

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Multimedia home networks – Home network communication protocol over IP for multimedia household appliances

Réseaux résidentiels multimédia – Protocole de communication de réseau résidentiel sur IP destiné aux appareils domestiques multimédia

IECNORM.COM : Click to view the full PDF of IEC 62457:2007



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2007 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,...).

It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,...).

Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications de la CEI. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Multimedia home networks – Home network communication protocol over IP for multimedia household appliances

Réseaux résidentiels multimédia – Protocole de communication de réseau résidentiel sur IP destiné aux appareils domestiques multimédia

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

XB

ICS 30.040; 33.160.01

ISBN 978-2-83220-318-7

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

FOREWORD.....	6
INTRODUCTION.....	8
1 Scope.....	10
2 Normative reference	11
3 Terms, definitions and abbreviations	11
3.1 Terms and definitions	11
3.2 Abbreviations	15
4 TCP/IP interface and requirements	15
4.1 Overview	15
4.2 Topology	16
4.3 UDP interface.....	19
4.4 Packet format of Home Network frame	19
4.4.1 General	19
4.4.2 Home Network transmission frame transfer	21
4.4.3 MAC/IP address resolution request/response.....	22
4.4.4 IP/MAC address resolution request/response	23
4.4.5 Hardware/MAC address resolution request/response.....	24
4.4.6 MAC address initialization request/response	25
4.4.7 MAC address server initialization response/MAC address allocation response	26
4.4.8 MAC address confirmation request/response	27
4.4.9 MAC address request to all nodes/response	28
4.4.10 MAC address server detection request/response, MAC address server notification.....	29
4.4.11 Network control message (destination invalid)	30
4.4.12 Network control message (NMa overlap)	31
4.5 Basic communication sequences.....	32
4.5.1 General.....	32
4.5.2 MAC/IP address resolution request/response (resolution of the NMa into the IP address)	32
4.5.3 IP/MAC address resolution request/response (resolution of IP address into NMa)	33
4.5.4 Hardware/MAC address resolution request/response.....	35
4.5.5 MAC address request/response to all nodes	36
4.5.6 Network control message (destination invalid)	37
4.5.7 Special case pertaining to packets with invalid destination values	38
4.5.8 Network control message (NMa overlap)	39
4.6 NMa acquisition booting sequence	40
4.6.1 Overview of NMa acquisition booting sequence	40
4.6.2 Overview of the processing after acquisition of IP Address	40
4.6.3 Booting node	41
4.6.4 MAC address server	45
4.6.5 Operating nodes	45
4.7 MAC address server.....	47
4.7.1 Requirement of MAC address server	47
4.7.2 Processing sequence for MAC address server booting	47

4.7.3	Processing by operating MAC address server	48
4.8	Time period parameters	50
4.9	Provision for updating data after NMa acquisition	51
5	TCP/IP and requirements	51
5.1	IP	51
5.1.1	Protocols to be used	51
5.1.2	IP Address	51
5.1.3	Multicast address	51
5.1.4	DHCP	51
5.1.5	Method for obtaining IP Address by manual setting, etc.	52
5.1.6	Routing	52
5.2	UDP	52
5.2.1	Protocols to be used	52
5.2.2	Port Number	52
6	Lower-layer medium-specific interface and requirements	52
6.1	Interface and requirements on lower-layer medium	52
6.2	Software internal status transition	52
6.2.1	Overview	52
6.2.2	Stop status	54
6.2.3	Cold start status	54
6.2.4	Warm start status	55
6.2.5	Communication suspension status	55
6.2.6	Normal operation status	56
6.2.7	Error stop status	57
6.2.8	Temporary stop status	58
Annex A (informative)	Basic booting sequence	59
Annex B (informative)	Basic MAC address server booting sequence	66
Annex C (normative)	Requirements on IEEE 802.15.1	68
Bibliography		74
Figure 1	– Grouping of relationship between household appliances and audiovisual equipment, PCs and PC-related equipment	9
Figure 2	– Examples of data communication between household appliance and audiovisual equipment, PCs and PC-related equipment	9
Figure 3	– The composition of the Home Network layer and the specified portions	10
Figure 4	– Encapsulation of Home Network frame	16
Figure 5	– Example of a subnet using Layer 2 bridges	17
Figure 6	– Example of a subnet connection using Home Network routers	17
Figure 7	– Relationship between IP subnet and Home Network subnet	18
Figure 8	– Home Network frame packet format	19
Figure 9	– Notation for bits in the flag field	21
Figure 10	– IEEE 802.15.1 Address described in bits	21
Figure 11	– Basic MAC/IP address resolution sequence	33
Figure 12	– Basic IP/MAC address resolution sequence	34

Figure 13 – Basic Hardware/MAC address resolution sequence.....	35
Figure 14 – Basic “MAC address request/response to all nodes” sequence.....	37
Figure 15 – Basic “destination invalid” processing sequence.....	38
Figure 16 – Basic sequence for handling detected NMa overlap	39
Figure 17 – Flowchart for determining provisional NMa to be used.....	42
Figure 18 – Check for NMAs in use by other nodes	43
Figure 19 – Example of duplicated provisional NMa	44
Figure 20 – Format for UsedMAC.....	46
Figure 21 – Example of UsedMAC	46
Figure 22 – Internal software status transitions	53
Figure A.1 – A-MODE booting, NMAs not retained (with MAC address server)	60
Figure A.2 – SR-MODE booting, NMAs not retained (with MAC address server).....	61
Figure A.3 – A-MODE booting, NMAs not retained (without MAC address server)	62
Figure A.4 – SR-MODE booting, NMAs not retained (without MAC address server).....	63
Figure A.5 – A-MODE booting, NMAs retained (with MAC address server)	64
Figure A.6 – A-MODE booting, NMAs retained (without MAC address server)	65
Figure B.1 – Booting of a single MAC address server	66
Figure B.2 – Near-simultaneous booting of two or more MAC address servers.....	67
Figure C.1 – Layer structure	68
Figure C.2 – Basic form of subnet.....	69
Figure C.3 – Example of a subnet connection using Home Network routers	69
Figure C.4 – Example of an unacceptable subnet connection (scatternet).....	70
Figure C.5 – Example of a connection using a home network gateway.....	70
Figure C.6 – Example of a subnet using Layer 2 bridges.....	71
Figure C.7 – Examples of Home Network communication software implementation	72
Figure C.8 – Packet structure	73
Table 1 – Packet type numbers of the Home Network frame	20
Table 2 – Hardware type.....	20
Table 3 – Format for “Home Network transmission frame transfer” packets.....	22
Table 4 – Format for “MAC/IP address resolution request” packets	22
Table 5 – Format for “MAC/IP address resolution response” packets	23
Table 6 – Format for “IP/MAC address resolution request” packets	23
Table 7 – Format for “IP/MAC address resolution response” packets	24
Table 8 – Format for “hardware/MAC address resolution request” packets.....	24
Table 9 – Format for “hardware/MAC address resolution response” packets	25
Table 10 – Format for “MAC address initialization request” packets	26
Table 11 – Format for “MAC address initialization response” packets	26
Table 12 – Format for “MAC address server initialization response” packets.....	27
Table 13 – Format for “MAC address allocation response” packets	27
Table 14 – Format for “MAC address confirmation request” packets	28
Table 15 – Format for “MAC address confirmation response” packets.....	28
Table 16 – Format for “ MAC address request to all nodes” packets.....	28

Table 17 – Format for “MAC address response to all nodes” packets	29
Table 18 – Format for “MAC address server detection request” packets	29
Table 19 – Format for “MAC address server notification” packets	30
Table 20 – Format for “MAC address server detection response” packets	30
Table 21 – Format for “network control message (destination invalid)” packets	31
Table 22 – Format for “NMa overlap” network control message packets	31
Table 23 – Address Relation table	32
Table 24 – Booting modes	40
Table 25 – Sample for storing allocated NMas	48
Table 26 – Time period parameters	50

IECNORM.COM : Click to view the full PDF of IEC 62457:2007

INTERNATIONAL ELECTROTECHNICAL COMMISSION

MULTIMEDIA HOME NETWORKS – HOME NETWORK COMMUNICATION PROTOCOL OVER IP FOR MULTIMEDIA HOUSEHOLD APPLIANCES

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62457 has been prepared by technical area 9: Audio, video and multimedia applications for end-user network, of IEC technical committee 100: Audio, video and multimedia systems and equipment.

This bilingual version (2012-10) corresponds to the monolingual English version, published in 2007-09.

The text of this standard is based on the following documents:

CDV	Report on voting
100/1197/CDV	100/1271/RVC

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

The French version of this standard has not been voted upon.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

IECNORM.COM : Click to view the full PDF of IEC 62457:2007

INTRODUCTION

By enabling standalone-type household appliances (household appliances other than audiovisual equipment, PCs and PC-related equipment) such as white appliances (e.g. air conditioners, refrigerators), sensors, health, exercise and fitness equipment to connect to and work in conjunction with audiovisual equipment, PCs and/or PC-related equipment, it becomes possible to deliver multimedia application services, such as displaying a “washing completed” message of a washing machine on a TV screen or operating an air conditioner via a TV screen, that otherwise would not be possible (see Figure 1).

To achieve these services, a home network standard for networks of standalone-type household appliances and network standards for audiovisual equipment, PCs and PC-related equipment are needed. It is also necessary to establish a system that allows equipment belonging to a network to exchange data with other equipment of different types of networks. A commonly used approach to allow networks of different types to exchange data with each other is to use Gateways.

Because data transferred within, into and out of networks of standalone-type household appliances are control data, which are much smaller in volume than data similarly transferred for networks of audiovisual equipment, PCs and PC-related equipment, and because standalone-type household appliances have longer service lives than audiovisual equipment, PCs and PC-related equipment, home network standards for networks of standalone-type household appliances have been established separately from network standards for audiovisual equipment, PCs and PC-related equipment, and many different protocol standards have been in use for a long time in different countries¹.

On the other hand, recent advances in device and software technology have made it possible to implement TCP/IP (which has been adopted worldwide for audiovisual equipment, PCs and PC-related equipment) in certain standalone-type household appliances, and so establishing a home network standard for networks of standalone-type household appliances in the form of a standard for layers above TCP/IP would allow data to be directly exchanged between household appliances and audiovisual equipment, PCs and PC-related equipment via TCP/IP (see Figure 2 example1, example2). In turn, this would allow the creation of multimedia application services that enable household appliances to work in conjunction with audiovisual equipment, PCs and PC-related equipment.

The advantages of applying this standard are:

- it can be applied to many types of Home Network standards.
- both Home Network nodes with TCP/IP Layer and without can coexist under the same Home Network middleware.
- Household appliances can communicate with audiovisual equipment, PCs and PC-related equipment, and vice versa, without requiring any gateway.
- Household appliances can handle text and audiovisual data.
- Audiovisual equipment, PCs and PC-related equipment can handle Household appliances data.
- Household appliances can freely select a suitable lower-layer medium from various lower-layer media below TCP/IP.

¹ CEBus, ECHONET, Konnex, LonTalk, others.

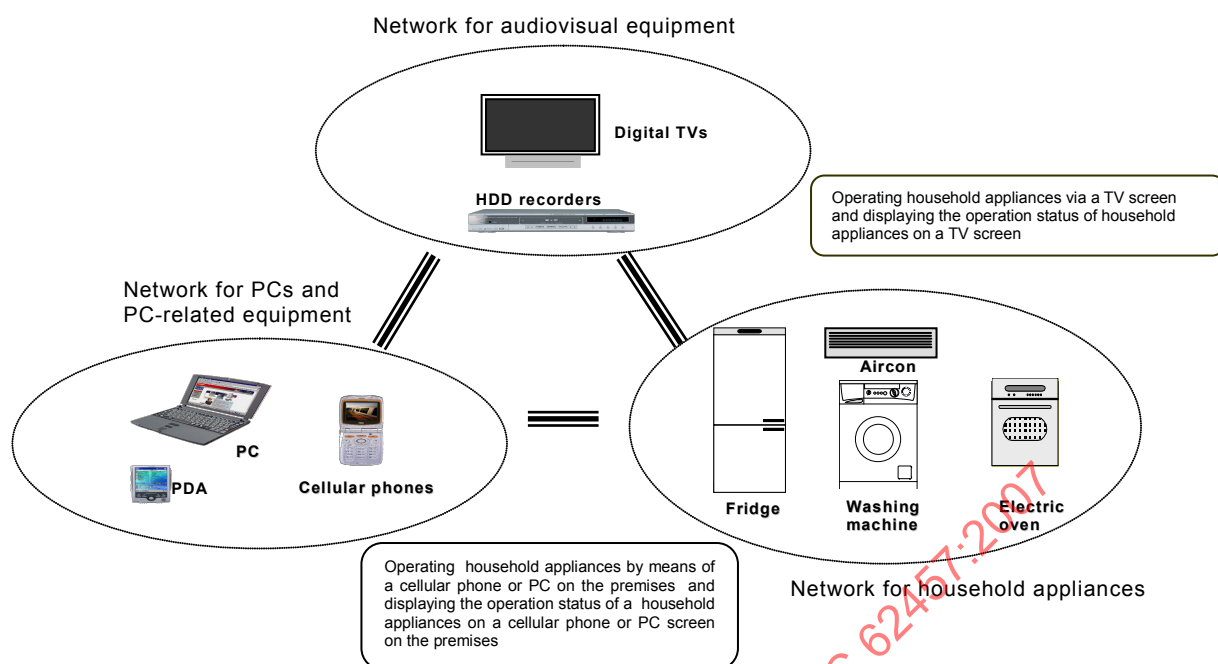


Figure 1 – Grouping of relationship between household appliances and audiovisual equipment, PCs and PC-related equipment

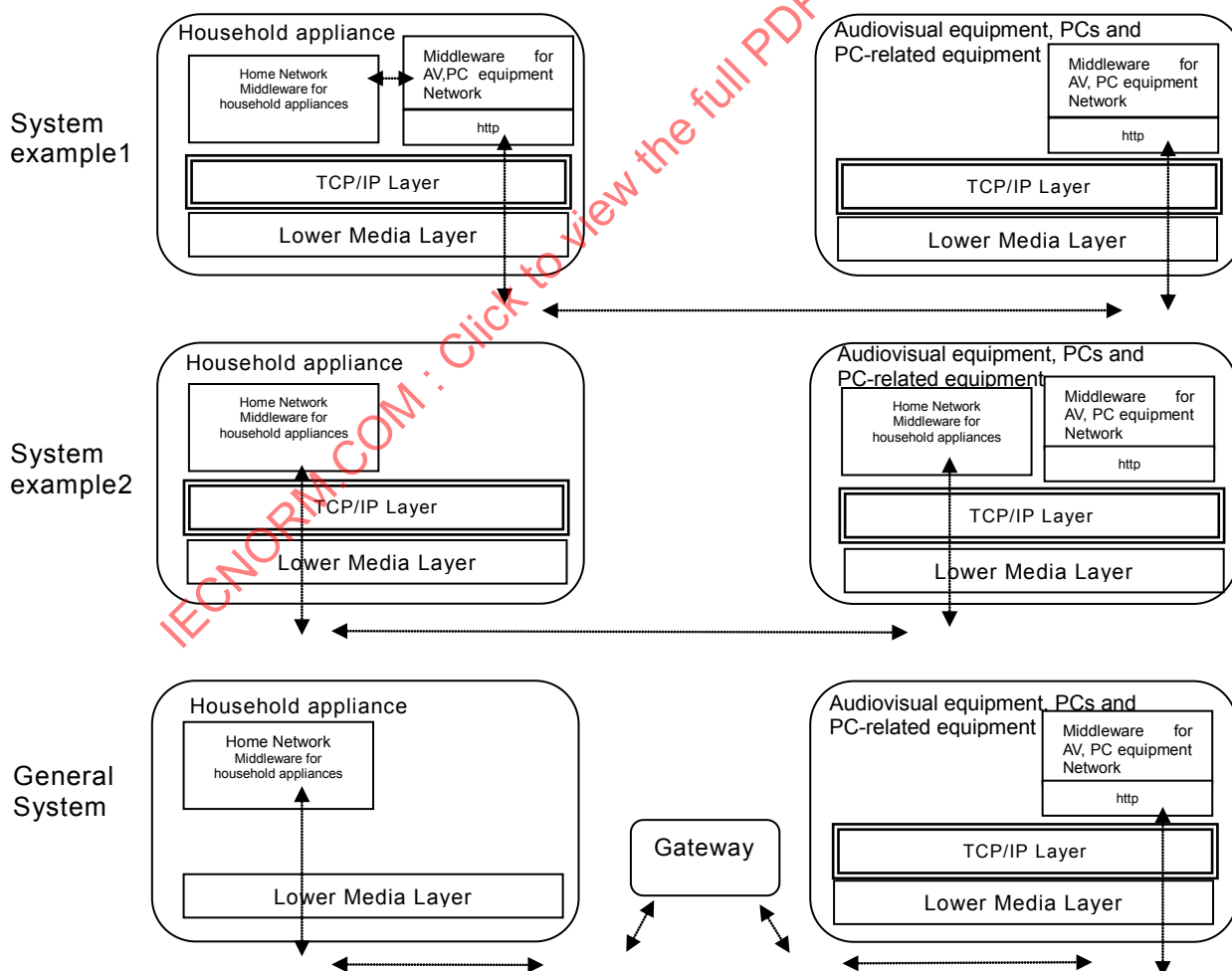
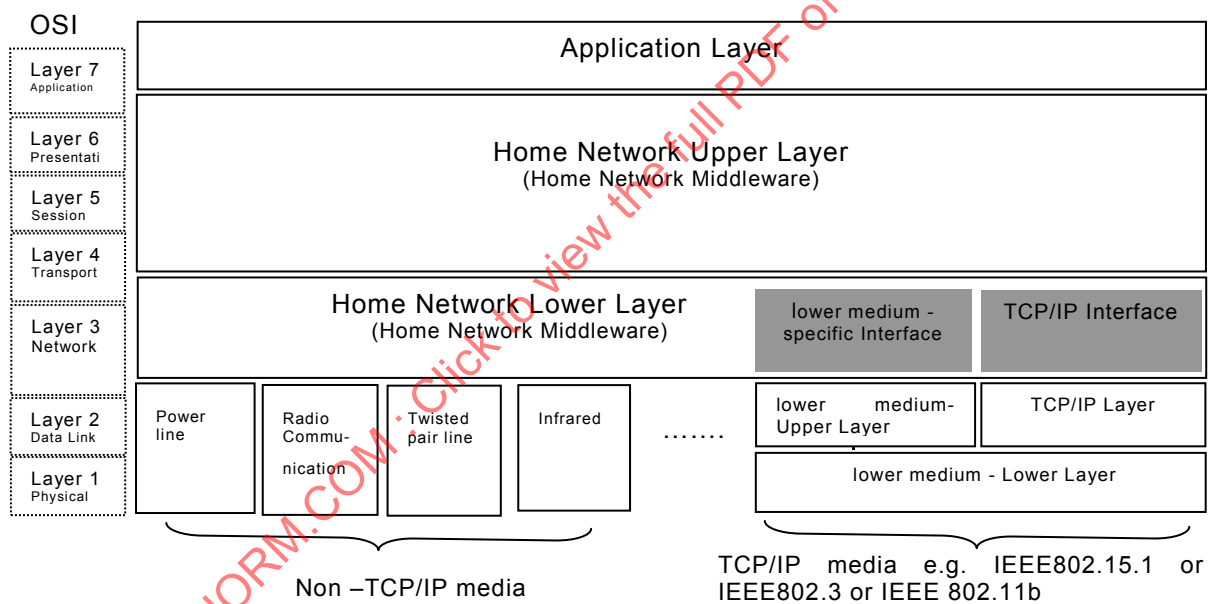


Figure 2 – Examples of data communication between household appliance and audiovisual equipment, PCs and PC-related equipment

MULTIMEDIA HOME NETWORKS – HOME NETWORK COMMUNICATION PROTOCOL OVER IP FOR MULTIMEDIA HOUSEHOLD APPLIANCES

1 Scope

This International Standard specifies the requirements for the interface between the Home Network Lower Layer for a country's home network of standalone-type household appliances and the TCP/IP Layer for cases where it is intended to introduce a TCP/IP Layer to each of the nodes comprising such home network of standalone-type household appliances. The specified interface in the Home Network Lower Layer consists of 2 portions, the TCP/IP Interface and the lower medium-specific Interface. Figure 3 shows the composition of the Home Network Layer and the standardized portions. In Annex C, this standard specifies the requirements for the lower medium-specific Interface One of these layers shall be IEEE 802.15.1, short-distance radio standard additional layers can be added in the future).



NOTE 1 Grey coloured portions are standardized.

NOTE 2 TCP/IP Interface is the same even if the lower medium is different, however the lower medium-specific Interface is different.

NOTE 3 Home Network Lower Layer and Home Network Upper Layer are prepared for CEBus, ECHONET, Konnex, LonTalk, others respectively.

NOTE 4 Each OSI Layer is roughly mapped to each Home Network Layer.

Figure 3 – The composition of the Home Network layer and the specified portions

2 Normative reference

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEEE Std 802.15.1-2005, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs)*

3 Terms, definitions and abbreviations

For the purposes of this document, the following terms and definitions apply.

3.1 Terms and definitions

3.1.1

Bluetooth

wireless technology that is a worldwide specification for a small-form factor, low-cost radio solution providing links between mobile computers, mobile phones, other portable handheld devices, and connectivity to the Internet

NOTE The specification is developed, published and promoted by the Bluetooth Special Interest Group (SIG). Main specifications are adopted as IEEE Std 802.15.1. In this standard, Bluetooth means IEEE 802.15.1.

3.1.2

Bluetooth Network Encapsulation Protocol BNEP

protocol specified in Bluetooth. IP packet is encapsulated according to this protocol

3.1.3

cold start

method for starting the Home Network node by starting initial setting processing while abandoning previous information related to network addresses

3.1.4

Group ad-hoc Networks GN

Piconet which comprises a master and a slave as defined in IEEE 802.15.1 and which is not connected to any outside network or node

3.1.5

Hardware address Ha

address based on a medium-specific addressing scheme

3.1.6

Home Network

generic name for various equipment-type Home Network standards mainly for household appliances

NOTE Specifically, it refers to CEBus, Konnex, ECHONET, LonTalk, etc.

3.1.7

Home Network device

a home device, home electric product, or building/store device, such as lighting, air conditioning, refrigeration, power equipment, ordinary home appliances, sensors, actuators, etc.

NOTE A Home Network node provided with a communication interface and system compatible function conforming to the Home Network standard. A Home Network node provided with a controller function for the centralized control unit with functions to monitor, control, and operate them or an operating unit (remote control, etc.).

3.1.8

Home Network domain

a range on the network within which information transmission is logically guaranteed by the Home Network

NOTE Property and security control, including homes and stores, are generally thought to use the same range as a domain, but the domain is not limited by any standard.

3.1.9

Home Network frame

frame which is generated in the Home Network lower layer as specified in this standard; the frame consists of a Home Network transmission frame or an associated managing packet

3.1.10

Home Network gateway

a Home Network node which connects a home network domain to an external system (including other Home Network domains)

NOTE Multiple Home Network gateways may exist in the domain depending on differences in the external system(s) to be connected.

3.1.11

Home Network lower-layer

interface between Home Network upper layer and the lower medium upper-layer

NOTE Some parts depend on the medium characteristics. This standard is contained in this layer. This layer mainly consists of OSI Layer 3, 4, and 2.

3.1.12

Home Network master router

a router that acquires a Net ID at the time of initialization and stores it; there is one Home Network master router in each Home Network subnet

3.1.13

Home Network node

communication node conforming to a Home Network standard, referred to as “node” herein unless otherwise specified

NOTE In a Home Network, a Home Network node is a Home Network communication function which is uniquely identified by a Network address. There is no distinction between the application functions of nodes. The term node is used to describe the function of one communication terminal of the Home Network.

3.1.14

Home Network router

a Home Network node used to connect Home Network subnets

NOTE A Home Network router connects the subnets of different lower-layer communication protocols (for different protocols, regardless of transmission media type) or divides the same protocol into subnets. The lower-layer communication protocol is connected seamlessly on the system using routing processing based on Network addresses as a function.

3.1.15

Home Network subnet

a group of nodes in the Home Network domain, using the same media or different media connected by layer 2 bridges, referred to as a “subnet” herein unless otherwise specified

NOTE Each subnet has a Net ID. Different subnets can be connected by a Home Network router.

3.1.16**Home Network transmission frame**

frame that is generated in the Home Network upper layer and transmitted between nodes via the Home Network lower layer

NOTE Each Home Network has its own frame format, but a Home Network transmission frame normally contains headers, address information, acquisition and setting information for other nodes.

3.1.17**Home Network upper layer**

processing block of the Home Network communication middleware

NOTE The Home Network upper layer performs the communication protocol processing to simplify the processing performed when the application software remotely controls or monitors devices, stores the information necessary for that purpose, and manages various pieces of information including that on the status of the device itself and of other devices. This layer mainly consists of OSI Layers 4, 5, 6, and 7.

3.1.18**IPme****IP multicast address**

this address is used for IP multicasting. The specific number is assigned to this standard

3.1.19**layer 2 bridge**

device used to store and transfer packets

NOTE Layer 2 bridges cover up to OSI Layer 2 (the data link layer). Layer 2 bridges are classified into several types by function including transparent bridges that discard or transfer packets based on MAC address values, converter bridges that perform MAC header conversions and source routing bridges with the additional capability to handle destination path information. Layer 2 bridges are defined in IEEE Std 802.1D.

3.1.20**MAC address server**

server which allocates Network MAC addresses in a subnet

3.1.21**net ID**

a subnet identifier; it is also a component of a Network address

3.1.22**Network Access Points****NAP**

an access point connected to the Internet which acts as a IEEE 802.15.1 master. IEEE 802.15.1 slaves are connected to a IEEE 802.15.1 master to form a Piconet and thus are connected to the Internet

3.1.23**Network address****Na**

an address permitting unique identification of a Home Network node in the domain

NOTE This address enables the Home Network communication processing block and the application software to disregard differences in the lower-layer communication software. A Network address is a logical address that is defined separately from the Hardware address to lower-layer communication software; it consists of at least a Net ID and a Node ID.

3.1.24**Network MAC address****NMa**

a unique Home Network lower layer address that allows Layer 2 communication (transmission medium) to be performed

NOTE This address for each Home Network node is uniquely assigned in the Home Network subnet by the Home Network lower layer of the Home Network node itself or MAC address server.

3.1.25

node ID

an identifier used to identify a Home Network node uniquely within the Home Network subnet.

NOTE A node ID is a logical address converted from the NMa by the Home Network upper layer. This is a component of a Network address.

3.1.26

park mode

a low power consumption mode defined in the IEEE 802.15.1 specification

NOTE Upon entry into this mode, two different addresses are given by the master and synchronization is maintained thereafter by periodic beacon pulses from the master. While in Park mode, a negotiation to cancel Park mode can be made within the preset window period.

3.1.27

Personal Area Networking Profile

PAN

specified in Bluetooth

NOTE This profile is for IP communication over IEEE 802.15.1. IP Packet is encapsulated by BNEP and behaves like Ethernet networking.

3.1.28

Personal Area Networking Profile User

PANU

slave nodes specified in Personal Area Networking

3.1.29

Piconet

a network that has a single master and two or more slaves as specified in the IEEE 802.15.1.

3.1.30

profile

profiles specify Bluetooth communication functions and protocol requirements by purpose to maintain interconnectivity

NOTE In the Bluetooth specification version 1.1, Generic Access Profile, Serial Port Profile, etc. are defined.

3.1.31

scatternet

network that looks like two or more Piconets connected together because of the “time-series” manner in which a node belongs to one of the two or more Piconets

3.1.32

Service Discovery Protocol

SDP

upon establishment of a link between two nodes, this protocol (which is defined in IEEE 802.15.1) is used to acquire service records (service class, protocol, etc.) held by the nodes

3.1.33

warm start

method of starting the Home Network node by starting initial setting processing while keeping previous Network addresses and initial setting information

3.2 Abbreviations

BNEP	Bluetooth Network Encapsulation Protocol
DHCP	Dynamic Host Configuration Protocol
GN	Group Ad-hoc Networks
Ha	Hardware address
IP	Internet Protocol
Ipme	IP multicast address
LSB	the Least Significant Bit
MAC	Media Access Control
MSB	the Most Significant Bit
Na	Network Address
NAP	Network Access Point
Nma	Network MAC address
OSI	Open System Interface
PAN	Personal Area Networking Profile
PANU	Personal Area Networking Profile User
SDP	Service Discovery Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

4 TCP/IP interface and requirements

4.1 Overview

When introducing lower layer media into Home Networks, some Home Networks require a definition on an Internet Protocol (IP) network whereas others do not; the selection should be made according to the application requirements. This standard provides International Standards for protocols that operate on IP. In the case where Home Networks operate in an IP network, each Home Network subnet is mapped onto an IP subnet and the Home Network frames (Home Network transmission frames or associated control packets) are encapsulated into IP packets and transferred over the IP network (see Figure 4). IP networks are classified into IPv4 and IPv6 networks; this standard uses IPv4. Each Home Network node shall have an IP address, which shall be either a unique global IP address or a private IP address, in addition to a Hardware address. Although this standard does not specify a method for acquiring IP addresses, the operation of a node as a Home Network node is premised on the acquisition of an IP address. The IP network transfer protocol used to transfer a Home Network frame shall be the connectionless User Datagram Protocol (UDP). When transferring a Home Network frame, the UDP shall permanently use the port number specified in this standard. Each Home Network frame is encapsulated into one UDP packet. Each Home Network node shall also have a Network Address (Na) in the Home Network Upper Layer and Network MAC address (NMa) in the Home Network Lower Layer, in addition to the IP address. For destination addresses and sender addresses for Home Network transmission frames, Na shall be used. For destination addresses and sender addresses for Home Network frames, for IP headers, IP addresses shall be used. All Home Network nodes operating on an IP subnet shall be capable of using the IP multicast addresses assigned for the Home Network. A Home Network frame to be broadcast or group-broadcast is mapped onto IP multicast packets addressed to the specified IP multicast address. Because there are many media other than IEEE 802.15.1, IEEE 802.3, etc. that have been defined as lower layer media, they have their own layer structures, functions, addressing schemes and topologies. This standard also defines interfaces as medium-specific interfaces that are separated from the TCP/IP interface.

