International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2060

(06/2012)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Frameworks and functional architecture models

Overview of the Internet of things

Recommendation ITU-T Y.2060

ITU-T

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

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
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Smart ubiquitous 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.3099

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

Recommendation ITU-T Y.2060

Overview of the Internet of things

Summary

Recommendation ITU-T Y.2060 provides an overview of the Internet of things (IoT). It clarifies the concept and scope of the IoT, identifies the fundamental characteristics and high-level requirements of the IoT and describes the IoT reference model. The ecosystem and business models are also provided in an informative appendix.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2060	2012-06-15	13

Keywords

Device, Internet of things, physical thing, reference model, thing, virtual thing.

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 2013

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	1
4	Abbreviations and acronyms	2
5	Conventions	2
6	Introduction of the IoT	2
6.1	Concept of the IoT	2
6.2	Technical overview of the IoT	3
7	Fundamental characteristics and high-level requirements of the IoT	5
7.1	Fundamental characteristics	5
7.2	High-level requirements	5
8	IoT reference model	6
8.1	Application layer	7
8.2	Service support and application support layer	7
8.3	Network layer	7
8.4	Device layer	8
8.5	Management capabilities	8
8.6	Security capabilities	9
Appendix I – IoT ecosystem and business models		10
I.1	Business roles	10
I.2	Business models	11
Bibliography		14

Recommendation ITU-T Y.2060

Overview of the Internet of things

1 Scope

This Recommendation provides an overview of the Internet of things (IoT) with the main objective of highlighting this important area for future standardization.

More specifically, this Recommendation covers the following:

– IoT-related terms and definitions
– concept and scope of the IoT
– characteristics of the IoT
– high-level requirements of the IoT
– IoT reference models.

IoT ecosystem and business models-related information is provided in Appendix I.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 next generation network (NGN) [b-ITU-T Y.2001]: A packet-based network which is able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 device: 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.

3.2.2 Internet of things (IoT): 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.

3.2.3 thing: 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.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

2G	Second Generation
3G	Third Generation
AAA	Authentication, Authorization and Accounting
CAN	Controller Area Network
DSL	Digital Subscriber Line
FCAPS	Fault, Configuration, Accounting, Performance, Security
ICT	Information and Communication Technology
IoT	Internet of Things
ITS	Intelligent Transport Systems
LTE	Long Term Evolution
NGN	Next Generation Network
PSTN	Public Switched Telephone Network
TCP/IP	Transmission Control Protocol/Internet Protocol

5 Conventions

None.

6 Introduction of the IoT

6.1 Concept of the IoT

The Internet of things (IoT) can be perceived as a far-reaching vision with technological and societal implications.

From the perspective of technical standardization, the IoT can be viewed as 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 (ICT).

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 – The IoT is expected to greatly integrate leading technologies, such as technologies related to advanced machine-to-machine communication, autonomic networking, data mining and decision-making, security and privacy protection and cloud computing, with technologies for advanced sensing and actuation.

As shown in Figure 1, the IoT adds the dimension "Any THING communication" to the information and communication technologies (ICTs) which already provide "any TIME" and "any PLACE" communication.

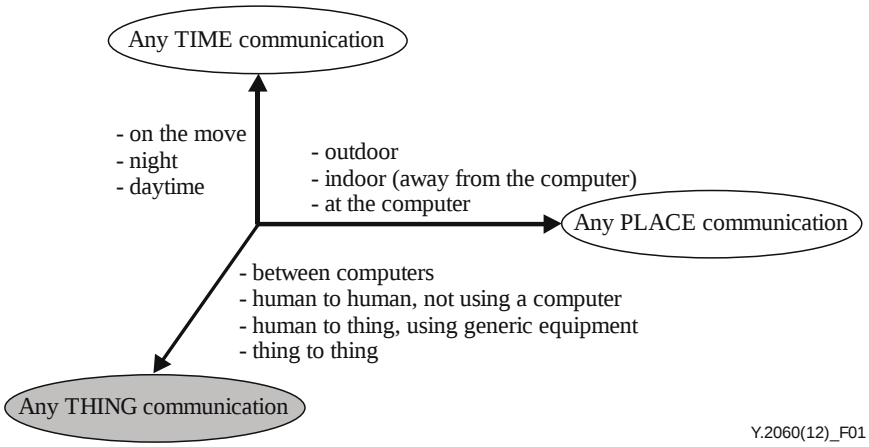

Figure 1 – The new dimension introduced in the Internet of things [b-ITU Report]

