International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4112/Y.2077

(02/2016)

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

Next Generation Networks – Frameworks and functional architecture models

Requirements of the plug and play capability of the Internet of things

Recommendation ITU-T Y.4112/Y.2077

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

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

Recommendation ITU-T Y.4112/Y.2077

Requirements of the plug and play capability of the Internet of things

Summary

Recommendation ITU-T Y.4112/Y.2077 specifies the requirements of the plug and play capability of the Internet of things (IoT), as a basis for further standardization work related to the plug and play aspects in the IoT.

This Recommendation first describes the concept and the purpose of the plug and play capability of the IoT, and it then provides the components of this capability as well as its requirements.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4112/Y.2077	2016-02-13	13	11.1002/1000/12706

Keywords

Internet of things, plug and play, plug and play capability.

* 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.4112/Y.2077

Requirements of the plug and play capability of the Internet of things

1 Scope

This Recommendation specifies the requirements of the plug and play (PnP) capability of the Internet of things (IoT). More specifically, this Recommendation covers the following:

- concept and purpose of the PnP capability of the IoT
- components of the PnP capability of the IoT
- requirements of the PnP capability of the IoT.

Use cases of the PnP capability are provided in Appendix I.

This Recommendation can be seen as complementary to the common requirements of IoT identified in [ITU-T Y.4100].

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 device [ITU-T Y.4000]: With regard to the Internet of things, 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 [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 – In a broad perspective, the IoT can be perceived as a vision with technological and societal implications.

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

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 plug and play (PnP) (capability): With regard to the IoT, a capability which enables automatic generation or acquisition of configurations for a device when it is connected to the communication network, in order for the device to satisfy the requirements of related IoT application(s).

NOTE – For the purpose of this Recommendation, the PnP capability can be considered as composed of the PnP management capability, PnP security capability, device PnP capability and gateway PnP capability.

3.2.2 PnP management capability: For the purpose of this Recommendation, this is the component of the PnP capability providing configuration management, fault management and activation/deactivation of PnP.

3.2.3 PnP security capability: For the purpose of this Recommendation, this is the component of the PnP capability providing PnP authorization and access control of both devices and applications, as well as the confidentiality and integrity protection of data generated by the PnP procedure.

3.2.4 device PnP capability: For the purpose of this Recommendation, this is the component of the PnP capability enabling a device to respond to PnP management capability requests for obtaining a device's properties.

3.2.5 gateway PnP capability: For the purpose of this Recommendation, this is the component of the PnP capability enabling a gateway to respond to PnP management capability requests on behalf of devices.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

IoT Internet of Things

PnP Plug and Play

XML Extensible Markup Language

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 Overview of the plug and play capability

6.1 Introduction

IoT is defined 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 [ITU-T Y.4000]. Among the fundamental characteristics of the IoT, the plug and play (PnP) capability is recommended in order to enable fast generation, composition or the acquisition of configurations for seamless integration and cooperation of interconnected devices with applications, and for a responsiveness to application requirements [ITU-T Y.4000].

NOTE – The PnP capability is not mandatory to support IoT applications. For example, some IoT applications have extra requirements for devices or need a highly secure operating environment; under such circumstances, the PnP capability might be disabled. Additionally, the service provider and/or user may have the permission to activate/deactivate the PnP capability.

The PnP capability of the IoT is responsible for triggering the configuration procedure automatically as soon as a device is connected to the network, without impacting security and privacy.

This Recommendation describes requirements for the PnP capability as a framework to enable functionalities such as:

– PnP capability discovery

– automatic generation of device configuration

– automatic fault recovery of the PnP procedure

– PnP security protection.

6.2 The components of the plug and play capability

For the purpose of this Recommendation, the PnP capability can be considered as composed of the PnP management capability, PnP security capability, device PnP capability and gateway PnP capability.

Figure 1 shows the IoT reference model [ITU-T Y.4000] with the positioning of the different PnP capability components.

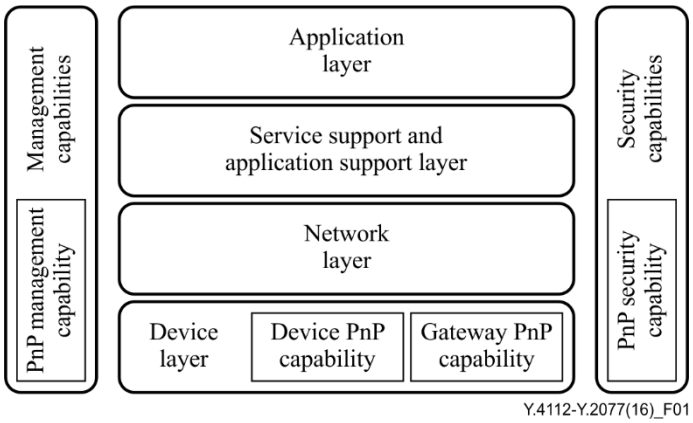

Figure 1 – The IoT reference model with the components of the PnP capability

6.2.1 PnP management capability

The PnP management capability belongs to the management capabilities of the IoT reference model [ITU-T Y.4000] and is the core part of the PnP capability. The PnP management capability covers configuration management, fault management and activation/deactivation of the PnP procedure.