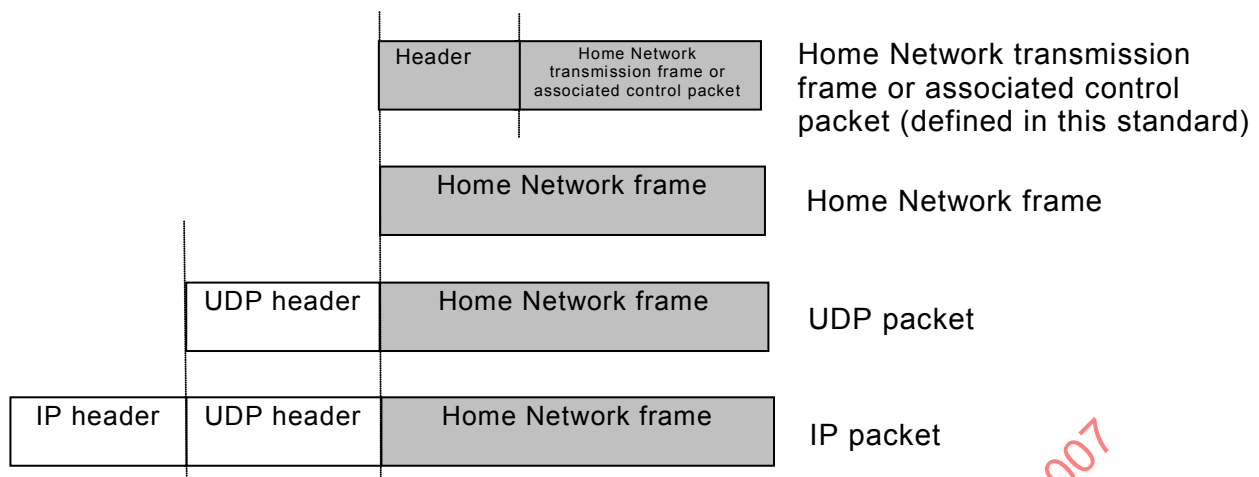


Figure 4 – Encapsulation of Home Network frame

NMa Acquisition Booting Sequence is specified in this standard. Each Home Network node has a unique Na which is held by the Home Network upper layer to allow the node to be identified regardless of the types of media or with IP or with non-IP. Each of the components of a Na corresponds uniquely to a NMa set by the Home Network lower layer at the time of initialization. This standard stipulates three NMa setting methods: the MAC Address Server Method, the Distributed Method that does not use any MAC address server, and the Manual Setting Method. In this standard, three address setting modes are acceptable: a) the “Server Required Mode” (SR-MODE), where a MAC address server shall always be used for NMa setting under some administrator; b) the “Automatic Mode” (A-MODE), where no MAC address server exists in which the NMa setting mechanism is operated in a distributed manner; and c) the “Manual Mode” (M-MODE), in which NMAs are defined manually.

4.2 Topology

The common accommodation requirements for all IP medium types are as follows:

- A single IP subnet that contains nodes using different media connected by means of Layer 2 bridges shall be treated as a Home Network subnet. That is, node sets using different Home Network media but connected using Layer 2 bridges are defined as a single Home Network subnet. This allows node sets using different media to be connected without using a Home Network router and eliminates Net ID changes during node transport within the subnet. When a Layer 2 bridge is to be used, the Home Network packet timeout requirement specified in this standard shall be satisfied. Figure 5 shows an example of a bridge connection Network A, B, C in this figure are basic networks with the same lower media and IP layer.
- Home Network nodes shall be connected by Home Network routers on a subnet-by-subnet basis regardless of whether the IP layer exists. An example is shown in Figure 6.
- In a network comprising two or more IP subnets connected by means of an IP router or IP routers, the Home Network subnets shall be contained in the respective IP subnet. That is, it is not allowed to use an IP network comprising two or more IP subnets connected by means of an IP router or IP routers as one Home Network subnet. Connection between Home Network subnets shall be made by means of a Home Network router or Home Network routers. Home Network communication via an IP router is not allowed. Figure 7 shows an example of this type of connection.

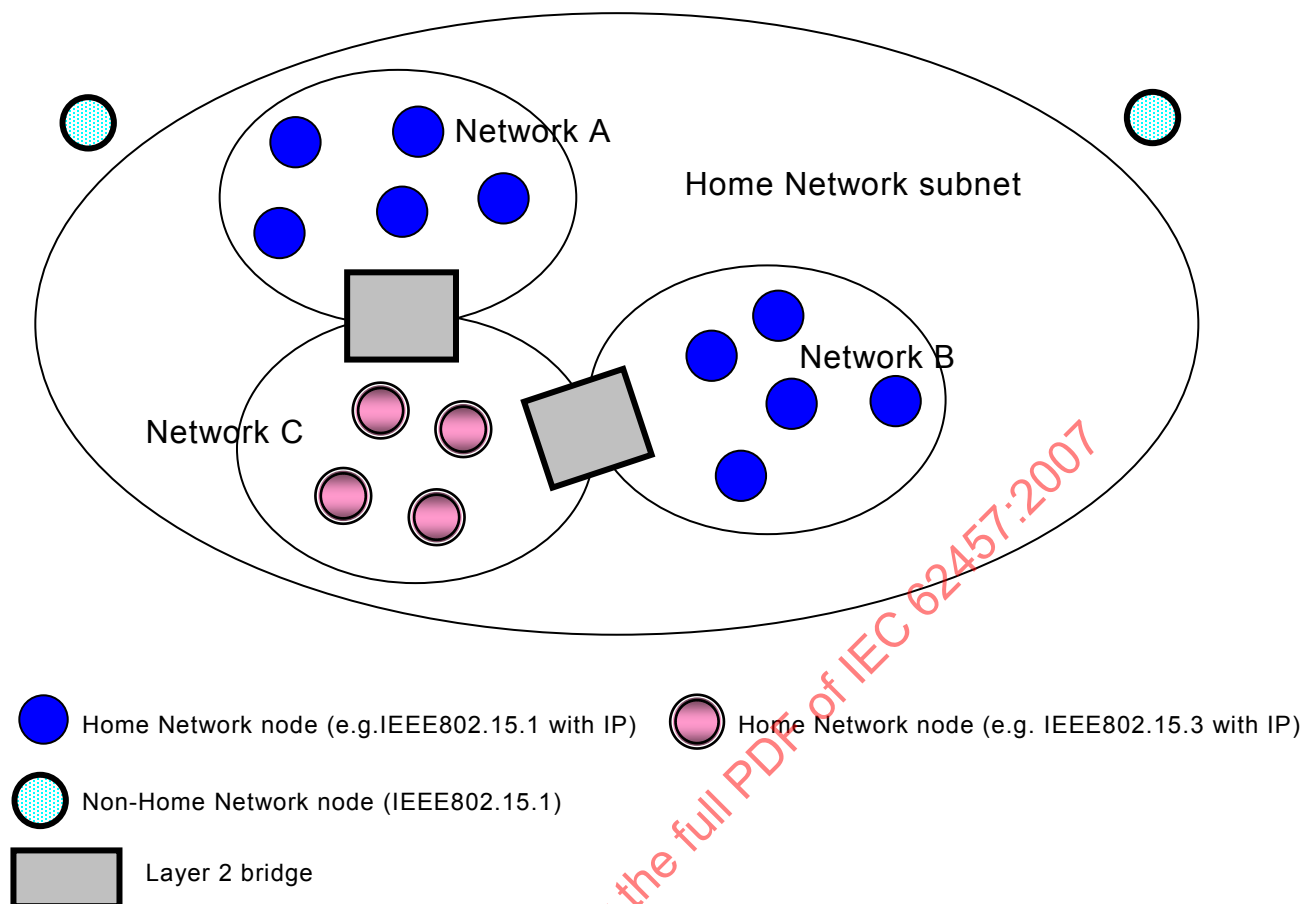


Figure 5 – Example of a subnet using Layer 2 bridges

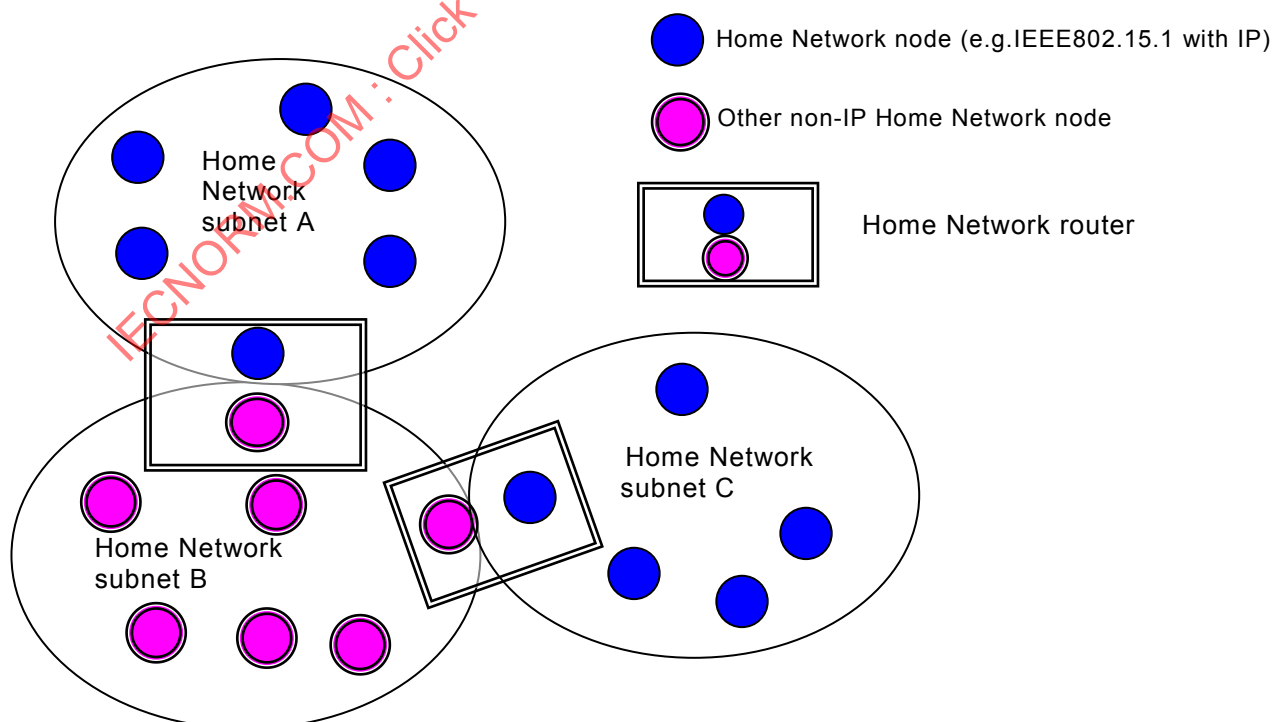


Figure 6 – Example of a subnet connection using Home Network routers

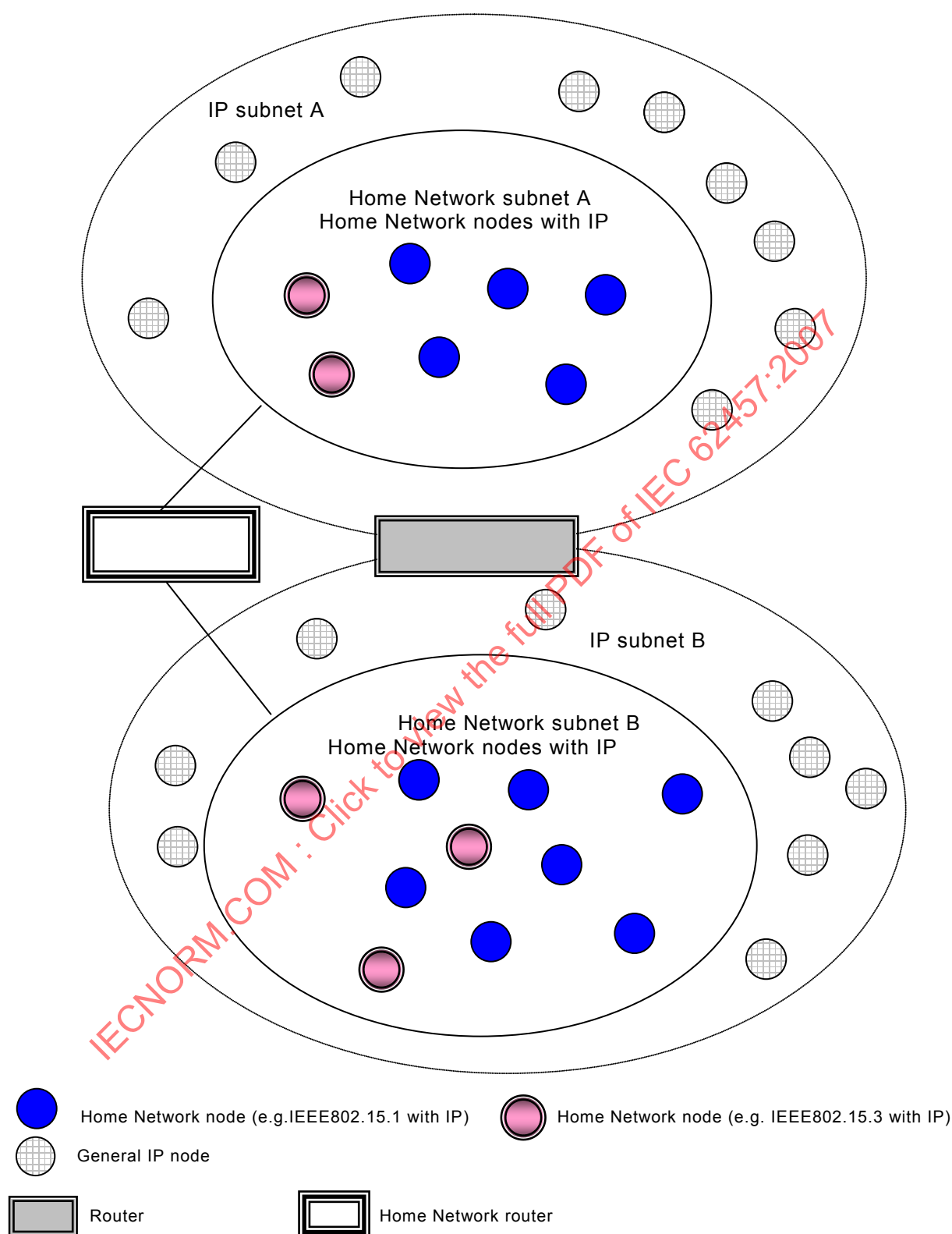


Figure 7 – Relationship between IP subnet and Home Network subnet

4.3 UDP interface

For access to UDP/IP by a UDP/IP application, a socket interface or equivalent interface is normally used. These interfaces depend on the operating system and development environment. For details, see the UDP/IP interface standards for the specific development platform.

4.4 Packet format of Home Network frame

4.4.1 General

Home Network frames which are generated by a TCP/IP Interface shall be encapsulated into UDP packets when transferred over the Internet. These packets shall be transferred with the UDP port number 3610 attached. This number shall be for the receiving port. The port number shall be the same regardless of packet type (unicast, multicast, or broadcast).

One Home Network frame packet prepared for a Home Network transmission frame and 9 types of Home Network frame packets for network management are specified as follows:

- Home Network transmission frame transfer
- MAC/IP address resolution request/response (resolution of IP address from NMa)
- IP/MAC address resolution request/response (resolution of NMa from IP address)
- Hardware/MAC address resolution request/response (resolution of NMa from Ha)
- MAC address initialization request/response, MAC address server initialization response
- MAC address allocation response
- MAC address confirmation request/response
- MAC address request/response to all nodes
- MAC address server detection request/response, MAC address server notification
- Network control message(destination invalid/NMa overlap)

Because all these packet types are multiplexed onto the same UDP port, it is necessary to use packet type numbers for multiplexing. Therefore, these packets are multiplexed onto UDP packets using the format shown in Figure 8 below. The entry in the “version number” section shall always be 0x01.

Version number (0x01)	Packet type number	Packet type number-dependent
-----------------------	--------------------	------------------------------

Figure 8 – Home Network frame packet format

Packet type numbers are shown in Table 1. “Mandatory for all nodes” in the “Support” column means that all Home Network nodes shall support packets having the packet type number shown. “Mandatory only for address servers” means that only those nodes that may become a MAC address server are required to support packets having the packet type number shown

Table 1 – Packet type numbers of the Home Network frame

Packet type number	Packet type	Support
0	Home Network transmission frame transfer	Mandatory for all nodes
1	MAC/IP address resolution request	Mandatory for all nodes
2	MAC/IP address resolution response	Mandatory for all nodes
3	IP/MAC address resolution request	Optional for all nodes
4	IP/MAC address resolution response	Mandatory for all nodes
5	Hardware/MAC address resolution request	Optional for all nodes
6	Hardware/MAC address resolution response	Mandatory for all nodes
7	MAC address initialization request	Mandatory for all nodes (not required for manual setting mode-only nodes)
8	MAC address initialization response	Mandatory for all nodes
9	MAC address server initialization response	Mandatory only for address servers
10	MAC address allocation response	Mandatory for all nodes (not required for manual setting mode-only nodes)
11	MAC address confirmation request	Mandatory for all nodes (not required for manual setting mode-only nodes)
12	MAC address confirmation response	Mandatory for all nodes
13	MAC address request to all nodes	Mandatory only for address servers
14	MAC address response to all nodes	Mandatory for all nodes
15	MAC address server detection request	Mandatory only for address servers
16	MAC address server notification	Mandatory only for address servers
17	MAC address server detection response	Mandatory only for address servers
18	Network control message (destination invalid)	Optional for all nodes
19	Network control message (NMA overlap)	Optional for all nodes
Other than above	Reserved for future use	

In this standard, the term “multicast” means “multicast to all Home Network nodes in the Home Network subnet” unless otherwise specified. Multicast packets are encapsulated into an IP packet addressed to the assigned IP multicast address (also referred to as “IPme”) and sent to the Home Network nodes.

The “Hardware type” and “Hardware address length” follow Table 2.

Table 2 – Hardware type

Hardware type	Hardware name	Hardware address type	Hardware address length
0x00	IEEE 802.15.1	IEEE 802	48 bit
0x01	Ethernet or IEEE 802.3	IEEE 802	48 bit
0x02	IEEE 802.11	IEEE 802	48 bit
Other than above	Reserved for future use		

For fields with the comment “Enter null” or “Padding,” “0x00” shall be used throughout the remainder of this standard. In the explanation of packet formats in this standard, MSB shall refer to the leftmost bit and LSB to the rightmost bit. In the Flag field in some packet format tables, bit 7 shall refer to MSB and bit 0 to LSB as shown in Figure 9. Multi-byte fields shall be transmitted with the MSB first and LSB last (Big-endian).

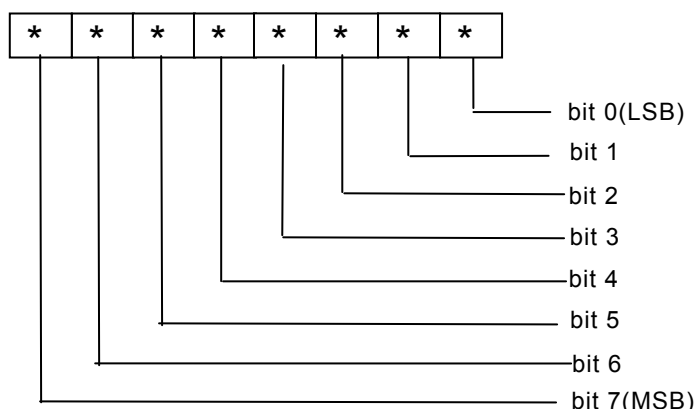


Figure 9 – Notation for bits in the flag field

The unit of size used in this standard is Octet.

A bit ordering example in case of the IEEE 802.15.1 address used as the Ha is shown in Figure 10. In this case, 0x “acde48000080” is entered into the packet.

MSB		LSB	
company_id		company_assigned	
NAP	UAP	LAP	
1010110011011110	01001000	000000000000000010000000	

Figure 10 – IEEE 802.15.1 Address described in bits

IP addresses represented in dotted decimal notation are treated similarly. For example, “192.168.10.5” is entered into the packet as “0xc0a80a05”.

4.4.2 Home Network transmission frame transfer

The definition and the format are described below.

- Stores a Home Network transmission frame, which was received from the Home Network upper layer or UDP Layer.
- The node that transmits the Home Network transmission frame shall be referred to as the transmission node and the node that receives the Home Network transmission frame shall be referred to as the receiving node.
- The Home Network transmission frame shall be transferred with the transmission node’s Hardware type, Ha length, Ha, NMa, and the receiving node’s NMa attached.
- When the Home Network transmission frame to be transmitted is a broadcasting or group-broadcasting frame, the transmission node’s NMa value shall be entered in the column for the receiving node’s NMa.

NOTE The detection of the frame from the protocol (CEBus, ECHONET, Konnex, LonTalk, others) is out of the scope of this standard.

Table 3 below shows the format for “Home Network transmission frame transfer” Packets.

Table 3 – Format for “Home Network transmission frame transfer” packets

Item	Size(octet)	Explanation
Version	1	Enter “0x01” (Version 1)
Type	1	Enter “0x00” (Home Network transmission frame transfer)
DMAC	1	NMa of receiving node
SMAC	1	NMa of transmission node
SHType	1	Hardware type of transmission node
SHLen	1	Ha length of transmission node
SHAddr	SHLen	Ha of transmission node
Msg		Direct storage of Home Network transmission frame

4.4.3 MAC/IP address resolution request/response

The definition and the format are described below.

- Used to obtain the IP address of a Home Network node that has a NMa.
- The node that wishes to resolve the NMa (i.e., that wishes to know the IP address) shall be referred to as the “requesting node” and the node that notifies the relationship between the addresses in response to the request shall be referred to as the “target node”.
- The requesting node multicasts to the Home Network subnet an IP address resolution request packet containing the NMa to be resolved. Upon receipt of the request, the target node sends an IP address resolution response packet containing the relevant addresses if TMac and THLen are exactly the same as the target node.

Table 4 below shows the format for MAC/IP address resolution request packets.

Table 4 – Format for “MAC/IP address resolution request” packets

Item	Size(octet)	Explanation
Version	1	Enter “0x01” (Version 1)
Type	1	Packet type (MAC/IP address resolution request ; enter “0x01”)
Padding	1	Padding
RMAC	1	NMa of requesting node
RIPAddr	4	IP address of requesting node
RHType	1	Hardware type of requesting node
RHLen	1	Ha length of requesting node
RHAddr	RHLen	Ha of requesting node
Padding	1	Padding
TMAC	1	NMa of target node
TIPAddr	4	IP address of target node (Enter “null”)
THType	1	Hardware type of target node (Enter “null”)
THLen	1	Ha length of target node (Enter “RHLen”)
THAddr	THLen	Ha of target node (Enter “null”)

Table 5 below shows the format for MAC/IP address resolution response packets.

Table 5 – Format for “MAC/IP address resolution response” packets

Item	Size(octet)	Explanation
Version	1	Enter “0x01” (Version 1)
Type	1	Packet type (MAC/IP address resolution response , enter “0x02”)
Padding	1	Padding
RMAC	1	NMa of requesting node
RIPAddr	4	IP address of requesting node
RHType	1	Hardware type of requesting node
RHLen	1	Ha length of requesting node
RHAddr	RHLen	Ha of requesting node
Padding	1	Padding
TMAC	1	NMa of target node
TIPAddr	4	IP address of target node
THType	1	Hardware type of target node
THLen	1	Ha length of target node
THAddr	THLen	Ha of target node

4.4.4 IP/MAC address resolution request/response

The definition and the format are described below.

- Used to obtain the NMa of a Home Network node that has an IP address.
- The node that wishes to resolve the IP address (i.e., that wishes to know the NMa) shall be referred to as the “requesting node” and the node that notifies the relationship between the addresses in response to the request shall be referred to as the “target node”.
- The requesting node sends to the destination IP address an IP/MAC address resolution request packet containing the target IP address to be resolved. Upon receipt of the request, the target node sends an IP/MAC address resolution response packet containing the relevant addresses if TIPAddr and THLen are exactly same as the target node.

Table 6, below, shows the format for IP/MAC address resolution request packets.

Table 6 – Format for “IP/MAC address resolution request” packets

Item	Size(octet)	Explanation
Version	1	Enter “0x01” (Version 1)
Type	1	Packet type (IP/MAC address resolution request ; enter “0x03”)
Padding	1	Padding
RMAC	1	NMa of requesting node
RIPAddr	4	IP address of requesting node
RHType	1	Hardware type of requesting node
RHLen	1	Ha length of requesting node
RHAddr	RHLen	Ha of requesting node
Padding	1	Padding
TMAC	1	NMa of target node (Enter “null”)
TIPAddr	4	IP address of target node
THType	1	Hardware type of target node (Enter “null”)
THLen	1	Ha length of target node (Enter “RHLen”)
THAddr	THLen	Ha of target node (Enter “null”)

Table 7 below shows the format for IP/MAC address resolution response packets.

Table 7 – Format for “IP/MAC address resolution response” packets

Item	Size(octet)	Explanation
Version	1	Enter “0x01” (Version 1)
Type	1	Packet type (IP/MAC address resolution response ; enter “0x04”)
Padding	1	Padding
RMAC	1	NMa of requesting node
RIPAddr	4	IP address of requesting node
RHType	1	Hardware type of requesting node
RHLen	1	Ha length of requesting node
RHAddr	RHLen	Ha of requesting node
Padding	1	Padding
TMAC	1	NMa of target node
TIPAddr	4	IP address of target node
THType	1	Hardware type of target node
THLen	1	Ha length of target node
THAddr	THLen	Ha of target node

4.4.5 Hardware/MAC address resolution request/response

The definition and the format are described below.

- Used to obtain the NMa of a Home Network node that has a Ha.
- The node that wishes to resolve the Ha (IEEE 802.15.1 address, etc.) (i.e., that wishes to know the NMa) shall be referred to as the “requesting node” and the node that notifies the relationship between the addresses in response to the request shall be referred to as the “target node”.
- The requesting node multicasts to the Home Network subnet a hardware/MAC address resolution request packet containing the target Hardware type, Ha length, and Ha to be resolved. Upon receipt of the request, the target node sends a hardware/MAC address resolution response packet if THType, THLen and THAddr are exactly same as the target node.

Table 8, below, shows the format for hardware/MAC address resolution request packets.

Table 8 – Format for “hardware/MAC address resolution request” packets

Item	Size(octet)	Explanation
Version	1	Enter “0x01” (Version 1)
Type	1	Packet type (hardware/MAC address resolution request; enter “0x05”)
Padding	1	Padding
RMAC	1	NMa of requesting node
RIPAddr	4	IP address of requesting node
RHType	1	Hardware type of requesting node
RHLen	1	Ha length of requesting node
RHAddr	RHLen	Ha of requesting node
Padding	1	Padding
TMAC	1	NMa of target node (Enter “null”)
TIPAddr	4	IP address of target node (Enter “null”)
THType	1	Hardware type of target node
THLen	1	Ha length of target node
THAddr	THLen	Ha of target node

Table 9 below shows the format for hardware/MAC address resolution response packets.

Table 9 – Format for “hardware/MAC address resolution response” packets

Item	Size(octet)	Explanation
Version	1	Enter “0x01” (Version 1)
Type	1	Packet type (hardware/MAC address resolution response; enter “0x06”)
Padding	1	Padding
RMAC	1	NMa of requesting node
RIPAddr	4	IP address of requesting node
RHType	1	Hardware type of requesting node
RHLen	1	Ha length of requesting node
RHAddr	RHLen	Ha of requesting node
Padding	1	Padding
TMAC	1	NMa of target node
TIPAddr	4	IP address of target node
THType	1	Hardware type of target node
THLen	1	Ha length of target node
THAddr	THLen	Ha of target node

4.4.6 MAC address initialization request/response

The definition and the format are described below.

- a) Used by Home Network nodes to initialize their NMAs at boot time.
- b) The booting node (i.e., the node requesting a NMa initialization) shall be referred to as the “requesting node”.
- c) When a Home Network node boots (whether warm start or cold start), it multicasts to the Home Network subnet a MAC address initialization request packet to initiate the NMa initialization process. Any Home Network node that boots up in Automatic Mode (A-MODE, see 4.6.2) or Server Required Mode (SR-MODE, see 4.6.2) shall send this packet at boot time.
- d) A MAC address initialization request packet functions to:
 - 1) confirm whether a MAC address server exists in the Home Network subnet;
 - 2) ask all other nodes located in the Home Network subnet to send their MAC address initialization response packets (a MAC address initialization response packet contains information on the relationship between the NMa, IP address, and other relevant addresses of the node in question); and
 - 3) confirm whether the subnet has a Home Network node already using a NMa that is the same as the NMa the requesting node intends to use (i.e., the provisional NMa set by the requesting node).
- e) Upon receipt of the MAC address initialization request packet, the other Home Network nodes (excluding the MAC address server) shall send to the requesting node their MAC address initialization response packets.

Table 10 below shows the format for MAC address initialization request packets.

