International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4702

(03/2016)

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 – Management, control and performance

Common requirements and capabilities of device management in the Internet of things

Recommendation ITU-T Y.4702

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

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

Recommendation ITU-T Y.4702

Common requirements and capabilities of device management in the Internet of things

Summary

Recommendation ITU-T Y.4702 provides the common requirements and capabilities of device management (DM) in the Internet of things (IoT).

The provided common requirements and capabilities are intended to be generally applicable in device management application scenarios.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4702	2016-03-15	20	11.1002/1000/12780

Keywords

Common requirements, common capabilities, device management, DM, Internet of things (IoT).

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.4072

Common requirements and capabilities of device management in the Internet of things

1 Scope

This Recommendation provides the common requirements and capabilities of device management (DM) in the Internet of things (IoT).

The provided common requirements and capabilities are intended to be generally applicable in device management application scenarios.

The scope of this Recommendation includes:

1) Common requirements of device management in the IoT.

2) Common capabilities of device management in the IoT.

NOTE – This Recommendation focuses on the requirements of DM for the interaction between devices and the various DM functional components. The DM client, a functional component optionally present in some IoT applications, and its specific requirements are outside of the scope of this Recommendation.

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 Internet of things.*

[ITU-T Y.2061] Recommendation ITU-T Y.2061 (2012), *Requirements for the support of machine-oriented communication applications in the next generation network environment.*

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

[ITU-T Y.2067] Recommendation ITU-T Y.4101/Y.2067 (2014), *Common requirements and capabilities of a gateway for Internet of things applications*.

[OMA-RD-LightweightM2M] OMA-RD-LightweightM2M (2013), *Lightweight Machine to Machine Requirements.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

3.1.2 gateway [ITU-T Y.2067]: A unit in the Internet of things which interconnects the devices with the communication networks. It performs the necessary translation between the protocols used in the communication networks and those used by devices.

3.1.3 Internet of things (IoT) [ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

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

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

3.2 Terms defined in this Recommendation

This Recommendation defines or uses the following terms:

3.2.1 Device management (DM) agent: The DM functional component responsible for collecting DM-related information from devices and gateways, reporting device related information to the DM manager or DM GW manager and analysing the commands from the DM manager or DM GW manager in order to execute DM-related tasks.

3.2.2 Device management (DM) client: The DM functional component optionally present in some IoT applications and interacting with the DM manager implemented by specific capabilities of the IoT SSAS capability set [ITU-T Y.4000]. It provides access to DM capabilities in order to enable device management functionalities in IoT applications.

3.2.3 Device management (DM) gateway (GW) manager: The DM functional component responsible for managing devices connected to a given gateway (GW).

3.2.4 Device management (DM) manager: With regard to device management in IoT, the DM functional component, responsible for managing devices and gateways.
NOTE – The device management manager interacts with other DM functional components to get DM-related information of devices and gateways and to send commands for execution of DM-related tasks. According to the IoT application deployment scenarios, it may be implemented by DM capabilities of the IoT service support and application support (SSAS) capability set [ITU-T Y.4000] or by the IoT applications themselves.

4 Abbreviations and acronyms

3G Third Generation

4G Fourth Generation

ADSL Asymmetric Digital Subscriber Line

API Application Programming Interface

CPU Central Processing Unit

DM Device Management

GPRS General Packet Radio Service

GW Gateway

ID Identifier

IoT Internet of Things

IP Internet Protocol

LAN Local Area Network

OS Operating System

OSS Operation Support System

QoS Quality of Service

SMS Short Message Service

SSAS Service Support and Application Support

WiFi Wireless Fidelity

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.

– The term "IoT applications" is used to identify applications which are operated over the IoT infrastructure.

6 Introduction

Device management (DM) is an essential set of management capabilities in the Internet of things (IoT), providing support for, but not being limited to, devices' remote activation and de-activation, diagnostics, firmware/software updating and sensor node working status management [ITU-T Y.4000].

DM provides a set of capabilities through which the users of these capabilities can exercise various management tasks for devices, locally and remotely. Via DM, the devices in IoT can be correctly configured and can correctly and efficiently operate through standardized interfaces and procedures. In addition, the users of these capabilities can know the current status of devices and get notification if there is something wrong with the devices. The ultimate aim of DM is to make sure that the applications running on a given device operate well.

