International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4451

(09/2016)

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 – Frameworks, architectures and protocols

Framework of constrained device networking in the IoT environments

Recommendation ITU-T Y.4451

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
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.4451

Framework of constrained device networking in the IoT environments

Summary

In Internet of things (IoT) environments, constrained devices, equipped with various low-power wireless interfaces, have connection capability to locally available networks for the purpose of interacting with the real world. Constrained devices have many different characteristics. Recommendation ITU-T Y.4451 specifies the framework of constrained device networking in the Internet of things (IoT) environments. This Recommendation therefore describes the concept and features of constrained device networking as well as network architectures of constrained device networking including functional requirements, such as fragmentation, reassembly, header compression, address configuration, network management, multi-hop routing protocol and higher layer considerations.

This Recommendation specifies the framework of constrained device networking in the Internet of things (IoT) environments with respect to IoT device communications. This Recommendation describes the concept of constrained device networking in the IoT environments and the communication of constrained devices. This Recommendation also describes network architecture and mechanisms of constrained device networking.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4451	2016-09-13	20	11.1002/1000/13026

Keywords

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

© ITU 2016

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

Recommendation ITU-T Y.4451

Framework of constrained device networking in the IoT environments

1 Scope

The scope of this Recommendation includes the following:

– An overview of constrained device networking in the IoT environments.

– Communication of constrained devices.

– Architectures of constrained device networking.

– Functionalities of constrained device networking.

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 G.9959] Recommendation ITU-T G.9959 (2015), *Short range narrow-band digital radiocommunication transceivers – PHY, MAC, SAR and LLC layer specifications.*

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

[ITU-T Y.4109] Recommendation ITU-T Y.4109/Y.2061 (2012), *Requirements for the support of machine-oriented communication applications in the next generation network environment.*

[IETF RFC 4862] IETF RFC 4862 (2007), *IPv6 Stateless Address Autoconfiguration.*

[IETF RFC 4944] IETF RFC 4944 (2007), *Transmission of IPv6 Packets over IEEE 802.15.4 Networks.*

[IETF RFC 5225] IETF RFC 5225 (2008), *RObust Header Compression Version 2 (ROHCv2): Profiles for RTP, UDP, IP, ESP and UDP-Lite.*

[IETF RFC 6282] IETF RFC 6282 (2011), *Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks.*

[IETF RFC 6550] IETF RFC 6550 (2012), *RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks.*

[IETF RFC 7400] IETF RFC 7400 (2014), *6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs).*

[IETF RFC 7428] IETF RFC 7428 (2015), *Transmission of IPv6 Packets over ITU-T G.9959 Networks.*

[IETF RFC 7668] IETF RFC 7668 (2015), *IPv6 over BLUETOOTH(R) Low Energy.*

[IETF RFC 7721] IETF RFC 7721 (2016), *Security and Privacy Considerations for IPv6 Address Generation Mechanisms.*

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 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 the following terms:

3.2.1 constrained device: A device that has constraints on characteristics such as limited processing capability, small memory capability, limited battery power, short range and low bit rate.

3.2.2 adaptation layer: A layer that is required for binding the network layer and the datalink layer in low-power network technologies.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BLE Bluetooth Low Energy

IoT Internet of Things

LLCP Logical Link Control Protocol

LoWPAN Low-power Wireless Personal Area Network

MP2P Multipoint-to-Point (MP2P)

MTU Maximum Transmission Unit

NFC Near Field Communication

POS Personal Operating Space

P2MP Point-to-Multipoint

P2P Point-to-Point

QoS Quality of Service

SNMP Simple Network Management Protocol

SSAP Source Service Access Point

5 Conventions

None.

6 Overview of constrained device networking in the IoT environments

6.1 IoT environments and constrained device networking

The ITU Report 2005 [b-ITU Report] states that Internet of things (IoT) can be defined as a vision "First, in order to connect everyday objects and devices to large databases and networks a simple, unobtrusive and cost-effective system of item identification is indispensable. Second, data collection can of course benefit from the ability to detect changes in the physical status of things. Finally, advances in miniaturization and nanotechnology mean that smaller and smaller things will have the ability to interact and connect".

According to the vision of the IoT, the smaller things, i.e., constrained IoT devices, equipped with various low-power wireless interfaces (e.g., IEEE 802.15.4, Bluetooth low energy (BLE), near field communication (NFC), etc.), need to have connection capability to locally available networks for the purpose of interacting with the real world including non-constrained IoT devices, see example in Figure 1. Various types of advanced IoT services applications can be deployed using the different types of connections and interactions.