Table 10 – Format for “MAC address initialization request” packets

Item	Size(octet)	Explanation
Version	1	Enter “0x01” (Version 1)
Type	1	Packet type (MAC address initialization request; enter “0x07”)
Flag	1	When in Server Required Mode, the value in the bit 7 field is “1”, and when in other than Server Required Mode, the value is “0”. Bit 0 to bit 6 are reserved and “0” shall be entered in the fields for these bits.
RMAC	1	Provisional NMa of requesting node
RIPAddr	4	IP address of requesting node
RHType	1	Hardware type of requesting node
RHAlen	1	Ha length of requesting node
RHAddr	RHAlen	Ha of requesting node

Table 11 shows the format for MAC address initialization response packets.

Table 11 – Format for “MAC address initialization response” packets

Item	Size(octet)	Explanation
Version	1	Enter “0x01” (Version 1)
Type	1	Packet type (MAC address initialization response; enter “0x08”)
Flag	1	For a node that is a Home Network master router, “1” shall be entered in the field for bit 7. Otherwise use “0”. Bit 0 to bit 6 are reserved and “0” shall be entered in the fields for these bits.
TMAC	1	NMa of responding node
TIPAddr	4	IP address of responding node
THType	1	Hardware type of responding node
THAlen	1	Ha length of responding node
THAddr	THAlen	Ha of responding node
UsedMAC	32	“NMa in use” flag (if NMa n is currently being used, bit n is “1”). (LSB corresponds to NMa “0” and MSB corresponds to NMa “255”).

4.4.7 MAC address server initialization response/MAC address allocation response

The definition and the format are described below.

- Upon receipt of a MAC address initialization request packet from a booting node, the MAC address server sends a MAC address server initialization response packet to the booting node. The node receiving this packet sends a MAC address allocation response packet to the MAC address server to confirm receipt of the packet.
- The booting node (i.e., the node requesting a NMa initialization) shall be referred to as the “requesting node”.
- The MAC address server initialization response packet sent by the MAC address server to the requesting node in response to the MAC address initialization request packet contains the NMa to be used by the requesting node. The requesting node receiving this packet shall use the NMa specified.
- Upon receipt of the MAC address server initialization response packet, the Home Network node sends a MAC address allocation response packet to the MAC address server.

Table 12 below shows the format for MAC address server initialization response packets.

Table 12 – Format for “MAC address server initialization response” packets

Item	Size(octet)	Explanation
Version	1	Enter “0x01” (Version 1)
Type	1	Packet type (MAC address server initialization response; enter “0x09”)
Flag	1	For a Home Network master router node, “1” shall be entered in the field for bit 7. Otherwise use “0”. Bit 0 to bit 6 are reserved and “0” shall be entered in the fields for these bits.
Padding	1	Padding
RMAC	1	NMa to be used by requesting node
SMAC	1	NMa of address server node
SIPAddr	4	IP address of address server node
SHType	1	Hardware type of address server node
SHALen	1	Ha length of address server node
SHAddr	SHALen	Ha of address server node

Table 13 below shows the format for MAC address allocation response packets.

Table 13 – Format for “MAC address allocation response” packets

Item	Size(octet)	Explanation
Version	1	Enter “0x01” (Version 1)
Type	1	Packet type (MAC address allocation response; enter “0x0a”)
SMAC	1	NMa of MAC address server
RMAC	1	NMa to be used by requesting node
RPAddr	4	IP address of requesting node
RHType	1	Hardware type of requesting node
RHALen	1	Ha length of requesting node
RHAddr	RHALen	Ha of requesting node

4.4.8 MAC address confirmation request/response

The definition and the format are described below.

- When the requesting node learns through the MAC address initialization request/response process described above that the NMa it intended to use (i.e., the provisional NMa set by the requesting node) is already being used by another node, the requesting node uses a NMa confirmation request packet to set a different provisional NMa and confirm whether there is a node in the Home Network subnet that is already using the new provisional NMa.
- Home Network nodes receiving the MAC address confirmation request packet check whether their NMAs coincide with the provisional NMa contained in the packet. A Home Network node with a NMa identical to the provisional NMa sends a MAC address confirmation response packet to the requesting node.
- If there is no response to the MAC address confirmation request packet within a certain time, the requesting node determines that no node in the Home Network subnet is using the provisional NMa and assumes the provisional NMa as its formal NMa.

Table 14 below shows the format for MAC address confirmation request packets.

Table 14 – Format for “MAC address confirmation request” packets

Item	Size(octet)	Explanation
Version	1	Enter “0x01” (Version 1)
Type	1	Packet type (MAC address confirmation request; enter “0x0b”)
Padding	1	Padding
RMAC	1	Provisional NMa of requesting node
RIPAddr	4	IP address of requesting node
RHType	1	Hardware type of requesting node
RHAlen	1	Ha length of requesting node
RHAddr	RHAlen	Ha of requesting node

Table 15 below shows the format for MAC address confirmation response packets.

Table 15 – Format for “MAC address confirmation response” packets

Item	Size(octet)	Explanation
Version	1	Enter “0x01” (Version 1)
Type	1	Packet type (MAC address confirmation response; enter “0x0c”)
Flag	1	For a Home Network master router, “1” shall be entered in the field for bit 7. Otherwise use “0”. Bit 0 to bit 6 are reserved and “0” shall be entered in the fields for these bits.
TMAC	1	NMa of responding node
TIPAddr	4	IP address of responding node
THType	1	Hardware type of responding node
THAlen	1	Ha length of responding node
THAddr	THAlen	Ha of responding node

4.4.9 MAC address request to all nodes/response

The definition and the format are described below.

- A node in a Home Network subnet can ask other nodes in the subnet to send their MAC address response to all nodes packets (a MAC address response to all nodes packet contains information on the relationship between the MAC address, IP address, and other relevant addresses of the node in question) by multicasting a MAC address request to all nodes packet to the subnet.
- Upon receipt of the MAC address request to all nodes packet, the Home Network nodes send their MAC address response to all nodes packets containing the relevant addresses to the requesting node.

Table 16, below, shows the format for MAC address request to all nodes packets.

Table 16 – Format for “MAC address request to all nodes” packets

Item	Size(octet)	Explanation
Version	1	Enter “0x01” (Version 1)
Type	1	Packet type (MAC address request to all nodes; enter “0x0d”)
RMAC	1	NMa of requesting node
RIPAddr	4	IP address of requesting node
RHType	1	Hardware type of requesting node
RHAlen	1	Ha length of requesting node
RHAddr	RHAlen	Ha of requesting node

Table 17, below, shows the format for MAC address response to all nodes packets.

Table 17 – Format for “MAC address response to all nodes” packets

Item	Size(octet)	Explanation
Version	1	Enter “0x01” (Version 1)
Type	1	Packet type (MAC address response to all nodes; enter “0x0e”)
Padding	1	Padding
TMAC	1	NMa of responding node
TIPAddr	4	IP address of responding node
THType	1	Hardware type of responding node
THALen	1	Ha length of responding node
THAddr	THALen	Ha of responding node

4.4.10 MAC address server detection request/response, MAC address server notification

The definition and the format are described below.

- A node in a Home Network subnet without a MAC address server that wishes to become the MAC address server can use MAC address server detection request/response and MAC address server notification packets.
- After confirming the existence of no MAC address server, a node wishing to become the MAC address server shall be referred to as the “requesting node”.
- The requesting node multicasts a MAC address server detection request packet to the Home Network subnet. If there is no response within a certain time, the requesting node determines that there is no MAC address server in the subnet and multicasts a MAC address server notification packet to the Home Network subnet to declare that it shall serve as the MAC address server.
- If a MAC address server already exists in the subnet, a MAC address server detection response packet is sent in response to the MAC address server detection request packet.

Table 18, below, shows the format for MAC address server detection request packets.

Table 18 – Format for “MAC address server detection request” packets

Item	Size(octet)	Explanation
Version	1	Enter “0x01” (Version 1)
Type	1	Packet type (MAC address server detection request; enter “0x0f”)
RMAC	1	NMa of requesting node

Table 19, below, shows the format for MAC address server notification packets.

Table 19 – Format for “MAC address server notification” packets

Item	Size(octet)	Explanation
Version	1	Enter “0x01” (Version 1)
Type	1	Packet type (MAC address server notification; enter “0x10”)
Padding	1	Padding
SMAC	1	NMa of MAC address server node
SIPAddr	4	IP address of MAC address server node
SHType	1	Hardware type of MAC address server node
SHALen	1	Ha length of MAC address server node
SHAddr	SHALen	Ha of MAC address server node

Table 20, below, shows the format for MAC address server detection response packets.

Table 20 – Format for “MAC address server detection response” packets

Item	Size(octet)	Explanation
Version	1	Enter “0x01” (Version 1)
Type	1	Packet type (MAC address server detection response; enter “0x11”)
Padding	1	Padding
SMAC	1	NMa of MAC address server node
SIPAddr	4	IP address of MAC address server node
SHType	1	Hardware type of MAC address server node
SHALen	1	Ha length of MAC address server node
SHAddr	SHALen	Ha of MAC address server node

4.4.11 Network control message (destination invalid)

The definition and the format are described below.

- This packet is used when the DMAC (destination NMa) value of a received Home Network transmission frame transfer packet is different from the receiving node’s NMa value, to notify the Home Network transmission frame transfer packet transmission node of the discrepancy.
- The node that transmits the network control message (destination invalid) shall be referred to as the “transmission node”, and the node that receives the network control message (destination invalid) shall be referred to as the “receiving node”.
- A node that has received this message (receiving node) shall perform the address resolution (MAC/IP address resolution) process again.

Table 21, below, shows the format for network control message (destination invalid) packets.

Table 21 – Format for “network control message (destination invalid)” packets

Item	Size(octet)	Explanation
Version	1	Enter “0x01” (Version 1)
Type	1	Packet type (enter “0x12” (destination invalid))
Padding	1	Padding
SMAC	1	NMa of transmission node
SIPAddr	4	IP address of transmission node
SHType	1	Hardware type of transmission node
SHLen	1	Ha length of transmission node
SHAddr	SHLen	Ha of transmission node
DMAC	1	DMAC value contained in the received Home Network transmission frame transfer Packet

4.4.12 Network control message (NMa overlap)

The definition and the format are described below.

- This packet is used by a node that has discovered a NMa overlap (i.e. there are two or more nodes that have the same NMa), to notify these nodes of the overlap.
- The node that transmits the “NMa overlap” network control message shall be referred to as the “transmission node”.
- This message shall be broadcast throughout the subnet.
- Nodes that have received this message (i.e. all of the nodes sharing the same NMa) shall perform the address resolution process again after confirming the NMa overlap.

Table 22, below, shows the format for Network control message (NMa overlap).

Table 22 – Format for “NMa overlap” network control message packets

Item	Size(octet)	Explanation
Version	1	Enter “0x01” (Version 1)
Type	1	Packet type (enter “0x13” (NMa overlap))
Padding	1	Padding
SMAC	1	NMa of transmission node
SIPAddr	4	IP address of transmission node
SHType	1	Hardware type of transmission node
SHLen	1	Ha length of transmission node
SHAddr	SHLen	Ha of transmission node
DMAC	1	NMa being shared by two or more nodes

4.5 Basic communication sequences

4.5.1 General

A Home Network node first performs the NMa initialization procedure. Upon completion of this procedure, the Home Network node's NMa is established and the Home Network node is now ready to be handled by the Home Network upper layer and lower layer. In an IP network, the IP address of a node may change (for several reasons, including the fact that the IP address allocated by the DHCP server may differ from time to time). Similarly, the NMa of a node may change for such reasons as a change in the location of the node and a NMa overlap. Therefore, the Home Network nodes should always have the latest address information (i.e., information on the relationship between the hardware, IP, and NMAs of each of the nodes). Table 23, below, shows a sample of an Address Relation table.

Table 23 – Address Relation table

Hardware type	Ha	IP address	NMa
0	Ha	IPa	MACa
1	Hb	IPb	MACb
1	Hc	IPc	MACc
2			

For this reason, all Home Network nodes shall collect address information on surrounding nodes (by sending a NMa initialization packet and receiving the response) at boot time and shall notify the Home Network nodes located in the domain of their established address to keep their address relation tables up to date. The timeout periods contained in the tables are implementation-dependent.

A Home Network node with an established Na can perform Home Network communication. Such a node may encounter any of the following cases:

- It knows the NMa of the node with which it wishes to communicate, but does not know the node's IP address;
- It knows the IP address of the node with which it wishes to communicate, but does not know the node's NMa; or
- It knows the Ha (e.g., IEEE 802.15.1 address) of the node with which it wishes to communicate, but does not know the node's NMa.

To solve the problem, the Home Network node can use: 4.5.2 MAC/IP address resolution request/response packets, 4.5.3 IP/MAC address resolution request/response packets, or 4.5.4 hardware/MAC address resolution request/response packets. A detailed explanation of each method is given in 4.5.2 to 4.5.4. MAC address request/response to all nodes packets which are used to investigate NMAs of all Home Network nodes in the Home Network subnet is explained in 4.5.5. The procedures to solve NMa -related problems such as the receiving of 4.5.6, 4.5.7 a "destination invalid" Home Network transmission frame transfer packet or 4.5.8 the discovery of a NMa overlap during Home Network communication are explained in 4.5.6, 4.5.7 and 4.5.8.

4.5.2 MAC/IP address resolution request/response (resolution of the NMa into the IP address)

The details are described below.

- a) The node seeking to resolve the NMa shall be referred to as the "requesting node" and the node on which resolution is to be performed shall be referred to as the "target node".
- b) A Home Network node uses a MAC/IP address resolution request packet when it wishes to know the IP address of another Home Network node with a NMa.

- c) The requesting node multicasts to the Home Network subnet an address resolution request packet containing the target NMa to be resolved. Upon receipt of the request, the target node sends a MAC/IP address resolution response packet that contains its NMa, IP address, transmission medium Hardware type, Ha length, and Ha.
- d) The timeout period between the transmission of the IP address resolution request and the receipt of the IP address resolution response packet shall be T3 as described in Table 26. If no IP address resolution response packet is received within the timeout period, an error shall occur.
- e) The content of the IP address resolution response packet should be reflected in the address relation.
- f) To prevent an ARP flood, the frequency of MAC/IP address resolution request packet transmissions shall be one packet per second or less. The maximum number of MAC/IP address resolution request packets that can be sent in succession shall be 5 (the interval between a MAC/IP address resolution request packet and the succeeding one shall be at least 1 s). If no MAC/IP address resolution response packet is received after the fifth attempt, an error shall occur.

The formats for MAC/IP address resolution request and response packets are shown in Table 4 and Table 5, respectively.

The basic sequence is as shown in Figure 11 .

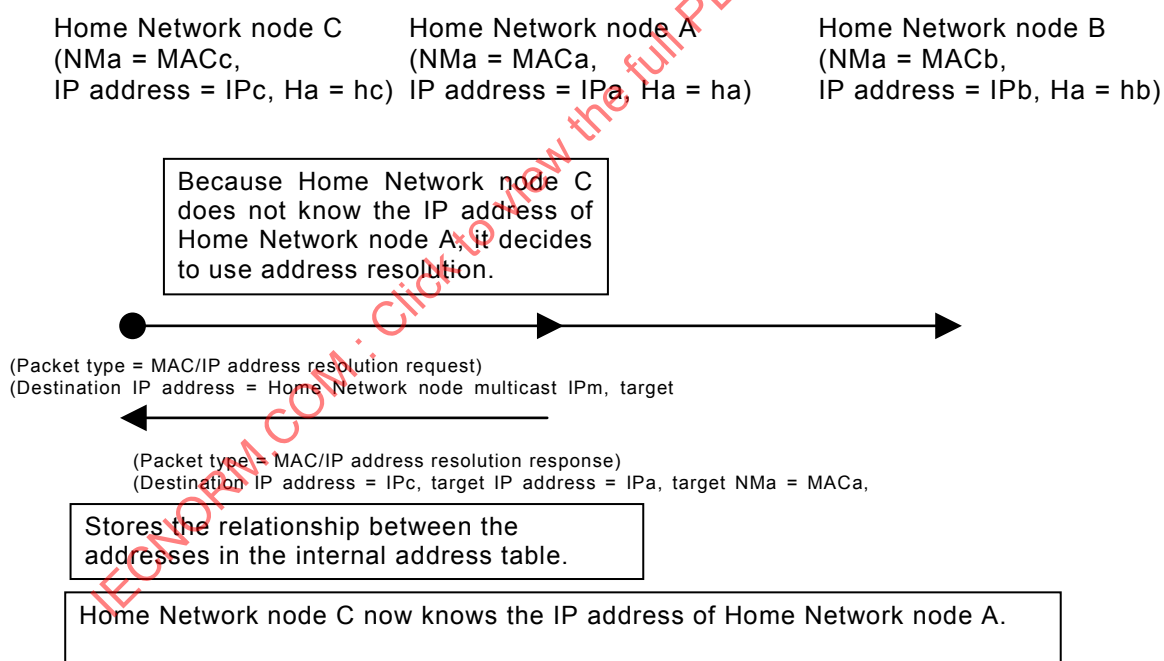


Figure 11 – Basic MAC/IP address resolution sequence

4.5.3 IP/MAC address resolution request/response (resolution of IP address into NMa)

The details are described below.

- a) The node seeking to resolve the IP address shall be referred to as the “requesting node” and the node on which resolution is to be performed shall be referred to as the “target node”.
- b) A Home Network node uses an IP/MAC address resolution request packet when it wishes to know the NMa of another Home Network node with an IP address.

- c) The requesting node sends to the destination IP address an IP/MAC address resolution request packet containing the target IP address to be resolved. Upon receipt of the request, the target node sends an IP/MAC address resolution response packet containing its NMa, IP address, transmission medium Hardware type, Ha length, and Ha.
- d) The timeout period between the transmission of the IP/MAC address resolution request packet and the receipt of the IP/MAC address resolution response packet shall be T4 in Table 26. If no IP address resolution response packet is received within the timeout period, an error shall occur.
- e) The content of the IP/MAC address resolution response packet should be reflected in the address relation.
- f) To prevent an ARP flood, the frequency of IP/MAC address resolution request packet transmissions shall be one packet per second or less. The maximum number of IP/MAC address resolution request packets that can be sent in succession shall be 5 (the interval between an IP/MAC address resolution request packet and the succeeding one shall be at least 1 s). If no IP/MAC address resolution response packet is received after the fifth attempt, an error shall occur.

The formats for IP/MAC address resolution request and response packets are shown in Table 6 and Table 7, respectively. The basic sequence is as shown in Figure 12 below.

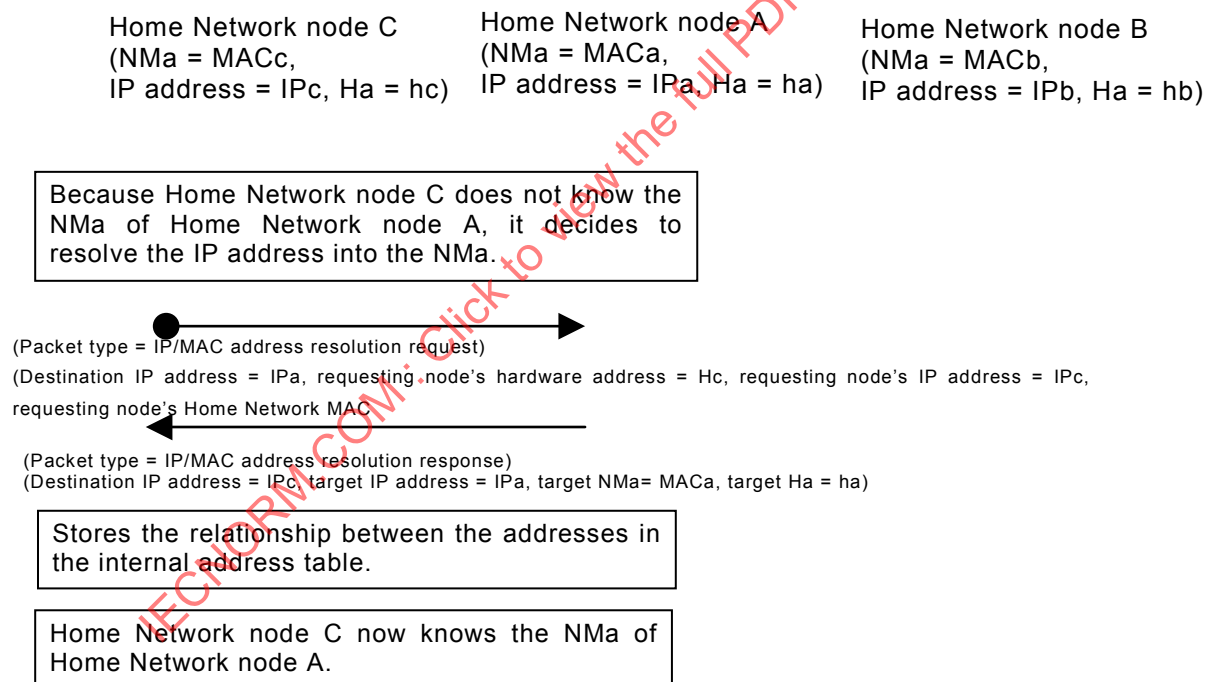


Figure 12 – Basic IP/MAC address resolution sequence

4.5.4 Hardware/MAC address resolution request/response

The details are described below.

- The node seeking to resolve the Ha shall be referred to as the “requesting node” and the node on which resolution is to be performed shall be referred to as the “target node”.
- A Home Network node uses a hardware/MAC address resolution request packet when it wishes to know the NMa of another Home Network node with a Ha.
- The requesting node multicasts to the Home Network subnet a hardware/MAC address resolution request packet that contains the target Hardware type, Ha length, and Ha to be resolved. Upon receipt of the request, the target node sends a hardware/MAC address resolution response packet containing its NMa, IP address, transmission medium Hardware type, Ha length, and Ha.
- The timeout period between the transmission of the hardware/MAC address resolution request packet and the receipt of the hardware/MAC address resolution response packet shall be T4 as given in Table 26. If no IP address resolution response packet is received within the timeout period, an error shall occur.
- The content of the hardware/MAC address resolution response packet should be reflected in the address relation.
- To prevent an ARP flood, the frequency of hardware/MAC address resolution request packet transmissions shall be one packet per second or less. The maximum number of hardware/MAC address resolution request packets that can be sent in succession shall be 5 (the interval between a hardware/MAC address resolution request packet and the succeeding one shall be at least 1 s). If no hardware/MAC address resolution response packet is received after the fifth attempt, an error shall occur.

The formats for hardware/MAC Network address resolution request and response packets are shown in Table 8 and Table 9, respectively. The basic sequence is as shown in Figure 13.

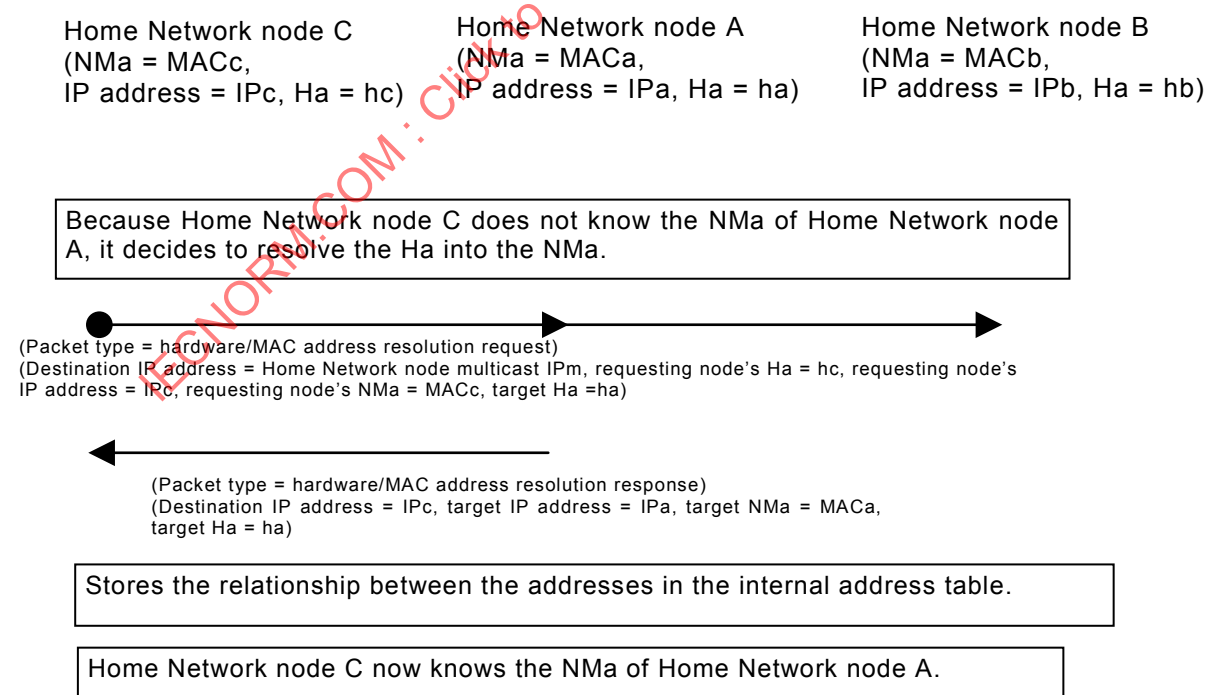


Figure 13 – Basic Hardware/MAC address resolution sequence

Unicast Home Network frames are mapped onto unicast UDP/IP packets. Multicast/broadcast Home Network frames are mapped onto UDP/IP packets addressed to a dedicated IP multicast address assigned for Home Network.

In Home Network, the mapping of Home Network subnets onto IP subnets shall be always one-to-one. Therefore, no Home Network node shall send a Home Network frame to a node located in another IP subnet (in other words, no Home Network node can send an IP packet with a destination IP address representing another IP subnet). By the same token, no Home Network node shall receive a Home Network frame from a node located in another IP subnet. In other words, a Home Network node receiving an IP packet with an origination IP address representing another IP subnet shall discard the packet.

4.5.5 MAC address request/response to all nodes

The details are described below.

- a) The node that confirms the NMa of all Home Network nodes in the Home Network subnet shall be referred to as the “requesting node” and the nodes that respond to the request shall be referred to as the “responding nodes”.
- b) “MAC address request/response to all nodes” packets are used, for example, when it is necessary for a MAC address server to confirm the MAC addresses of all Home Network nodes located within the Home Network subnet to which it belongs, in which case the MAC address server becomes the requesting node.
- c) The requesting node multicasts throughout the Home Network subnet a MAC address request to all nodes packet containing its NMa. In response to this packet, every Home Network node in the Home Network subnet sends a MAC address response to all nodes packet containing its NMa, IP address, transmission medium Hardware type, Ha length and Ha.
- d) The timeout period between the transmission of the MAC address request to all nodes packet and the receiving of the MAC address response to all nodes packet shall be T14 as given in Table 26. If no MAC address response to all nodes packet is received during this timeout period, it means that there is no other Home Network node in the Home Network subnet.
- e) The content of the MAC address response to all nodes packets should be reflected in the address relation.

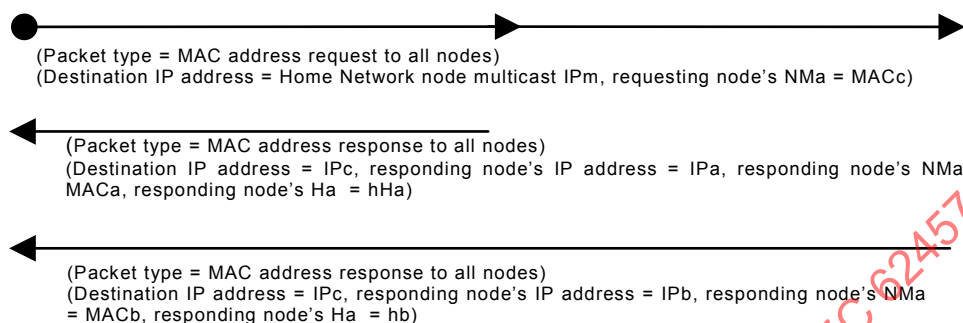
The formats for MAC address request to all nodes packets and MAC address response to all nodes packets are shown in Table 16 and Table 17, respectively. The sequence is as follows:

Home Network device C
(NMa = MACc,
IP address = IPc, Ha = hc)

Home Network device A
(NMa = MACa,
IP address = IPa, Ha = ha)

Home Network device B
(NMa = MACb,
IP address = IPb, Ha = hb)

Because the device C wishes to know all node's NMa,Ha,IP.



Stores the relationship between the addresses in the internal address

Figure 14 – Basic “MAC address request/response to all nodes” sequence

4.5.6 Network control message (destination invalid)

The details are described below.

- If the DMAC (receiving node's NMa) value contained in the received Home Network transmission frame transfer packet is different from the node's NMa value, the receiving node cannot pass the Home Network transmission frame transfer packet to the upper layer. Instead, the node notifies the transmission node that the destination of the received Home Network transmission frame transfer packet is invalid.
- Because the node that transmits the original Home Network transmission frame transfer packet and the node that receives that packet are called the “transmission node” and “receiving node”, respectively, the node that transmits this network control message and the node that receives it are called the “receiving node” and “transmission node”, respectively.
- A node that has received this message (transmission node) shall perform the address resolution (MAC/IP address resolution) process again.