Traditionally, IoT applications interact directly with devices (and gateways) to realize DM functionalities. Nowadays, with the advent of service support and application support (SSAS) capabilities [ITU-T Y.4000] in the IoT infrastructure, the DM functionalities can be provided as a common service to IoT applications. IoT applications may directly use the DM service provided by DM capabilities of the SSAS capability set in order to realize DM functionalities without interacting with devices (and gateways) directly. This is a simpler and more efficient way to realize DM functionalities for IoT applications.

In the IoT, the DM functional components can be deployed in devices, gateways, components which provide SSAS capabilities and IoT applications.

Four DM functional components are identified: DM manager, DM agent, DM gateway (GW) manager and DM client. Figure 1 shows the positioning of these components in the IoT from the layering perspective of the IoT reference model [ITU-T Y.4000].

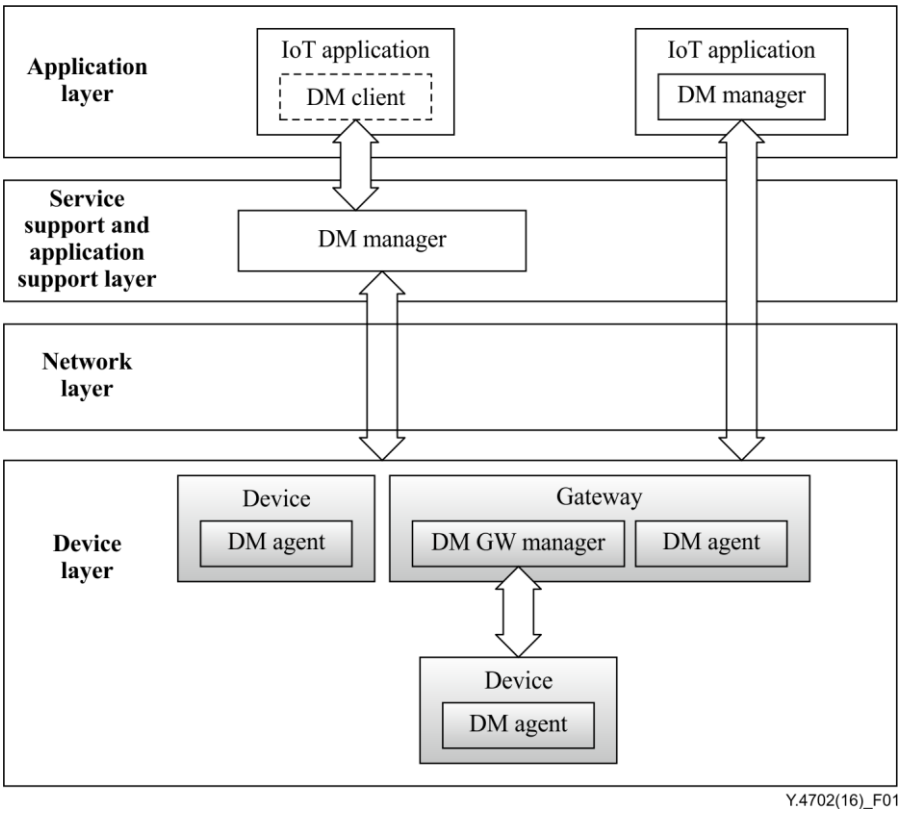

Figure 1 – The DM functional components in the IoT from a layering perspective

The DM manager is a functional component, responsible for managing devices and gateways. The DM manager interacts with DM agents and DM GW managers to get DM-related information of devices and gateways and sends them commands for execution of DM-related tasks. According to the IoT application deployment scenarios, a DM manager may be implemented by DM capabilities of the IoT SSAS capability set [ITU-T Y.4000] or by the IoT applications themselves.

NOTE 1 – When implemented by DM capabilities of the IoT SSAS capability set, the DM Manager provides DM capabilities to IoT applications as a common service, enabling an indirect way of interaction between IoT applications and devices (and gateways).

The DM agent is responsible for collecting DM-related information local to devices and gateways, reporting status and fault information local to devices and gateways and analysing the commands from the DM manager or DM GW manager in order to execute DM-related tasks.

The DM GW manager is responsible for managing devices connected to a given gateway. The DM GW manager acts as a proxy between devices and the DM manager, so that the DM manager and DM agent interact with each other through the DM GW manager.

The DM client is the functional component optionally present in some IoT applications and interacting with the DM manager implemented by specific capabilities of the IoT SSAS capability set. It provides access to DM capabilities in order to enable device management functionalities in IoT applications.

