart meters.

I.1.2.1 Data to/from devices for the IoT and data to/from other devices

Congestion in the network may potentially be caused by processing massive amounts of data from large numbers of devices for the IoT. Even if all of these data from IoT devices inside the network are prioritized as low, the issue may be unavoidable.

For example, the processing of data from smart meters (data from IoT devices) in gateways and the network may not be guaranteed even if the priority of these data is set as low due to the huge amount of data from other devices that as not IoT devices. Neither may it be guaranteed even if the network can still have enough capacity of data processing when numerous data re-transmissions are triggered or a gateway fails causing unbalanced traffic, i.e., traffic originally assigned to the failed gateway which is re-routed to other gateways when the failure happens. Even if the data from smart meters are de-prioritized (see Figure I.5), the impact of the huge quantity of data from devices which are not part of the IoT may still cause the mentioned issue.

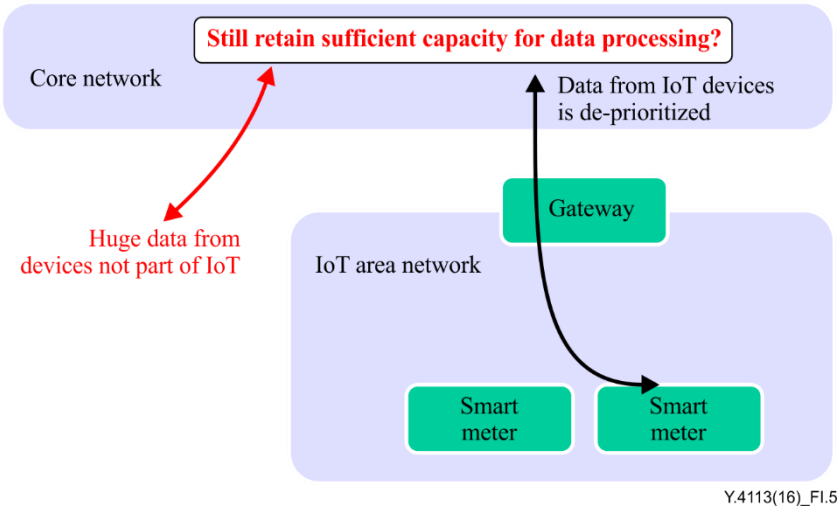

Figure I.5 – Data from smart meters and data from devices not for the IoT

I.1.2.2 Unbalanced traffic within IoT area network

If the left side gateway in Figure I.6 fails, the data originally assigned to this failed gateway may be re-routed to the right side gateway in the Figure I.6. This can cause an overflow in the right side gateway, or at the connecting point of the network with the right side gateway.

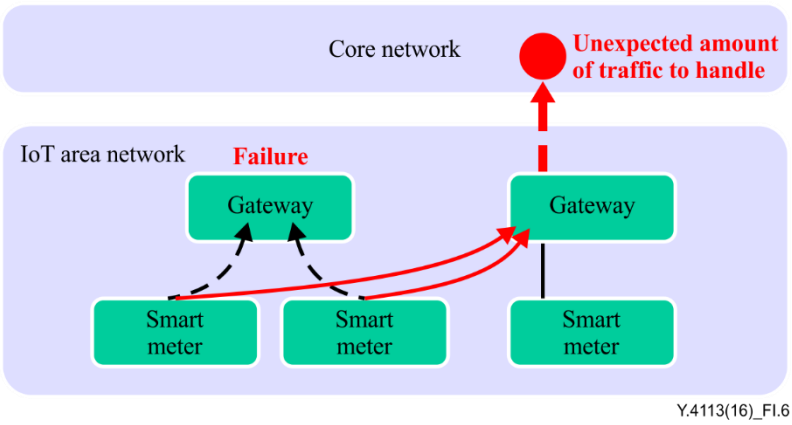

Figure I.6 – Re-route provoking unbalanced traffic

I.2 IoT area network

This clause describes typical use cases and potential issues with IoT area network.

I.2.1 Topology modification

When an IoT area network is established based on autonomous or distributed policy or any other policies, it may not be sufficiently balanced from a load point of view. Figure I.7 shows a case with five smart meters connected to the left side gateway and one smart meter connected to the right side gateway. In this case, the traffic from the IoT area network to the core network is unbalanced from the network point of view.