Regarding the IoT, things are objects of the physical world (physical things) or of the information world (virtual world) which are capable of being identified and integrated into communication networks. Things have associated information, which can be static and dynamic.

Physical things exist in the physical world and are capable of being sensed, actuated and connected. Examples of physical things include the surrounding environment, industrial robots, goods and electrical equipment.

Virtual things exist in the information world and are capable of being stored, processed and accessed. Examples of virtual things include multimedia content and application software.

6.2 Technical overview of the IoT

Figure 2 shows the technical overview of the IoT.

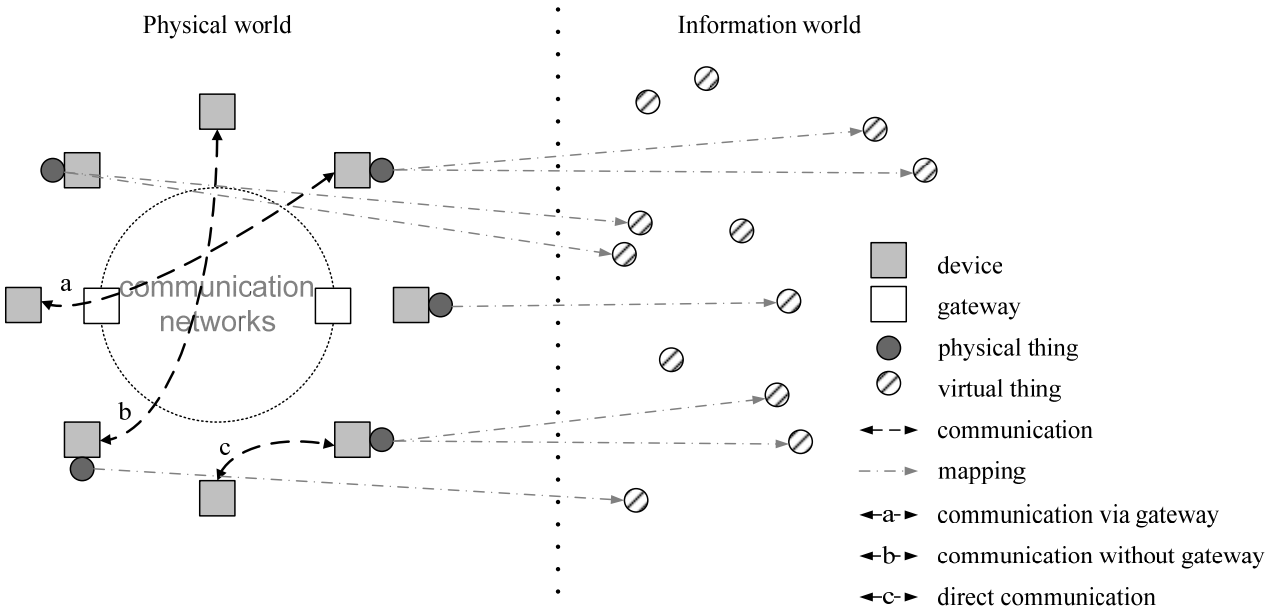

Figure 2 – Technical overview of the IoT

A physical thing may be represented in the information world via one or more virtual things (mapping), but a virtual thing can also exist without any associated physical thing.

A device is a piece of equipment with the mandatory capabilities of communication and optional capabilities of sensing, actuation, data capture, data storage and data processing. The devices collect various kinds of information and provide it to the information and communication networks for further processing. Some devices also execute operations based on information received from the information and communication networks.