The PnP management capability does not increase the freedom of the device configuration; on the contrary it increases the level of device configuration automation by restricting the configuration procedure. When a device connects to the network and is discovered by the PnP management capability, the PnP management capability tries to obtain the properties of the device, including manufacturer, model, application level protocol, memory space, average response time, etc. The configuration file is generated by the PnP management capability by taking into consideration the device properties and the requirements of related IoT application(s). As the application(s) can interact with the device based on the configuration file, the device can work automatically.

In all scenarios when it is required or recommended to deactivate the PnP procedure, the PnP management capability takes charge of its deactivation.

If any error happens during the configuration procedure or the device cannot fulfil the requirements of the IoT application after the configuration file is generated, the PnP management capability acts according to the specific policies, e.g., it repeats the configuration procedure or produces an error notification to guide an external intervention.

6.2.2 PnP security capability

After a device has connected to the network, mutual authentication and authorization between the device and IoT are required [ITU-T Y.4100]. This is the task of the IoT basic security capability.

After a device has connected to the network, the configuration procedure of the device is executed. Manual configuration is considered as a safe mechanism, which does not need extra security protection. However, if the IoT has PnP capability and the configuration procedure is automatic, some basic security functionalities may be skipped and this may increase vulnerability to network attacks. The PnP security capability is necessary in this situation.

The PnP security capability is part of the security capabilities of the IoT and, with respect to the IoT reference model [ITU-T Y.4000], includes:

– at the device layer, PnP authorization and access control of the device, device data confidentiality and integrity protection;

– at the service support and application support layer, PnP authorization and access control of the application and application data protection.

6.2.3 Device PnP capability

There are many different kinds of devices in the IoT. If a device cannot support the PnP capability, e.g., a basic sensor directly accessing the network, the PnP procedure does not work even if the network supports the PnP capability. In order to start the PnP procedure, the device has to be capable of responding to the PnP management capability's requests.

The device PnP capability refers to the ability of the device to respond to PnP requests with the device's properties.

As described in clause 6.2.4, a gateway with gateway PnP capability can enable the PnP procedure for devices connected through it to the network which do not support device PnP capability.

6.2.4 Gateway PnP capability

Some devices may connect to the network through a gateway. A gateway is required to support the management of device related information, e.g., device identification, device configuration, etc. [ITU-T Y.4101].

If the devices connected to the network through a gateway have no device PnP capability, the gateway can respond to PnP management capability requests with devices' properties on behalf of them.

7 Requirements of the PnP capability

In addition to the IoT common requirements [ITU-T Y.4100], which constitute the basic support for the PnP capability, the following subclauses describe the specific requirements of the PnP capability.

7.1 PnP management capability related requirements

7.1.1 PnP discovery

In addition to the common requirements of IoT for discovery services [ITU-T Y.4100], PnP discovery is necessary for the support of the PnP management capability. This functionality is used to identify whether a device or a gateway has PnP capability. Without identifying this, potential network problems may arise after the device is connected to the network.

The following are the PnP discovery related requirements:

– The IoT is required to support PnP discovery.

7.1.2 PnP configuration management

PnP configuration management is responsible for generating the device configuration. It first sends a request to the device or gateway to obtain the properties of the device, a configuration is then generated by taking into consideration the device properties and IoT application's requirements.

The following are the PnP configuration management related requirements:

– The IoT is required to have the capability of sending PnP configuration requests to devices or gateways.

– The IoT is required to have the capability of processing the device properties replied by devices or gateways.

– The IoT is required to have the capability of disabling unnecessary device capabilities according to the IoT application's requirements.

– The IoT is required to have the capability of generating device configurations built using predefined syntax and semantics.

– The IoT is required to support the manual modification of configurations generated by the PnP procedure.

– The IoT is required to store device configurations, e.g., for possible future usage by the same application and same device.

– The IoT is required to have the capability to store different configurations for the same device, e.g., according to the associated application.

7.1.3 PnP fault management

If any error happens during the configuration procedure or the device cannot fulfil the requirements of the IoT application after the configuration file is generated, the PnP fault management will operate according to the specific policies, e.g., it will repeat the configuration procedure or produce an error notification to guide an external intervention.

The following are the PnP fault management related requirements:

– The IoT is required to recognize, isolate and correct faults that occur during the PnP procedure.