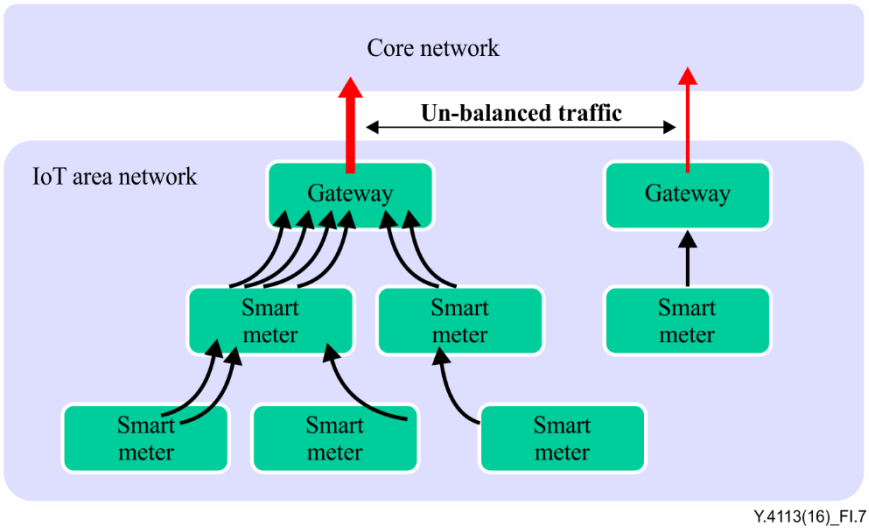

Figure I.7 – Unbalanced IoT area network from a load point of view

From the core network point of view, even though the IoT area network load is managed by the IoT area network itself, the network load may be unbalanced, i.e., based on the required resources for the point of interconnect to the core network. Figure I.8 shows the case with traffic from smart meters connected to the left side gateway which is balanced from the IoT area network point of view, but still unbalanced from the network point of view.

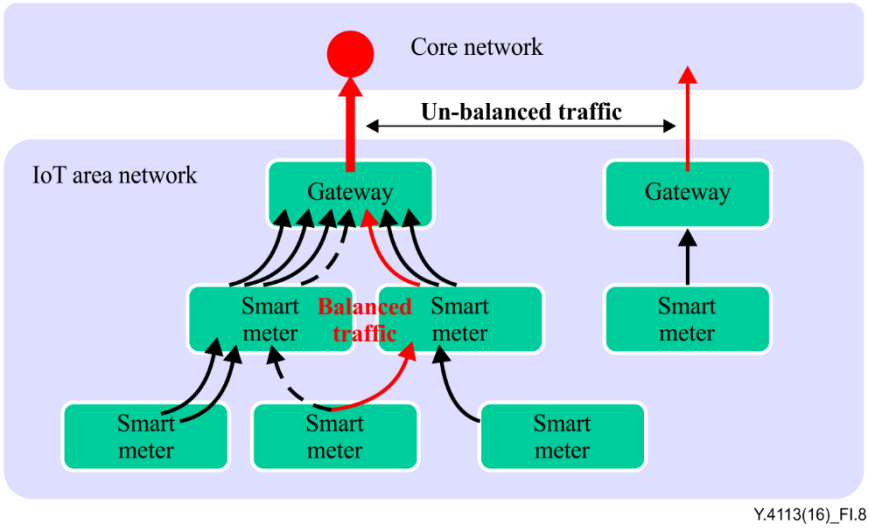

Figure I.8 – Load optimization from the IoT area network point of view

In order to mitigate the unbalanced traffic within the IoT area network and the point of interconnect between the IoT area network and the core network, by using the information obtained with status monitoring, the core network is capable of calculating the topology of the current IoT area network and also calculating the effective optimal topology. In addition, the core network is capable of providing appropriate actions, based on calculation results, to the devices and gateways which are critical to maintain the IoT area network topology in order to allow reformulation of the IoT area network topologies by themselves. Figure I.9 shows the case where, based on the request from the core network, the IoT area network reformulates the topology inside the IoT area network.