The format for “destination invalid” network control messages is shown in Table 21. The sequence is as follows:

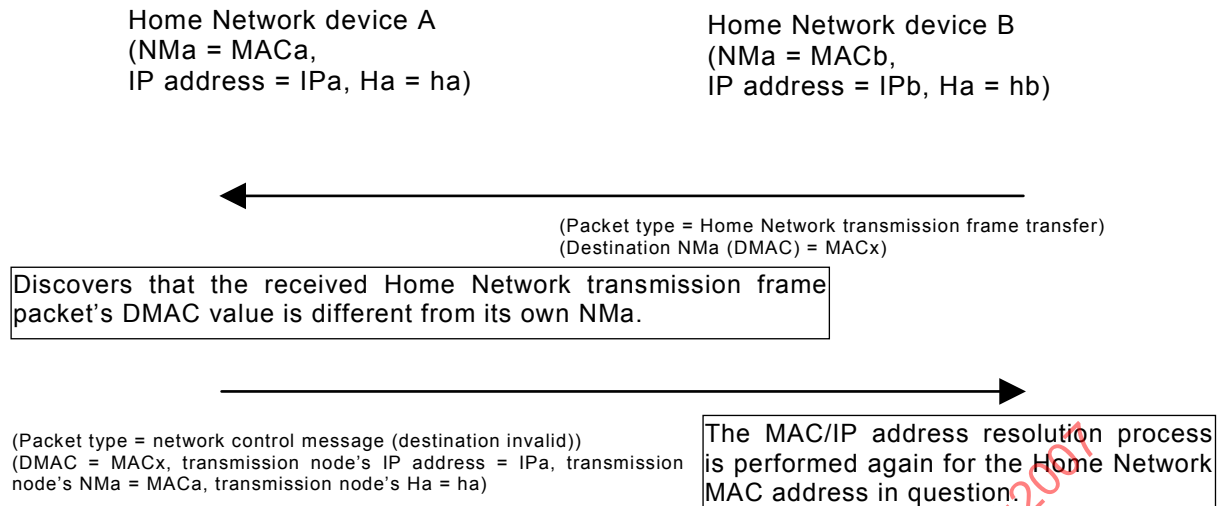


Figure 15 – Basic “destination invalid” processing sequence

However, this processing need not be performed if the received Home Network transmission frame transfer packet's SMAC and DMAC values are the same (i.e. the packet is a broadcasting or group-broadcasting packet). There may also be a case where the received Home Network transmission frame transfer packet's SMAC value is the same as the receiving node's NMa value, in which case there may be a NMa overlap in the subnet and so the processing described in 4.5.7, below, shall be performed.

4.5.7 Special case pertaining to packets with invalid destination values

The details are described below.

- As mentioned in 4.5.6, in some cases the sender address (SMAC) value of a received Home Network transmission frame transfer packet with an invalid destination value may be the same as the receiving node's NMa value, in which case there may be a NMa overlap in the subnet.
- When this happens, the node that has received the Home Network transmission frame transfer packet with the invalid destination value shall make a MAC/IP address resolution request using the packet's sender address (SMAC) as the target node's NMa .
- If the node that has received the Home Network transmission frame transfer packet with the invalid destination value receives a MAC/IP address resolution response from the target node (which is a confirmation that there is a NMa overlap), it shall initiate a cold start and initialize its Na.
- If no MAC/IP address resolution response is received from the target node, it shall judge the received Home Network transmission frame transfer packet with the invalid destination value to be an invalid packet and discard it.

4.5.8 Network control message (NMa overlap)

The details are described below.

- a) A node that has discovered a NMa overlap (i.e. there are two or more nodes that have the same NMa) shall notify the nodes sharing the same NMa of the overlap. A node usually knows the presence of a NMa overlap when MAC/IP address resolution responses are received from two or more nodes for a MAC/IP address resolution request for a single NMa or when it detects a NMa in its address relation table that corresponds to two or more IP addresses. Upon discovery of a NMa overlap, it broadcasts throughout the subnet a network control message (NMa overlap).
- b) The node that transmits this message shall be referred to as the “transmission node”.
- c) The network control message is broadcast throughout the subnet using the IP multicast address allocated by the Home Network.
- d) All nodes that have received this message (i.e. all of the nodes that are sharing the same NMa) shall perform the address determination process again using a cold start after confirming the overlap. This confirmation is usually made by making a MAC/IP address resolution request on the node’s own NMa.

The format for “destination overlap” network control message packets is shown in Table 22. The sequence is as follows:

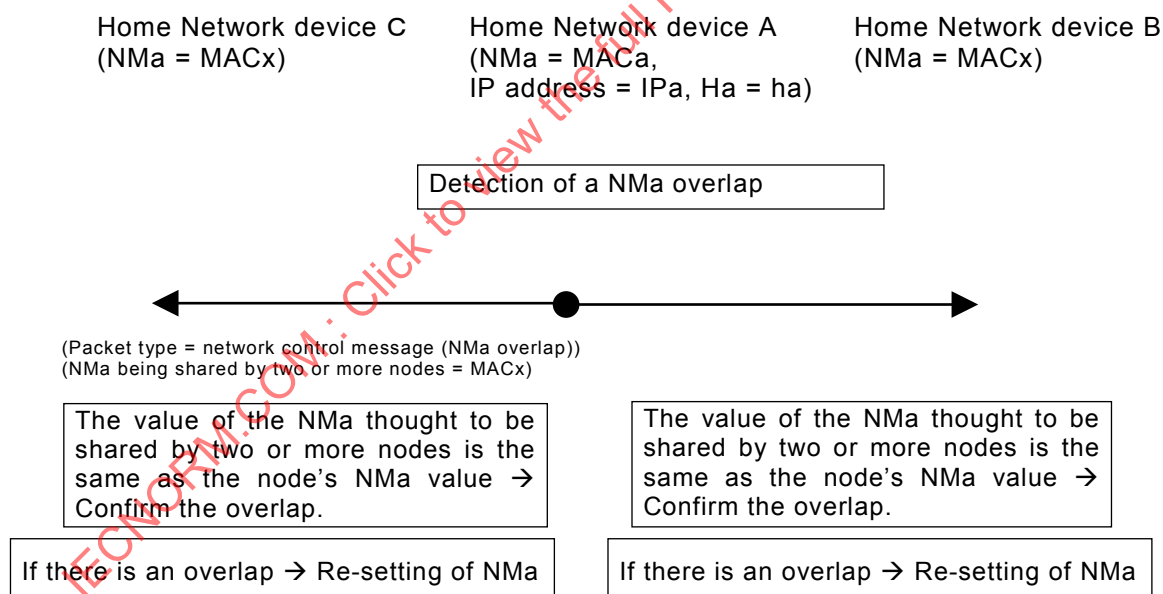


Figure 16 – Basic sequence for handling detected NMa overlap

4.6 NMa acquisition booting sequence

4.6.1 Overview of NMa acquisition booting sequence

The NMa acquisition booting processing can be divided into the following three processing stages:

- a) Processing up to establishment of the lower medium (in case of IEEE 802.15.1, PANU-NAP/GN Connection using BNEP and Formation of Piconet) (lower medium Layer)
- b) Processing up to acquisition/establishment of IP Address (IP layer)
For processing up to the acquisition/establishment of an IP address with IPv4, it is recommended that DHCP be used for IP address acquisition. The implementation of a function to acquire addresses as a DHCP client shall be mandatory. (TCP/IP Layer)
- c) Processing after Acquisition of IP Address (Home Network Lower Layer)

Overview of the processing after acquisition of IP Address is described in 4.6.2 and the detailed description is given in 4.6.3 .

4.6.2 Overview of the processing after acquisition of IP Address

All nodes shall determine their NMAs at boot time by performing the sequence specified below. The “Automatic Mode” (A-MODE), “Server Required Mode” (SR-MODE), or “Manual Mode” (M-MODE) can be used to achieve this, depending on the administrator’s settings, etc. However, it is recommended that the Automatic Mode (A-MODE) be used unless another mode has been configured in the settings. Either the Manual Mode (M-MODE) or the Automatic Mode (A-MODE) shall be provided. The implementation of the Server Required Mode (SR-MODE) is optional. Mixed use of nodes using the Manual Mode (M-MODE) for booting and nodes using another booting mode shall be avoided. This standard does not specify any functional requirements for such mixed use (e.g., effects of improper settings made in Manual Mode).

Table 24 – Booting modes

Booting mode	Explanation
Automatic Mode (A-MODE)	Bootting of new nodes using the Address Server Method or Distributed Determination Method. Dynamic NMa acquisition is possible.
Server Required Mode (SR-MODE)	New nodes dynamically acquire NMAs from the address server. If no MAC address server is found, an error shall occur and processing shall stop.
Manual Mode (M-MODE)	NMAs of new nodes are set manually.

Step1. Booting mode check.If the Manual Mode (M-MODE) is used for booting, the booting node shall use the set value as its NMa. Here, the booting node ends this sequence.

Step 2. The booting node sets a provisional NMa.

Step3. The booting node multicasts a MAC address initialization request packet using the address IPme. When in Server Required Mode (SR-MODE), “1” shall be entered in the bit 7 field of the Flag. When in Automatic Mode (A-MODE), “0” shall be entered in the bit 7 field of the Flag. On receipt of the MAC address initialization request packet with “1” in the bit 7 field of the Flag, the MAC address server sends a MAC address server initialization response packet to the booting node. Nodes other than the MAC address server send their MAC address initialization response packets to the booting node only when the bit 7 field of the Flag of the MAC address initialization request packet they received is “0”.

Step4. If the booting node receives the MAC address server initialization response packet, it shall use the NMa contained therein as its formal NMa. In this case, the booting node sends a MAC address allocation response packet and ends this sequence.

Step5. If the booting node does not receive this MAC address server initialization response packet while in Server Required Mode (SR-MODE), the sequence shall fail and shall be forcefully terminated.

Step6. The booting node checks all MAC address initialization response packets it received before expiration of the timeout period to determine whether there is a NMa in use in the subnet that is the same as the provisional NMa set in Step 2. If no such NMa exists in the subnet, the booting node proceeds to Step 8.

Step7. If there is a NMa in use in the subnet that is the same as the provisional NMa set in Step2, the booting node sets a different provisional NMa.

Step8. The booting node multicasts a MAC address confirmation request packet using the address IPme. Nodes receiving the MAC address confirmation request packet check whether their NMAs are the same as the provisional NMa contained in the packet. A node whose NMa coincides with the provisional NMa sends a MAC address confirmation response packet to the booting node. The booting node repeats Steps 7 and 8 until it no longer receives a MAC address confirmation response packet. Nodes other than the MAC address server shall not send a MAC address server initialization response packet to nodes using the Server Required Mode (SR-MODE) for booting, which means that the initial booting-related packet traffic shall be lower when there are nodes using the Server Required Mode (SR-MODE) for booting. A detailed explanation of the processing sequences for booting nodes, the MAC address server, and operating nodes follows.

4.6.3 Booting node

Every node (including MAC Address Server) shall determine its NMa at boot time with the following sequence:

Step1. Booting mode is checked. When in Manual Mode (M-MODE), the booting node shall use the set value as its NMa. In this case, the booting node ends this sequence. The booting node proceeds to Step 2 when in Automatic Mode (A-MODE) or Server Required Mode (SR-MODE).

Step2. The booting node waits until time T10 (see Table 26) expires.

Step3. The booting node sets a provisional NMa. This address shall be determined based on the following algorithm:

- When the booting node has in memory the NMa used before the last shutdown, it shall use that NMa as its provisional NMa.
- When the booting node does not have in memory the NMa used, the booting node shall use the last 8 bits of the Ha as its provisional NMa. When the booting node is to discard the NMa at the time of initialization or when the booting node is starting up for the first time.

Provision of a function to store the NMa used before the last shutdown is mandatory. Figure 17 shows the flowchart for determining the provisional NMa to be used.

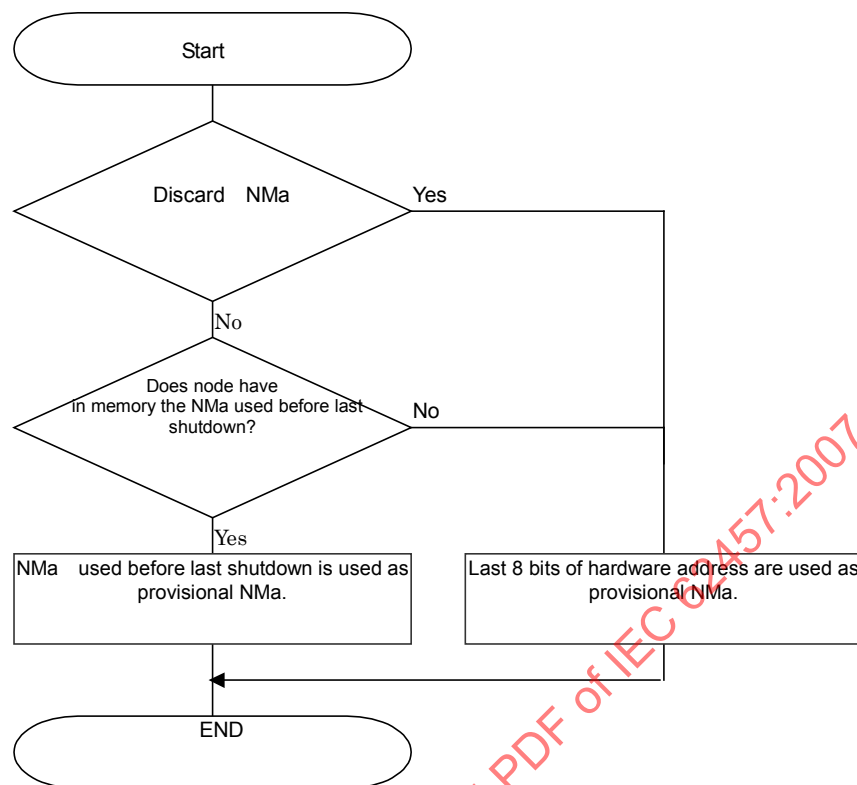


Figure 17 – Flowchart for determining provisional NMa to be used

Step4. The booting node multicasts a MAC address initialization request packet using the address IPme. The packet shall be transmitted twice with an interval of T6 (see Table 26). However, the second transmission may be omitted if the booting node received the MAC address server initialization response packet explained below before expiration of period T6. The format for MAC address initialization request packets is shown in Table 10. In this packet, set bit 7 of the Flag to “1” for Server Required Mode (SR-MODE) and to “0” for Automatic Mode (A-MODE).

Step5. If the booting node receives a MAC address server initialization response packet within the timeout period T2 (see Table 26) as measured from the transmission of the last MAC address initialization request packet, it shall use the NMa (RMAC) contained therein as its NMa. In this case, the booting node sends a MAC address allocation response packet to the sender of the MAC address server initialization response packet and ends this sequence. If the booting node receives the MAC address server initialization response packet again after determining which NMa to use, it shall send the MAC address allocation response packet again. Also if any different values of SMAC fields in all received MAC address server initialization response packets are discovered, this sequence shall fail as an error and shall be forcefully terminated. Table 13 provides the format for MAC address allocation response packets. The allocated NMa and the MAC address server’s NMa are stored in RMAC and SMAC, respectively.

Step6. If the booting node does not receive this MAC address server initialization response packet by the expiration of timeout time T2 (see Table 26) while in Server Required Mode (SR-MODE), the sequence shall fail and shall be forcefully terminated. When in Automatic Mode (A-MODE), the booting node proceeds to Step 7.

Step7. The booting node checks all used NMAs in the Home Network subnet by means of all MAC address initialization response packets received by expiration of timeout period T2. Used NMAs are TMAC addresses or NMAs represented by “1” in the UsedMAC Flag in MAC address initialization response packets. UsedMAC logical sum calculation may be used for

implementation. Figure 18 shows this sequence. If the provisional NMA satisfies any one of the following conditions, the booting node proceeds to Step 8 of this sequence. Otherwise, the booting node skips Step 8 and proceeds to Step 9 of this sequence.

- The provisional NMa coincides with a TMAC address (responding node's NMa) contained in a received MAC address initialization response packet (which means that the NMa is being used in the Home Network subnet) or the NMa represented by "1" in the UsedMAC Flag of a received MAC address initialization response packet.
- The provisional NMa coincides with a provisional NMa (RMAC) contained in a received MAC address initialization request packet.
- The provisional NMa coincides with a provisional NMa (RMAC) contained in a received MAC address confirmation request packet.

Above second and third conditions are necessary to prevent a booting node from using the same NMA that another booting node is attempting to use.

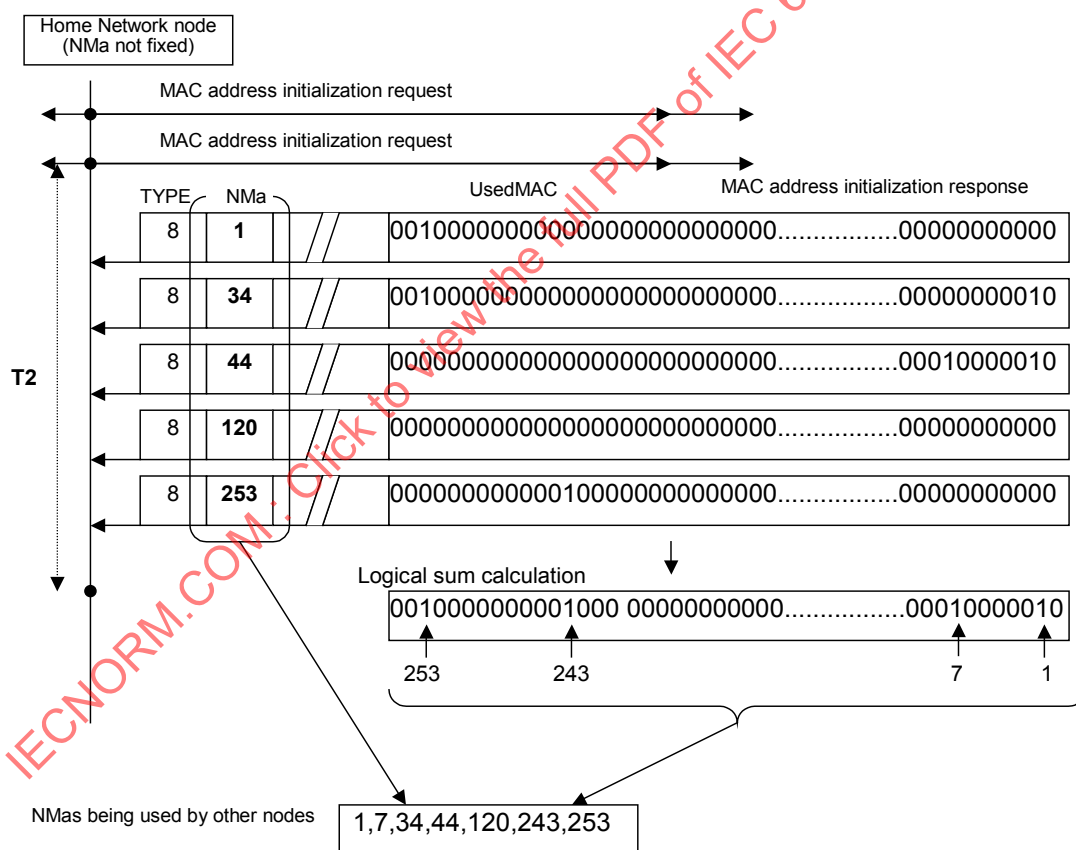


Figure 18 – Check for NMas in use by other nodes

Step8. The booting node changes the provisional NMA to a new one using a random number. The following addresses shall not be used as the provisional NMA:

- The responding nodes' NMA (TMACs) contained in the MAC address initialization response packets received in this sequence.
- The NMA represented by "1" in the UsedMAC Flags of the MAC address initialization response packets received in this sequence.

- The provisional NMa (RMACs) contained in the MAC address initialization request packets received in this sequence (see NOTE below).
- The provisional NMa (RMACs) contained in the MAC address confirmation request packets received in this sequence (see NOTE below).
- The provisional NMa already used by the booting node in this sequence (see NOTE below).

Figure 19 shows the procedure of Step8.

NOTE There is one exception to above third, forth and fifth conditions. A NMa noted in third or forth condition may be used as the provisional NMa after a period T8 (see Figure 19 and Table 26) has elapsed since receipt of the packet. This exception is optional and need not be implemented. In this case, the provisional NMa should not be used. The exception is provided to prevent a situation in which two or more nodes booting simultaneously attempt to use the same NMa, making it impossible for any node to use the address in question.

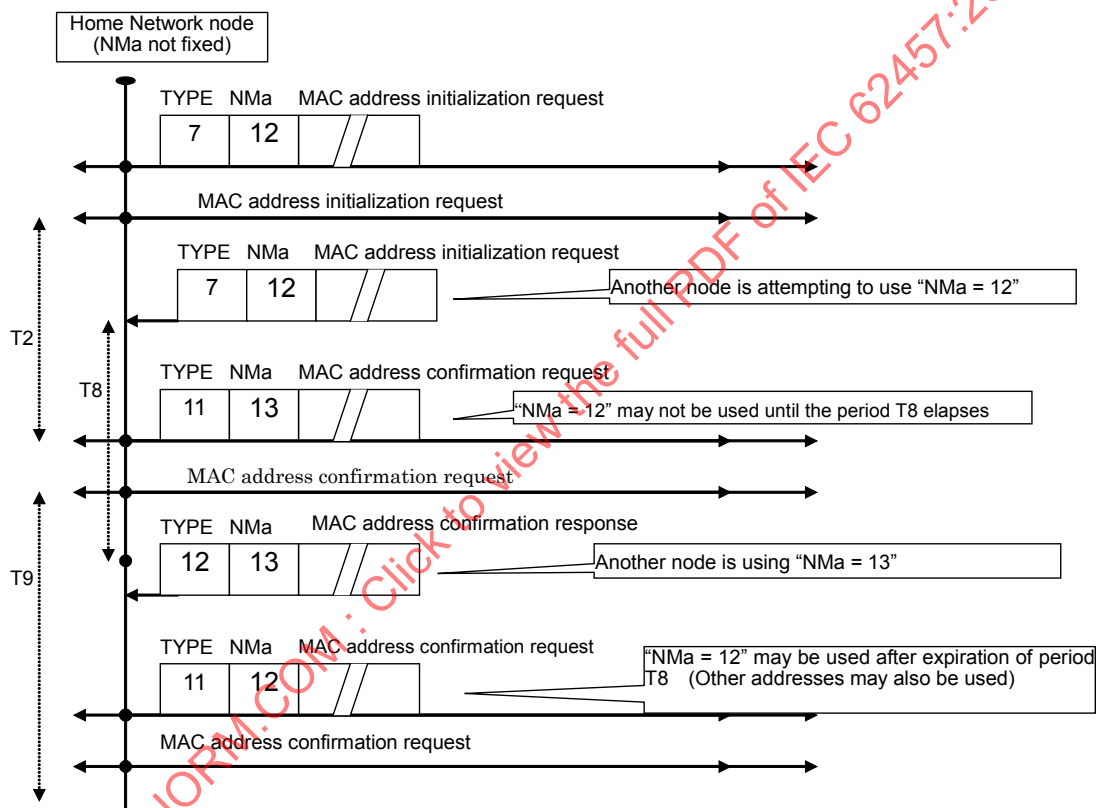


Figure 19 – Example of duplicated provisional NMa

Step9. The booting node multicasts a MAC address confirmation request packet using the address IPme. The MAC address confirmation request packet shall be transmitted twice with an interval of T6 (see Table 26). However, the second transmission may be omitted if the booting node receives a MAC address confirmation response packet. Table 14 shows the format for MAC address confirmation request packets.

Step10. If the booting node receives any of the following packets before expiration of timeout period T9 (see Table 26) as measured from transmission of the last MAC address confirmation request packet, it shall return to Step 8:

- A MAC address confirmation response packet.
- A MAC address initialization request packet whose provisional NMa (RMAC) coincides with the provisional NMa of Step 8.

- A MAC address confirmation request packet whose provisional NMa (RMAC) coincides with the provisional NMa of Step8.

Step11. If the booting node does not receive any of the packets listed in Step 10, it shall use the provisional NMa as its formal NMa. In this case, the booting node ends this sequence.

The NMa information (TMAC), Ha information (THAddr) and IP address information (TIPAddr) contained in the MAC address initialization response packets, MAC address confirmation response packets, and MAC address server initialization response packets received in this sequence (or after completion of this sequence) may be used as the address relation information referred to in “4.5 Basic communication sequences”. The NMa of the Home Network master router may be obtained from the master flag information (bit 7 of the Flag) of a MAC address initialization response packet or MAC address server initialization response packet.

4.6.4 MAC address server

For the processing sequence for the MAC address server, refer to 4.7.

4.6.5 Operating nodes

The operating nodes (i.e., nodes that have completed the sequence described in 4.6.3 and have an established NMa, except for the address server explained in 4.6.4) shall perform the following two steps:

Step1. If an operating node receives a MAC address initialization request packet and bit 7 of the Flag is “0”, it shall send a MAC address initialization response packet to the sender after expiration of period T7(see Table 26). This transmission is not necessary when the operating node receives a MAC address initialization request packet containing the same Ha within period T6. T7 shall be calculated as follows:

$$T7 = [\text{Operating node's NMa}] \times [T1] + [T0]$$

When bit 7 of the Flag is “1”, no node other than the MAC address server is to respond, because it means that the transmission is from a node using the Server Required Mode (SR-MODE) for booting. Table 11 shows the format for MAC address initialization response packets. Figure 20 shows the format for UsedMAC.



- A packet has been received from a node whose NMa is n within the past period T13 (see Table 26), except when the Ha contained in the packet coincides with that contained in the MAC address initialization request packet.

The use of "1" for bit n of UsedMAC prevents the nodes receiving the packet from using NMa n. This allows a device that communicates frequently with a device having a particular NMa to prevent other devices from using that NMa. In the implementation, a function may be used that: a) records upon receipt of a packet the time of reception and the packet's NMa using the Ha as the key, and b) checks at the time of request whether period T13 has elapsed since reception. When the power to the operating node has been switched off or shut down within the past period T13, all packets received before the switch-off/shutdown shall be ignored.



The implementer shall be very careful about using “1” in UsedMAC. Specifically, the implementer shall properly compare the Has, and if they are the same, shall never use “1”, because it would unnecessarily force the device using that NMA before the last shutdown to change it at boot time. For a simplified implementation, the implementer should use “0” for all

bits of UsedMAC or decide whether to use “0” or “1” only for certain bits and unconditionally enter “0” for the rest.

Step2. If an operating node receives a MAC address confirmation request packet and the provisional NMa contained therein is the same as the operating node's NMa, the operating node shall send a MAC address confirmation response packet to the sender. Table 15 shows the format for MAC address confirmation response packets. The data to be stored in UsedMAC are described in the previous paragraph.

Examples of basic booting sequence are shown in Annex A. If these sample sequences are not consistent with this clause, the wording in this clause takes precedence.

4.7 MAC address server

4.7.1 Requirement of MAC address server

All NMAs in a Home Network subnet shall be controlled by a MAC address server. Each node in a Home Network subnet can obtain a NMa from the MAC address server at boot time. The MAC address server shall allocate an appropriate NMa to each newly booted node such that the NMa of each device in the subnet is different from that of the other devices. The MAC address server shall allocate the same address to the nodes having the same Ha. It is usually necessary for the MAC address server to remember which NMAs it has allocated to which Has. A subnet shall not have more than one MAC address server. When there is no MAC address server in a subnet (or when there is no node seeking to become the MAC address server), any node in the subnet may become the MAC address server according to the procedure of 4.7.2. However, once a node has become the MAC address server node, it shall continue to be the MAC address server node until the subnet belonged to is reconstructed. And if a MAC address server node wants to join a subnet newly, 4.7.2 procedure shall be performed after it joins as a general node.

4.7.2 Processing sequence for MAC address server booting

When there is no MAC address server in a subnet (or when there is no node attempting to become the MAC address server), any non-MAC address server node (general node) in the subnet may become the MAC address server if and when it desires to do so. To become the MAC address server, a general node shall perform the following sequence:

Step1. The general node sends a MAC address server detection request packet twice using the address IPme at an interval of T6. The second transmission may be omitted if it receives a MAC address server detection response packet or a MAC address server notification packet.

Step2. If the general node receives a MAC address server detection response packet or MAC address server notification packet before the expiration of timeout period T5, this sequence shall fail and shall be forcefully terminated.

Step3. If the general node receives a MAC address server detection request packet, it shall repeat this sequence from Step 1 after a waiting period of T12 or greater. Processing in Step 2 shall continue even during the waiting period.

Step4. The MAC address server begins operation.

Step5. A MAC address server notification packet is multicast twice or more using the address IPme at intervals of T6. A MAC address server notification packet is shown in Table 19.

The waiting period T12 is a randomly determined period before the node may perform this sequence again when it is determined that another node is attempting to start this sequence simultaneously (see Table 26). This waiting period prevents two or more nodes from becoming MAC address servers. Normally this waiting period enables the other node to

become the MAC address server, in which case the sequence fails and is forcefully terminated. When there is at least one operating node when the NMa server is booted, the MAC address server should not allocate the NMa being used by the node to another device. Therefore, the MAC address server should obtain Has and NMAs of nodes located in the subnet using MAC address request to all-nodes packets, etc.

4.7.3 Processing by operating MAC address server

An operating MAC address server shall perform the following:

- a) When the operating MAC address server receives a MAC address server detection request packet:

The MAC address server shall send a MAC address server detection response packet to the sender.

Table 20 shows the format for MAC address server detection response packets.

- b) When the operating MAC address server receives a MAC address initialization request packet:

The MAC address server shall determine the NMa to allocate to the sender and send a MAC address server initialization response packet containing the address to the sender. The NMa allocated to the sender shall be determined as follows:

- 1) If the MAC address server has responded in the past using this sequence to the Hardware type (RHType), Ha length (RHLen) and Ha (RHAddr) contained in the MAC address initialization request packet, the NMa allocated to the sender in that response shall be used.
- 2) In all other cases except 1), a NMa not being used in the subnet shall be allocated to the sender. The following shall not be used: a NMa allocated in the past using this sequence, a NMa determined to be in use in the subnet via received packets, a NMa reserved by the administrator, etc., and the MAC address server's NMa. If the provisional NMa contained in the MAC address initialization request packet satisfies this condition, the provisional NMa should be allocated as the NMa. Depending on the implementation, a function may be used that checks the received packets and allows NMAs used prior to a certain point in the past to be used as addresses not currently being used in the subnet.