– The IoT is required to have the capability of restarting the PnP procedure.

– The IoT is required to have the capability of interrupting or terminating the PnP procedure.

– The IoT is required to have the capability of setting the duration time of the PnP procedure.

– The IoT is required to log the PnP related activities.

7.1.4 PnP activation/deactivation

As described in clause 6.1, under certain circumstances, the PnP capability might be deactivated.

The following are the PnP activation/deactivation related requirements:

– The IoT is required to support the capability of activating/deactivating the PnP capability.

7.2 PnP security capability related requirements

Mutual authentication between a device and IoT makes sure that it is impossible for a third party to masquerade as a device by spoofing its identity. Mutual authentication between an application and IoT makes sure that it is impossible for a third party to masquerade as an application by spoofing its identity [ITU-T Y.4100]. However, authenticated entities still need to be authorized for any PnP related operation.

The PnP procedure, including the generated configurations, is controlled by access rules and protected by firewall capabilities.

7.2.1 PnP authorization

The following are the PnP authorization related requirements:

– Any PnP related operation on the device is required to be authorized.

– An application is required to be authorized to perform any PnP related operation.

– If the PnP procedure involves user information, or the user needs to manually modify the PnP configuration, the user is required to be authorized.

– If a device without PnP capability connects to the IoT through a gateway, the gateway is required to be authorized to perform any PnP related operation on the device.

7.2.2 PnP access control

The following are the PnP access control related requirements:

– The IoT is required to only run the PnP procedure if the necessary device configuration does not exist, e.g., when the device connects to the network for the first time or a new application wants to access the connected device.

7.2.3 Firewall protection

The following are the firewall protection related requirements:

– The IoT is recommended to support firewall protection between devices and the IoT infrastructure (including gateways).

– Firewall protection is required to have the capability to stop the PnP procedure if the properties provided by the device are suspicious (e.g., the data transmission redundancy of a device is too high).

– Firewall protection is required to have the capability to stop the PnP procedure if the request made by the application is suspicious (e.g., the data upload frequency required by the application is too high).

– Firewall protection is required to have the capability to protect the PnP procedure from any illegal access or attack.

7.2.4 Device and application data security

The following are the device and application data security related requirements:

– The IoT is required to provide integrity protection to all data generated during the PnP procedure.

– The IoT is required to provide confidentiality protection to all data generated during the PnP procedure.
– The IoT is required to store the device configurations generated by the PnP procedure in a safe manner.

7.3 Device PnP capability related requirements

The following requirements are related to devices which support the PnP capability.

The following are the device PnP capability related requirements:

– The device is required to support PnP discovery triggered by the IoT.
– The device is required to be able to communicate to the IoT, on demand, all its relevant properties.
– The device is required to have the capability of refusing PnP configuration requests from the IoT, e.g., the device provides sensitive data but the current network access connectivity is unsecure.

7.4 Gateway PnP capability related requirements

The following requirements are related to gateways which support the PnP capability.

NOTE – In case of deployment scenarios where both gateway and devices which are connected through it to the network support the PnP capability, the gateway is transparent to the PnP procedure.

– The gateway is required to support PnP discovery triggered by the IoT.
– The gateway is required to be able to communicate to the IoT, on demand, all properties of the connected devices.
– The gateway is required to have the capability of refusing PnP configuration requests from the IoT.

Appendix I

Use cases of the PnP capability

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

I.1 Large scale sensor deployment: greenhouse example

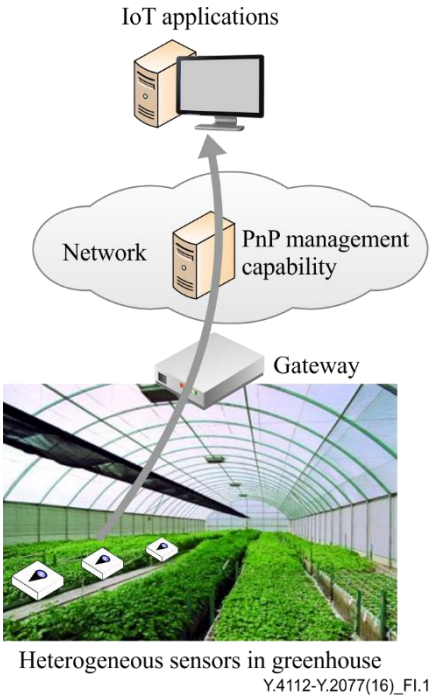

Figure I.1 – Use case of PnP capability in greenhouse sensor deployment

Deploying environmental sensors in a greenhouse is a typical scenario of smart agriculture applications. There are a large number and different types of sensors used in greenhouses, which can collect data such as temperature, humidity, illumination, CO_2 etc. Users who subscribe to this greenhouse monitoring service are normally farmers who lack network and communication knowledge. Following deployment, sensors need to work for a long time without any manual maintenance.