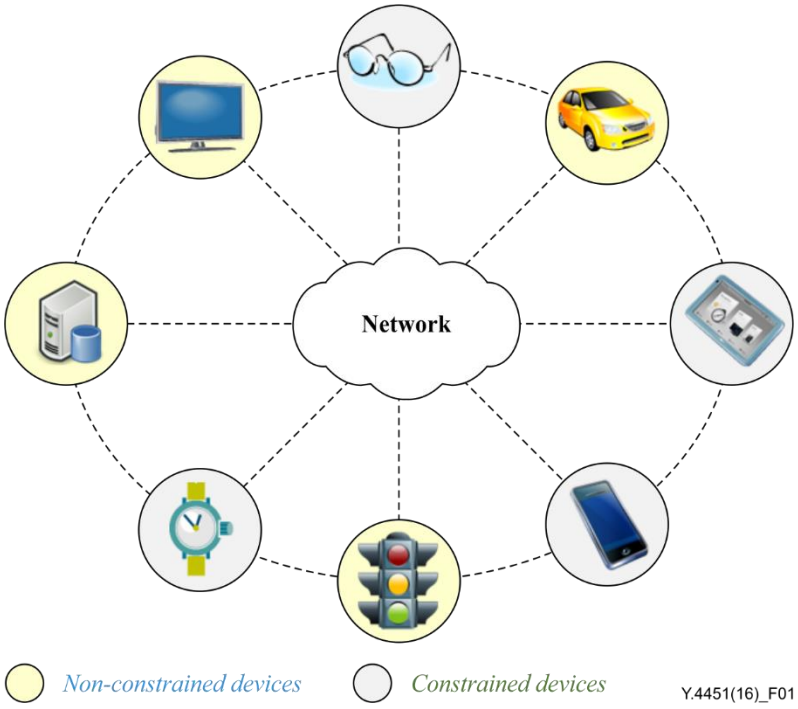

Figure 1 – Connected constrained and non-constrained devices

6.2 General characteristics of constrained devices

To develop the advanced IoT services and applications, various aspects of the requirements should be considered in advance. One such aspect is the type of constraint that characterizes the IoT devices. Constraint types for IoT devices are listed as follows:

– **Limited processing capability**: The constrained IoT devices have limited processing capability. For example, the smallest common low-power wireless personal area network (LoWPAN) nodes have 8-bit processors with clock rates of around 10 MHz. Other models exist with 16-bit and 32-bit cores (typically ARM7), running at frequencies in the range of tens of MHz.

– **Small memory capacity**: In the case of monitoring and target-tracking IoT services, the constrained IoT devices have a limited memory capacity. These constrained IoT devices have a few kilobytes of RAM with a few dozen kilobytes of ROM/flash memory. While

memory sizes of nodes continue to grow, the nature of small memory capacity for the constrained IoT devices remains a challenge.

– **Limited battery power and low power consumption**: Wireless radios for mobile devices are normally battery-operated. For the sake of longevity, mobile devices should conserve energy and not waste the limited battery power.

– **Short range**: The personal operating space (POS) defined by [b-IEEE 802.15.4] and Bluetooth LE implies a range of 10 metres and NFC implies a range of 10 centimetres. Likewise, almost all constrained IoT devices have short ranges.

– **Low bit rate**: A maximum over-the-air rate of 250 kbit/s, which is most commonly used in current deployments, is defined in [b-IEEE 802.15.4]. Alternatively, three lower data rates of 20, 40 and 100 kbit/s are defined. Furthermore, the over-the-air data rate of Bluetooth LE is 1 Mbit/s and NFC is 424 kbit/s.

7 Communication features and attributes

7.1 Features of constrained devices in IoT environment

As defined in [ITU-T Y.4000] and [ITU-T Y.4109], the communication and networking paradigms in the IoT environments are focused on the domain of devices and machines. The new dimension introduced in the IoT is communication and it includes the communication between computers, of human to human, of human to things and between things [b-ITU Report]. With regard to the IoT, things are objects of the physical world or the information world. Physical things exist in the physical world and are capable of being sensed, actuated and connected. Virtual things exist in the information world and are capable of being stored, processed and accessed. Physical things include devices and gateways. With regard to the IoT, the mandatory capability of a device is communication and optional capabilities are sensing, actuation, data capture, data storage and data processing. In [ITU-T Y.4000], there are three types of device communications;

– Communication through the communication network via a gateway

– Communication through the communication network without a gateway

– Communication without using the communication network (directly)

The devices in the IoT environments are heterogeneous and are based on different hardware and network access technologies. There are various types of IoT devices and some of them have low performance and limited functionality while others have powerful capabilities. Constrained IoT devices have different features of communication.

7.2 Considerations for constrained device networking

Some networking mechanisms such as routing protocols, address generation and network configuration are not suitable for the constrained IoT devices. Considerations for constrained device networking are as follows:

– **Deployment**: Deployment can occur at once, or as an iterative process. The selected type of deployment has an impact on node density and location.

– **Network size**: The network size takes into account devices that provide the intended network capability. The number of devices involved in a service could be small, moderate (several hundred), or large (over a thousand).

– **Power source**: The power source of devices, which are battery-powered or mains-powered, influences the service and application design.

– **Connectivity**: Devices can be considered "always connected" when there is a network connection among any two or more devices. However, due to external factors, such as mobility and device failures, network connectivity can be from "intermittent" to "sporadic".