If the MAC address server does not receive a MAC address allocation response packet before the expiration of timeout period T11 (see Table 26) as measured from the transmission of the MAC address server initialization response packet, the MAC address server shall send the MAC address server initialization response packet again (up to a total of 3 times).

It is usually necessary for the MAC address server to remember which MAC addresses it has allocated to which Has in order to perform (Table 25 shows an example of a table for storing the allocated NMa for reference for the implementer).

Table 25 – Sample for storing allocated NMAs

Hardware type	Hardware address	Allocation time	Allocated NMa
1	ff-01-23-45-67-03	1232567	03
1	ff-cd-ef-78-45-05	1231763	05
1	ff-cd-aa-00-11-07	1233923	07

When the MAC address server receives a new allocation request (i.e., a request from a node with a Ha not included in the address table), it shall allocate a NMa it has not allocated in the past. However, when the MAC address server has used all the allocatable addresses, it shall allocate an appropriate address using an allocation method suitable for the implementation. This can be achieved by:

- A function to use the oldest NMa the MAC address server has allocated in the past; or
- A function that stores all incoming packets, checks all packets received, and allows NMAs allocated to the Has of nodes that have not performed communication for a certain period of time to be allocated to new requesting nodes.

Whatever method is chosen should minimize or eliminate the possibility of an address overlap.

Examples of basic booting sequence are shown in Annex B. If these sample sequences are not consistent with this clause, the wording in this clause takes precedence.

IECNORM.COM : Click to view the full PDF of IEC 62457:2007

4.8 Time period parameters

Table 26 below shows mandatory or recommended values for the time period.

Table 26 – Time period parameters

Parameter	Value	Type (mandatory or recommended)	Definition
T0	Within 50 ms	recommended	Waiting period before MAC address initialization response packet may be sent after reception of MAC address initialization request packet when NMa is "0"
T1	0	mandatory	Incremental unit of waiting period that is multiplied by NMa value and added to T0 to calculate T7
T2	3,0 s	mandatory	Interval between multicasting of a MAC address initialization request packet and reception of corresponding MAC address initialization response packet
T3	3,0 s	mandatory	Timeout period for reception of MAC/IP address resolution response packet after transmission of MAC/IP address resolution request packet
T4	3,0 s	mandatory	Timeout period for reception of IP/MAC address resolution response packet after transmission of IP/MAC address resolution request packet Timeout period for reception of hardware/MAC address resolution response packet after transmission of hardware/MAC address resolution request packet
T5	3,0 s	mandatory	Timeout period for reception of MAC address server detection response packet after transmission of MAC address server detection request packet
T6	not over 100 ms	recommended	MAC address initialization request packet transmission interval MAC address confirmation request packet transmission interval MAC address server detection request packet transmission interval MAC address server notification packet transmission interval
T7	-	-	Waiting period before MAC address initialization response packet may be sent after reception of MAC address initialization request packet $T7 = [NMa \text{ value}] \times [T1] + [T0]$
T8	24 h	recommended	Waiting period before NMa contained in received MAC address initialization request packet may be reused Waiting period before NMa contained in received MAC address confirmation request packet may be reused
T9	3,0 s	mandatory	Timeout period for reception of MAC address confirmation response packet, MAC address initialization request packet (when RMAC is the same as the provisional self NMa) or packet (when RMAC is the same as the provisional self NMa) after transmission of MAC address confirmation request packet
T10	0-100 ms	recommended	Waiting period before initialization sequence may be performed (random number)
T11	200 ms	mandatory	Timeout period for reception of MAC address allocation response packet after transmission of MAC address initialization response packet by MAC address server
T12	20 s	recommended	Waiting period before MAC address server detection request packet may be resent after reception of MAC address server detection request packet
T13	24 h	recommended	Waiting period before "1" may be entered in UsedMAC field after reception of packet
T14	3,0 s	recommended	Waiting period for reception of MAC address response to all nodes packet after transmission of MAC address request to all nodes packet

4.9 Provision for updating data after NMa acquisition

This subclause describes recommended mechanisms for updating data after NMa acquisition.

- a) Even when a node is fixed in a subnet, its NMa may change upon rebooting when it rejoins the network after leaving it as a result of a power switching or a link disconnection, especially with the Distributed Method. Therefore, it is recommended to implement in the associated layers a mechanism that updates, when a node rejoins the network, the NMa and Na values it is keeping and managing on the databases of associated information in conjunction with its NMa and Na using MAC address initialization response packet and/or any address resolution request packets.
- b) It is possible that, while a node is temporarily detached from the network, the NMa of a node in another subnet may change. In this case, the detached node cannot recognize the new address of that node. Therefore, it is recommended to introduce a mechanism similar to that described in a) so that, during the initialization of a node when it rejoins the network after leaving it, the databases of associated information including NMa and Na of the node are updated.

5 TCP/IP and requirements

UDP shall be used for the transport layer.

5.1 IP

5.1.1 Protocols to be used

The following protocols, as referenced in the bibliography, shall be implemented.

IPv4 : IETF RFC 791 Internet Protocol

ARP: IETF RFC 826 Address Resolution

IGMP: IETF RFC 792 Internet Control Message Protocol, IETF RFC 950 Internet Standards Subnetting Procedure

DHCP: IETF RFC1541 Dynamic Host Configuration Protocol, IETF RFC1122 Requirements for Internet Hosts

The following documents are to be used for reference:

IGMP: IETF RFC1112 Internet Group Multicast Protocol

IETF RFC1597 Address Allocation for Private Internets

5.1.2 IP Address

Each node supporting IP layer shall have an IPv4 address. This standard does not specify the range of IP addresses that can be used by individual nodes. Either a private or a global IP address may be used.

5.1.3 Multicast address

The multicast address **224.0.23.0** (IPme) shall be used for this layer. Each node supporting this layer shall be capable of sending packets to this address and receiving the packets sent to this address.

5.1.4 DHCP

Each node supporting this layer shall have a function to obtain address setting information using a DHCP server. For operation, it is recommended that a DHCP server be deployed in the IP network.

5.1.5 Method for obtaining IP Address by manual setting, etc.

This standard does not specify any IP address setting method other than DHCP.

5.1.6 Routing

Operations in which Home Network/IP packets are transferred beyond an IP router are not allowed. This layer shall not send a packet addressed to a node located in another IP subnet. All packets received from a node or nodes located in another IP subnet shall be discarded.

5.2 UDP

5.2.1 Protocols to be used

The following protocol, as referenced in the bibliography, shall be implemented.

IETF RFC 768 User Datagram Protocol

5.2.2 Port Number

The destination port number for UDP packets shall be **3610**. This standard does not specify an origination port number.

6 Lower-layer medium-specific interface and requirements

6.1 Interface and requirements on lower-layer medium

The Interface and requirements on each Lower-layer medium are specified in Annex C.

6.2 Software internal status transition

6.2.1 Overview

This subclause outlines the sequence for each of the seven internal statuses of the Home Network Lower-Layer software. The seven statuses are as follows:

- a) Stop Status
- b) Cold Start Status
- c) Warm Start Status
- d) Communication Suspension Status
- e) Normal Operation Status
- f) Error Stop Status
- g) Temporary Stop Status

The software internal status transition is executed by the service request from the Home Network Upper-Layer or the other triggers. The Home Network Lower-Layer returns the response or performs the processing at each status. Figure 22 depicts how the Home Network Lower-Layer software transitions from one status to another.

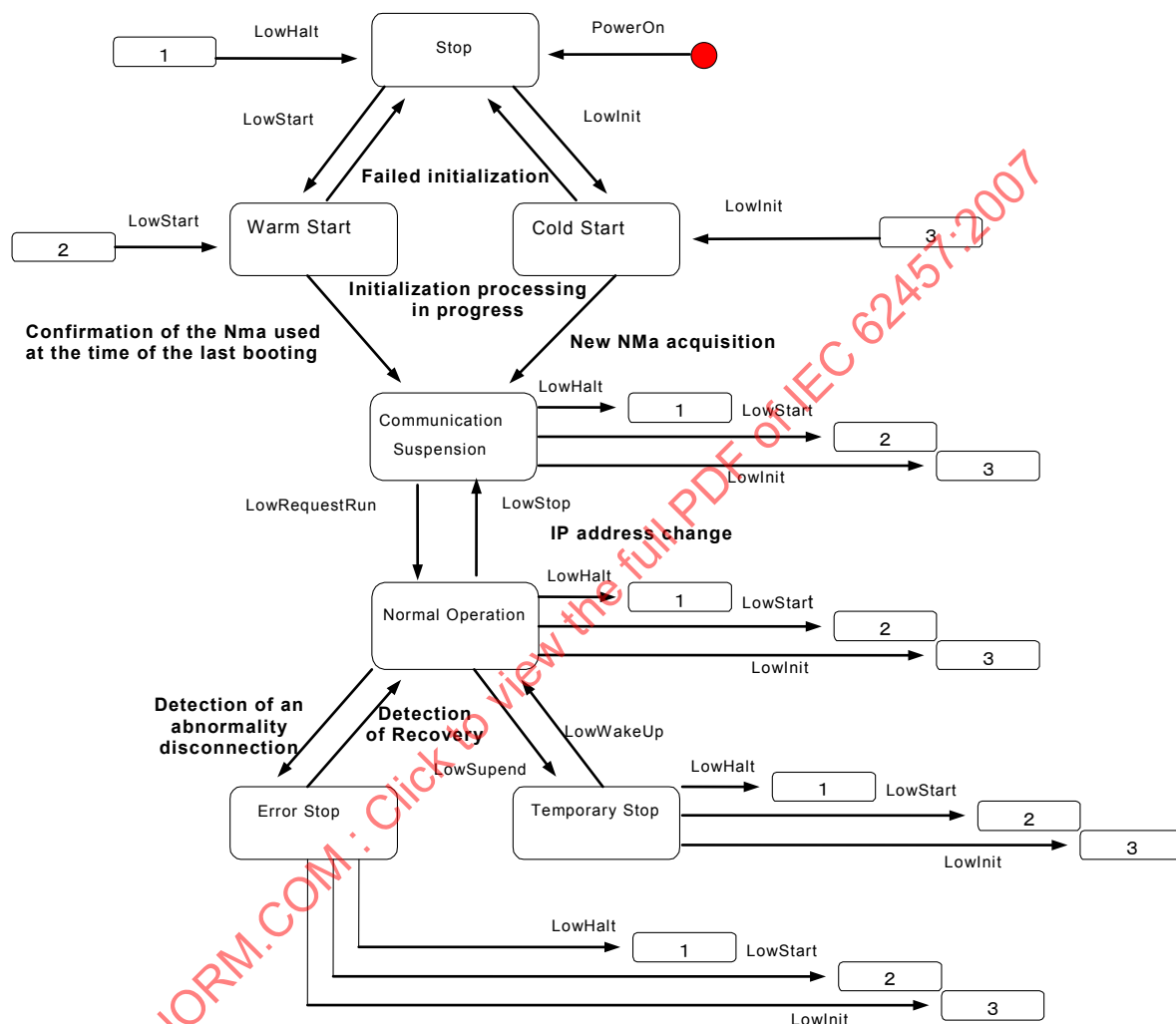


Figure 22 – Internal software status transitions

6.2.2 Stop status

In the Stop Status, the Home Network Lower-Layer software shall not perform any processing. An outline of the processing performed immediately after changing into this status and the lower-layer communication software interface services that can be handled by the software in this status are described below.

a) Triggers and Processing

The software shall enter this status immediately after the power is turned on or when it receives a request to stop operation (LowHalt) or after the initialization failure. The software shall then wait to receive a service request from the Home Network Upper-Layer software.

b) Status Acquisition Service

The software shall return the 0x00 as STOP status to the Home Network Upper-Layer according to the service request.

c) Lower-Layer Communication Software Type Acquisition Service

The software shall return the lower-layer communication software type (in case of IEEE 802.15.1, 0x70 shall be returned; otherwise, reserved for future use by other lower-layer communication software types) to the Home Network Upper-Layer according to the service request.

d) Triggers Causing Transition out of Stop Status

- Transition into Cold Start Status:
Initialization request service (LowInit)
- Transition into Warm Start Status:
Warm start request service (LowStart)

6.2.3 Cold start status

In the Cold Start Status, the Home Network Lower-Layer software shall be initialized. An outline of the processing performed immediately after changing into this status and the lower-layer communication software interface services that can be handled by the software in this status are described below.

a) Trigger and Processing

When an initialization request (LowInit) is received, the following sequence shall be performed: the establishment of a connection to the lower medium layer, an IP address acquisition/determination, and a NMa acquisition on the IP network.

b) Status Acquisition Service

The software shall return 0x01 as Cold Start status to the Home Network Upper-Layer according to the service request.

c) Lower-Layer Communication Software Type Acquisition Service

The software shall return the lower-layer communication software type (in case of IEEE 802.15.1, 0x70 shall be returned; otherwise, reserved for future use by other lower-layer communication software types) to the Home Network Upper-Layer according to the service request.

d) Triggers Causing Transition out of Cold Start Status

- Transition into Communication Suspension Status:
Completion of NMa acquisition booting processing
- Transition into Stop Status:
Failure to complete NMa acquisition booting processing

6.2.4 Warm start status

In the Warm Start Status, the Home Network Lower-Layer software shall be initialized without NMa acquisition. An outline of the processing performed immediately after changing into this status and the lower-layer communication software interface services that can be handled by the software in this status are described below.

a) Trigger and Processing

When a warm start request (LowStart) is received, the following sequence shall be performed:

- 1) Establishment of connection of lower medium,
- 2) Confirmation of whether IP address used at last boot and now stored in memory can be used for booting, and
- 3) Confirmation of whether NMa used at last boot and now stored in memory can be used for booting .

Bootting using IP and NMa described in 2) and 3) above.

b) Status Acquisition Service

The software shall return 0x04 as Warm Start status to the Home Network Upper-Layer according to the service request.

c) Lower-Layer Communication Software Type Acquisition Service

The software shall return the lower-layer communication software type (in case of IEEE 802.15.1, 0x70 shall be returned; otherwise, reserved for future use by other lower-layer communication software types) to the Home Network Upper-Layer according to the service request.

d) Triggers Causing Transition out of Warm Start Status

- Transition into Communication Suspension Status:
Completion of booting processing
- Transition into Stop Status:
Failure to complete booting processing

6.2.5 Communication suspension status

In the Communication Suspension Status, the initialized Home Network Lower-Layer software shall wait for a request to start operation from the Home Network Upper-Layer software. The software shall then wait to receive a service request from the Home Network Upper-Layer software. An outline of the processing performed immediately after changing into this status and the lower-layer communication software interface services that can be handled by the software in this status are described below.

a) Trigger and Processing

The software shall enter this status immediately after the completion of the initialization or when it receives a request to stop operation (LowStop) at Normal Operation Status. The software shall then wait to receive a service request to start operation from the Home Network Upper-Layer software.

b) Status Acquisition Service

The software shall return 0x05 as Communication Suspension Status to the Home Network Upper-Layer according to the service request.

c) Lower-Layer Communication Software Type Acquisition Service

The software shall return the lower-layer communication software type (in case of IEEE 802.15.1, 0x70 shall be returned; otherwise, reserved for future use by other lower-layer communication software types) to the Home Network Upper-Layer according to the service request.

d) Physical Address Acquisition Service

The software shall return the Ha to the Home Network Upper-Layer according to the service request.

e) Profile Data Acquisition Service

The software shall return profile data including the NMa, baudrate, vendercode, etc to the Home Network Upper-Layer, according to the service request.

f) Triggers Causing Transition out of Communication Suspension Status

- Transition into Normal Operation Status:
Operation start service (LowRequestRun)
- Transition into Stop Status:
Operation stop service (LowHalt)
- Transition into Cold Start Status:
Initialization request service (LowInit)
- Transition into Warm Start Status:
Warm start request service (LowStart)

6.2.6 Normal operation status

In the Normal Operation Status, the Home Network Lower-Layer software shall send messages to and receives messages from the transmission medium. An outline of the processing performed immediately after changing into this status and the lower-layer communication software interface services that can be handled by the software in this status are described below.

a) Trigger and processing

The software shall enter this status immediately after the recovery detection at Error Stop or when it receives a request to wake up (LowWakeUp) at Temporary Stop or a request to enter Normal Operation Status (LowRequestRun) at Communication Suspension. The software shall then wait to receive a service request from the Home Network Upper-Layer software.

b) Status acquisition service

The software shall return 0x02 as the Normal Operation Status to the Home Network Upper-Layer according to the service request.

c) Lower-Layer communication software type acquisition service

The software shall return the lower-layer communication software type (in case of IEEE 802.15.1, 0x70 shall be returned; otherwise, reserved for future use by other lower-layer communication software types) to the Home Network Upper-Layer according to the service request.

d) Physical address acquisition service

The software shall return the Ha to the Home Network Upper-Layer according to the service request.

e) Profile data acquisition service

The software shall return profile data including the NMa, baudrate, vendercode, etc to the Home Network Upper-Layer according to the service request.

f) Message transmission service

The software shall transmit the messages from the Home Network Upper-Layer to transmission medium with Header to the Home Network Upper-Layer according to the service request.

g) Message reception service

The software shall receive the messages from the transmission medium and pass the messages with deleted headers to the Home Network Upper-Layer.

h) Triggers causing transition out of normal operation status.

- Transition into Stop Status:
Operation stop service (LowHalt)
or
IP address change at IP layer
- Transition into Communication Suspension Status:
Stop service (LowStop)
- Transition into Cold Start Status:
Initialization request service (LowInit)
- Transition into Warm Start Status:
Warm start request service (LowStart)
- Transition into Error Stop Status:
Detection of abnormality by lower-layer communication medium
or
Disconnection of lower medium layer connection
- Transition into Temporary Stop Status:
Lower-layer communication section stop service (LowSuspend)

6.2.7 Error stop status

In the Error Stop Status, the lower-layer communication software's operation shall be discontinued if an error is detected. An outline of the processing performed immediately after changing into this status and the lower-layer communication software interface services that can be handled by the software in this status are described below.

a) Trigger and processing

The software shall enter this status immediately after the detection of an abnormal disconnection at Normal Operation Status. The software shall then perform processing to deal with errors.

b) Status acquisition service

The software shall return 0x03 as error Stop status to the Home Network Upper-Layer according to the service request.

c) Lower-Layer communication software type acquisition service

The software shall return the lower-layer communication software type (in case of IEEE 802.15.1, 0x70 shall be returned; otherwise, reserved for future use by other lower-layer communication software types) to the Home Network Upper-Layer according to the service request.

d) Triggers Causing Transition out of Error Stop Status

- Transition into Stop Status:
Operation stop service (LowHalt)
- Transition into Normal Operation Status:
Removal of cause of error
- Transition into Cold Start Status:
Initialization request service (LowInit)

- Transition into Warm Start Status:
Warm start request service (LowStart)

6.2.8 Temporary stop status

In the Temporary Stop Status, the lower-layer communication software's operation shall be temporarily stopped. An outline of the processing performed immediately after changing into this status and the lower-layer communication software interface services that can be handled by the software in this status are described below.

a) Trigger and processing

The software shall enter this status when it receives a request to temporarily stop (LowSuspend) at Normal Operation Status. The software shall then stop the lower-layer communication software's operation.

b) Status acquisition service

The software shall return 0x06 as Temporary Stop status to the Home Network Upper-Layer according to the service request.

c) Lower-Layer communication software type acquisition service

The software shall return the lower-layer communication software type (in case of IEEE 802.15.1, 0x70 shall be returned; otherwise, reserved for future use by other lower-layer communication software types) to the Home Network Upper-Layer, according to the service request.

d) Triggers causing transition out of temporary stop status

- Transition into Normal Operation Status:
Operation resumption service (LowWakeUp)
- Transition into Stop Status:
Operation stop service (LowHalt)
- Transition into Cold Start Status:
Initialization request service (LowInit)
- Transition into Warm Start Status:
Warm start request service (LowStart)

Annex A (informative)

Basic booting sequence

Sample sequences for the following basic cases are provided below for reference:

- A-MODE booting, NMAs not retained (with MAC address server)
Refer to Figure A.1.
- SR-MODE booting, NMAs not retained (with MAC address server)
Refer to Figure A.2.
- A-MODE booting, NMAs not retained (without MAC address server)
Refer to Figure A.3.
- SR-MODE booting, NMAs not retained (without MAC address server)
Refer to Figure A.4.
- A-MODE booting, NMAs retained (with MAC address server)
Refer to Figure A.5.
- A-MODE booting, NMAs retained (without MAC address server)
Refer to Figure A.6.

If these sample sequences are not consistent with clause 4, the wording in clause 4 takes precedence.

IECNORM.COM : Click to view the full PDF of IEC 62457:2007

A.1 MODE booting, NMa not retained (with MAC address server)

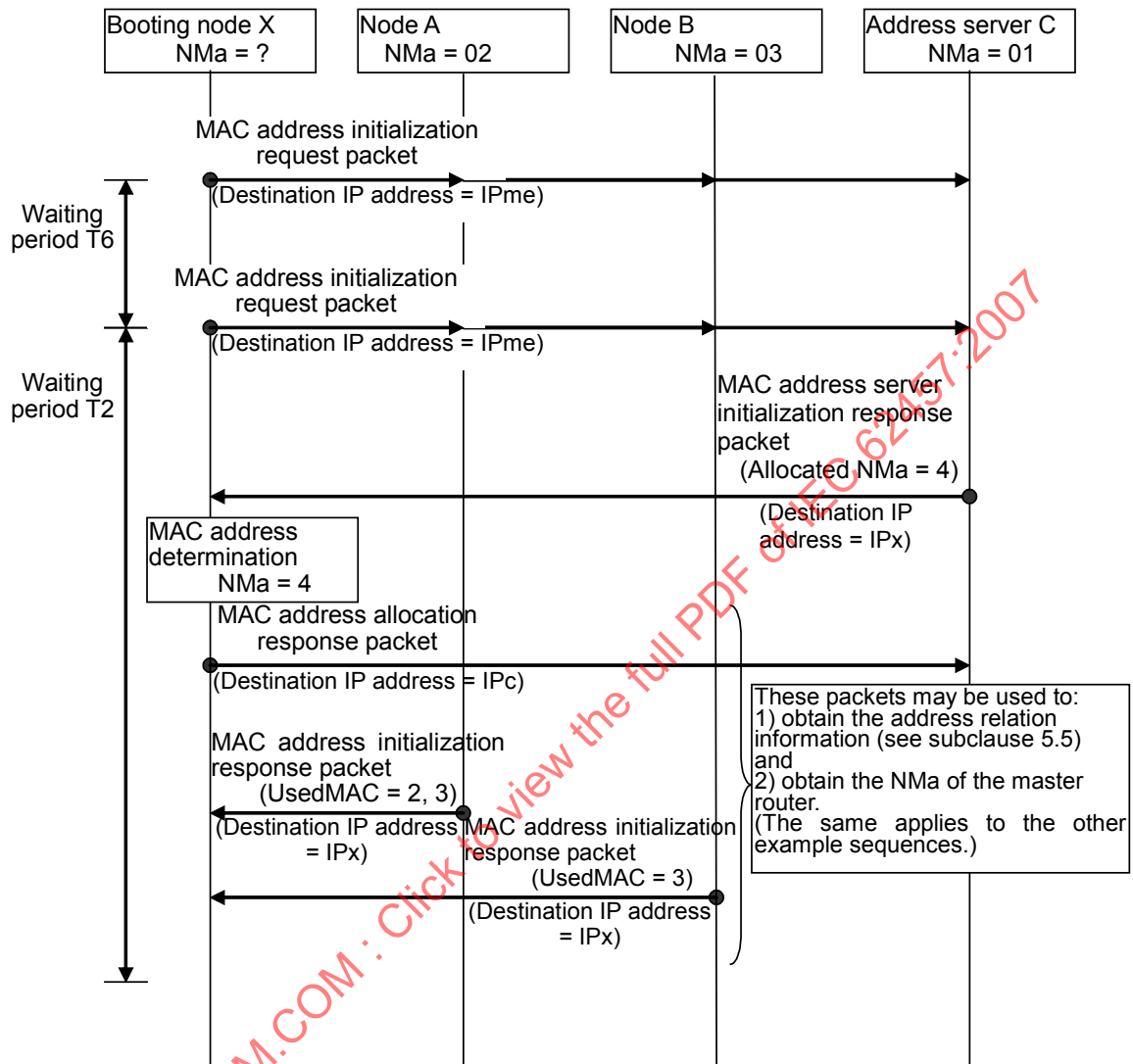


Figure A.1 – A-MODE booting, NMas not retained (with MAC address server)

A.2 SR-MODE booting, NMAs not retained (with MAC address server)

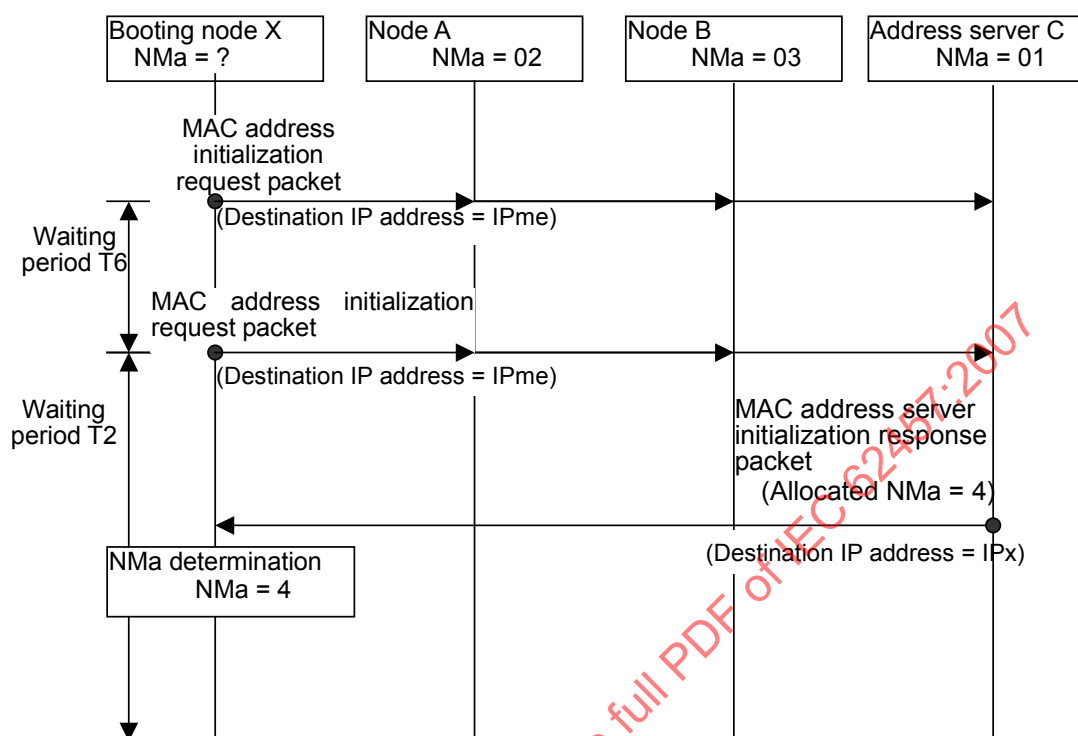


Figure A.2 – SR-MODE booting, NMAs not retained (with MAC address server)

A.3 A-MODE booting, NMAs not retained (without MAC address server)

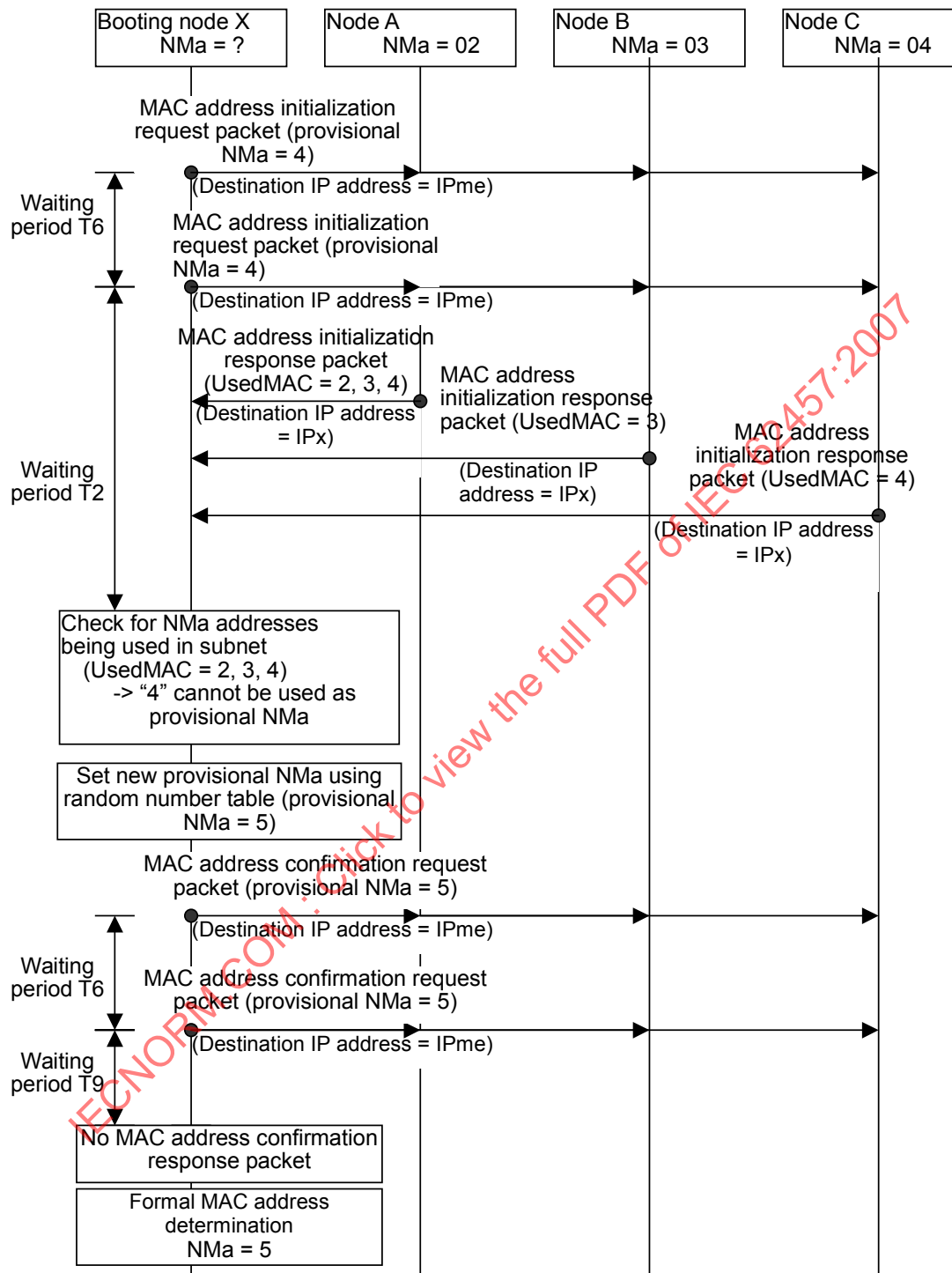


Figure A.3 – A-MODE booting, NMAs not retained (without MAC address server)