NOTE 2 – This Recommendation focuses on the requirements of DM for the interaction between devices and the various DM functional components. The DM client and its specific requirements are outside of the scope of this Recommendation.

As far as deployment is concerned, the various DM functional components are deployed as follows:

– The DM agents are deployed in devices and gateways.

– The DM GW managers are deployed in gateways.

According to the IoT application deployment scenarios, the DM manager may be deployed in IoT applications or in components which provide SSAS capabilities.

7 Requirements of device management in the IoT

7.1 Characteristics specific to device management in the IoT

Device management in IoT has some specific characteristics (implying corresponding requirements to be met).

The following specific characteristics are identified:

1) In some IoT application scenarios it is necessary to manage a large number of devices [ITU-T Y.2066].

2) It is frequent to have IoT application scenarios where a lot of devices are connected to the same gateway, with their DM agents interacting with the DM GW manager located in that gateway. In some of these cases, these devices are managed by the DM GW manager directly, in other ones they are managed by the DM manager through the DM GW manager.

   NOTE 1 – A gateway manages devices based on gateway policies or instructions received from IoT applications.

3) Different devices may have different capabilites. Resource constrained devices have limited computing capabilities (e.g., small central processing unit (CPU), small memory size, limited battery) or constrained communication capabilities (such as general packet radio service (GPRS)): these devices are not often able to support full DM functionalities. Other devices have rich computing capabilities (e.g., large CPU, large memory size) or rich communication capabilities (e.g., Third Generation (3G), Fourth Generation (4G), wireline) and are able to support full DM functionalities.

4) It is frequent to have IoT application scenarios where a lot of devices are powered by battery. These devices often run in power-saving modes, such as sleeping mode [ITU-T Y.2061].

5) Different devices may use different communication technologies, such as wireless access networks (e.g., GPRS, 3G, 4G, wireless fidelity (WiFi)) and wireline access networks (e.g., asymmetric digital subscriber line (ADSL), local area network (LAN) and power line) [ITU-T Y.2066]. For devices characterized by a small amount of transmitted data,

bandwidth constrained wireless networks are often used, such as GPRS, etc. In these cases, DM protocols should be simple and concise.

6) There are IoT application scenarios where it is not only necessary to communicate with devices to retrieve device related information, but where it is also necessary to communicate with the network to get connectivity status information.

NOTE 2 – Device related information includes information about operating status, configuration, fault and performance of device hardware, peripherals, operating system (OS), communication service, DM services, applications running on the device, etc.

7) There are IoT application scenarios with not only multi-purpose devices, but also dedicated devices. Multi-purpose devices may interact with multiple IoT applications via the SSAS capabilities of the IoT infrastructure. Dedicated devices, from their initial activation, support only a single IoT application, without supporting other applications in the future.

7.2 Common requirements of device management in the IoT

The common requirements of device management in the IoT are as follows:

1) Each device managed by the DM manager is required to be identified or addressable in order to be recognized and managed.

2) The scope of the device identification scheme is recommended to be large enough to support scenarios with a huge number of devices to be managed.

3) The DM manager and DM GW manager are required to manage devices independently of the devices' capabilities, including devices having different DM capabilities.

4) It is required to enable open access to the DM capabilities.

NOTE 1 – The open access to the DM capabilities allows some IoT applications to directly use the DM services provided by the DM capabilities of the SSAS capability set in order to realize DM functionalities and administrators of such IoT applications to also use the DM services through a web portal.

5) In case of open access to the DM capabilities, it is required to provide open application programming interfaces (APIs) for access by IoT applications.

6) It is recommended that the devices be manageable by groups and that different ways to group devices be supported, including by device identifier (ID), location, software version and application type [ITU-T Y.2061].

7) The DM manager and DM GW manager are recommended to be robust enough to support a large number of devices accessing the DM manager simultaneously.

8) It is recommended that different devices have different DM service access levels.

NOTE 2 – Devices with low service access levels may be denied access to DM services by the DM manager or DM GW manager when a large number of devices access the service at the same time.

9) It is recommended that the DM manager and DM GW manager use scheduling mechanisms in order to avoid communication congestion issues.

10) It is required to support mechanisms for device discovery when devices connect to the DM GW manager or DM manager for the first time.

11) It is required to support mechanisms for device capability discovery [OMA-RD-LightweightM2M].

12) It is required to support mechanisms for service discovery when new services are published by applications in devices [ITU-T Y.2067].

