International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4212
(11/2021)

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

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

Requirements and capabilities of network connectivity management in the Internet of things

Recommendation ITU-T Y.4212

Recommendation ITU-T Y.4212

Requirements and capabilities of network connectivity management in the Internet of things

Summary

Recommendation ITU-T Y.4212 specifies the requirements and capabilities of network connectivity management in the Internet of Things (IoT).

The specified requirements and capabilities are intended to be generally applicable in network connectivity management application scenarios.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T Y.4212	2021-11-29	20	11.1002/1000/14814

Keywords

IoT, network connectivity management, requirements.

---

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.4212

Requirements and capabilities of network connectivity management in the Internet of things

1 Scope

This Recommendation specifies the requirements and capabilities of network connectivity management in the Internet of things (IoT).

The scope of this Recommendation includes:

1)   Requirements of network connectivity management in IoT.

2)   Capabilities of network connectivity management in IoT.

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.4101]   Recommendation ITU-T Y.4101/Y.2067 (2017), *Common requirements and capabilities of a gateway for Internet of things applications*.

[ITU-T Y.4702]   Recommendation ITU-T Y.4702 (2016), *Common requirements and capabilities of device management in the Internet of things*.

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.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.

3.1.3   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

None.

4   Abbreviations and acronyms

This Recommendation uses the following abbreviations:

ADSL   Asymmetric Digital Subscriber Line

API   Application Programming Interface

BSS   Business Support System

GPRS   General Packet Radio Service

IoT   Internet of Things

IP   Internet Protocol

NB-IoT   Narrow Band Internet of Things

NCM   Network Connectivity Management

OSS   Operation Support System

SIM   Subscriber Identity Module

SMS   Short Message Service

SSAS   Service Support and Application Support

URL   Uniform Resource Locator

WAN   Wide Area Network

5   Conventions

In this Recommendation:

–   The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance with this Recommendation is to be claimed.

–   The keywords "is recommended" indicate a recommendation which is not absolutely required. Thus this requirement need not be fulfilled to claim conformance.

–   The keywords "can optionally" and "may" indicate an option which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6   Introduction to network connectivity management

In the Internet of Things (IoT) scenarios, enterprises and IoT service providers offer products and services to end users, which include access to a wide area network (WAN). To ensure the quality and reliability of services, they also need to ensure the quality and reliability of the network connectivity of each IoT device. With a large number of deployed devices, it is difficult to monitor and manage network connections manually by enterprises and IoT service providers through traditional customer care services provided by network operators.

To solve this problem, network connectivity management (NCM) should be provided to enterprises and IoT service providers by network operators.

NCM is a set of management capabilities of the IoT, providing support for, but not being limited to, self-service provisioning, network connectivity status monitoring, network connectivity status diagnosis, network connectivity control, network connectivity event notification and network connectivity analysis.

In the IoT, NCM capabilities can be deployed in IoT applications or in functional components which provide service support and application support (SSAS) [ITU-T Y.4000] capabilities. When deployed in the IoT SSAS layer, NCM capabilities can be provided as a common service to IoT applications. When located in IoT applications, NCM capabilities may be integrated with other functional components of IoT applications.

NOTE – This Recommendation focuses on the NCM requirements and the NCM capabilities for the interaction between IoT device(s)/IoT gateway(s) and network elements provided by network operators. The NCM capabilities in IoT applications and their specific requirements are out of the scope of this Recommendation.

Figure 1 shows the positioning and the interaction of the NCM capabilities in the IoT from the layering perspective of the IoT reference model [ITU-T Y.4000].

The NCM capabilities are responsible for managing the quality and reliability of the network connections of each IoT device. The NCM capabilities interact with network elements and with the business support system (BSS) and/or the operation support system (OSS) to obtain NCM-related information of IoT device(s)/IoT gateway(s), and to send them commands for execution of NCM-related tasks.