– **Multi-hop communication**: When there is a network connection among three or more devices, multi-hop communication can be required from a device to another device which is not directly connected, depending on their network topology.
– **Traffic pattern**: Several traffic patterns may be used in point-to-multipoint (P2MP), multipoint-to-point (MP2P) and point-to-point (P2P) manners.
– **Security level**: IoT services and applications may carry sensitive information and require high-level security support where the availability, integrity and confidentiality of the information are crucial.
– **Mobility**: According to the wireless characteristics of IoT services and applications, devices can move or be moved around.
– **Quality of service (QoS)**: Parameters for QoS could consider collective data for latency, packet loss, data throughput and so on. In addition, QoS requirements can be different based on the data delivery model, such as event-driven, query-driven, continuous real-time and continuous non-real-time.

8 Constrained device network architectures

8.1 Network components

Constrained devices having various network interface technologies (e.g., IEEE 802.15.4, Bluetooth low energy, near field communication, etc.) can communicate with each other in IoT environments. However, two or more devices having different network interfaces cannot communicate with each other directly and use a gateway with each of the two different network interfaces to relay data between the two heterogeneous devices. Likewise, network architectures, to which constrained devices belong, can be different from those of legacy networks.

A constrained device network consists of constrained devices, gateways and proxies as follows:

– **Constrained devices**: They have limited processing capability, small memory capability, limited battery power, short range and low bit rate; thus, they use low-energy based network interfaces, such as NFC, BLE, IEEE 802.15.4 and so on for networking.
– **Gateways**: There are two types of gateways in constrained device networks. One type of gateway is a border gateway. The border gateway provides connectivity to a legacy network. The other type of gateway is an intermediate gateway. The intermediate gateway provides connectivity between two different constrained devices, such as a NFC device and a BLE device.

8.2 Network topologies

Constrained device networks have two types of network topologies and they are described as follows:

– **Connected constrained device networks**: Connected constrained device networks are access networks which have connectivity to the legacy network. One of the constrained devices serves as a border gateway for connectivity to the legacy network. In addition, two different connected constrained device networks can be linked with each other by an intermediate gateway.
– **Isolated constrained device networks**: Isolated constrained device networks do not have any connections to the legacy network, but they can have connections to other constrained device networks through intermediate gateways.

8.2.1 Connected constrained device networks

Figure 2 shows an example of three connected networks to which different constrained devices belong.

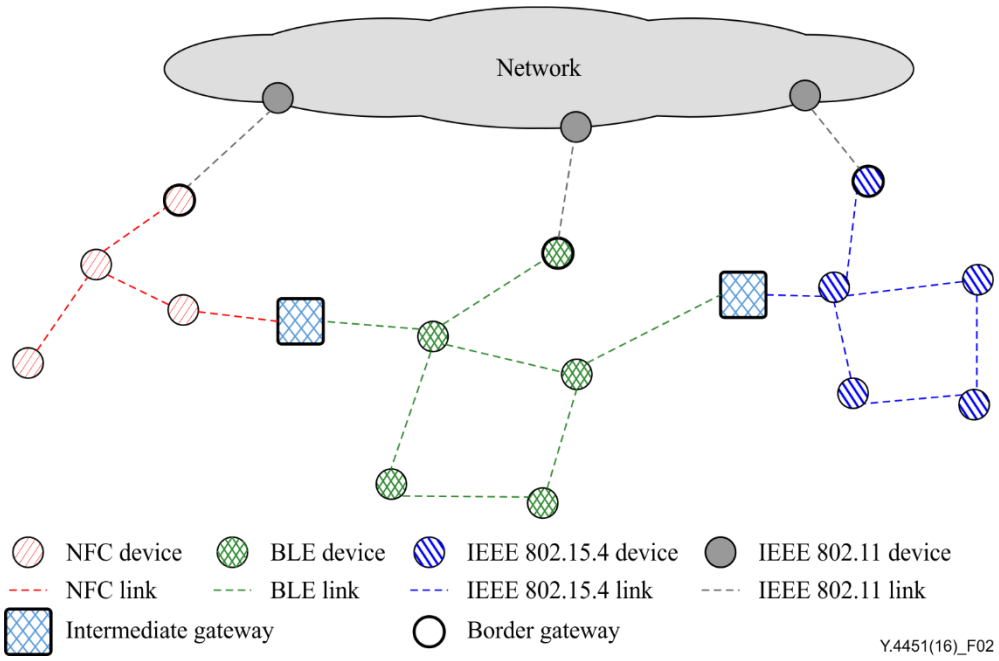

Figure 2 – Connected constrained device networks

Three access networks, such as a NFC device network, a BLE device network and an IEEE 802.15.4 network as well as an IEEE 802.11 legacy network, are connected through border gateways. Furthermore, some heterogeneous devices (e.g., a NFC-enabled device and a Bluetooth device) are indirectly connected via an intermediate gateway having both a NFC interface and a Bluetooth interface. In this case, there are two communication types: one is a communication between two heterogeneous constrained devices and the other is a communication between a constrained device and a non-constrained device.

8.2.2 Isolated constrained device networks

If each access network is not connected to the network, the constrained device networks become isolated networks as shown in Figure 3. In isolated constrained device networks, there are only communications between constrained devices.