13) It is required to support mechanisms for device registration and different registration modes, including active registration by devices, manual registration by administrators, etc.

14) It is recommended to support mechanisms for device software/firmware image management, including image inventory management, update results reporting, integrity check of image before update process, update process monitoring and fallback when update fails [ITU-T Y.2061], [ITU-T Y.2067].

15) It is recommended to support manager initiated mode and/or device initiated mode for device software/firmware image fallback mechanism.

NOTE 3 – For the manager initiated mode, the DM manager sends a request to devices to go back to the former software/firmware image version when it discovers problems concerning the devices. For the device initiated mode, the devices request restoration of the former software/firmware image version when they discover that the software/firmware update has failed.

16) It is recommended to enable activation and de-activation of the reporting of device related information from devices to the DM manager or DM GW manager.

17) It is recommended that some configuration parameters of a device with its DM agent directly interacting with the DM manager can be set locally and remotely by the DM manager.

18) It is recommended that the DM manager and DM GW manager be able to upload and download DM-related files to/from devices.

NOTE 4 – Examples of DM-related files are the device configuration file and the device log file.

19) It is required to support factory reset of devices [OMA-RD-LightweightM2M].

20) It is required that the DM manager and DM GW manager be able to get device related information.

NOTE 5 – Such information can be reported by devices and/or retrieved by the DM manager and DM GW manager from devices [ITU-T Y.4000].

21) It is recommended to support plug and play mechanisms for initialization of devices [ITU-T Y.4000], [b-ITU-T Y.4112].

22) It is recommended to enable the provisioning of not only the current device related information for a specified range of devices, but also historical device related information.

23) It is recommended to enable device reporting of DM-related events, and different reporting mechanisms be supported (e.g., configurable time-based mechanism, configurable threshold-based mechanism).

NOTE 6 – Examples of DM-related events include some key configuration parameters being changed locally, or CPU load exceeding the threshold.

24) If supported by devices, the DM manager and DM GW manager are required to support device reporting's policy setting, including what kind of device related information should be reported and when to report.

25) It is required that devices, any service running on devices and the device peripherals can be activated and de-activated locally and remotely by the DM manager [ITU-T Y.4000], [ITU-T Y.2066], [OMA-RD-LightweightM2M].

26) It is required that the DM manager be able to remotely restart devices, any service running on devices and device peripherals [OMA-RD-LightweightM2M].

27) It is recommended that the DM manager be able to support a mechanism to trigger the device establishment of an application level connection to the DM manager.

28) It is recommended that the device power status be reported at a certain frequency to the DM manager or DM GW manager if a device is powered by battery.

29) It is recommended that the DM manager and DM GW manager be able to request to set the power saving mode for a device if the device supports such a mode.

30) It is recommended that the DM manager be able to obtain location information of devices.

NOTE 7 – Device location information can be obtained from devices or from the network.

31) It is recommended that the DM manager and DM GW manager be able to receive and process results of self-diagnostics reported by devices.

32) It is recommended that the DM manager and DM GW manager provide diagnostic analysis results.

33) DM protocols are recommended to be simple and concise, if bandwidth constrained wireless networks are used and/or devices are resource constrained [ITU-T Y.2061].

34) DM protocols are recommended to support compression mechanisms if bandwidth constrained wireless networks are used [ITU-T Y.2061].

35) If some abnormal condition occurs, it is recommended for the DM manager and DM GW manager to execute a diagnostic device fault location, isolation and restoration procedure.

36) It is recommended that trouble tickets be generated by proactive failure detection of devices and be reported to the DM capabilities' users.

37) It is required to be able to get network connectivity information from network(s) and/or device connectivity from devices.

NOTE 8 – Network connectivity information includes whether the device has connected to the network, identification of the radio cell in case of cellular network connectivity, etc.

38) It is required for the DM manager and DM GW manager to support a mechanism to prohibit the connection of IoT devices to the network for a certain duration [OMA-RD-LightweightM2M].

39) It is required to support a mechanism to retrieve the connection log information from devices [OMA-RD-LightweightM2M].

40) It is recommended for the DM manager and DM GW manager to support mechanisms to control the device access to the network based on time and/or location.

41) In the case of open access to the DM capabilities, it is recommended to implement accounting management based on access time of DM services, use of DM services and number of managed devices.

42) It is recommended for the DM manager and DM GW manager to support accounting mechanisms to collect DM service usage data, to calculate accounting information.

43) It is recommended that the ability to log DM-related operations be supported.