A.4 SR-MODE booting, NMAs not retained (without MAC address server)

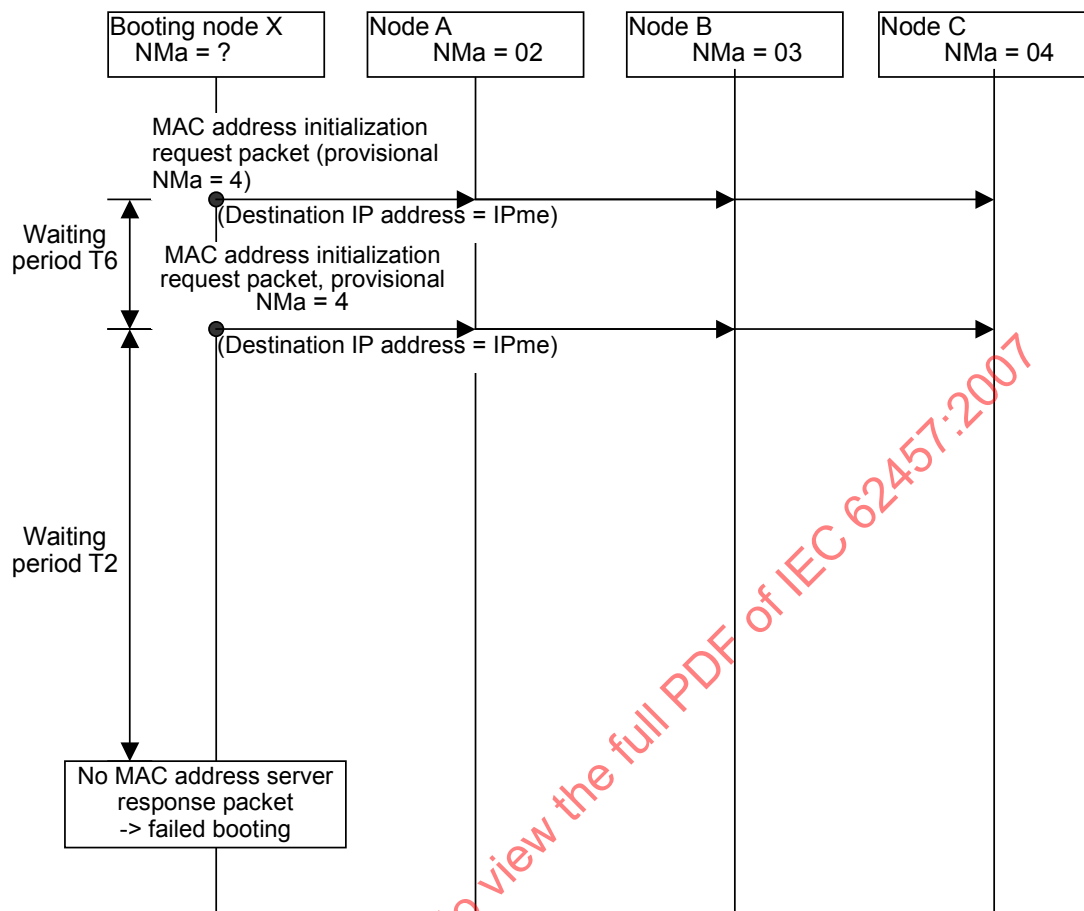


Figure A.4 – SR-MODE booting, NMAs not retained (without MAC address server)

A.5 A-MODE booting, NMaS retained (with MAC address server)

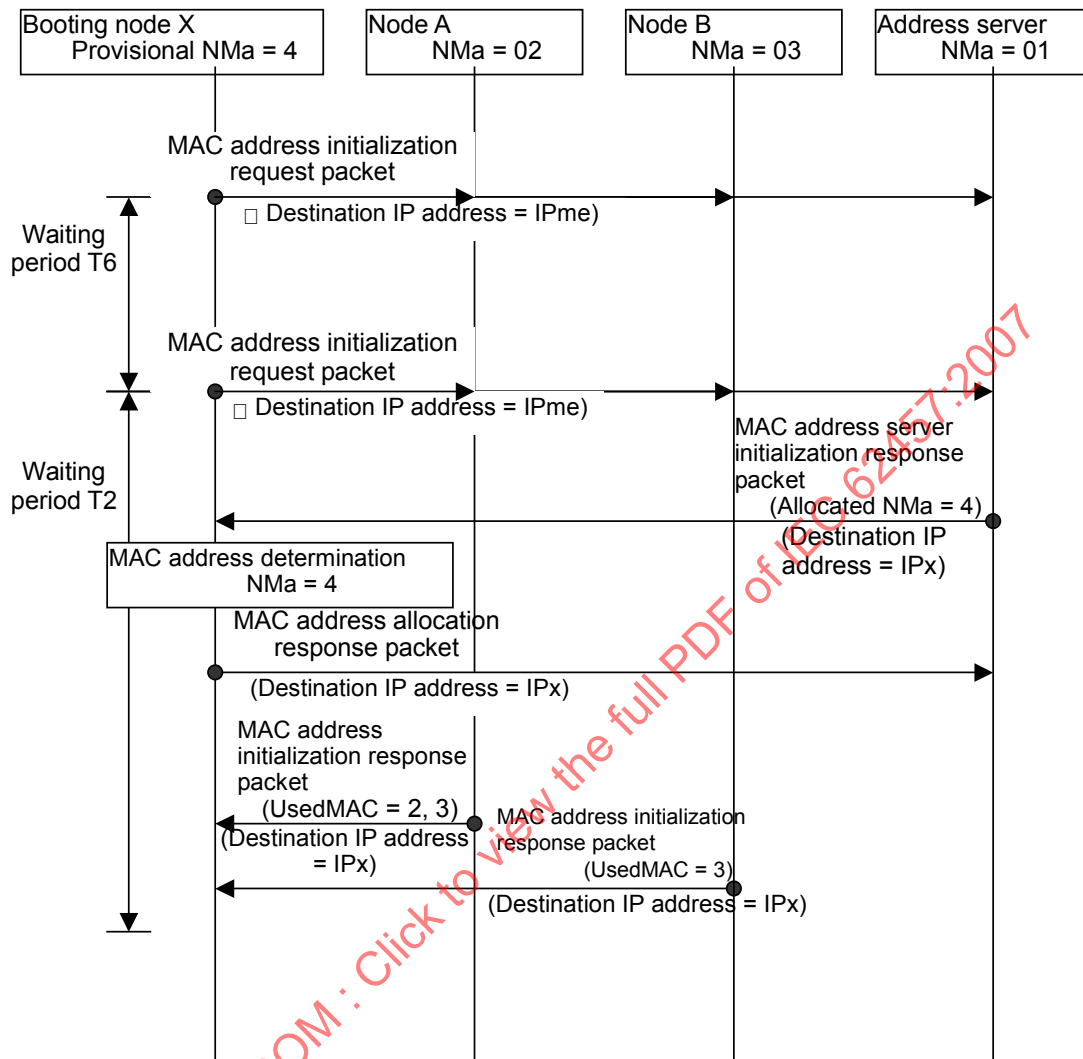


Figure A.5 – A-MODE booting, NMaS retained (with MAC address server)

A.6 A-MODE booting, NMaS retained (without MAC address server)

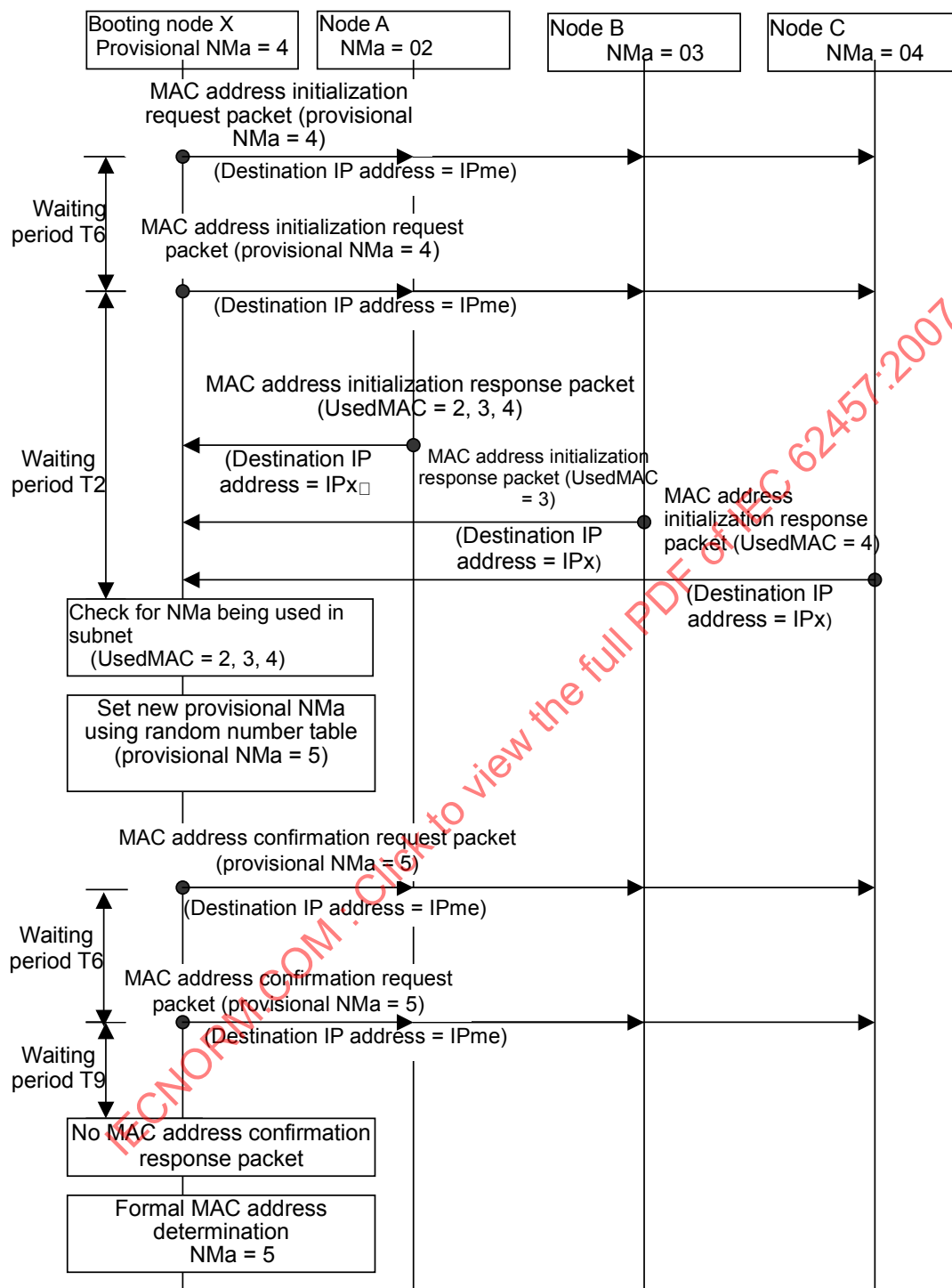


Figure A.6 – A-MODE booting, NMaS retained (without MAC address server)

Annex B (informative)

Basic MAC address server booting sequence

Sample MAC address server booting sequences for the following basic cases are given below for reference:

- Booting of a single MAC address server
Refer to Figure B.1.
- Near-simultaneous booting of two or more MAC address servers
Refer to Figure B.2.

If these sample sequences are not consistent with clause 4, the wording in clause 4 takes precedence.

B.1 Booting of a single MAC address server

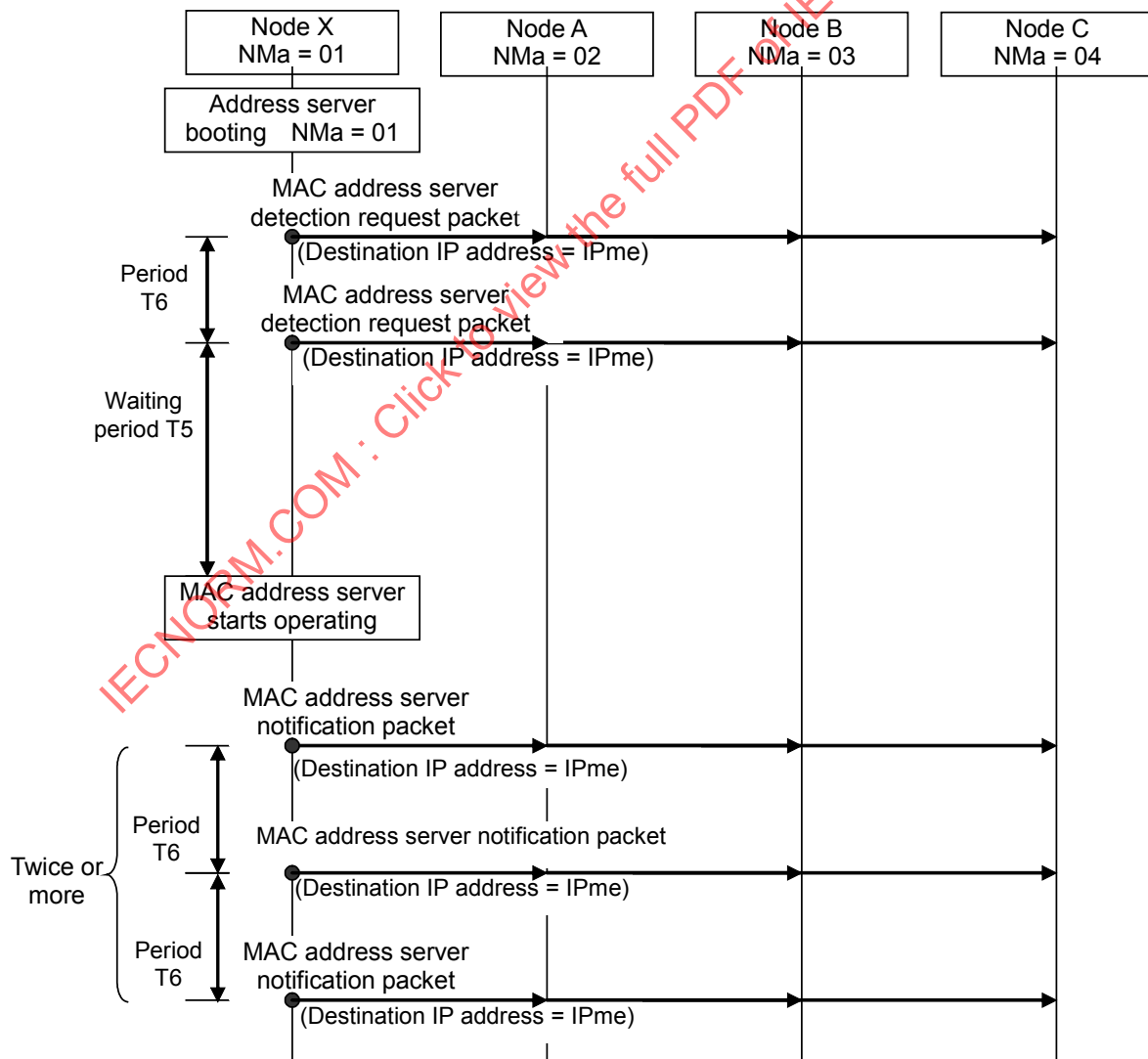


Figure B.1 – Booting of a single MAC address server

B.2 Near-simultaneous booting of two or more MAC address servers

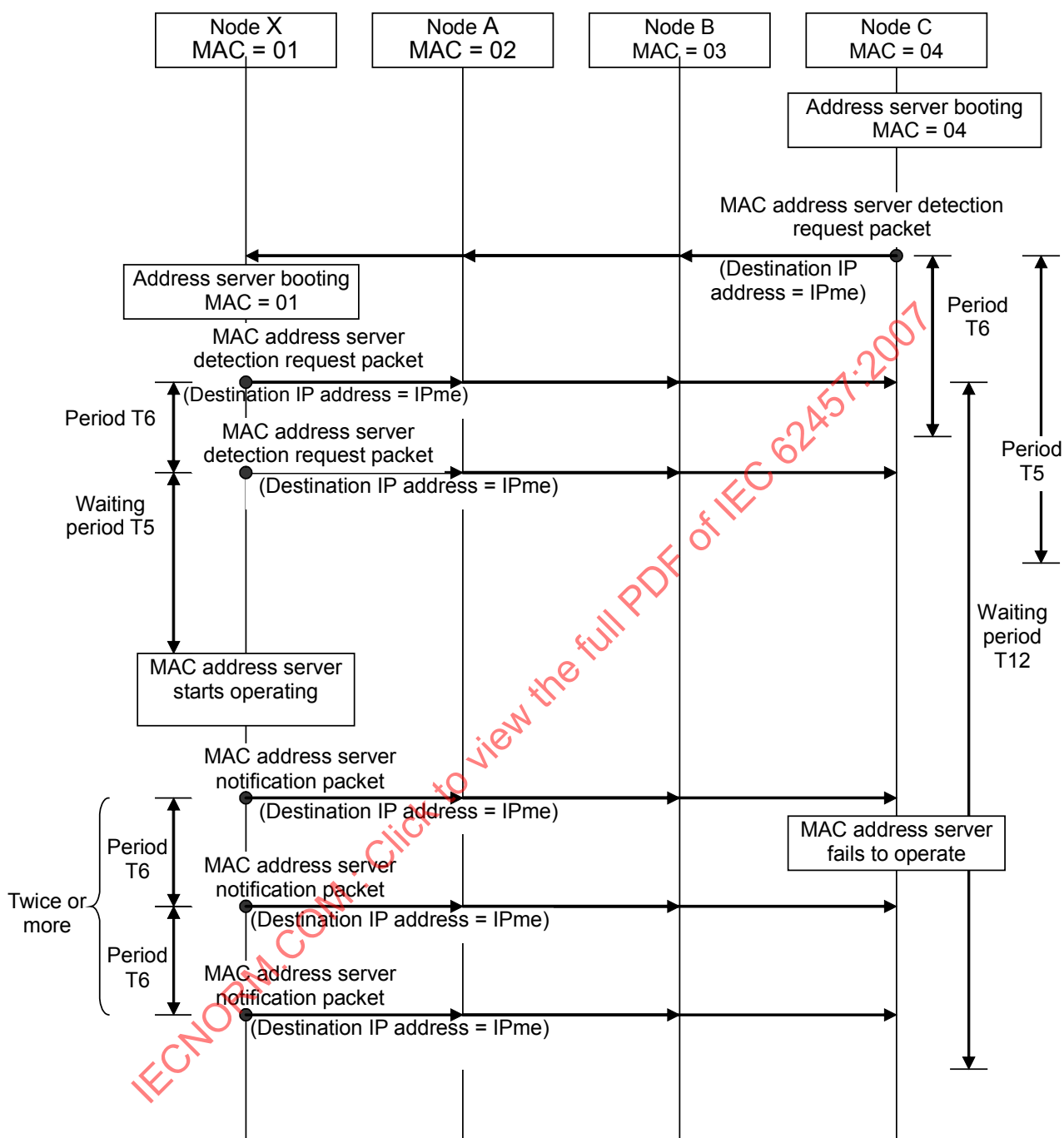


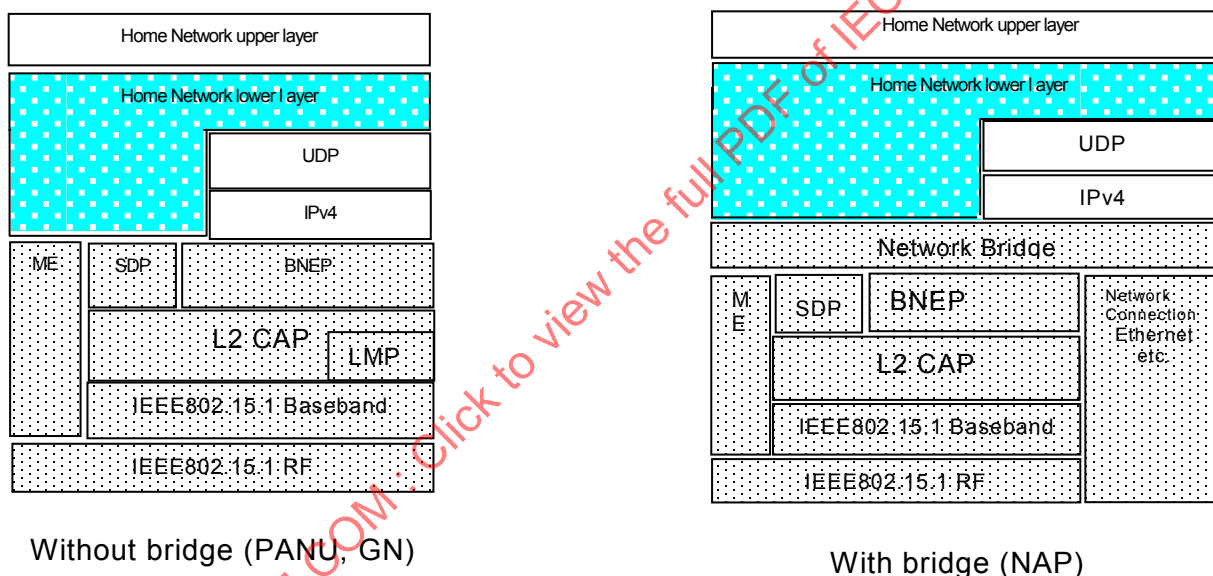
Figure B.2 – Near-simultaneous booting of two or more MAC address servers

Annex C (normative)

Requirements on IEEE 802.15.1

C.1 Usage of profile and layer structure

In this standard, one of the lower medium layers is IEEE 802.15.1 (refer to Normative reference, IEEE Std 802.15.1-2005, in clause 2). In this case, the Profile -PAN shall be used. Figure C.1 shows the layer structure. There are two cases defined by the PAN, depending on whether the Network Bridge layer is present or not. The Home Network layer is located above the UDP, IP and IEEE 802.15.1 related layers (BNEP, SDP, ME, etc) and the Network Bridge. The Home Network frames generated and processed in the Home Network layer are encapsulated into UDP/IP and IEEE 802.15.1 packets and transmitted between nodes. The portion defined for this standard is treated as an application layer by IEEE 802.15.1 and UDP/IP. For the Home Network lower layer, there is no distinction between master and slave as defined by IEEE 802.15.1.



NOTE1 :  Part defined in this standard

NOTE2 :  Part defined in IEEE802.15.1

Figure C.1 – Layer structure

C.2 Topology

The topology used in a Piconet defined by IEEE 802.15.1 is the star type topology. Communication between slave nodes, i.e., PAN User nodes in a Piconet, is made via one Network Access Point (NAP) or one Group Ad-hoc Network (GN) which behaves as a master. No PANU and GN node shall have a bridge function. Requirements for the accommodation of IEEE 802.15.1 are as follows:

- The smallest subnet unit in Home Network shall be Piconet. Each Piconet comprises a number of IEEE 802.15.1 nodes that are defined in IEEE 802.15.1. Connection between subnets shall be made by means of one or more Home Network routers, as with other media. Of course, a Piconet may contain a general IEEE 802.15.1 node.

Figure C.2 shows sample configurations. Figure C.3 is the case of IEEE 802.15.1 as it is shown in Figure 6 as a general case.

Figure C.4 provides an example of an unacceptable connection, in which Scatternet is used instead of Home Network routers for connection. Connection with other network shall be made using a Home Network Gateway that uses NAP/GN as shown in Figure C.5. A Piconet shall have only one Layer 2 bridge (NAP), and a Piconet shall be connected with other subnet by NAP, as shown Figure C.6.

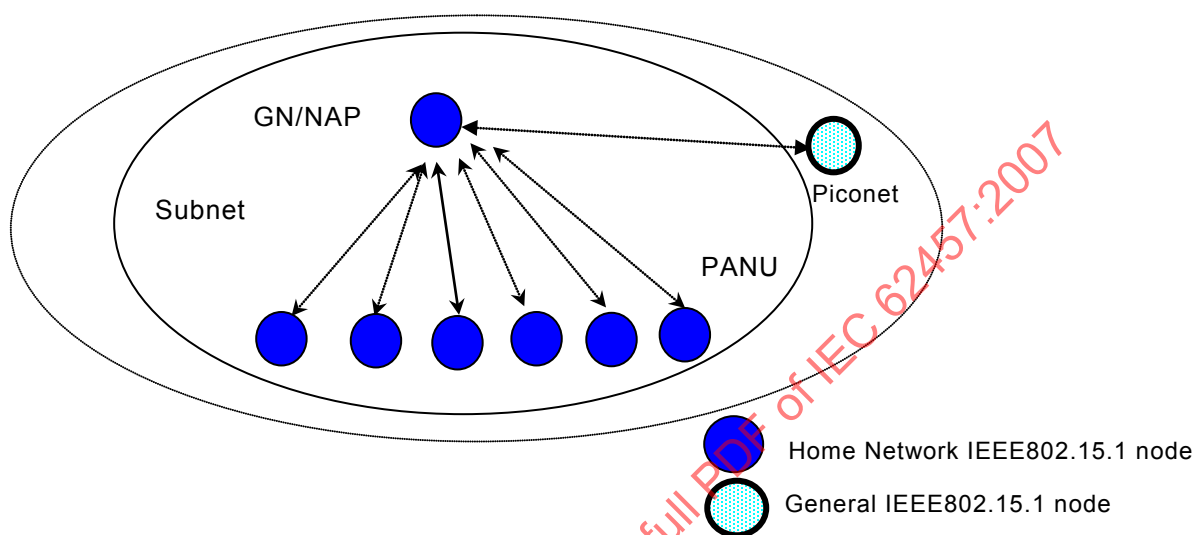


Figure C.2 – Basic form of subnet

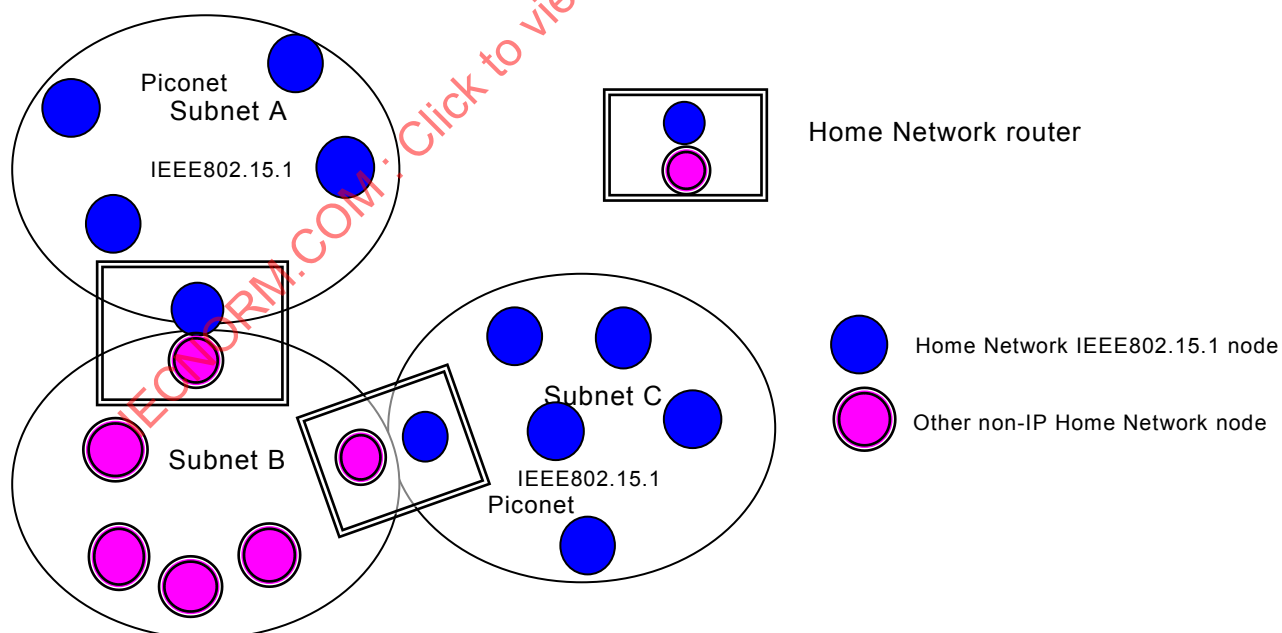


Figure C.3 – Example of a subnet connection using Home Network routers

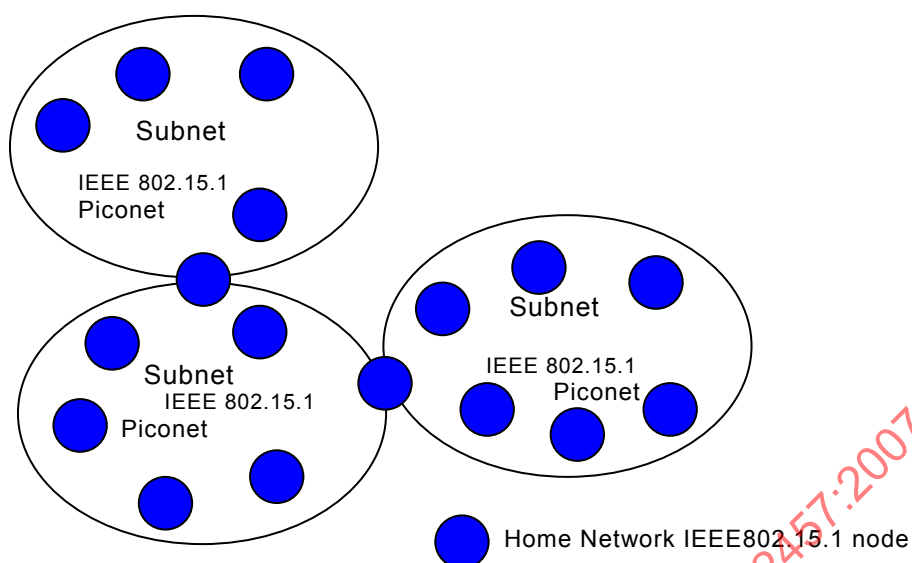


Figure C.4 – Example of an unacceptable subnet connection (scatternet)