Devices communicate with other devices: they communicate through the communication network via a gateway (case a), through the communication network without a gateway (case b) or directly, that is without using the communication network (case c). Also, combinations of cases a and c, and cases b and c are possible; for example, 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) (case c) and then communication through the communication network via a local network gateway (case a).

NOTE 1 – Although Figure 2 shows only interactions taking place in the physical world (communications between devices), interactions also take place in the information world (exchanges between virtual things) and between the physical world and the information world (exchanges between physical things and virtual things).

The IoT applications include various kinds of applications, e.g., "intelligent transportation systems", "smart grid", "e-health" or "smart home". The applications can be based on proprietary application platforms, but can also be built upon common service/application support platform(s) providing generic enabling capabilities, such as authentication, device management, charging and accounting.

The communication networks transfer data captured by devices to applications and other devices, as well as instructions from applications to devices. The communication networks provide capabilities for reliable and efficient data transfer. The IoT network infrastructure may be realized via existing networks, such as conventional TCP/IP-based networks, and/or evolving networks, such as next generation networks (NGN) [b-ITU-T Y.2001].

Figure 3 shows the different types of devices and the relationship between devices and physical things.

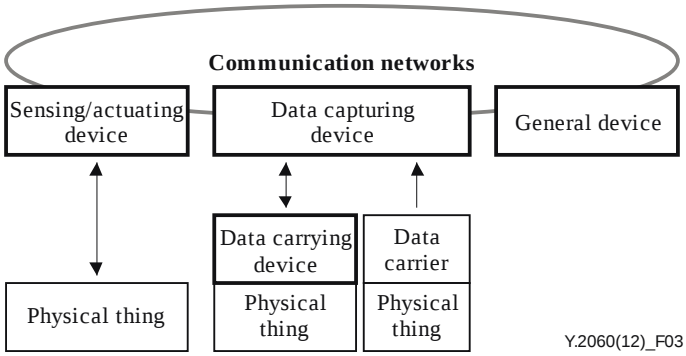

Figure 3 – Types of devices and their relationship with physical things

NOTE 2 – A "general device" is also a (set of) physical thing(s).

The minimum requirement of the devices in the IoT is their support of communication capabilities. Devices are categorized into data-carrying devices, data-capturing devices, sensing and actuating devices and general devices as described as follows:

– Data-carrying device: A data-carrying device is attached to a physical thing to indirectly connect the physical thing with the communication networks.

– Data-capturing device: A data-capturing device refers to a reader/writer device with the capability to interact with physical things. The interaction can happen indirectly via data-carrying devices, or directly via data carriers attached to the physical things. In the first case, the data-capturing device reads information on a data-carrying device and can

optionally also write information given by the communication networks on the data-carrying device.

NOTE 3 – Technologies used for interaction between data-capturing devices and data-carrying devices or data carriers include radio frequency, infrared, optical and galvanic driving.

– Sensing and actuating device: A sensing and actuating device may detect or measure information related to the surrounding environment and convert it into digital electronic signals. It may also convert digital electronic signals from the information networks into operations. Generally, sensing and actuating devices form local networks communicate with each other using wired or wireless communication technologies and use gateways to connect to the communication networks.

– General device: A general device has embedded processing and communication capabilities and may communicate with the communication networks via wired or wireless technologies. General devices include equipment and appliances for different IoT application domains, such as industrial machines, home electrical appliances and smart phones.

7 Fundamental characteristics and high-level requirements of the IoT

7.1 Fundamental characteristics

The fundamental characteristics of the IoT are as follows:

– Interconnectivity: With regard to the IoT, anything can be interconnected with the global information and communication infrastructure.

– Things-related services: The IoT is capable of providing thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual things. In order to provide thing-related services within the constraints of things, both the technologies in physical world and information world will change.

– Heterogeneity: The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks.

– Dynamic changes: The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically.

– Enormous scale: The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet. The ratio of communication triggered by devices as compared to communication triggered by humans will noticeably shift towards device-triggered communication. Even more critical will be the management of the data generated and their interpretation for application purposes. This relates to semantics of data, as well as efficient data handling.