In the case of open access to the NCM capabilities, they can be enabled automatically and in self-service mode by enterprises and IoT service providers. In this way, the NCM capabilities can be enabled efficiently in the case of a large number of IoT devices by enterprises and IoT service providers.
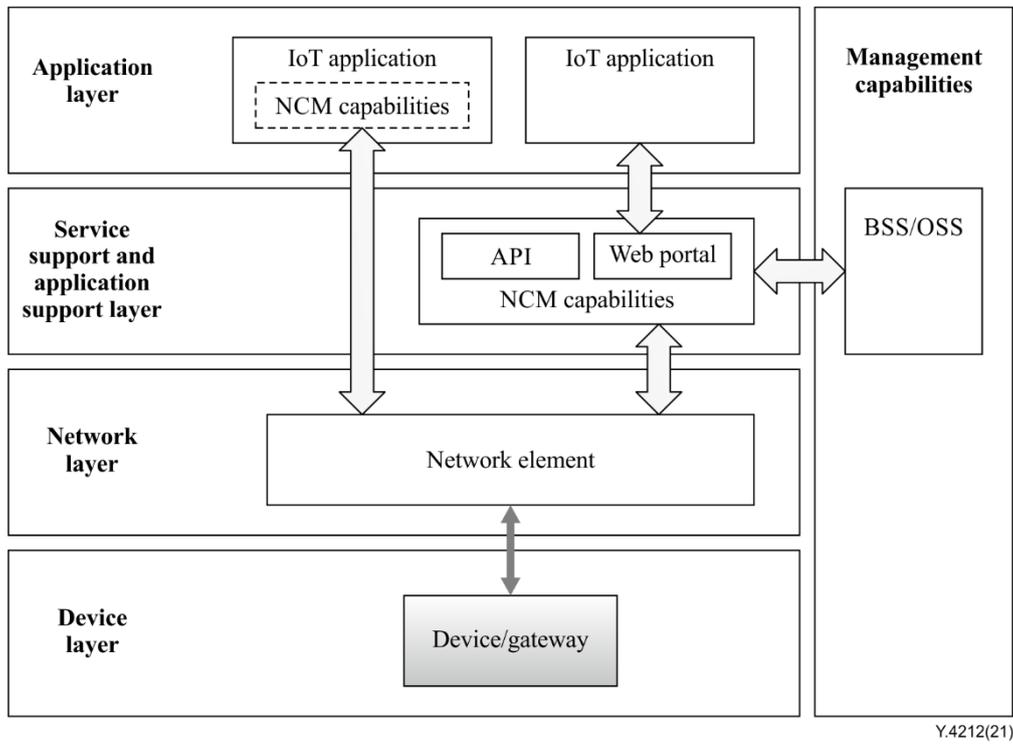
Key: API — Application Programming Interfaces

**Figure 1 – The NCM capabilities in the IoT from the
IoT reference model layering perspective**

7 Requirements of network connectivity management in the IoT

7.1 Characteristics specific to network connectivity management in the IoT

The NCM capabilities in the IoT have 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 network connections for related IoT devices [ITU-T Y.4702].

2) As shown in Figure 2, different communication networks may use different relationship patterns between IoT devices and related gateway(s). Wireless and wireline communication networks both have a one-to-one relationship and a many-to-one relationship. Some IoT devices may interact directly with network elements of a WAN without access to IoT gateway(s). The NCM capabilities not only deal with IoT device(s) with direct access to a WAN, but also deal with IoT gateway(s) with direct access to a WAN. In this case, wireless and wireline communication networks have a one-to-one relationship between IoT device(s)/IoT gateway(s) accessed by a WAN and network element.

   NOTE 1 – In the case of NCM capabilities dealing with IoT gateway(s) with direct access to a WAN, this Recommendation addresses only the NCM capabilities with WAN connectivity, i.e. the NCM capabilities between IoT gateway(s) and its/their connected IoT device(s) are out of the scope of this Recommendation.
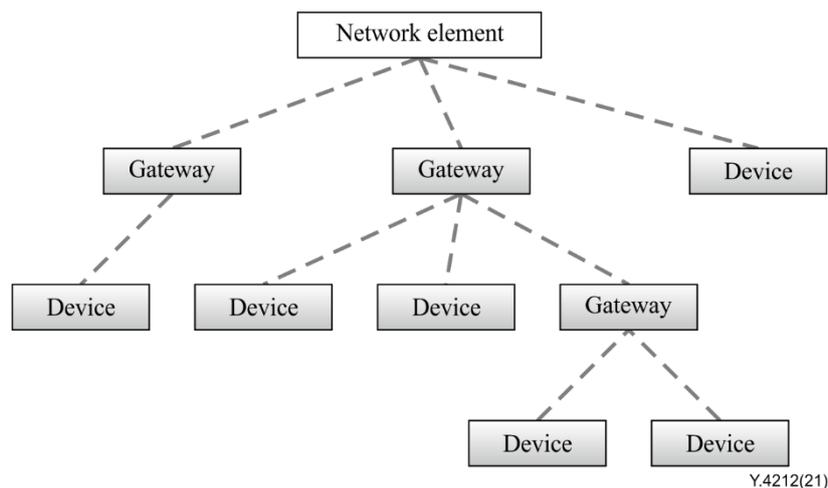
**Figure 2 – Typical relationship patterns among network element,
IoT gateway(s) and IoT device(s)**