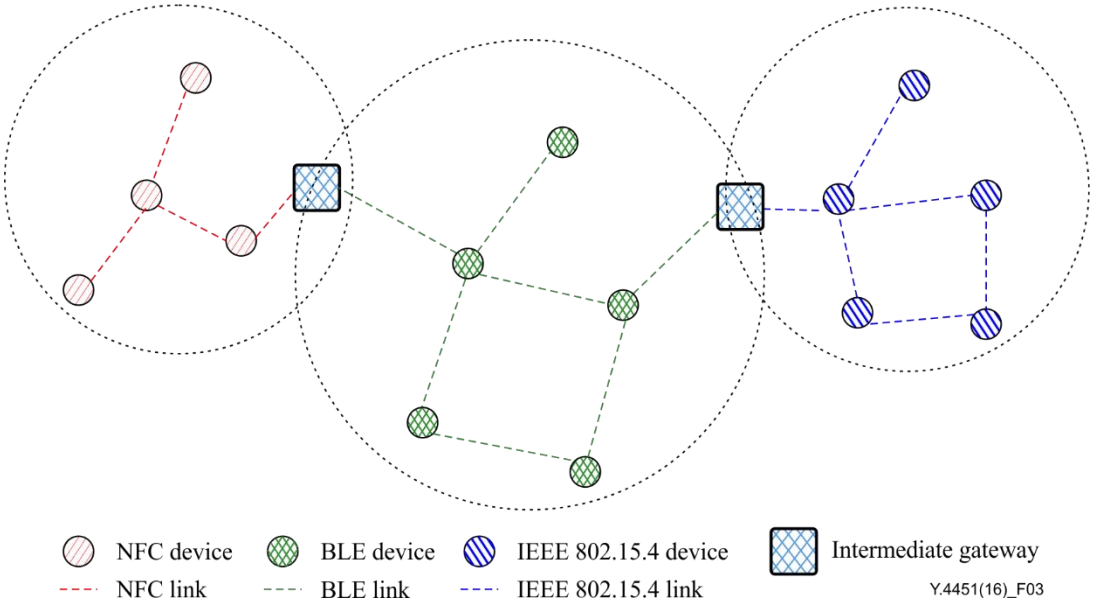

Figure 3 – Isolated constrained device networks

8.3 Protocol stacks for constrained device networking

Low-power network interface technologies (e.g., IEEE 802.15.4, BLE, NFC, etc.) are equipped with constrained devices. Low-power network interface technologies have characteristics that differ from legacy network interfaces such as IEEE 802.11 [b-IEEE 802.11] and IEEE 802.3 [b-IEEE 802.3]. For example, they are specialized for less energy consumption in packet transmission. Therefore, the size of their maximum transmission unit (MTU) is smaller than that of IEEE 802.3 and IEEE 802.11.

For this reason, an "adaptation layer" is required for binding the network layer and the datalink layer of low-power network interfaces. Figure 4 shows protocol stacks for constrained device networking. The adaptation layer supports packet header compression, packet fragmentation and reassembly and network address configurations, etc., for constrained device networking.

These functions are related to network architectures and networking features, so capabilities of the adaptation layer can be included in the network layer in the IoT reference model of [ITU-T Y.4000].

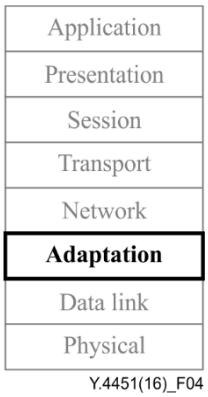

Figure 4 – Protocol stacks for constrained device networking

Figure 5 and Figure 6 describe two types of constrained device networking. Figure 5 shows networking between two heterogeneous constrained devices, where the two heterogeneous constrained devices require an intermediate gateway to communicate with each other. Figure 6 shows networking between a constrained device and a non-constrained device.

Figure 5 shows an example of networking between a NFC device and a BLE device.