7.2 High-level requirements

The following provide high-level requirements which are relevant for the IoT:

– Identification-based connectivity: The IoT needs to support that the connectivity between a thing and the IoT is established based on the thing's identifier. Also, this includes that possibly heterogeneous identifiers of the different things are processed in a unified way.

– Interoperability: Interoperability needs to be ensured among heterogeneous and distributed systems for provision and consumption of a variety of information and services.

– Autonomic networking: Autonomic networking (including self-management, self-configuring, self-healing, self-optimizing and self-protecting techniques and/or mechanisms) needs to be supported in the networking control functions of the IoT, in order to adapt to different application domains, different communication environments and large numbers and types of devices.
– Autonomic services provisioning: The services need to be able to be provided by capturing, communicating and processing automatically the data of things based on the rules configured by operators or customized by subscribers. Autonomic services may depend on the techniques of automatic data fusion and data mining.
– Location-based capabilities: Location-based capabilities need to be supported in the IoT. Something-related communications and services will depend on the location information of things and/or users. It is needed to sense and track the location information automatically. Location-based communications and services may be constrained by laws and regulations, and should comply with security requirements.
– Security: In the IoT, every 'thing' is connected which results in significant security threats, such as threats towards confidentiality, authenticity and integrity of both data and services. A critical example of security requirements is the need to integrate different security policies and techniques related to the variety of devices and user networks in the IoT.
– Privacy protection: Privacy protection needs to be supported in the IoT. Many things have their owners and users. Sensed data of things may contain private information concerning their owners or users. The IoT needs to support privacy protection during data transmission, aggregation, storage, mining and processing. Privacy protection should not set a barrier to data source authentication.
– High quality and highly secure human body related services: High quality and highly secure human body related services needs to be supported in the IoT. Different countries have different laws and regulations on these services.

  NOTE – Human body related services refer to the services provided by capturing, communicating and processing the data related to human static features and dynamic behaviour with or without human intervention.
– Plug and play: Plug and play capability needs to be supported in the IoT in order to enable on-the-fly generation, composition or the acquiring of semantic-based configurations for seamless integration and cooperation of interconnected things with applications, and responsiveness to application requirements.
– Manageability: Manageability needs to be supported in the IoT in order to ensure normal network operations. IoT applications usually work automatically without the participation of people, but their whole operation process should be manageable by the relevant parties.

8 IoT reference model

Figure 4 shows the IoT reference model. It is composed of four layers as well as management capabilities and security capabilities which are associated with the four layers.

The four layers are as follows:

– application layer
– service support and application support layer
– network layer
– device layer.