3) The NCM capabilities may use different communication technologies, such as wireless WANs (e.g., General Packet Radio Service (GPRS), 3G, 4G, 5G, narrowband Internet of Things (NB-IoT), satellite, unlicensed band access technologies such as Lora) and wireline access networks (e.g., asymmetric digital subscriber line (ADSL)) [ITU-T Y.4702].

4) The NCM capabilities are necessary to interact with network elements and BSSs and/or OSSs provided by network operators in order to obtain NCM-related information of IoT devices as well as to send commands for the execution of NCM-related tasks by enterprises and IoT service providers. NCM-related information can also be made available, if applicable, from a local repository, which collects and assembles the information from network elements and BSS and/or OSS provided by network operators.

NOTE 2 – NCM-related information includes the status information of a subscriber identity module (SIM) card, network configuration information, rate plan information, the status information of the communication bearer between a device and network elements, association relationship among enterprises and/or IoT service providers, end users, IoT devices and SIM cards, etc. Examples of SIM card state include SIM card activating, SIM card pausing, SIM card deactivating, SIM card terminating and SIM card reactivating.

NOTE 3 – NCM-related tasks include self-service provisioning, self-service recharging and pre-configuring threshold limit setting of data usage.

5) Different communication networks may have different network elements, and even if two different communication networks are both based on the same technology, they may have different network elements.

6) Different network connectivity types may be used for different devices. Concerning resource constrained devices characterized by limited battery capacity, short-term network connectivity is often used. Concerning applications for home appliance control, always-on network connectivity is often used.

NOTE 4 – For short-term network connectivity, network connections are usually released immediately after communication completion for power-saving devices such as remote metering devices.

7.2 General requirements of network connectivity management in the IoT

The general requirements of NCM in the IoT are as follows.

1) It is recommended to enable open access by IoT applications to the NCM capabilities, e.g., via application programming interfaces (APIs) and/or web portals.

NOTE 1 – The open access to the NCM capabilities allows some IoT applications to directly use the NCM capabilities of the SSAS layer, and administrators of such IoT applications to also use the NCM capabilities (e.g., through a web portal, i.e., via a specific type of IoT application).

2) It is required to support the ability to self-service provision/query/modify/delete NCM-related information related to one, some or all of IoT devices by enterprises and IoT service providers.

NOTE 2 – The prerequisite is to complete batch pre-provisioning process within the BSS and/or the OSS, and also within the related network elements, before self-service provision/query/modification/deletion can be executed.

3) It is required that the NCM capabilities be able to obtain/check the current and historical NCM-related information of connections for one, some or all IoT devices from network elements, BSS, OSS and/or, if applicable, local repository.

NOTE 3 – Such information can be also directly reported by network elements, BSS, OSS and local repository.

4) It is required that the NCM capabilities be able to send commands for execution of NCM-related tasks to network elements and BSS and/or OSS, which include self-service provisioning, self-service recharging, pre-configuring threshold limit setting of data usage, etc.

5) It is required that each network connection for the related IoT device managed by the NCM capabilities be uniquely identified in order to be recognized and managed.

6) It is recommended that the NCM capabilities be robust enough to support a large number of network connections for related IoT devices accessing the NCM capabilities simultaneously.

7) It is recommended for the NCM capabilities to be able to obtain/check the current and historical NCM-related information periodically, on request or triggered by events according to the pre-configured rules.

8) It is required to support the analysis of the current and historical NCM-related information, such as providing policies for network access and a better rate plan for users according to the analysis.

9) It is recommended that the network connectivity be manageable by groups and that different groupings be supported, such as by identifier (ID) or location.

10) It is recommended to support different NCM capability access levels. For instance, access to NCM capabilities of devices with low access levels may be denied when a large number of devices access NCM capabilities at the same time.

11) If some abnormal network connectivity condition occurs, it is recommended to execute diagnostic analysis, including obtaining and analysing NCM-related information and executing network connectivity tests, such as network ping test, short message service (SMS) connectivity test, etc.