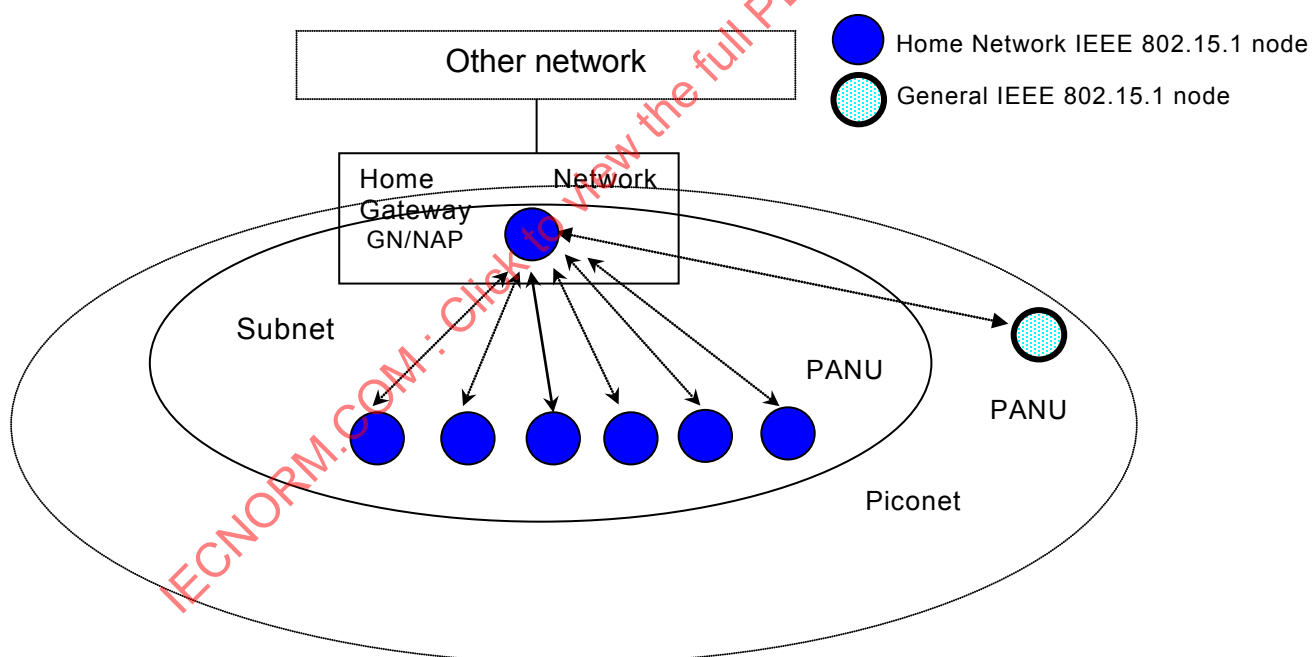


Figure C.5 – Example of a connection using a home network gateway

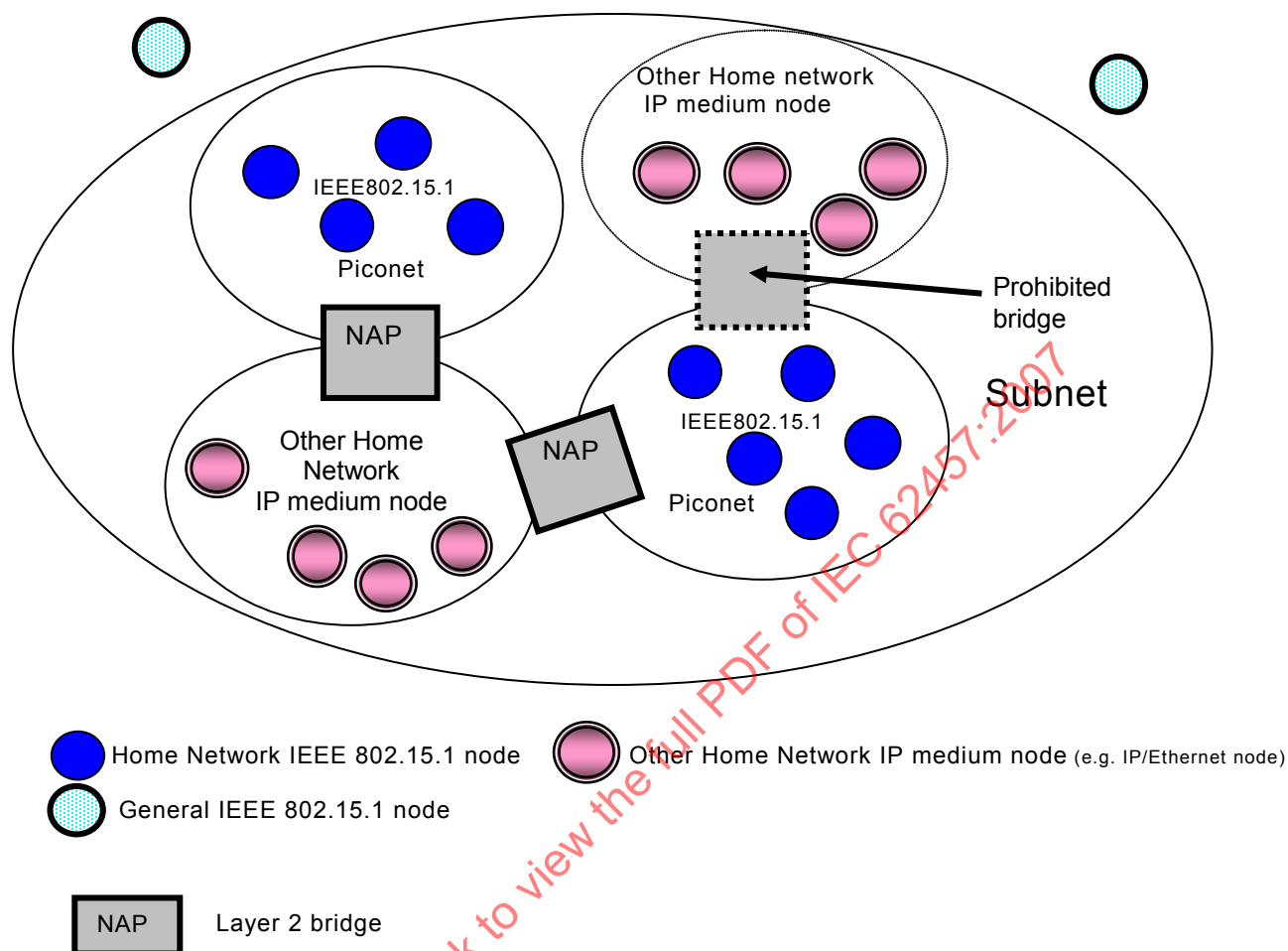


Figure C.6 Example of a subnet using Layer 2 bridges

a) Limit on the number of nodes

With the use of the Park mode defined in IEEE 802.15.1, a Piconet can be configured with IEEE 802.15.1 nodes with a theoretical maximum of 256 Network addresses. System designers, system operators, and other specialist shall determine the topology and the maximum number of nodes in the Piconet (the recommended maximum number of nodes in a Piconet is 32) in full consideration of the necessary response time, duration of operation, etc. The maximum number of nodes in a Piconet that can perform communication simultaneously (i.e., the maximum number of active PANU nodes) is 7.

b) Timeout period

The length of time during which the response packet from the destination node for a PANU, GN, or NAP packet is to be transmitted varies between systems and states depending on such factors as the NAP/GN packet transfer processing time, the number of PANUs, whether the Park mode is used, and whether the link is occupied by other applications. It also varies depending on whether or not a bridge is used, on the performance of the bridge, the processing speeds of individual nodes in the subnet, including the bridge, and the total number of nodes. This version of the standard specifies standard fixed timeout period values taking into account these conditions and interconnectivity considerations. Methods for dynamically determining timeout periods and related matters shall be specified in subsequent versions of this standard, as necessary.

In this standard, the standard for the interface with the IEEE 802.15.1 layer is given in relation to the Home Network lower layer shown in Figure C.7. This standard can be applied to Case 1 and Case 2 when there is a coexisting application other than a Home Network

application using the PAN, and to Case 3 when there is a coexisting profile other than the PAN. However, this standard does not specify a method for achieving coexistence with another application on the IEEE 802.15.1 layer. This standard shall be applied to PANUs, NAPs, and GNs as defined by the PAN Specification.

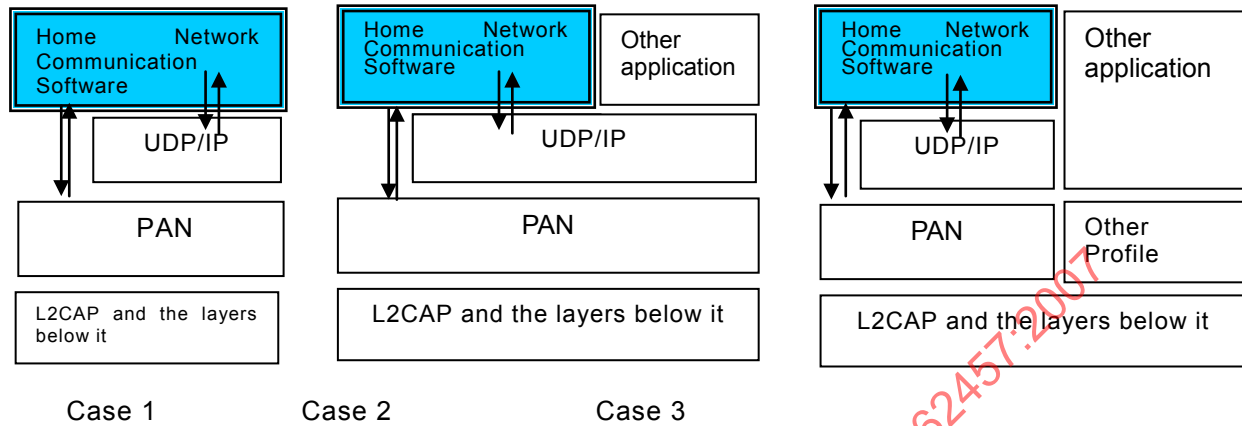


Figure C.7 – Examples of Home Network communication software implementation

C.3 Packet structure

The protocol specified for IP packet transfers over IEEE 802.15.1 is the BNEP. As shown in Figure C.8, BNEP replaces the Ethernet header of each Ethernet frame with a BNEP header to form a packet and transfers it over the IEEE 802.15.1 L2CAP link.

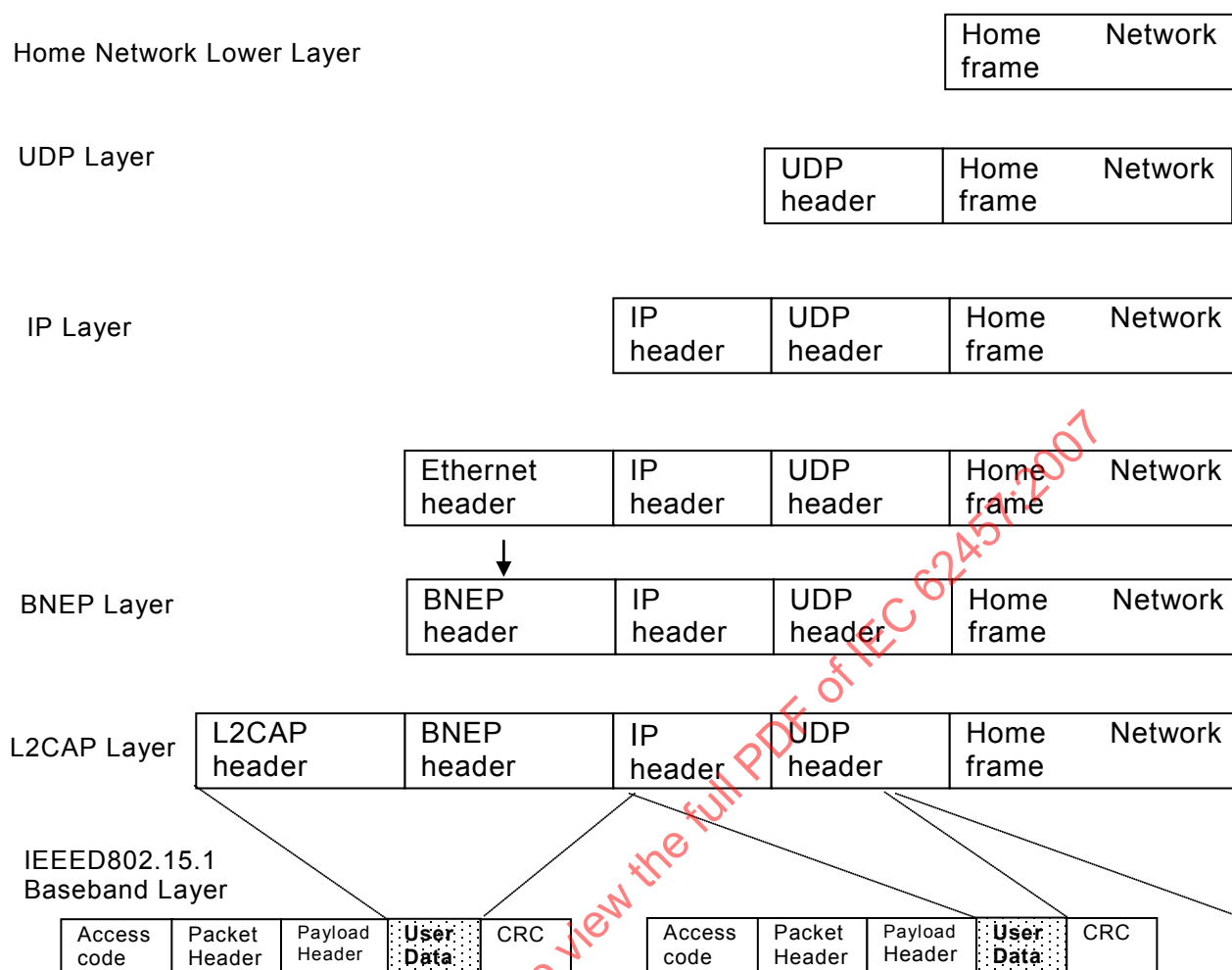


Figure C.8 – Packet structure

Bibliography

Bluetooth Specification Version 1.1 (Profile Specification)

Bluetooth Specification (Personal Area Networking Profile Version 1.0)

Bluetooth Specification (Bluetooth Network Encapsulation Protocol Version 1.0)

ECHONET Specification version 3.21 Part3,others

http://www.echonet.gr.jp/english/8_kikaku/index.htm

IETF RFC 791 Internet Protocol

IETF RFC 826 Address Resolution

IETF RFC 792 Internet Control Message Protocol

IETF RFC 950 Internet Standards Subnetting Procedure

IETF RFC 768 User Datagram Protocol

IETF RFC1541 Dynamic Host Configuration Protocol

IETF RFC1122 Requirements for Internet Hosts

IETF RFC1112 Internet Group Multicast Protocol

IETF RFC1597 Address Allocation for Private Internets

IECNORM.COM : Click to view the full PDF of IEC 62457:2007

IECNORM.COM : Click to view the full PDF of IEC 62457:2007

SOMMAIRE

AVANT-PROPOS	81
INTRODUCTION	83
1 Domaine d'application	88
2 Références normatives	90
3 Termes, définitions et abréviations	90
3.1 Termes et définitions	90
3.2 Abréviations	94
4 Interface TCP/IP (Protocole de commande de transmission/Protocole Internet, en anglais « Transmission Control Protocol/Internet Protocol ») et exigences	95
4.1 Vue d'ensemble	95
4.2 Topologie	97
4.3 Interface UDP (Protocole de datagramme utilisateur, en anglais « User Datagram Protocol »)	101
4.4 Format des paquets d'une trame d'un réseau résidentiel	101
4.4.1 Généralités	101
4.4.2 Transfert d'une trame de transmission d'un réseau résidentiel	104
4.4.3 Demande/réponse de résolution d'adresse MAC/IP	105
4.4.4 Demande/réponse de résolution d'adresse IP/MAC	106
4.4.5 Demande/réponse de résolution d'adresse matérielle/MAC	107
4.4.6 Demande/réponse d'initialisation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control »)	108
4.4.7 Réponse à l'initialisation de serveur d'adresses MAC/réponse à l'allocation d'adresse MAC	110
4.4.8 Demande/réponse de confirmation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control »)	111
4.4.9 Demande/réponse d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») à tous les nœuds	112
4.4.10 Demande/réponse de détection de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »), notification de serveur d'adresses MAC	113
4.4.11 Message de pilotage du réseau (destination invalide)	114
4.4.12 Message de pilotage du réseau (conflit de NMa (Adresses MAC de réseau, en anglais « Network MAC addresses »))	115
4.5 Séquences de communication de base	116
4.5.1 Généralités	116
4.5.2 Demande/réponse de résolution d'adresses MAC/IP (résolution de la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») dans l'adresse IP (Protocole Internet (en anglais, « Internet Protocol »))	117
4.5.3 Demande/réponse de résolution d'adresse IP/MAC (résolution de l'adresse IP (Protocole Internet, en anglais « Internet Protocol ») dans la NMa (Adresse MAC de réseau, en anglais « Network MAC address »))	118
4.5.4 Demande/réponse de résolution d'adresse matérielle/MAC	121
4.5.5 Demande/réponse d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») à tous les nœuds	123
4.5.6 Message de pilotage du réseau (destination invalide)	125
4.5.7 Cas particulier concernant les paquets avec des valeurs de destination invalides	126

4.5.8	Message de pilotage du réseau (conflit de NMa (Adresses MAC de réseau, en anglais « Network MAC addresses »)).....	127
4.6	Séquence d'amorçage d'acquisition de NMa (Adresse MAC de réseau, en anglais « Network MAC address »).....	129
4.6.1	Vue d'ensemble de la séquence d'amorçage d'acquisition de NMa (Adresse MAC de réseau, en anglais « Network MAC address »)	129
4.6.2	Vue d'ensemble du traitement après acquisition d'une adresse IP (Protocole Internet (en anglais, « Internet Protocol »).....	129
4.6.3	Nœud d'amorçage	130
4.6.4	Serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »).....	137
4.6.5	Nœuds fonctionnels.....	137
4.7	Serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »).....	140
4.7.1	Exigence concernant le serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »)	140
4.7.2	Séquence de traitement pour l'amorçage du serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »)	140
4.7.3	Traitement par serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») fonctionnel	141
4.8	Paramètres de période de temps.....	142
4.9	Disposition pour la mise à jour des données après acquisition de la NMa (Adresse MAC de réseau, en anglais « Network MAC address »)	144
5	TCP/IP (Protocole de commande de transmission/Protocole Internet, en anglais « Transmission Control Protocol/Internet Protocol ») et exigences	144
5.1	IP (Protocole Internet (en anglais, « Internet Protocol »)	144
5.1.1	Protocoles à utiliser	144
5.1.2	Adresse IP (Protocole Internet (en anglais, « Internet Protocol »).....	144
5.1.3	Adresse de multidiffusion.....	145
5.1.4	DHCP (Protocole de configuration de serveur dynamique, en anglais « Dynamic Host Configuration Protocol »)	145
5.1.5	Méthodes d'obtention d'une adresse IP (Protocole Internet, en anglais « Internet Protocol ») par détermination manuelle, etc.....	145
5.1.6	Routage.....	145
5.2	UDP (Protocole de datagramme utilisateur, en anglais « User Datagram Protocol »)	145
5.2.1	Protocoles à utiliser	145
5.2.2	Numéro de port	145
6	Interface et exigences spécifiques au support de couche inférieure.....	145
6.1	Interface et exigences du support de couche inférieure	145
6.2	Transition d'état interne logiciel.....	145
6.2.1	Vue d'ensemble.....	145
6.2.2	État d'arrêt	148
6.2.3	État de démarrage à froid	148
6.2.4	État de démarrage à chaud.....	149
6.2.5	État de suspension de communication	149
6.2.6	État de fonctionnement normal	150
6.2.7	État d'arrêt sur erreur	151
6.2.8	État d'arrêt temporaire.....	152
	Annexe A (informative) Séquence d'amorçage de base.....	153

Annexe B (informative) Séquence d'amorçage du serveur d'adresses MAC de base	164
Annexe C (normative) Exigences concernant l'IEEE 802.15.1	168
Bibliographie.....	179
Figure 1 – Groupe de relations entre des appareils domestiques et des matériels audiovisuels, des PC (Ordinateurs personnels, en anglais « Personal Computers ») et des matériels associés à un PC	85
Figure 2 – Exemples de communication de données entre un appareil domestique et des matériels audiovisuels, des PC (Ordinateurs personnels, en anglais « Personal Computers ») et des matériels associés à un PC	87
Figure 3 – Composition de la couche du réseau résidentiel et des parties spécifiées	89
Figure 4 – Encapsulation d'une trame de réseau résidentiel.....	96
Figure 5 – Exemple de sous-réseau utilisant des ponts de la couche 2	98
Figure 6 – Exemple de raccordement de sous-réseau utilisant des routeurs du réseau résidentiel.....	99
Figure 7 – Relation entre le sous-réseau IP (Protocole Internet, en anglais « Internet Protocol ») et le sous-réseau du réseau résidentiel.....	101
Figure 8 – Format des paquets d'une trame d'un réseau résidentiel	102
Figure 9 – Notation des bits dans le champ indicateur	104
Figure 10 – Adresse IEEE 802.15.1 décrite en bits	104
Figure 11 – Séquence de résolution d'adresse MAC/IP de base.....	118
rget IP address	120
Figure 12 – Séquence de résolution d'adresse IP/MAC de base.....	120
Figure 13 – Séquence de résolution d'adresse matérielle/MAC de base.....	122
Figure 14 – Séquence de base de « demande/réponse d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») à tous les nœuds ».....	124
Figure 15 – Séquence de traitement de base de « destination invalide »	126
Figure 16 – Séquence de base pour traiter le conflit de NMa (Adresses MAC de réseau, en anglais « Network MAC addresses ») détectée.....	128
Figure 17 – Organigramme de détermination de la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») provisoire à utiliser.....	132
Figure 18 – Vérification des NMa (Adresses MAC de réseau, en anglais « Network MAC addresses ») utilisées par les autres nœuds.....	134
Figure 19 – Exemple de NMa (Adresse MAC de réseau, en anglais « Network MAC address ») provisoire dupliquée	136
Figure 20 – Format pour UsedMAC	138
Figure 21 – Exemple de UsedMAC	139
Figure 22 – Transitions d'état interne logiciel	147
Figure A.1 – Amorçage A-MODE, NMa (Adresse MAC de réseau, en anglais « Network MAC address ») non conservées (avec serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »)).....	155
Figure A.2 – Amorçage SR-MODE, NMa (Adresse MAC de réseau, en anglais « Network MAC address ») non conservées (avec serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »))	156
Figure A.3 – Amorçage A-MODE, NMa (Adresse MAC de réseau, en anglais « Network MAC address ») non conservées (sans serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »)).....	158

Figure A.4 – Amorçage SR-MODE, NMa (Adresse MAC de réseau, en anglais « Network MAC address ») non conservées (sans serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »))	159
Figure A.5 – Amorçage A-MODE, NMa (Adresse MAC de réseau, en anglais « Network MAC address ») conservées (avec serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »))	161
Figure A.6 – Amorçage A-MODE, NMa (Adresse MAC de réseau, en anglais « Network MAC address ») conservées (sans serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »))	163
Figure B.1 – Amorçage d'un unique serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »)	165
Figure B.2 – Amorçage presque simultané de deux serveurs d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») ou plus	167
Figure C.1 – Structure de couche	169
Figure C.2 – Forme de base d'un sous-réseau	170
Figure C.3 – Exemple de raccordement de sous-réseau utilisant des routeurs de réseau résidentiel	171
Figure C.4 – Exemple de raccordement de sous-réseau inacceptable (scatternet)	172
Figure C.5 – Exemple de raccordement utilisant une passerelle de sous-réseau	173
Figure C.6 – Exemple de sous-réseau utilisant des ponts de la couche 2	174
Figure C.7 – Exemples de mise en œuvre de logiciel de communication de réseau	176
Figure C.8 – Structure d'un paquet	178
Tableau 1 – Numéros de type de paquet de la trame d'un réseau résidentiel	103
Tableau 2 – Type de matériel	104
Tableau 3 – Format des paquets de « Transfert de trame de transmission du réseau résidentiel »	105
Tableau 4 – Format des paquets de « demande de résolution d'adresse MAC/IP »	106
Tableau 5 – Format des paquets de « réponse à la résolution d'adresse MAC/IP »	106
Tableau 6 – Format des paquets de « demande de résolution d'adresse IP/MAC »	107
Tableau 7 – Format des paquets de « réponse à la résolution d'adresse IP/MAC »	107
Tableau 8 – Format des paquets de « demande de résolution d'adresse matérielle/MAC »	108
Tableau 9 – Format des paquets de « réponse à la résolution d'adresse matérielle/MAC »	108
Tableau 10 – Format des paquets de « demande d'initialisation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») »	109
Tableau 11 – Format des paquets de « réponse à l'initialisation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») »	110
Tableau 12 – Format des paquets de « réponse à l'initialisation de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») »	111
Tableau 13 – Format des paquets de « réponse à l'allocation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») »	111
Tableau 14 – Format des paquets de « demande de confirmation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») »	112
Tableau 15 – Format des paquets de « réponse à la confirmation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») »	112
Tableau 16 – Format des paquets de « demande d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») à tous les nœuds »	113

Tableau 17 – Format des paquets de « réponse à l'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») à tous les nœuds »	113
Tableau 18 – Format des paquets de « demande de détection de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») »	114
Tableau 19 – Format des paquets de « notifications de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») »	114
Tableau 20 – Format des paquets de « réponse à la détection de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») »	114
Tableau 21 – Format des paquets de « message de pilotage du réseau (destination invalide) »	115
Tableau 22 – Format des paquets de message de pilotage du réseau « conflit de NMa (Adresses MAC de réseau, en anglais « Network MAC addresses ») »	116
Tableau 23 – Tableau de relations d'adresses	116
Tableau 24 – Modes d'amorçage	129
Tableau 25 – Exemple de mémorisation des NMa (Adresses MAC de réseau, en anglais « Network MAC addresses ») allouées.....	142
Tableau 26 – Paramètres de période de temps	143

IECNORM.COM : Click to view the full PDF of IEC 62457:2007

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

**RÉSEAUX RÉSIDENTIELS MULTIMÉDIA –
PROTOCOLE DE COMMUNICATION DE RÉSEAU RÉSIDENTIEL
SUR IP DESTINÉ AUX APPAREILS DOMESTIQUES MULTIMÉDIA**

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 62457 a été établie par le domaine technique 9: Applications audio, vidéo et multimédia pour réseau d'utilisateur final, du comité d'études 100 de la CEI: Systèmes et appareils audio, vidéo et multimédia.

La présente version bilingue (2012-10) correspond à la version anglaise monolingue publiée en 2007-09.

Le texte anglais de cette norme est issu des documents 100/1197/CDV et 100/1271/RVC.

Le rapport de vote 100/1271/RVC donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française n'a pas été soumise au vote.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI sous "<http://webstore.iec.ch>" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

IECNORM.COM : Click to view the full PDF of IEC 62457:2007

INTRODUCTION

En permettant à des appareils domestiques de type autonome (appareils domestiques autres que les matériels audiovisuels, PC (Ordinateurs personnels, en anglais « Personal Computers ») et matériels associés à un PC), tels que des appareils électroménagers (par exemple, des climatiseurs, des réfrigérateurs), des capteurs, des appareils pour la santé, l'entraînement et la condition physique, de se raccorder et de fonctionner conjointement avec des matériels audiovisuels, des PC et/ou des matériels associés à un PC, il devient possible de proposer des services d'application multimédia tels que l'affichage sur un écran de télévision d'un message « lavage terminé » d'un lave-linge ou le fonctionnement d'un climatiseur par l'intermédiaire d'un écran de télévision, ce qui ne serait pas possible dans le cas contraire (voir Figure 1).