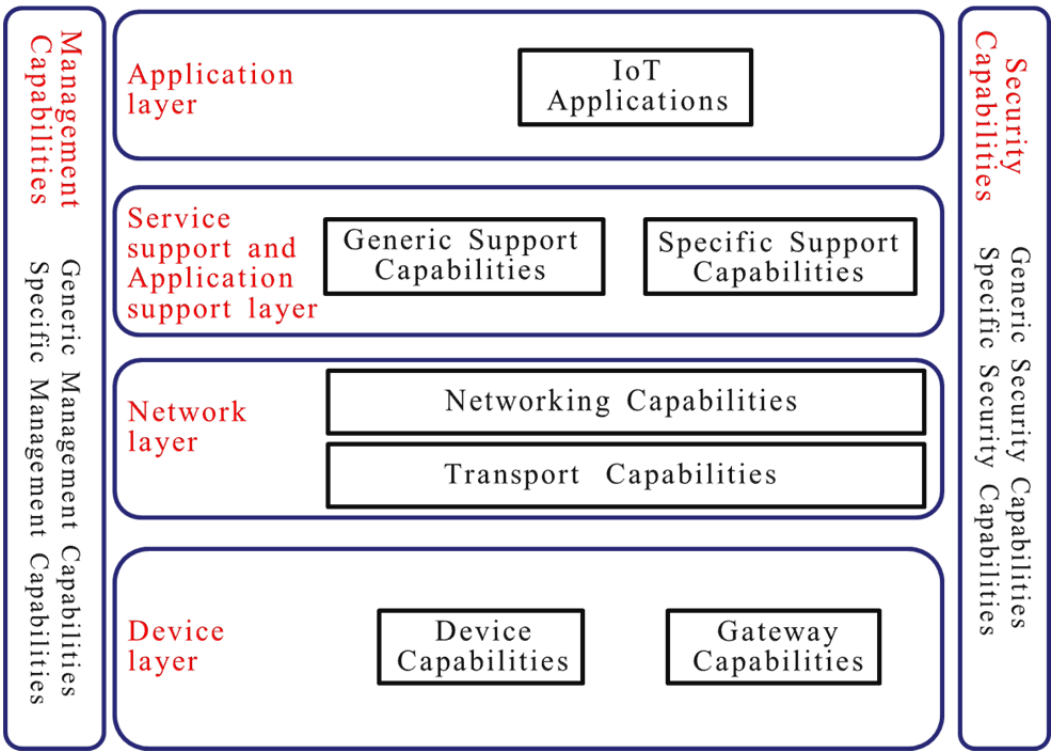

Figure 4 – IoT reference model

8.1 Application layer

The application layer contains IoT applications.

8.2 Service support and application support layer

The service support and application support layer consists of the following two capability groupings:

– Generic support capabilities: The generic support capabilities are common capabilities which can be used by different IoT applications, such as data processing or data storage. These capabilities may be also invoked by specific support capabilities, e.g., to build other specific support capabilities.

– Specific support capabilities: The specific support capabilities are particular capabilities which cater for the requirements of diversified applications. In fact, they may consist of various detailed capability groupings, in order to provide different support functions to different IoT applications.

8.3 Network layer

This consists of the following two types of capabilities:

– Networking capabilities: provide relevant control functions of network connectivity, such as access and transport resource control functions, mobility management or authentication, authorization and accounting (AAA).

– Transport capabilities: focus on providing connectivity for the transport of IoT service and application specific data information, as well as the transport of IoT-related control and management information.

8.4 Device layer

Device layer capabilities can be logically categorized into two kinds of capabilities:

– **Device capabilities**:

The device capabilities include but are not limited to:

Direct interaction with the communication network: Devices are able to gather and upload information directly (i.e., without using gateway capabilities) to the communication network and can directly receive information (e.g., commands) from the communication network.

Indirect interaction with the communication network: Devices are able to gather and upload information to the communication network indirectly, i.e., through gateway capabilities. On the other side, devices can indirectly receive information (e.g., commands) from the communication network.

Ad-hoc networking: Devices may be able to construct networks in an ad-hoc manner in some scenarios which need increased scalability and quick deployment.

Sleeping and waking-up: Device capabilities may support "sleeping" and "waking-up" mechanisms to save energy.

NOTE – The support in a single device of both capabilities of direct interaction with the communication network and indirect interaction with the communication network is not mandatory.

– **Gateway capabilities**:

The gateway capabilities include but are not limited to:

Multiple interfaces support: At the device layer, the gateway capabilities support devices connected through different kinds of wired or wireless technologies, such as a controller area network (CAN) bus, ZigBee, Bluetooth or Wi-Fi. At the network layer, the gateway capabilities may communicate through various technologies, such as the public switched telephone network (PSTN), second generation or third generation (2G or 3G) networks, long-term evolution networks (LTE), Ethernet or digital subscriber lines (DSL).

Protocol conversion: There are two situations where gateway capabilities are needed. One situation is when communications at the device layer use different device layer protocols, e.g., ZigBee technology protocols and Bluetooth technology protocols, the other one is when communications involving both the device layer and network layer use different protocols e.g., a ZigBee technology protocol at the device layer and a 3G technology protocol at the network layer.

8.5 Management capabilities

In a similar way to traditional communication networks, IoT management capabilities cover the traditional fault, configuration, accounting, performance and security (FCAPS) classes, i.e., fault management, configuration management, accounting management, performance management and security management.