44) It is recommended that the configuration parameters of a device with its DM agent indirectly interacting with the DM manager via the DM GW manager be obtained and/or set by the DM GW manager or the DM manager through the DM GW manager.

45) It is recommended that for a device with its DM agent indirectly interacting with the DM manager via the DM GW manager, any service running on that device and that device's peripherals be activated and de-activated locally and remotely by the DM GW manager or DM manager through the DM GW manager.

46) It is required that the DM GW manager be able to remotely restart a device with its DM agent indirectly interacting with the DM manager via the DM GW manager, any service running on that device and that device's peripherals [OMA-RD-LightweightM2M].

47) It is recommended to support mechanisms to remotely lock or erase contents of IoT devices (e.g., in order to protect sensitive personal information from the possibility of loss/theft of a device).

48) It is required to support different levels of security according to the IoT applications' requirements.

NOTE 9 – Low resource-consumption security mechanisms should be used for resource constrained devices.

49) It is required to support device integrity checking [ITU-T Y.2066].

50) It is recommended to support mutual authentication between DM functional components.

51) It is recommended to support non-repudiation and to support countermeasures against replay attacks to the communication between DM functional components.

52) It is recommended to support encryption of DM-related communications.

53) It is required that credentials of devices have appropriate protection mechanisms.

54) In the case of open access to the DM capabilities, it is required that IoT applications and administrators of IoT applications be allowed to manage only authorized devices.

55) It is required to support DM functional components' protection mechanisms against threats such as denial of service attacks.

8 Common capabilities of device management in the IoT

The following clauses describe common capabilities of device management in the IoT.

NOTE – Not all the capabilities listed here are required to be implemented by all IoT systems or applications.

8.1 Configuration management capability

The configuration management capability provides functions to identify, collect and exercise control over configuration data from devices and to provide configuration data to devices [b-ITU-T M.3400].

The configuration management capability supports the following functions:

1) Discovery, provisioning and registration

   (i) Discovery is the process to allow devices, capabilities of the devices and applications running on devices to be found and identified by the DM manager and/or DM GW manager.

   (ii) Provisioning consists of procedures which are necessary to bring a device into service, including the bootstrap procedure, installing parameters and/or applications on a device to establish given services, such as DM services, applications, etc.

   (iii) Registration is the process of recording the information of the device in the DM manager and/or DM GW manager the first time the device accesses the DM manager and/or DM GW manager if the registration is successful, enabling then the DM manager and/or DM GW manager to interact with the device for DM services.

   NOTE – If a registration attempt fails, the DM manager and/or DM GW manager should support the logging of the registration attempt. In addition, the device will not be able to get DM services provided by the DM manager and/or DM GW manager.

2) Firmware/Software image management

Firmware/Software image management consists of image inventory management, update results reporting, integrity check of image before update process, update process monitoring, fallback mechanism when update fails, etc.

3) Configuration status monitoring

Configuration status monitoring is the process to get the current status of device configuration parameters and device components. It can take place periodically, on request, or triggered by events.

4) Configuration control

Configuration control provides the ability to control on demand certain aspects of a device, including setting the device configuration parameters, changing the service state of the device or components of the device, activating and de-activating the device, etc.

8.2 Performance management capability

The performance management capability provides functions to evaluate and report upon the behaviour of a device. Its role is to gather and analyse statistical data for the purpose of monitoring and correcting behaviour and effectiveness of a device and to aid in planning, provisioning, maintenance and measurement of quality [b-ITU-T M.3400].

The performance management capability supports the following functions:

1) Performance monitoring

Performance monitoring involves the collection of data concerning the performance of devices and the measurement of the overall quality in order to detect service degradation, including performance monitoring policy setting, performance data collection and processing, performance alarm rule setting, performance alarm collection and processing, performance status reporting, etc.

2) Performance control

Performance control supports the management of schedules, thresholds and other attributes for performance management.

3) Performance analysis

Performance analysis involves additional processing and analysis on the collected data from devices in order to evaluate the performance level of devices, such as performance summary, performance forecasting, performance exception analysis, etc.

8.3 Fault management capability

The fault management capability provides functions enabling the detection, isolation and correction of abnormal operation of devices [b-ITU-T M.3400].

The fault management capability supports the following functions:

1) Alarm surveillance

Alarm surveillance provides the ability to monitor device failures in time, including alarm policy setting, alarm reporting, alarm summary, alarm correlation and filtering, failure event detection and reporting, etc.