The PnP management capability is important in this situation. Figure I.1 shows a use case of PnP capability in greenhouse sensor deployment. All the sensors only need to be deployed in the appropriate position, without any manual configuration. The PnP management capability will automatically generate or acquire the corresponding configuration for every kind of sensor, according to their properties and related IoT application. All sensors will work automatically in the end.

If a sensor is broken, the user only needs to change it with an identical one (or updated version), and the new sensor will work in the same way as before.

I.2 Security protection from counterfeit device

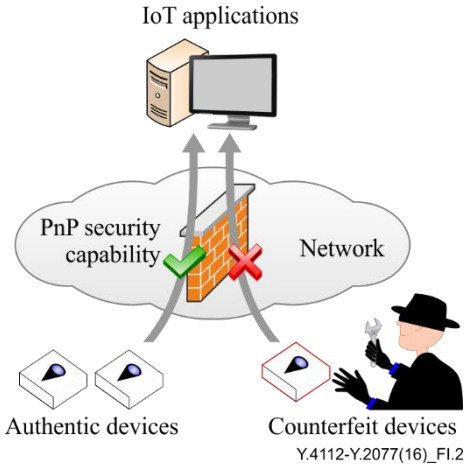

Figure I.2 – Use case of PnP security capability for protection from counterfeit devices

Unlike mobile phones, a large number of IoT devices will be placed in locations with difficult accessibility, without any manual maintenance. In this situation, the PnP management capability will reduce the maintenance issue. However, this situation also provides hackers with an opportunity to hack into the IoT from the device side. If a hacker connects a counterfeit device to the IoT supporting the PnP capability, the device configuration procedure will run automatically to make the device work. As a result, the counterfeit device will provide misleading data to IoT application(s), or block the transmission channel using redundant data.

The PnP security capability is important in this situation. Figure I.2 shows a use case of PnP security protection from counterfeit devices. The counterfeit devices will pass the authentication procedure of IoT by simulating the authentic devices. However, the configuration parameters provided by the counterfeit devices will differ from those of the authentic ones. The PnP security capability will detect the potential risk and terminate the configuration procedure.

I.3 Enablement of customized configuration of IoT device

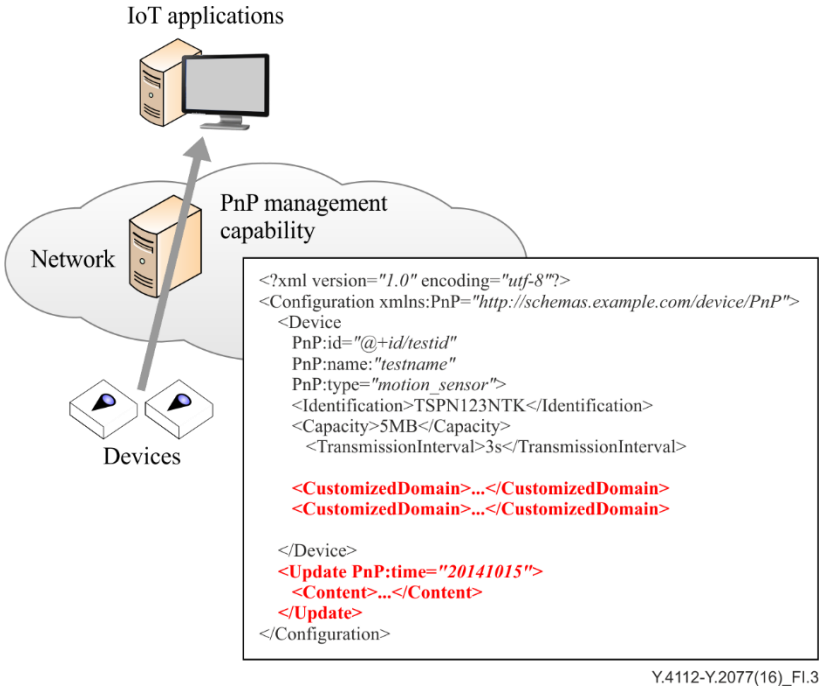

Figure I.3 – Use case of customized configuration of IoT device

There are many different kinds of devices in IoT, and the requirements of IoT applications are diverse. Unless highly customized for a certain kind of IoT application, it is possible that a device does not work immediately after connecting to the network. The most important mission of the PnP management capability is to automatically generate the configuration for the device. However, the automatic generation of the configuration does not mean that a user cannot change the configuration. Figure I.3 shows a use case of customized configuration enablement of an IoT device. The user can interrupt the PnP procedure by updating the configuration file manually, and the device works according to the new configuration. The new configuration is recorded and re-generated automatically for the same device and IoT application.

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, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016