The IoT management capabilities can be categorized into generic management capabilities and specific management capabilities.

Essential generic management capabilities in the IoT include:

– device management, such as remote device activation and de-activation, diagnostics, firmware and/or software updating, device working status management;

– local network topology management;

– traffic and congestion management, such as the detection of network overflow conditions and the implementation of resource reservation for time-critical and/or life-critical data flows.

Specific management capabilities are closely coupled with application-specific requirements, e.g., smart grid power transmission line monitoring requirements.

8.6 Security capabilities

There are two kinds of security capabilities: generic security capabilities and specific security capabilities. Generic security capabilities are independent of applications. They include:

– at the application layer: authorization, authentication, application data confidentiality and integrity protection, privacy protection, security audit and anti-virus;

– at the network layer: authorization, authentication, use data and signalling data confidentiality, and signalling integrity protection;

– at the device layer: authentication, authorization, device integrity validation, access control, data confidentiality and integrity protection.

Specific security capabilities are closely coupled with application-specific requirements, e.g., mobile payment, security requirements.

Appendix I

IoT ecosystem and business models

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

I.1 Business roles

The IoT ecosystem is composed of a variety of business players. Each business player plays at least one business role, but more roles are possible. The identified IoT business roles are shown in Figure I.1.

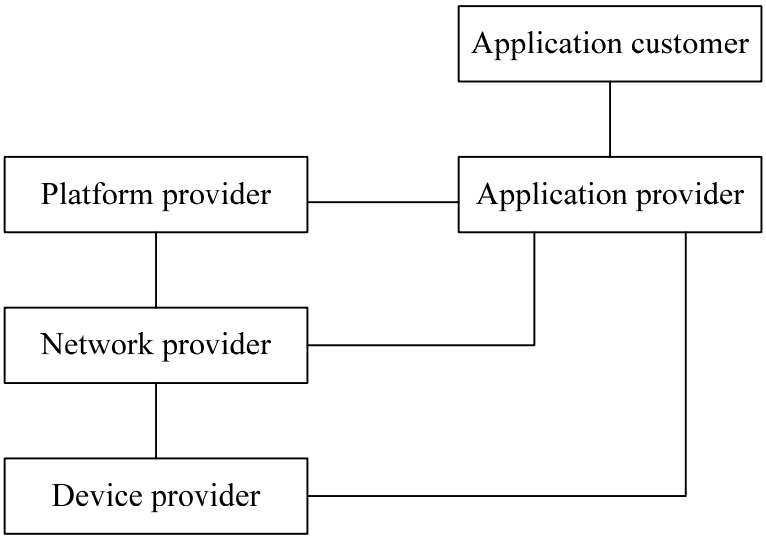

Figure I.1 – IoT ecosystem

NOTE – The identified business roles and their relationships as described in the IoT ecosystem do not represent all possible relevant roles and relationships which can be found across IoT business deployments.

I.1.1 Device provider

The device provider is responsible for devices providing raw data and/or content to the network provider and application provider according to the service logic.

I.1.2 Network provider

The network provider plays a central role in the IoT ecosystem. In particular, the network provider performs the following main functions:

– access and integration of resources provided by other providers;

– support and control of the IoT capabilities infrastructure;

– offering of IoT capabilities, including network capabilities and resource exposure to other providers.

I.1.3 Platform provider

The platform provider provides integration capabilities and open interfaces. Different platforms can provide different capabilities to application providers. Platform capabilities include typical integration capabilities, as well as data storage, data processing or device management. Support for different types of IoT applications is also possible.

I.1.4 Application provider

The application provider utilizes capabilities or resources provided by the network provider, device provider and platform provider, in order to provide IoT applications to application customers.

I.1.5 Application customer

The application customer is the user of IoT application(s) provided by the application provider.

NOTE – An application customer may represent multiple applications users.

I.2 Business models

The IoT ecosystem players may have a variety of relationships in real deployments.

The motivations for this variety of relationships are based on different possible business models. This appendix examines only some IoT business models from the perspective of telecom service and network operators. From this perspective, five business models are described below.