2) Fault localization and diagnosis

Where the initial failure information is insufficient for fault localization, it has to be augmented with information obtained by additional failure localization routines. Fault

localization, or diagnosis, includes running of diagnostic functions in devices, getting network connection information from the underlying network, summarizing all information from different sources and providing diagnostic reporting.

3) Fault correction

Fault correction deals with repairing a device fault if the device supports fault correction or restoration functions, such as using redundant units, isolating a faulty unit, etc.

4) Trouble administration

Trouble administration deals with investigating and clearing fault reports originated by end users and trouble tickets originated by proactive failure detection, including fault reporting, fault information query, trouble ticket management, etc.

8.4 Security management capability

The security management capability provides the following functions:

1) Security management for communications

The security management capability provides security management mechanisms for communications such as authentication, access control, data confidentiality, data integrity and non-repudiation, which may be exercised in the course of any DM-related communications between devices and the DM manager and/or DM GW manager.

2) Security event detection and reporting

The security management capability provides mechanisms of security event detection and reporting of related results concerning any activity that may be construed as a security violation, such as unauthorized user access, physical tampering with devices, etc.

3) Device security assurance

The security management capability provides mechanisms of device security assurance in order to make sure the device security is not damaged or, at least, to make sure the device has not been intruded by device integrity checking.

4) Device security control

The security management capability provides mechanisms to control device security settings, such as remotely locking or erasing contents of a device if the device has been stolen.

8.5 Connectivity management capability

For device management in the IoT, connectivity is crucial. The connectivity management capability is a necessity for a device's working status monitoring and fault location. The connectivity management capability deals with the communication bearer between device and DM manager (dealing with it as a whole and not dealing with the management of the different network elements and communication links between them, concerned by the communication bearer).

The connectivity management capability supports the following functions:

1) Device connectivity status monitoring

Device connectivity status monitoring provides the ability to get device connectivity status information through direct communication with a device. It is often implemented by the heartbeat mechanism.

2) Device connectivity configuration management

Device connectivity configuration management provides the ability to get and set parameters related to the device connectivity configuration.

3) Network connectivity status monitoring

Network connectivity status monitoring provides the ability to get the status information of the communication bearer between a device and the DM manager. Such information is collected from the network, instead of devices.

4) Network connectivity control

Network connectivity control provides the ability for the DM manager to prohibit the connection of devices to the network for a certain period of time if and as needed.

8.6 DM protocol engine capability

The DM protocol engine capability provides the protocol engine to process DM protocol messages.

The DM protocol engine capability supports the following functions:

1) DM protocol message encapsulation and de-capsulation
2) DM protocol flow control
3) DM protocol adaptation (between two or more DM protocols)
4) DM protocol statistics collection and reporting

8.7 Accounting management capability

In the case of open access to the DM capabilities, the accounting management capability is necessary to enable measurement of DM services' usage and determination of related accounting information.

The accounting management capability includes the following functions:

1) Usage measurement

Usage measurement provides the ability to collect DM service usage data based on access time of DM services, use of DM services and number of managed devices.

2) Accounting

Accounting involves the processes responsible for calculating metrics related to DM service usage data.

8.8 Service exposure – web portal capability

In the case of open access to the DM capabilities, the service exposure – web portal capability is a necessity. Via such capability, any DM service provided to administrators of IoT applications, such as configuration management, performance management, fault management, etc., can be accessed through a web portal.

8.9 Service exposure – API capability

In the case of open access to the DM capabilities, the service exposure – API capability is a necessity. Via such capability, any DM service provided to IoT applications, such as configuration management, performance management, fault management, etc., can be accessed through open APIs by IoT applications.

Bibliography

[b-ITU-T M.3400] Recommendation ITU-T M.3400 (2000), *TMN management functions*.

[b-ITU-T Y.4112] Recommendation ITU-T Y.4112/Y.2077 (2016), *Requirements of the plug and play capability of the Internet of things.*

[b-ITU-T Y.4401] Recommendation ITU-T Y.4401/Y.2068 (2015), *Functional framework and capabilities of the Internet of things.*

[b-OMA-RD-DM] Recommendation OMA-RD-DM (2013), *Device Management Requirements*.

[b-OneM2M TS-0002] Recommendation OneM2M TS-0002 (2015), *OneM2M Technical Specification Requirements*.

[b-TR-069] Technical Report DSL Forum TR-069 (2004), *CPE WAN Management Protocol*.

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