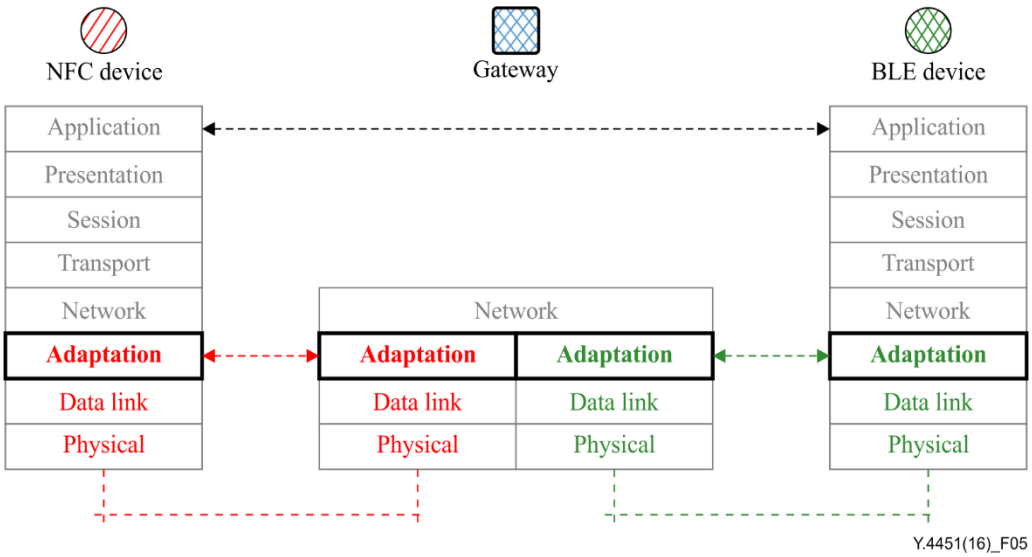

Figure 5 – An example of constrained device networking

The NFC device should be indirectly connected to a Bluetooth device via a gateway that has both a NFC and a Bluetooth interface. Thus, the gateway has two adaptation layers, one for NFC and the other for Bluetooth.

Figure 6 shows an example of the protocol stacks when a constrained device communicates with a non-constrained device in a legacy network. The constrained device belongs to an access network and is indirectly connected to the legacy network through a border gateway.

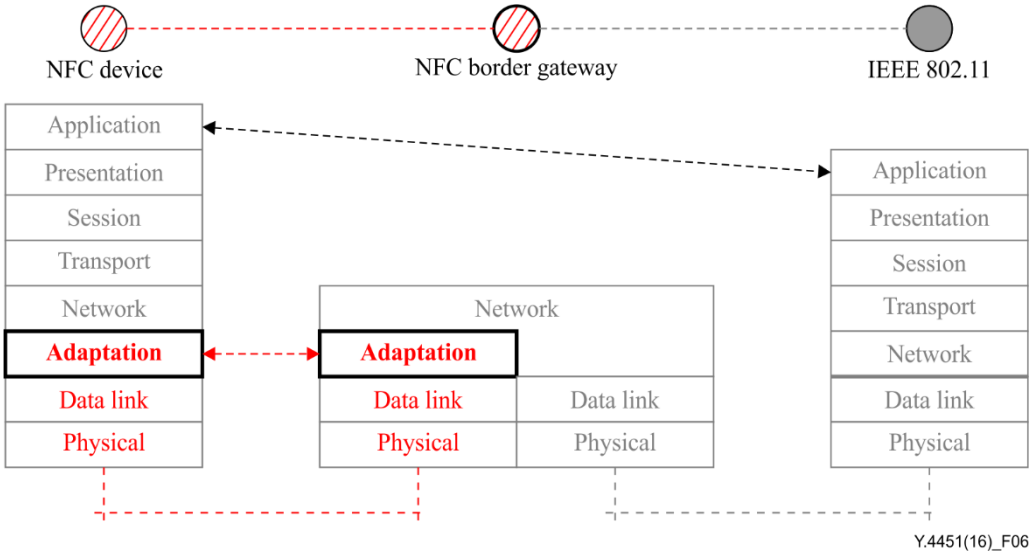

Figure 6 – Example of networking between a constrained device and non-constrained device

9 Functional requirements of constrained device networking

9.1 Fragmentation and reassembly

The MAC/PHY protocol data units may be smaller than upper layer protocol data units. For example, the MTU of IEEE 802.15.4 is 127 bytes, but the minimum IPv6 packet size is 1280 bytes. The upper layer packet should be divided based on the size of lower layer protocol data unit. Then the divided packets, delivered to the destination device, should be reassembled into the original packet for the upper layer protocol [IETF RFC 4944]. Fragmentation and reassembly functions are required on the adaptation layer.

9.2 Header compression

Given that in the worst case the maximum size available for transmitting IP packets over an IEEE 802.15.4 frame is 81 octets, while the IPv6 header is 40 octets long, (without optional headers), this leaves only 41 octets for upper-layer protocols, like UDP and TCP [IETF RFC 4944], [IETF RFC 6282], [IETF RFC 7400], [IETF RFC 5225]. This would lead to excessively fragmented packets. The upper layer headers should be compressed to the minimum in the adaptation layer.

9.3 Address configuration

The adaptation layer is required for the stateless address autoconfiguration method for the network layer [IETF RFC 4944], [IETF RFC 7668], [IETF RFC 7428]. Stateless autoconfiguration [IETF RFC 4862] is effective for the protocol of the adaptation layer, because it reduces the configuration overhead on the constrained devices. There is a need for a method to generate a "network address" assigned to the constrained device. The network address can be generated with link layer identifiers of the constrained devices. Lengths of the link layer identifiers of the constrained devices may not be long enough for network scalability. Therefore, network address generation is required to extend network scalability and avoid address duplication. Annex A describes network scalability in constrained devices.

In addition, when addresses are configured, network stability should be considered due to network connectivity and continuity. In the case that dynamic link layer addresses are used for the generation of network addresses, network sessions can be changed frequently. This would produce a negative effect on network stability. Annex B shows an example of a mechanism for providing stability through network continuity.

9.4 Network management

The adaptation layer is required to address relevant network management solutions based on the resource constraints as well as the minimal configuration and self-healing functionality. The existing network management protocol (e.g., SNMP) can be widely used for monitoring data sources and sensors in conventional networks. However, network management protocol should be designed for the resource constraints, such as the memory, processing and message size constraints.