I.2.1 Model 1

In model 1, player A operates the device, network, platform and applications and serves the application customer directly, as shown in Figure I.2.

In general, telecom operators and some vertically integrated businesses (such as smart grid and intelligent transport systems (ITS) businesses) act as player A in model 1.

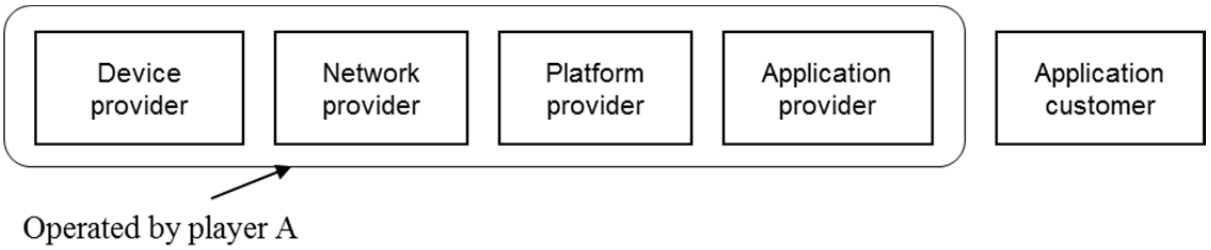

Figure I.2 – Model 1

I.2.2 Model 2

In model 2, player A operates the device, network, and platform, and player B operates the application and serves the application customers, as shown in Figure I.3.

In general, telecom operators act as player A, other service providers as player B in model 2.

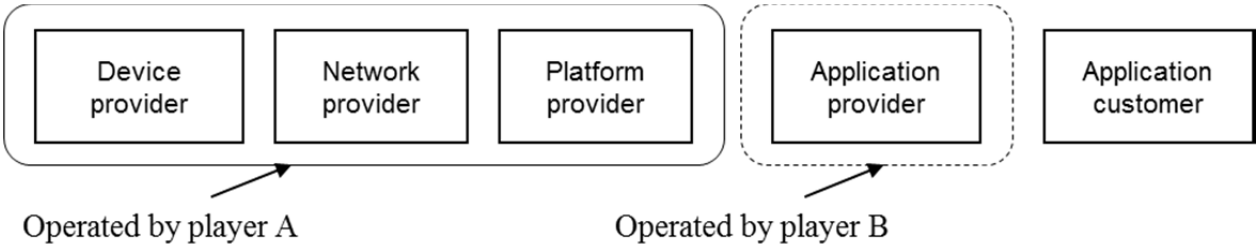

Figure I.3 – Model 2

I.2.3 Model 3

In model 3, player A operates the network and platform, player B operates the device and applications and serves the application customers, as shown in Figure I.4.

In general, telecom operators act as player A and other service providers act as player B.

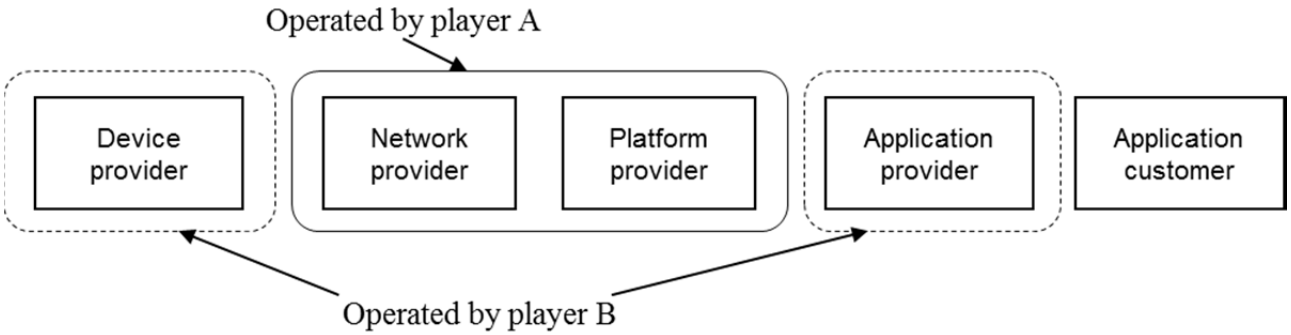

Figure I.4 – Model 3

I.2.4 Model 4

In model 4, player A only operates the network and player B operates the device and platform, providing applications to the application customers, as shown in Figure I.5.