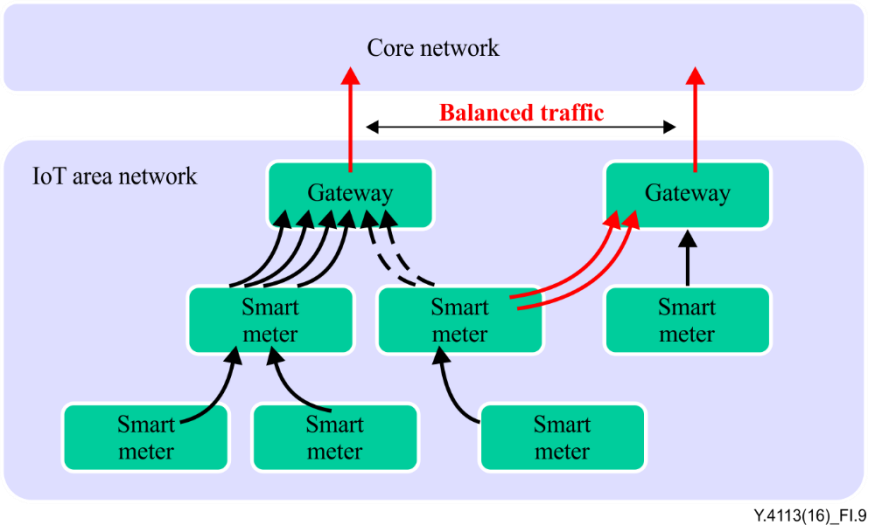

Figure I.9 – Balancing the topology from the core network point of view

I.2.2 Traffic route diversion

In the IoT area network, some factors may cause the unavailability of data transfer from devices and gateways. For example, a node may fail due to overload or hardware malfunctions. Devices may also have limited battery capacity, therefore affecting hardware capabilities. For example, a low battery may impact the radio power of the device. Figure I.10 shows the case with one smart meter having a low battery and getting loss of radio power to maintain connectivity with the gateway.

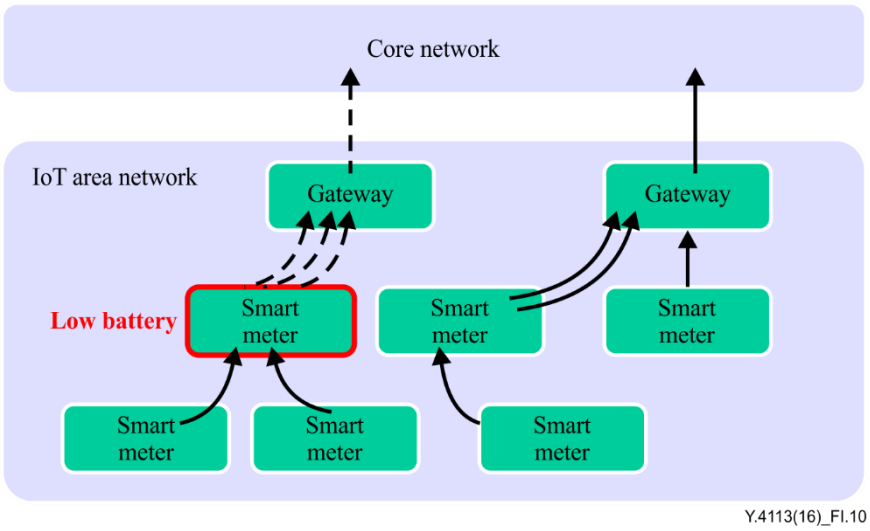

Figure I.10 – Low battery may impact radio power of devices

In order to maintain correct traffic routing from the entire IoT system point of view, it may be efficient to request appropriate actions to devices and gateways, including appropriate neighbours, in order to regenerate the traffic routes based on consideration of the current status of the IoT area network. The status information monitored by the network can be used for this purpose. Figure I.11 shows the case where, based on the request from the core network to the IoT area network to regenerate the traffic routes inside the IoT area network, traffic diversion takes place.