9.5 Higher layer considerations

The networking performance also depends on the efficiency of application layer protocols. Heavyweight protocols may not be suitable for constrained devices. More compact higher layer protocols (e.g., at the application layer) may be required.

9.6 Multi-hop routing protocol

Support of multi-hop routing protocol [IETF RFC 6550] is required. There are many existing multi-hop routing protocols, but these protocols are designed to use IP-based addresses with large overheads. For example, some routing protocol uses 48 octets for a route request based on IPv6 addressing. It is hard to use this routing protocol in constrained device networking.

10 Security considerations

In constrained device networking, address configurations in the adaptation layer may have security issues, especially when generating network addresses by using link layer identifiers. Various security threats such as correlation of protocol over time, location tracking, device-specific vulnerability exploitation and address scanning may exist [IETF RFC 7721]. These threats should be mitigated.

Annex A

Network scalability in constrained devices

(This annex forms an integral part of this Recommendation.)

Constrained devices, which are based on low-power link layer technologies, such as Z-Wave [ITU-T G.9959], LoBAC (MS/TP), NFC, etc., use short addresses for node identifiers. This node identifier is used for a link layer address. For instance, NFC devices have a node identifier (i.e., SSAP) of 6 bits as shown in Figure A.1 and MS/TP devices have 8 bits. Such short length node identifiers can result in a scalability problem of the local network topology.

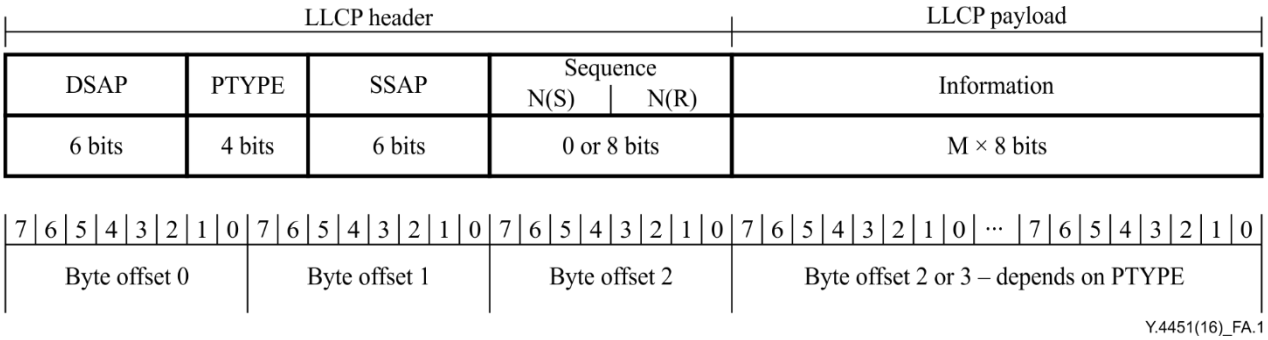

Figure A.1 – Format of I PDU in NFC [b-LLCP1.1]

In an instance of NFC link layer, the maximum number of network device addresses using a node identifier length of 6 bits is 2^6. In other words, a local network of NFC can consist of 2^6 devices at the most. Furthermore, the node identifier or source service access point (SSAP) is not a permanent physical value but temporary logical value. When two NFC devices make a connection, their SSAP values are created. As shown in Figure A.2, if 2^6+n devices belong to a local network, the n devices can have redundant addresses. NFC link layer does not support mesh-under. This means redundant addresses can be created in not only the link layer but also in the network layer. This can result in a network scalability problem of constrained device networks.

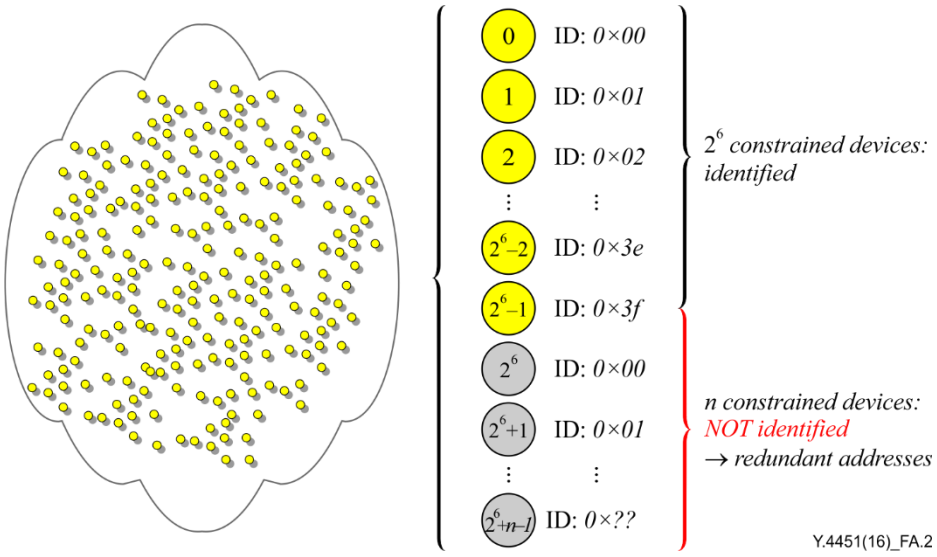

Figure A.2 – Network scalability problem of a constrained device network

The solutions required to support two kinds of mechanisms are as follows:

– Mechanisms for extending the limited network addresses

– Mechanisms for avoiding network address duplication.

NOTE – As one of possible mechanisms to extend the limited network address, there is an example method, which is applicable for various network schemes (e.g., IPv6), for redefining the short node identifier. The method comprises evenly defining two parts of the node identifier. The first part and the second part in the node identifier are located into a network address identifier. The network address identifier is also evenly separated into two parts with a predefined value. The first part of the node identifier is assigned to the first part of network address identifier and the second part of the node identifier is assigned to the second part of network address identifier. According to the network connecting condition of a communication device, one of the two parts of the network address identifier can additionally correspond to the other value except when assigning one of the parts of the node identifier for address duplication avoidance. Likewise, the new created network address identifier can be used for supporting extended size of a local constrained device network.

Annex B

Mechanism for providing network stability through IP continuity of NFC devices in the Internet

(This annex forms an integral part of this Recommendation.)

NFC devices have an extremely short radio range (i.e., 10cm), so they use a single-touch based approach to communicate between two devices. Every single-touch has a different network connection. Thus, Internet connection between them is also extremely short and can be unstable. Owing to such a physical constraint of NFC devices, mechanisms for providing network stability are required. Figure B.1 shows networking between two NFC devices based on the Internet as an example.

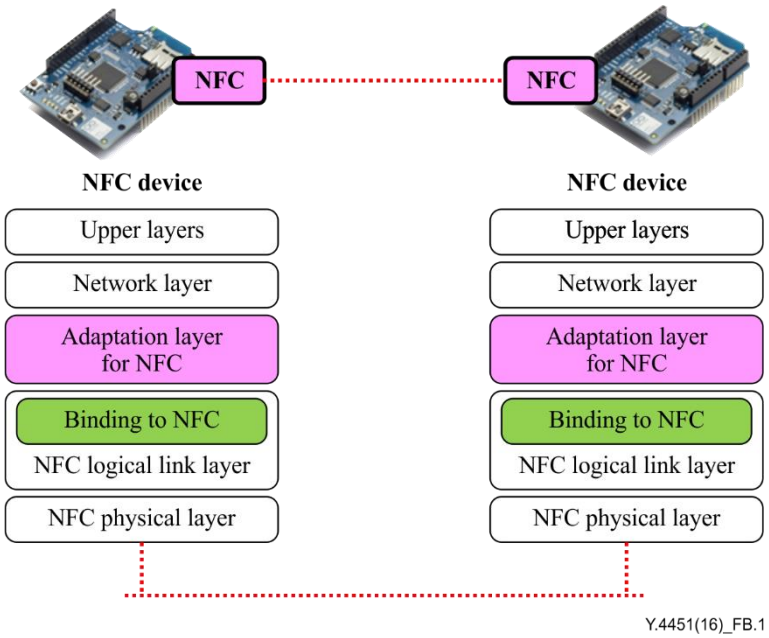

Figure B.1 – Example of networking between two NFC devices based on the Internet

To guarantee network stability through IP continuity, a cooperative mechanism of the adaptation layer for NFC and a "Binding to NFC" function of the NFC logical link layer are required. The binding to NFC function has the following operations:

– Binding logical link layer address of the NFC to the adaptation layer

– Caching logical link layer address for network connection

In addition, each of the adaptation layers for NFC and binding to NFC requires an algorithm as shown in Figure B.2 and Figure B.3.

– Adaptation layer for NFC

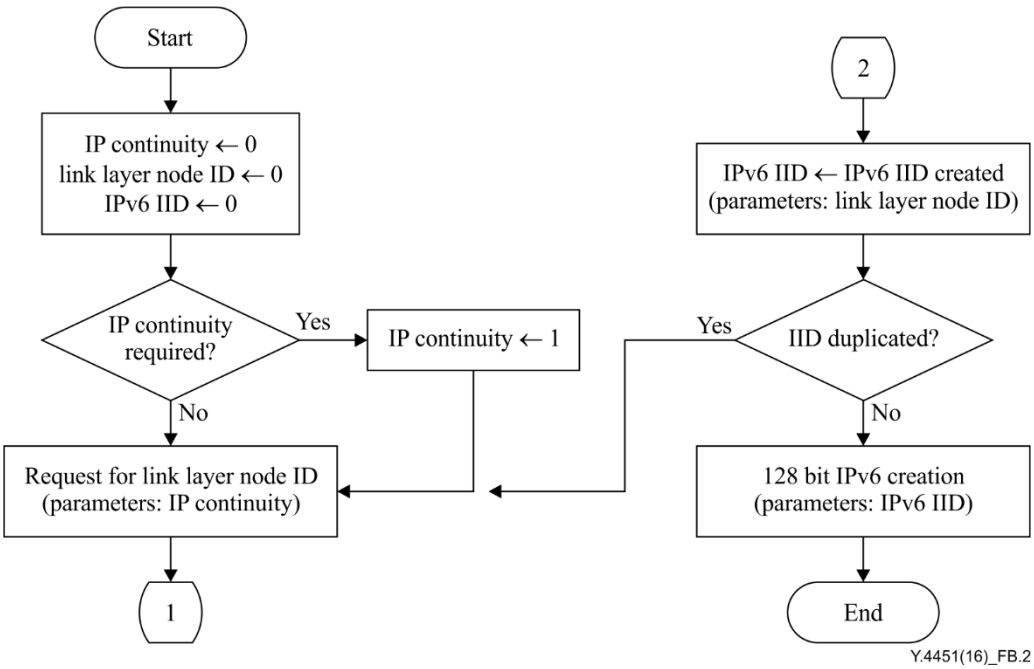

Figure B.2 – **Algorithm for requesting link layer node ID for IP continuity**

As a starting point, the adaptation layer for NFC checks whether IP continuity is required or not and then the result of IP continuity is delivered to binding to NFC.

– Binding to NFC

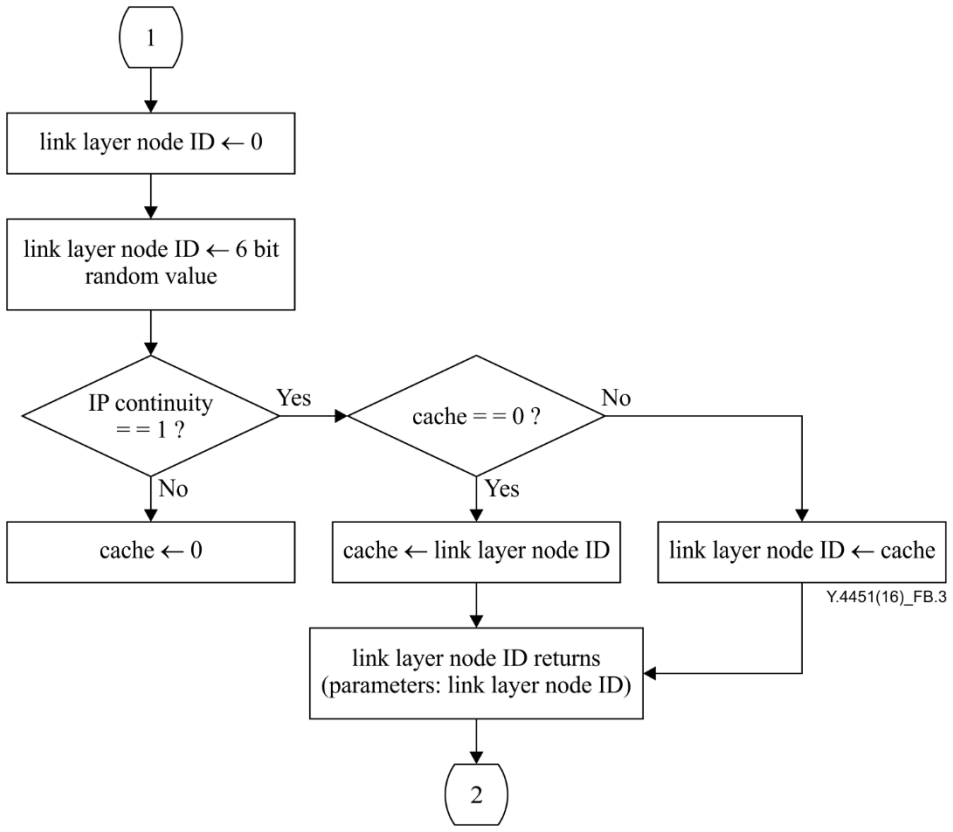

Figure B.3 – Algorithm for creating link layer node ID for IP continuity

If IP continuity is required, binding to NFC returns a link layer node ID which is stored in cache. If the cache is empty, a new link layer node ID is created and stored in cache and is returned to the adaptation layer for NFC. When IP continuity is not required, the cache becomes empty and a newly created link layer node ID is just returned to the adaptation layer for NFC.

Bibliography

[b-ITU Report] ITU Internet Reports (2005), *The Internet of Things.* http://www.itu.int/osg/spu/publications/internetofthings/

[b-IEEE 802.3] IEEE Std. 802.3 (2012), *IEEE Standard for Ethernet.* https://standards.ieee.org/findstds/standard/802.3-2012.html

[b-IEEE 802.11] IEEE Std. 802.11 (2012), *IEEE Standard for Information technology – Telecommunications and information exchange between systems Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* https://standards.ieee.org/findstds/standard/802.11-2012.html

[b-IEEE 802.15.4] IEEE Std. 802.15.4 (2006), *IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs).* https://standards.ieee.org/findstds/standard/802.15.4-2006.html

[b-LLCP1.1] NFC Forum Technical Specification (2011), *Logical Link Control Protocol version 1.1*. http://members.nfc-forum.org/specs/spec_list/#llcp

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