In general, telecom operators act as player A, other service providers and vertically integrated businesses act as player B in model 4.

NOTE – A variation of this model does not include a platform provider and associated platform functionalities (player B only provides applications).

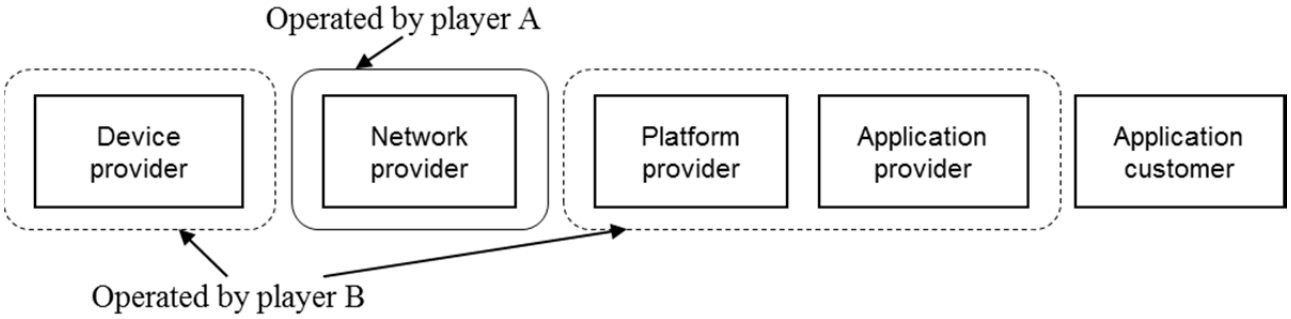

Figure I.5 – Model 4

I.2.5 Model 5

In model 5, player A only operates the network, player B operates the platform, and player C operates devices and provides applications to the application customers, as shown in Figure I.6.

In general, telecom operators act as player A, other service providers act as player B, and vertically integrated businesses act as player C in model 5.

NOTE – A variation of this model does not include a platform provider and associated platform functionalities (player B only provides applications).

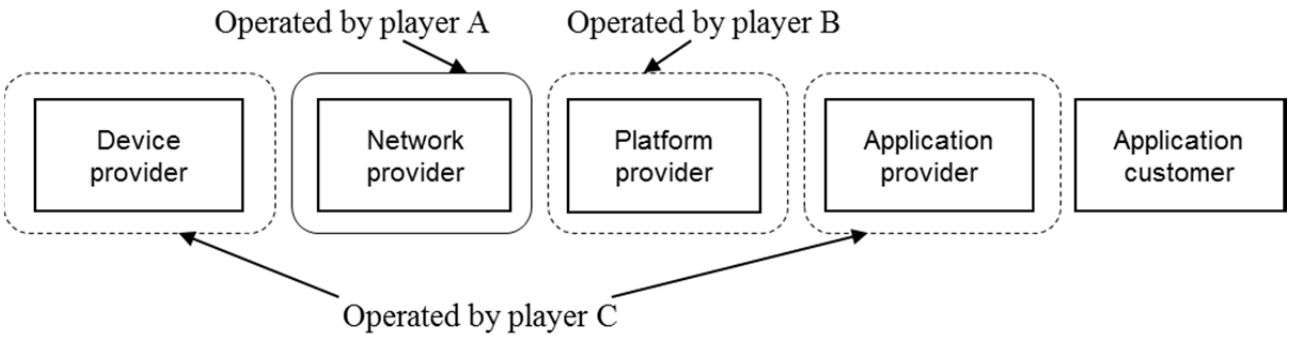

Figure I.6 – Model 5

Bibliography

[b-ITU Report] ITU Internet Reports (2005), *The Internet of Things*.

[b-ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.

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	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**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013