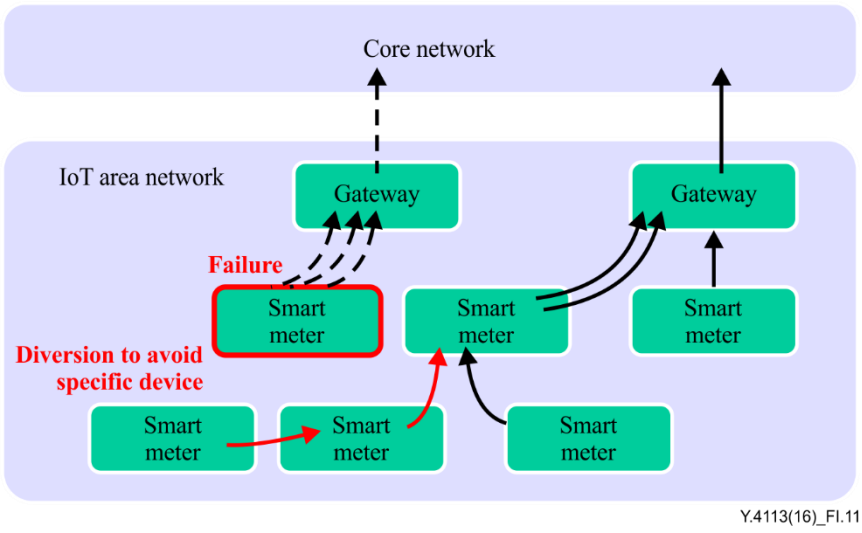

Figure I.11 – Traffic diversion

Appendix II

Access network and IoT area network technologies

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

II.1 Access-specific aspects relating to core network requirements

As shown in Figure 1, the network consists of three main parts, IoT area network, access network and core network.

For the access network, a variety of technologies may be used. Clause II.1.1 lists some technologies which may be used for the access network.

For the IoT area network, a variety of technologies may be used. Clause II.1.2 lists some technologies which may be used for the IoT area network.

The technologies listed in both clauses II.1.1 and II.1.2 are not meant to be exhaustive.

II.1.1 Technologies used for the access network

Table II.1 lists some technologies which may be used for the access network.

Table II.1 – Some technologies used for access networks

Technology	Description
Public switched telephone network (PSTN) technology	CCITT Signalling System No. 7 (SS7) technology.
2G/3G/LTE wireless technology	Second-generation wireless telephone technology (2G), third-generation wireless telephone technology (3G), LTE technologies.
xDSL technology	Digital subscriber line (DSL) technologies, e.g., asymmetric DSL (ADSL), symmetric DSL (SDSL).
FTTx technology	Fiber to the x (FTTx) technology (broadband network technologies using optical fiber).
LPWA wireless technology	Low power wide area (LPWA) network technology.

II.1.2 Technologies used for IoT area network

Table II.2 lists some technologies which may be used for the IoT area network.

Table II.2 – Some technologies used for IoT area networks

Technology	Description
Controller area network (CAN) bus technology	A serial communication technology that supports distributed real-time control and multiplexing.
ZigBee wireless technology	Wireless technology for short-range communication based on [b-IEEE 802.15.4].
Bluetooth wireless technology	Wireless technology for short-range communication [b-IEEE 802.15.1].
Wi-Fi wireless technology	Wireless local area network (LAN) technology (specifications known as IEEE 802.11 series specifications, e.g., 802.11, 802.11a, 802.11b, 802.11g, 802.11n and 802.1ac).
Wireless smart utility network (Wi-SUN) wireless technology	Low-rate wireless personal area networks (LR-WPANs) (PHY is defined in [IEEE 802.15.4g], MAC is defined in [IEEE 802.15.4e]).
Ultra low energy (ULE) technology	ULE technology ([b-ETSI TS 102 939-1]).

Bibliography

[b-ITU-T Q.1742.11] Recommendation ITU-T Q.1742.11 (2014), *IMT 2000 references (approved as of 31st December 2012) to ANSI-41-evolved core network with cdma2000 access network.*

[b-ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.

[b-ITU-T Y.2221] Recommendation ITU-T Y.2221 (2010), *Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment*.

[b-ETSI TS 102 939-1] ETSI TS 102 939-1 (2015), *Digital Enhanced Cordless Telecommunications (DECT); Ultra Low Energy (ULE); Machine to Machine Communications; Part 1: Home Automation Network (phase 1).*

[b-3GPP TS 36.300] 3GPP specification TS 36.300, *Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2*.

[b-IEEE 802.11] IEEE 802.11-2012, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.

[b-IEEE 802.15.1] IEEE 802.15.1-2005, *Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPANs).*

[b-IEEE 802.15.4] IEEE 802.15.4-2003, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs).*

[b-IEEE 802.15.4e] IEEE 802.15.4e-2012, *IEEE Standard for Local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer*.

[b-IEEE 802.15.4g] IEEE 802.15.4g-2012, *IEEE Standard for Local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 3: Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
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 and next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016