12) It is recommended to support the access to specific data services through uniform resource locator (URL) / Internet protocol (IP) addresses according to the configuration.

13) It is recommended to support pausing network connections or limiting the bandwidth of connections if the usage exceeds one or more configured thresholds.

14) It is required to support a mechanism to disable the connection of one or more IoT devices to the network for a certain time period, and to re-enable the connection of the IoT device(s) to the network after that period.

15) It is recommended to support mechanisms to control the access to the network based on different policies, such as time and/or location.

16) It is recommended to support automated network connectivity event notification when some event is triggered according to a pre-configured policy. The notification methods include email notification, SMS notification and API push message notification.

17) It is recommended to support the self-service pre-configuration of threshold limit setting, such as usage limit, time limit and/or location limit of services.

18) It is recommended to support mutual authentication between related entities in the course of NCM-related communications, such as the communication between an NCM capable entity and network elements or between an NCM capabe entity and an OSS/BSS, etc.

19) It is recommended to support the encryption of NCM-related information.

20) In the case of open access to the NCM capabilities, it is required for IoT applications and administrators of IoT applications to be allowed to manage only authorized network connections.

8 Capabilities of network connectivity management in the IoT

8.1 Network connectivity self-service management

The network connectivity self-service management capability provides functions to enable enterprises and IoT service providers to deal with NCM by themselves.

The functionalities of network connectivity self-service management are as follows:

–   Support capability of self-service provisioning for one, some or all IoT devices, such as activating SIMs or setting rate plan.

–   Support capability of self-service NCM-related information query, such as the status information of SIM cards, current network connectivity status, network configuration information, rate plan information and network connectivity event notification.

–   Support capability of self-service NCM-related information modification, such as changing the rate plan and changing the status information of SIM cards.

–   Support capability of self-service NCM-related information deletion, including but not being limited to terminating one or more network connections.

–   Support capability of self-service configuration setting, including configuration in advance and configuration on demand.

–   Support capability of self-service recharging.

8.2   Network connectivity status monitoring

The network connectivity status monitoring capability provides functions to obtain/check the current and historical NCM-related information, as appropriate. It can take place periodically, on request or be triggered by events.

8.3   Network connectivity analysis

The network connectivity analysis capability provides functions to analyse current and historical NCM-related information and provide recommendations for network connectivity.

The functionalities of network connectivity analysis are as follows:

–   Support capability of analysing the current and historical NCM-related information, such as network connectivity status and rate plan analysis.

–   Support capability of providing recommendations for network connectivity, such as policies for network access, and/or better rate plan for users according to the analysis.

8.4   Network connectivity status diagnosis

The network connectivity status diagnosis capability provides functions to execute fault localization and diagnosis when an abnormal network connectivity condition occurs.

The functionalities of network connectivity status diagnosis are as follows:

–   Support capability of network connectivity fault localization and diagnosis through methods including network connectivity testing, NCM-related information diagnosis from different sources such as network elements and BSS/OSS.

–   Support capability of providing diagnostic reporting to enterprises and/or IoT service providers.

8.5   Network connectivity control

The network connectivity control capability provides functions to control the network connectivity settings according to the configuration.

The functionalities of network connectivity control are as follows:

–   Support capability of access to specific data services through URL/IP addresses according to the configuration.

–   Support capability of pausing network connections or limiting the bandwidth of connections if the usage exceeds one or more configured thresholds.

–   Support capability of disabling the connection of one or more IoT devices to the network for a certain time period, and re-enabling the connection of the IoT device(s) to the network after that period.

–   Support capability of controlling access to the network according to the configuration, such as based on time and/or location.

–   Support different NCM capability access levels according to the configuration.

8.6 Network connectivity event notification management

The network connectivity event notification management capability provides functions to enable the notification of a network connectivity event.

The functionalities of network connectivity event notification management are as follows:

– Support capability of network connectivity event notification when an event is triggered according to the pre-configuration of the rule. The methods of event notification include e-mail notification, short message notification and API push message notification.

8.7 Service exposure

The service exposure capability provides functions to make NCM capabilities available to IoT applications and administrators of IoT applications through methods such as open APIs and web portals in the case of open access to the NCM capabilities.

8.8 Security management

The functionalities of security management are as follows:

– Supporting capabilities such as authentication, access control, data confidentiality, data integrity and non-repudiation.

– Supporting capability of related incident detection and reporting such as unauthorized user access and data compromise.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems