International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.1611

(01/2021)

SERIES J: CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

Artificial intelligence (AI) assisted cable networks – Requirements for the set-top box

Functional requirements for a smart home gateway

Recommendation ITU-T J.1611

Recommendation ITU-T J.1611

Functional requirements for a smart home gateway

Summary

Recommendation ITU-T J.1611 specifies functional requirements for a smart home gateway from both the hardware and software point of view to ensure secure interoperability among consumers, businesses and industries by delivering a standardized communications platform and allowing devices to communicate across operating systems, service providers, transport technologies or ecosystems.

In a smart home solution, a gateway is incorporated to connect various appliances. In addition, a connection management platform based on the Internet of things (IoT) is required to enable various applications. These applicable solutions include home health, entertainment, security and home automation, which promote a safer, happier, as well as a more comfortable and convenient lifestyle.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T J.1611	2021-01-13	9	11.1002/1000/14586

Keywords

IoT, residential gateway, STB, smart home.

---

* 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

Introduction

A smart home is a kind of home automation system based on the Internet of things (IoT), through which home appliances, sensors and services can be connected by a communication network and remotely accessed, monitored and controlled. A smart home gateway, sometimes called a smart home bridge, collects and translates various protocol communications from smart home devices.

In a smart home solution, a gateway is incorporated to connect appropriate appliances. In addition, an IoT-based connection management platform is required to enable various applications. These applicable solutions include home health, entertainment, security, and home automation, which promote a safer, happier, as well as a more comfortable and convenient lifestyle. The solution will help operators to adapt heritage home broadband services to provide intelligent home services and increase subsequent service income revenues.

As such, a gateway acts as the heart of a smart home network, tying together various devices and systems in a centralized platform. This also simplifies the network for users and gives them a single smart home application to manage all systems and applications. Another important function of the gateway is to act as a protocol converter and translator. Considering that there are different wireless access technologies and different protocols and eco-systems, this function will make it possible to have different smart home systems or even different interoperable ecosystems, which will bring great convenience to the customer.

A gateway can be a standalone device in a smart home solution. It can also be incorporated into a set-top box or other residential gateway devices. The common requirement of the solution is that a smart home gateway should have the capabilities of broadband connection with an IoT management platform, and a long life cycle in the home environment.

Recommendation ITU-T J.1611

Functional requirements for a smart home gateway

1 Scope

This Recommendation specifies functional requirements for a smart home gateway (also called "gateway" in this Recommendation) from both the hardware and software point of view to ensure secure interoperability among consumers, businesses and industries by delivering a standardized communications platform and allowing devices to communicate across operating systems, service providers, transport technologies or ecosystems.

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.

[BBF TR-069] Broadband Forum Technical Report BBF TR-069 Issue:1 Amendment 6 (2018), *CPE WAN management protocol*.

[IETF RFC 7252] IETF RFC 7252 (2014), *The constrained application protocol (CoAP)*.

[IETF RFC 8446] IETF RFC 8446 (2018), *The transport layer security (TLS) protocol version 1.3*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 device [b-ITU-T Y.2060]: 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 Internet of things (IoT) [b-ITU-T Y.2060]: 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.

3.1.3 thing [b-ITU-T Y.2060]: With regard to the Internet of things, this is an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 smart home gateway: A unit in the Internet of things that interconnects smart home devices with communication networks. It performs the necessary translation between the protocols used in the communication networks and those used by smart home devices.

3.2.2 onboarding service: A software module in a smart home gateway that manages and implements onboarding flows and procedures.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3G	third Generation
4G	fourth Generation
5G	fifth Generation
ACS	Auto-Configuration Server
API	Application Programming Interface
BLE	Bluetooth Low Energy
CoAP	Constrained Application Protocol
CPE	Customer Premises Equipment
CPU	Central Processing Unit
GSM	Global System for Mobile communication
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IoT	Internet of Things
IR	Infrared
LED	Light-Emitting Diode
LTE	Long-Term Evolution
MIC	Microphone
MPU	Micro-Processor Unit
MQTT	Message Queuing Telemetry Transport
NB-IoT	Narrowband Internet of Things
NFC	Near-Field Communication
NPU	Neural Processing Unit
OS	Operating System
OTA	Over The Air
PSU	Power Supply Unit
RF	Radio Frequency
SD	Secure Digital
Sub-1G	Sub-1 GHz
TLS	Transport Layer Security
USB	Universal Serial Bus
UI	User Interface
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity

5 Conventions

The following conventions are used in this Recommendation:

– The phrase "is required to" indicates a requirement that must be strictly followed and from which no deviation is permitted, if conformity to this Recommendation is to be claimed.

– The phrase "is recommended" indicates a requirement that is recommended, but which is not absolutely required. Thus, this requirement need not be present to claim conformity.

– The phrase "is optionally required" indicates an optional requirement that is permissible, without implying any sense of being recommended.

6 Overview

6.1 Overall smart home system

The architecture of the overall smart home system is shown in Figure 1, basically it contains following parts:

- smart home cloud server: The data and logic centre of a whole smart home system;
- third party service: A service provided by a third party, e.g., voice assistant or media content;
- client and its software applications: Smart mobile phone, tablet, personal computer and the smart home applications for these clients;
- smart home devices: All smart home equipment like a camera, doorbell, sensor, actuator, power plug, power switch and light;
- smart home gateway: A device or piece of equipment that connects various smart home devices and acts as a bridge between smart home cloud and smart home devices.

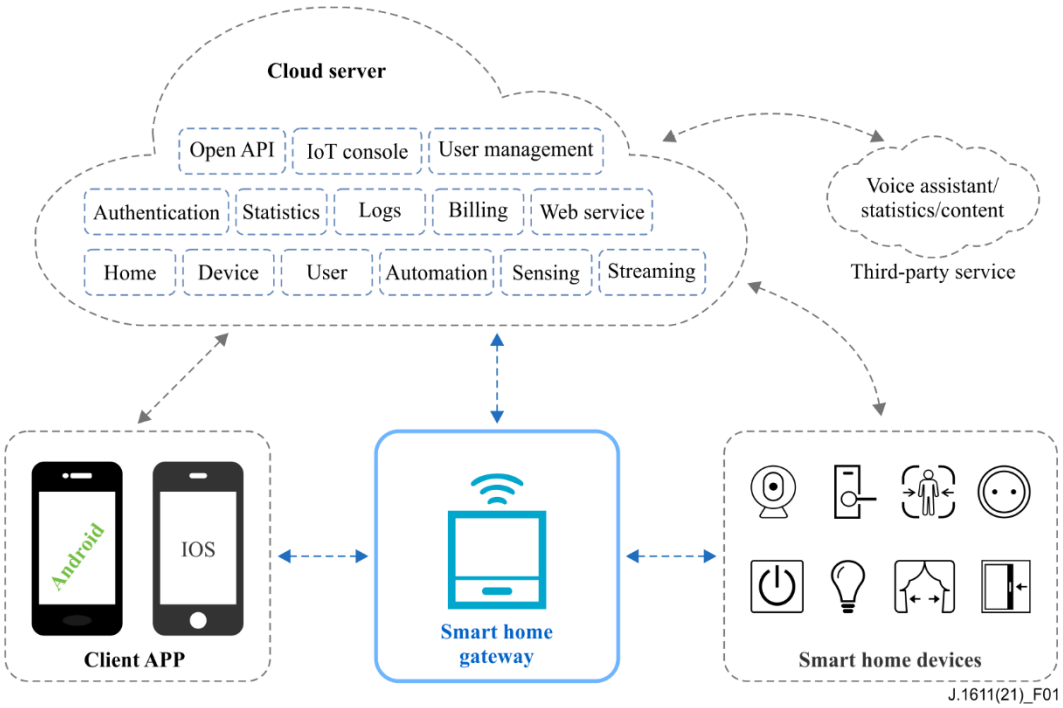

Figure 1 – The overall smart home system

6.2 Smart home gateway

Figure 2 illustrates the basic function modules and interfaces of the gateway.

The major function of the smart home gateway is to bridge and translate between different IoT protocols or different IoT eco-systems. It provides one endpoint for the various things on one hand,

while interacting with backend services deployed over the cloud to accomplish more service capability on the other.

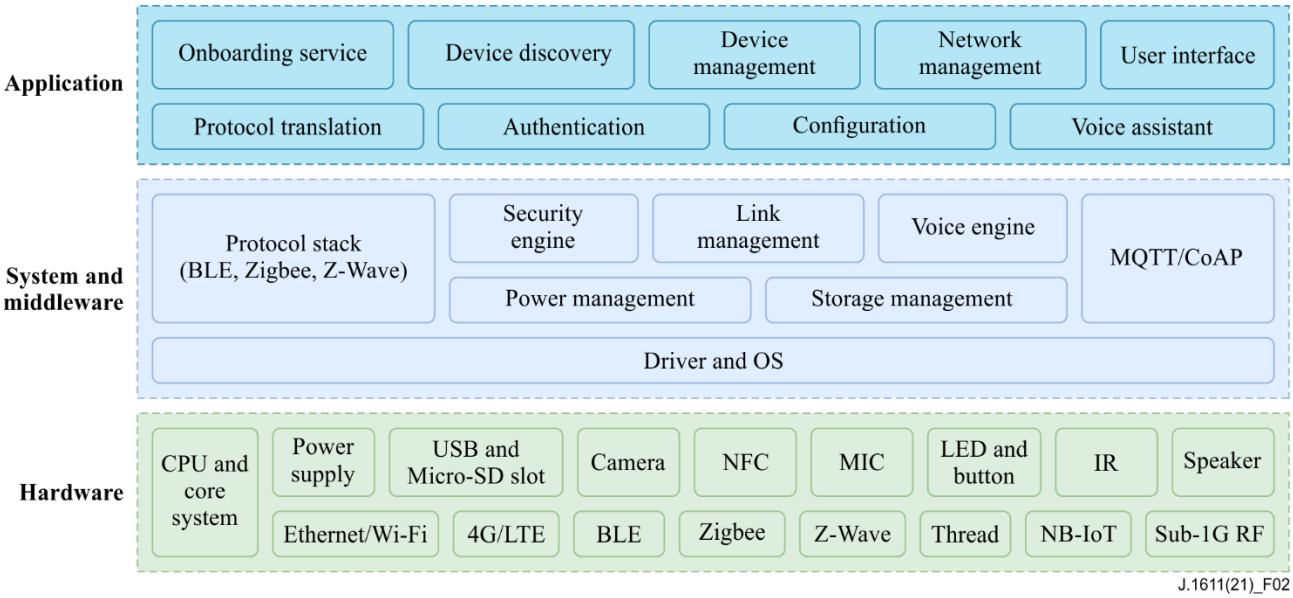

Figure 2 – Function modules of the smart home gateway

BLE: Bluetooth low energy; LTE: long-term evolution; OS: operating system; Sub-1G RF: sub 1 GHz radio frequency

The gateway hardware usually consists of a micro-processor unit (MPU), memory, power supply, essential communication interfaces and accessory interfaces required in a smart home application. Above the hardware layer, there is a driver and operating system layer, which serves as a basic software platform to manage all hardware resources and to provide application programming interfaces (APIs) for upper layer software. The various protocol stacks are built for different communication hardware interfaces. In the top layer are all kinds of applications, such as a protocol translation service, which bridge and translate operations between different IoT protocols. Other applications consist of device discovery, onboarding service, device management, network management, etc.

7 Requirements

7.1 Basic hardware capability

7.1.1 System on chip platform

[smgw-HWReq-01] The gateway is required to be independent of any specific type of central processing unit (CPU) architecture.

[smgw-HWReq-02] The gateway is optionally required to support a neural processing unit (NPU) to provide edge computing capability.

7.1.2 Button and light-emitting diode indicator

[smgw-HWReq-03] At least one hardware button is required to support system reset, device pairing and their relevant features.

[smgw-HWReq-04] At least one light-emitting diode (LED) indicator is required to indicate the working status of the smart home gateway.

7.1.3 Universal serial bus and micro-secure digital slot

[smgw-HWReq-05] A universal serial bus 2.0 (USB2.0) or above slot is recommended for supporting external peripheral devices, such as USB storage, USB camera and USB microphone (MIC), etc.

[smgw-HWReq-06] A micro-secure digital (micro-SD) card slot is recommended for supporting an external micro-SD card for storage.

7.1.4 Camera

[smgw-HWReq-07] A camera module is optionally required to provide image- or video-related features, such as human face and object recognition, and video calls.

7.1.5 Microphone array

[smgw-HWReq-08] An MIC array module is recommended to provide voice input for a far-field voice assistant feature.

7.1.6 Loudspeaker

[smgw-HWReq-09] A built-in loudspeaker is recommended for audio playback and voice feedback.

7.1.7 Near-field communication

[smgw-HWReq-10] A near-field communication (NFC) hardware module is optionally required.

7.1.8 Infrared

[smgw-HWReq-11] An infrared (IR) blaster is optionally required to support appliances with legacy IR control.

7.1.9 Power supply

[smgw-HWReq-12] The gateway is recommended to work with an external power supply unit (PSU) adaptor.

[smgw-HWReq-13] The gateway is optionally required to have built-in rechargeable battery for providing uninterrupted power supply.

7.2 IoT hardware connectivity

7.2.1 Ethernet or wireless fidelity

[smgw-ConnectReq-01] An Ethernet or wireless fidelity (Wi-Fi) module is required to access the Internet or home network.

7.2.2 Mobile data interface

[smgw-ConnectReq-02] A mobile data interface for global system for mobile communication/third generation/fourth generation/fifth generation (GSM/3G/4G/5G) is optionally required as an alternative for the Internet interface.

7.2.3 Bluetooth low energy

[smgw-ConnectReq-03] A BLE hardware module is recommended for connecting Bluetooth-based IoT devices. Bluetooth version 4.2 or above is recommended.

7.2.4 Zigbee

[smgw-ConnectReq-04] A Zigbee hardware module is recommended for connecting Zigbee-based IoT devices. Zigbee version 3.0 or above is recommended.

7.2.5 Z-Wave

[smgw-ConnectReq-05] A Z-Wave hardware module is recommended for connecting Z-Wave-based IoT devices.

7.2.6 Thread

[smgw-ConnectReq-06] A thread hardware module is recommended for connecting thread-based IoT devices.

7.2.7 Narrowband Internet of things

[smgw-ConnectReq-07] A narrowband Internet of things (NB-IoT) hardware module is recommended for connecting the NB-IoT-based IoT devices.

7.2.8 Sub-1G

[smgw-ConnectReq-08] A sub-1G hardware module is recommended for connecting sub-1G-based IoT devices.

7.3 Basic software function

7.3.1 Bridging of things

[smgw-SWReq-01] The gateway is required to bridge various things and sensors with different connection protocols.

7.3.2 Bridging of the platforms

[smgw-SWReq-02] The gateway is required to bridge different IoT platform to support interoperability of the various IoT eco-systems.

7.3.3 Open application environment

[smgw-SWReq-03] The gateway is recommended to support an open application framework on top of which developers develop applications.

7.3.4 Local decision making

[smgw-SWReq-04] The gateway is required to support local control capability to keep essential functions operable such as turning on or off the light or air conditioner while the Internet is temporarily disconnected.

7.3.5 Linkage function

[smgw-SWReq-05] The gateway is recommended to support a linkage function with user editable triggers.

7.3.6 Over the air programming and firmware upgrade

[smgw-SWReq-06] The gateway is required to support over the air (OTA) firmware upgrades for the gateway and things connected to the gateway.

7.3.7 Internet of things wireless protocol stack

[smgw-SWReq-07] The wireless protocol stacks are required to be implemented corresponding to the wireless hardware modules equipped in the gateway.

7.3.8 Internet protocol version 4 or Internet protocol version 6

[smgw-SWReq-08] Support for Internet protocol version 4 or Internet protocol version 6 (IPv4/IPv6) protocol is required in the smart home gateway.

7.3.9 Constrained application protocol

[smgw-SWReq-09] Support for the constrained application protocol (CoAP) [IETF RFC 7252] is recommended in a smart home gateway.

7.3.10 Message queuing telemetry transport

[smgw-SWReq-10] The message queuing telemetry transport (MQTT) [b-ISO/IEC 20922] protocol is optionally required for communication with an IoT service platform.

7.3.11 Transport layer security

[smgw-SWReq-11] Support for the transport layer security (TLS) protocol [IETF RFC 8446] is required to ensure secure communication between the gateway and backend platform.

7.4 Internet of things device management

7.4.1 Device installation and configuration

[smgw-DevManagementReq-01] The gateway is required to actively discover, connect and register IoT devices in the home.

[smgw-DevManagementReq-02] The gateway is required to provide an onboarding function for IoT devices.

[smgw-DevManagementReq-03] The gateway is required to provide an authentication mechanism for the registration of IoT devices.

[smgw-DevManagementReq-04] The gateway is required to support the auto-configuration function provided by the auto-configuration server (ACS).

[smgw-DevManagementReq-05] The [BBF TR069] protocol is recommended for implementing the auto-configuration functions of the gateway.

7.4.2 Device control

[smgw-DevManagementReq-06] The gateway is required remotely to receive control instructions from the backend IoT service platform and execute the instructions on IoT devices.

[smgw-DevManagementReq-07] The gateway is recommended to implement a voice recognition module to support voice control.

7.4.3 Device monitoring

[smgw-DevManagementReq-08] The gateway is required to support data collection from IoT devices and deliver the data to the backend IoT platform for storage.

7.4.4 Network management and diagnosis

[smgw-DevManagementReq-9] The gateway is required to support remote reboot.

[smgw-DevManagementReq-10] The gateway is required to support remote diagnosis.

[smgw-DevManagementReq-11] The gateway is required to provide a function to monitor the network connection of IoT devices.

7.5 Security

7.5.1 Connection security

[smgw-SecurityReq-01] The gateway is required to support a TLS and client-side certificate to secure connection between the IoT gateway and the IoT application server.

7.5.2 Data security

[smgw-SecurityReq-02] Encryption of the data transferred between a cloud server and the gateway is required.

[smgw-SecurityReq-03] Encryption of the data transferred between the gateway and an IoT device is recommended.

[smgw-SecurityReq-04] Encryption of the user data stored in the gateway is recommended.

7.5.3 Authentication

[smgw-SecurityReq-05] Implementation in the gateway of the authentication mechanism is required for device installation and registration.

7.5.4 Certification

[smgw-SecurityReq-06] Certification by the official organization of the gateway and IoT device is required.

Bibliography

[b-ITU-T Y.2060] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.

[b-ISO/IEC 20922] ISO/IEC 20922:2013, *Information Technology — Message Queuing Telemetry Transport (MQTT) V3.1.1*.

[b-IETF RFC 6347] IETF RFC 6347 (2012), *Datagram transport layer security version 1.2*.

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

Printed in Switzerland
Geneva, 2021