Pour réaliser ces services, une norme concernant les réseaux résidentiels pour des réseaux d'appareils domestiques de type autonome et des normes concernant les réseaux pour les matériels audiovisuels, PC (Ordinateurs personnels, en anglais « Personal Computers ») et matériels associés à un PC sont nécessaires. Il est également nécessaire de créer un système permettant à des matériels appartenant à un réseau d'échanger des données avec d'autres matériels de types de réseaux différents. Une approche couramment utilisée pour permettre à des réseaux de types différents d'échanger des données entre eux consiste à utiliser des passerelles.

Puisque les données transférées au sein de réseaux, dans les réseaux et hors des réseaux d'appareils domestiques de type autonome sont des données de commande, dont le volume est beaucoup plus petit que les données transférées de façon similaire sur des réseaux de matériels audiovisuels, de PC (Ordinateurs personnels, en anglais « Personal Computers ») et de matériels associés à un PC, et puisque les appareils domestiques de type autonome ont des durées de vie plus longues que les matériels audiovisuels, les PC et les matériels associés à un PC, les normes concernant les réseaux résidentiels pour des réseaux d'appareils domestiques de type autonome ont été élaborées séparément des normes de réseaux pour les matériels audiovisuels, les PC et les matériels associés à un PC, et un grand nombre de normes avec des protocoles différents sont utilisées depuis longtemps dans différents pays¹).

Par ailleurs, les progrès récents dans la technologie des dispositifs et des logiciels ont permis de mettre en œuvre TCP/IP (Protocole de commande de transmission/Protocole Internet, en anglais « Transmission Control Protocol/Internet Protocol ») (qui a été adopté dans le monde entier pour les matériels audiovisuels, les PC (Ordinateurs personnels, en anglais « Personal Computers ») et les matériels associés à un PC) dans certains appareils domestiques de type autonome et ainsi, la détermination d'une norme pour les réseaux résidentiels pour des réseaux d'appareils domestiques de type autonome prenant la forme d'une norme pour les couches supérieures à TCP/IP, permettent d'échanger directement des données entre des appareils domestiques et des matériels audiovisuels, PC et matériels associés à un PC, par l'intermédiaire de TCP/IP (voir Figure 2, exemple 1, exemple 2). Ceci permet alors la création de services d'application multimédia permettant à des appareils domestiques de fonctionner conjointement avec des matériels audiovisuels, des PC et des matériels associés à un PC.

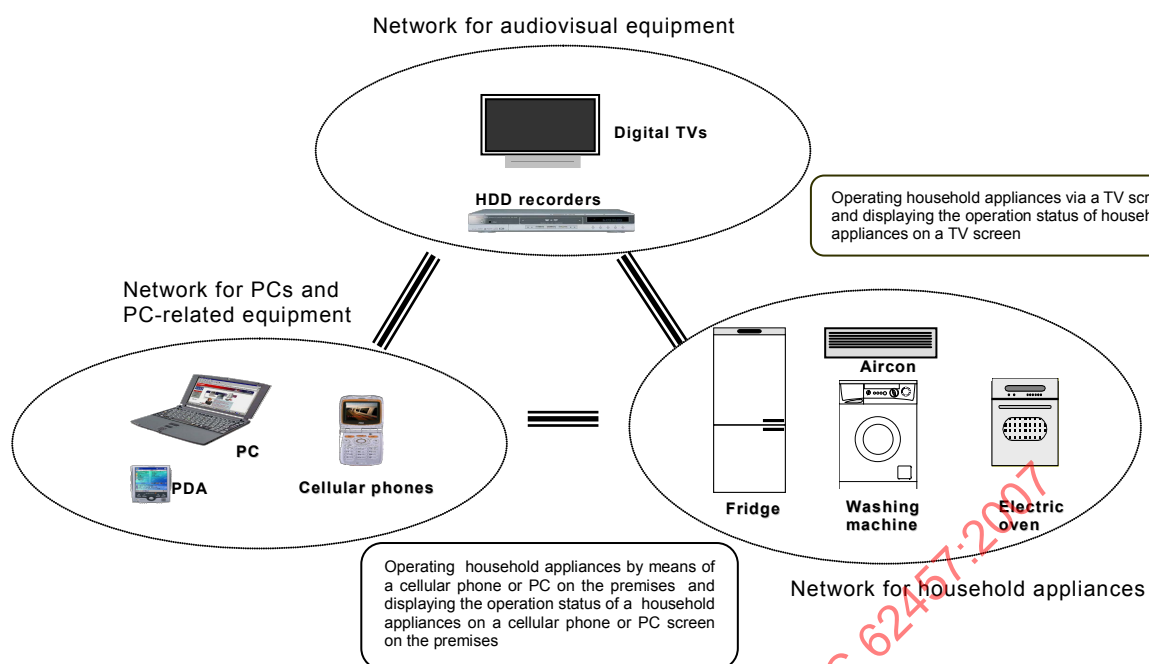
Les avantages de l'application de cette norme sont les suivants:

- Elle peut être appliquée à un grand nombre de types de normes de réseaux résidentiels.
- Les nœuds d'un réseau résidentiel avec et sans couche TCP/IP (Protocole de commande de transmission/Protocole Internet, en anglais « Transmission Control Protocol/Internet Protocol ») peuvent coexister dans le même logiciel médiateur de réseaux résidentiels.
- Les appareils domestiques peuvent communiquer avec des matériels audiovisuels, des PC (Ordinateurs personnels, en anglais « Personal Computers ») et des matériels associés à un PC et inversement, sans nécessiter aucune passerelle.

¹ CEBus, ECHONET, Konnex, LonTalk, et d'autres.

- Les appareils domestiques peuvent gérer des données textuelles et audiovisuelles.
- Les matériels audiovisuels, les PC et les matériels associés à un PC peuvent gérer les données d'appareils domestiques.
- Les appareils domestiques peuvent choisir librement un support approprié d'une couche inférieure parmi divers supports de couches inférieures, en dessous de TCP/IP.

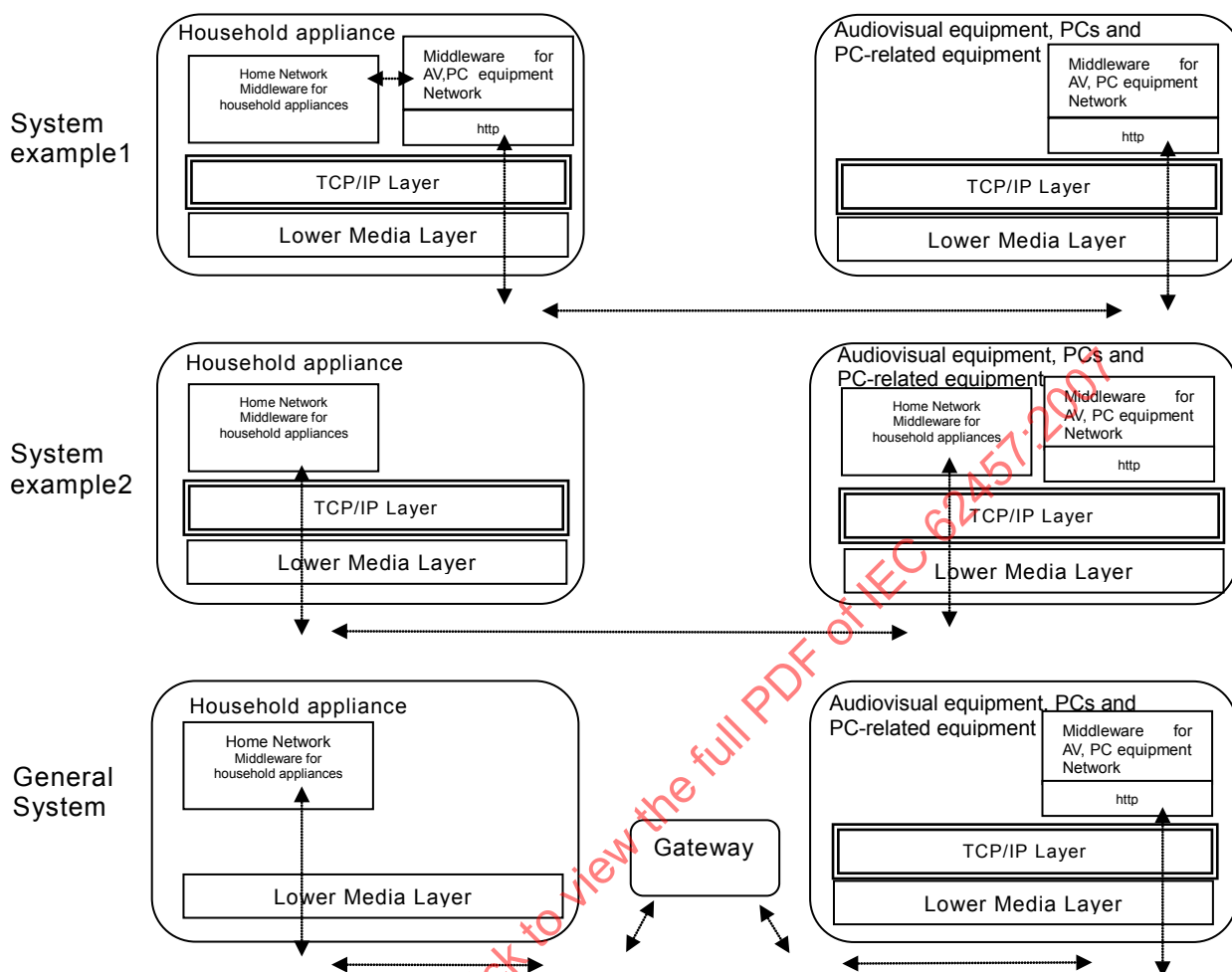
IECNORM.COM : Click to view the full PDF of IEC 62457:2007



Légende

Anglais	Français
Network for audiovisual equipment	Réseau d'appareils audiovisuels
Digital TVs	Téléviseurs numériques
HDD recorders	Magnétoscopes à disque dur
Network for PCs and PC-related equipment	Réseau de PC et matériels associés à un PC
PC	PC
PDA	Assistant numérique personnel
Cellular phones	Téléphones portables
Operating household appliances via a TV screen and displaying the operation status of household appliances on a TV screen	Exploitation des appareils domestiques par l'intermédiaire d'un écran de télévision et affichage de l'état de fonctionnement des appareils domestiques sur un écran de télévision
Fridge	Réfrigérateur
Aircon	Climatiseur
Washing machine	Lave-linge
Electric oven	Four électrique
Operating household appliances by means of a cellular phone or PC on the premises and displaying the operation status of a household appliances on a cellular phone or PC screen on the premises	Exploitation des appareils domestiques au moyen d'un téléphone portable ou d'un PC sur place et affichage de l'état de fonctionnement des appareils domestiques sur un téléphone portable ou sur un écran de PC sur place
Network for household appliances	Réseau d'appareils domestiques

Figure 1 – Groupe de relations entre des appareils domestiques et des matériels audiovisuels, des PC (Ordinateurs personnels, en anglais « Personal Computers ») et des matériels associés à un PC



Légende

Anglais	Français
System example 1	Exemple de système 1
Household appliance	Appareil domestique
Home Network Middleware for household appliances	Logiciel médiateur de réseau résidentiel pour appareils domestiques
Middleware for AV, PC equipment Network	Logiciel médiateur pour réseau d'appareils AV, PC
TCP/IP Layer	Couche TCP/IP
Lower Media Layer	Couche support inférieure
Audiovisual equipment, PCs and PC-related equipment	Matériel audiovisuel, PC et matériels associés à un PC
Middleware for AV, PC equipment Network	Logiciel médiateur de réseau résidentiel pour appareils domestiques
TCP/IP Layer	Couche TCP/IP
Lower Media Layer	Couche support inférieure
System example 2	Exemple de système 2
Household appliance	Appareil domestique
Home Network Middleware for household appliances	Logiciel médiateur de réseau résidentiel pour appareils domestiques
TCP/IP Layer	Couche TCP/IP
Lower Media Layer	Couche support inférieure

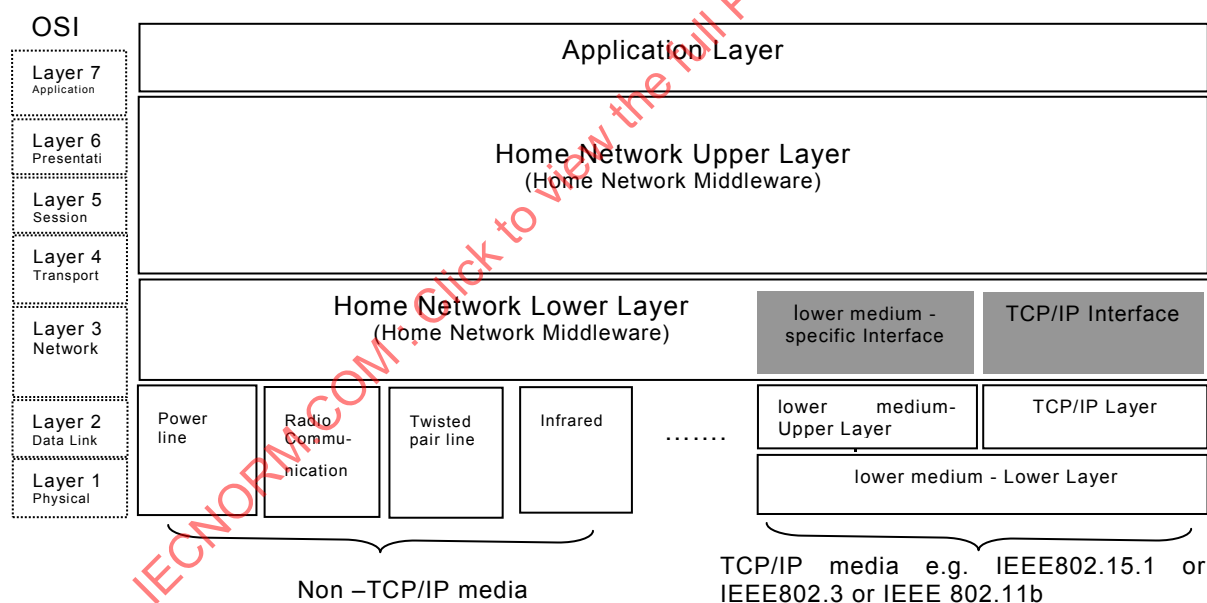
Anglais	Français
Audiovisual equipment, PCs and PC-related equipment	Matériel audiovisuel, PC et matériels associés à un PC
Home Network Middleware for household appliances	Logiciel médiateur de réseau résidentiel pour appareils domestiques
Middleware for AV,PC equipment Network	Logiciel médiateur pour réseau d'appareils AV, PC
TCP/IP Layer	Couche TCP/IP
Lower Media Layer	Couche support inférieure
General system	Système général
Household appliance	Appareil domestique
Home Network Middleware for household appliances	Logiciel médiateur de réseau résidentiel pour appareils domestiques
Lower Media Layer	Couche support inférieure
Gateway	Passerelle
Audiovisual equipment, PCs and PC-related equipment	Matériel audiovisuel, PC et matériels associés à un PC
Middleware for AV,PC equipment Network	Logiciel médiateur pour réseau d'appareils AV, PC
TCP/IP Layer	Couche TCP/IP
Lower Media Layer	Couche support inférieure

Figure 2 – Exemples de communication de données entre un appareil domestique et des matériels audiovisuels, des PC (Ordinateurs personnels, en anglais « Personal Computers ») et des matériels associés à un PC

RÉSEAUX RÉSIDENTIELS MULTIMÉDIA – PROTOCOLE DE COMMUNICATION DE RÉSEAU RÉSIDENTIEL SUR IP DESTINÉ AUX APPAREILS DOMESTIQUES MULTIMÉDIA

1 Domaine d'application

La présente Norme internationale spécifie les exigences relatives à l'interface entre la couche inférieure d'un réseau résidentiel pour un réseau résidentiel local d'appareils domestiques de type autonome et la couche TCP/IP (Protocole de commande de transmission/Protocole Internet, en anglais « Transmission Control Protocol/Internet Protocol ») lorsqu'on souhaite introduire une couche TCP/IP à chacun des nœuds comprenant ce réseau résidentiel d'appareils domestiques de type autonome. L'interface spécifiée dans la couche inférieure du réseau résidentiel est constituée de 2 parties, l'interface TCP/IP et l'interface inférieure spécifique au support. La Figure 3 montre la composition de la couche du réseau résidentiel et des parties normalisées. La présente norme spécifie à l'Annexe C, les exigences pour l'interface inférieure spécifique au support. L'une de ces couches doit être l'IEEE 802.15.1, (des couches supplémentaires relatives à la norme concernant la radio à courte portée pourront être ajoutées dans l'avenir).



NOTE 1 Les parties colorées en gris sont normalisées.

NOTE 2 L'interface TCP/IP (Protocole de commande de transmission/Protocole Internet, en anglais « Transmission Control Protocol/Internet Protocol ») est la même, même si le support inférieur est différent, toutefois l'interface spécifique au support intérieur est différente.

NOTE 3 La couche inférieure du réseau résidentiel et la couche supérieure du réseau résidentiel sont respectivement élaborées pour CEBus, ECHONET, Konnex, LonTalk et d'autres.

NOTE 4 Chaque couche OSI (Interface de systèmes ouverts, en anglais « Open System Interface ») est mappée grossièrement sur chaque couche du réseau résidentiel.

Légende

Anglais	Français
Layer 7 Application	Couche 7 Application
Layer 6 Presentation	Couche 6 Présentation
Layer 5 Session	Couche 5 Session
Layer 4 Transport	Couche 4 Transport
Layer 3 Network	Couche 3 Réseau
Layer 2 Data Link	Couche 2 Liaison de données
Layer 1 Physical	Couche 1 Physique
Application Layer	Couche application
Home Network Upper Layer (Home Network Middleware)	Couche supérieure du réseau résidentiel (Logiciel médiateur de réseau résidentiel)
Home Network Lower Layer (Home Network Middleware)	Couche inférieure du réseau résidentiel (Logiciel médiateur de réseau résidentiel)
Lower medium-specific interface	Interface spécifique au support inférieur
TCP/IP Interface	Interface TCP/IP
Power line	Réseau électrique
Radio communication	Communication radio
Twisted pair line	Ligne à paire torsadée
Infrared	Infrarouge
Non-TCP/IP media	Support non TCP/IP
lower medium- Upper Layer	Couche supérieure support inférieur
TCP/IP Layer	Couche TCP/IP
Lower medium - Lower Layer	Couche supérieure support moyen
TCP/IP media e.g. IEEE802.15.1 or IEEE802.3 or IEEE802.11b	Support TCP/IP, par exemple IEEE802.15.1 ou IEEE802.3 ou IEEE802.11b

Figure 3 – Composition de la couche du réseau résidentiel et des parties spécifiées

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEEE Std 802.15.1-2005, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs)*

3 Termes, définitions et abréviations

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1 Termes et définitions

3.1.1

Bluetooth

technologie sans fil constituant une spécification mondiale pour une solution radio économique à petite échelle, assurant des liaisons entre des ordinateurs mobiles, des téléphones portables, d'autres dispositifs portatifs et la connectivité avec Internet

NOTE La spécification est élaborée, publiée et promue par le « Bluetooth Special Interest Group » (SIG). Les principales spécifications sont adoptées dans la norme IEEE 802.15.1. Dans cette norme, Bluetooth signifie IEEE 802.15.1.

3.1.2

protocole d'encapsulation de réseau Bluetooth BNEP

protocole spécifié dans Bluetooth. Un paquet IP (Protocole Internet, en anglais « Internet Protocol ») est encapsulé conformément à ce protocole

3.1.3

démarrage à froid

méthode de démarrage du réseau résidentiel en lançant un traitement de paramétrage initial tout en abandonnant les informations antérieures relatives aux adresses réseau

3.1.4

réseaux ad hoc de groupe

GN

picoréseau comprenant un maître et un esclave, comme défini dans l'IEEE 802.15.1 et qui n'est raccordé à aucun réseau ou nœud extérieur

3.1.5

adresse matérielle

Ha

adresse basée sur une configuration d'adressage spécifique au support

3.1.6

réseau résidentiel

nom générique pour diverses normes de réseau résidentiel de type matériel pour des appareils domestiques

NOTE Ceci se réfère de façon spécifique à CEBus, Konnex, ECHONET, LonTalk, etc.

3.1.7

dispositif de réseau résidentiel

dispositif domestique, dispositif électrique domestique ou dispositif d'un bâtiment/magasin, par exemple un éclairage, un climatiseur, la réfrigération, des matériels d'alimentation électrique, des appareils domestiques ordinaires, des capteurs, des dispositifs d'actionnement, etc.

NOTE Un nœud de réseau résidentiel muni d'une interface de communication et d'une fonction compatible du système conforme à la norme relative aux réseaux résidentiels. Un nœud de réseau résidentiel muni d'une fonction de contrôleur pour l'unité de commande centralisée avec des fonctions de surveillance, de commande et leur exploitation ou une unité fonctionnelle (commande à distance, etc.).

3.1.8

domaine de réseau résidentiel

zone du réseau à l'intérieur de laquelle la transmission d'informations est logiquement garantie par le réseau résidentiel

NOTE On considère généralement que le contrôle de propriété et de sécurité incluant des domiciles et des magasins, s'effectue en utilisant la même zone qu'un domaine, mais le domaine n'est limité par aucune norme.

3.1.9

trame de réseau résidentiel

trame générée dans la couche inférieure du réseau résidentiel, comme spécifié par la présente norme; la trame est constituée d'une trame de transmission du réseau résidentiel ou d'un paquet de gestion associé

3.1.10

passerelle de réseau résidentiel

nœud du réseau résidentiel raccordant un domaine du réseau résidentiel à un système extérieur (incluant d'autres domaines de réseau résidentiel)

NOTE Il peut exister dans le domaine des passerelles de réseau résidentiel multiples selon les différences entre le ou les systèmes extérieurs à raccorder.

3.1.11

couche inférieure de réseau résidentiel

interface entre la couche supérieure du réseau résidentiel et la couche supérieure du support inférieur

NOTE Certaines parties dépendent des caractéristiques du support. La présente norme est contenue dans cette couche. Cette couche est principalement constituée des couches OSI (Interface de systèmes ouverts, en anglais « Open System Interface ») 3, 4, et 2.

3.1.12

routeur maître de réseau résidentiel

routeur effectuant l'acquisition d'un identifiant de réseau au moment de l'initialisation et le mémorisant; il existe un routeur maître de réseau résidentiel dans chaque sous-réseau du réseau résidentiel

3.1.13

nœud de réseau résidentiel

nœud de communication conforme à la norme des réseaux résidentiels appelé ici « nœud » sauf spécification contraire

NOTE Dans un réseau résidentiel, un nœud de réseau résidentiel est une fonction de communication du réseau résidentiel identifiée de manière unique par une adresse réseau. Il n'y a aucune distinction entre les fonctions d'application des nœuds. Le terme nœud est utilisé pour décrire la fonction d'un terminal de communication du réseau résidentiel.

3.1.14

routeur de réseau résidentiel

nœud d'un réseau résidentiel utilisé pour raccorder des sous-réseaux du réseau résidentiel

NOTE Un routeur de réseau résidentiel raccorde les sous-réseaux de différents protocoles de communication de couche inférieure (pour des protocoles différents, quel que soit le type de support de transmission) ou divise le même protocole en sous-réseaux. Le protocole de communication de couche inférieure est raccordé sans jonction sur le système utilisant le traitement de routage en se basant sur les adresses réseau comme fonction.

3.1.15

sous-réseau de réseau résidentiel

groupe de nœuds dans le domaine du réseau résidentiel utilisant le même support ou des supports différents raccordés par des ponts de couche 2, appelé ici « sous-réseau » sauf spécification contraire

NOTE Chaque sous-réseau possède un identifiant de réseau. Des sous-réseaux différents peuvent être raccordés par un routeur de réseau résidentiel.

3.1.16

trame de transmission de réseau résidentiel

trame générée par la couche supérieure du réseau résidentiel et transmise entre des nœuds par l'intermédiaire de la couche inférieure du réseau résidentiel

NOTE Chaque réseau résidentiel possède son propre format de trame mais une trame de transmission d'un réseau résidentiel contient normalement des en-têtes, des informations d'adresse, des informations d'acquisition et de paramétrage pour d'autres nœuds.

3.1.17

couche supérieure de réseau résidentiel

bloc de traitement du logiciel médiateur de communication du réseau résidentiel

NOTE La couche supérieure du réseau résidentiel exécute le traitement du protocole de communication pour simplifier le traitement réalisé lorsque le logiciel applicatif commande à distance ou surveille des dispositifs, enregistre les informations nécessaires à cet effet et gère diverses autres informations incluant celles qui concernent l'état du dispositif lui-même ainsi que des autres dispositifs. Cette couche est principalement constituée des couches OSI (Interface de systèmes ouverts, en anglais « Open System Interface ») 4, 5, 6 et 7.

3.1.18

IPme

adresse de multidiffusion IP

cette adresse est utilisée pour la multidiffusion IP (Protocole Internet (en anglais, « Internet Protocol »). Le numéro spécifique est assigné à la présente norme

3.1.19

pont de couche 2

dispositif utilisé pour mémoriser et transférer des paquets

NOTE Les ponts de couche 2 recouvrent jusqu'à la couche 2 OSI (Interface de systèmes ouverts, en anglais « Open System Interface ») (couche liaison de données). Les ponts de couche 2 sont classés en différents types par fonction incluant des ponts transparents qui suppriment ou transfert des paquets en se basant sur les valeurs d'adresse MAC (Commande d'accès au réseau, en anglais « Medium Access Control »), des ponts convertisseurs qui effectuent des conversions d'en-tête MAC et des ponts de routage source ayant la possibilité supplémentaire de gérer des informations de chemin de destination. Les ponts de couche 2 sont définis dans la norme IEEE Std 802.1D.

3.1.20

serveur d'adresses MAC

serveur qui alloue des adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») de réseau dans un sous-réseau

3.1.21

identifiant de réseau

identifiant de sous-réseau; c'est également un composant d'une adresse réseau

3.1.22**points d'accès au réseau****NAP**

point d'accès raccordé à Internet jouant le rôle de maître IEEE 802.15.1. Les esclaves IEEE 802.15.1 sont raccordés à un IEEE 802.15.1 maître pour former un picoréseau et ainsi, sont raccordés à Internet

3.1.23**adresse réseau****Na**

adresse permettant une identification unique d'un nœud d'un réseau résidentiel dans le domaine

NOTE Cette adresse permet au bloc de traitement de communication du réseau résidentiel et au logiciel applicatif d'ignorer les différences entre les logiciels de communication de la couche inférieure. Une adresse réseau est une adresse logique définie séparément de l'adresse matérielle pour le logiciel de communication de la couche inférieure; elle est constituée d'au moins un identifiant de réseau et un identifiant de nœud.

3.1.24**adresse MAC de réseau****NMa**

adresse unique de la couche inférieure du réseau résidentiel permettant d'effectuer une communication de couche 2 (support de transmission)

NOTE Cette adresse pour chaque nœud du réseau résidentiel est assignée de manière unique dans le sous-réseau du réseau résidentiel par la couche inférieure du réseau résidentiel du nœud du réseau résidentiel lui-même ou du serveur d'adresses MAC.

3.1.25**identifiant de nœud**

identifiant utilisé pour identifier de manière unique un nœud du réseau résidentiel dans le sous-réseau du réseau résidentiel

NOTE Un identifiant de nœud est une adresse logique convertie à partir de la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») par la couche supérieure du réseau résidentiel. C'est un composant d'une adresse réseau.

3.1.26**mode de parcade**

mode à faible consommation d'énergie, défini dans la spécification IEEE 802.15.1

NOTE Lorsqu'on entre dans ce mode, deux adresses différentes sont données par le maître et la synchronisation est maintenue après cela par des impulsions de balise périodiques provenant du maître. Dans le mode de parcade, une négociation pour annuler le mode de parcade peut être effectuée pendant la période de la fenêtre de pré-réglage.

3.1.27**profil d'interconnexion de réseau personnel****PAN**

spécifié dans Bluetooth

NOTE Ce profil est destiné à une communication IP (Protocole Internet, en anglais « Internet Protocol ») sur IEEE 802.15.1. Un paquet IP est encapsulé par le BNEP (Protocole d'encapsulation de réseau Bluetooth, en anglais « Bluetooth Network Encapsulation Protocol ») et se comporte comme une mise en réseau Ethernet.

3.1.28**utilisateur de profil d'interconnexion de réseau personnel****PANU**

nœuds esclaves spécifiés dans la mise en réseau personnel

3.1.29**picoréseau**

réseau ayant un seul maître et de deux esclaves ou plus, comme spécifié dans l'IEEE 802.15.1

3.1.30

profil

les profils spécifient les fonctions de communication Bluetooth et les exigences du protocole dans le but de maintenir l'interconnectivité

NOTE Dans la spécification Bluetooth, version 1.1, un profil d'accès générique, un profil de port série, etc., sont définis.

3.1.31

réseau éclaté

réseau ressemblant à deux picoréseaux ou plus raccordés entre eux en raison de la manière en « série temporelle » selon laquelle un nœud appartient à l'un des deux picoréseaux ou plus

3.1.32

protocole de découverte de service

SDP

lors de l'établissement d'une liaison entre deux nœuds, ce protocole (qui est défini dans l'IEEE 802.15.1) est utilisé pour acquérir des enregistrements de service (classe de service, protocole, etc.) détenus par les nœuds

3.1.33

démarrage à chaud

méthode de démarrage du réseau résidentiel en lançant un traitement de paramétrage initial tout en conservant les informations antérieures relatives aux adresses réseau et aux réglages initiaux

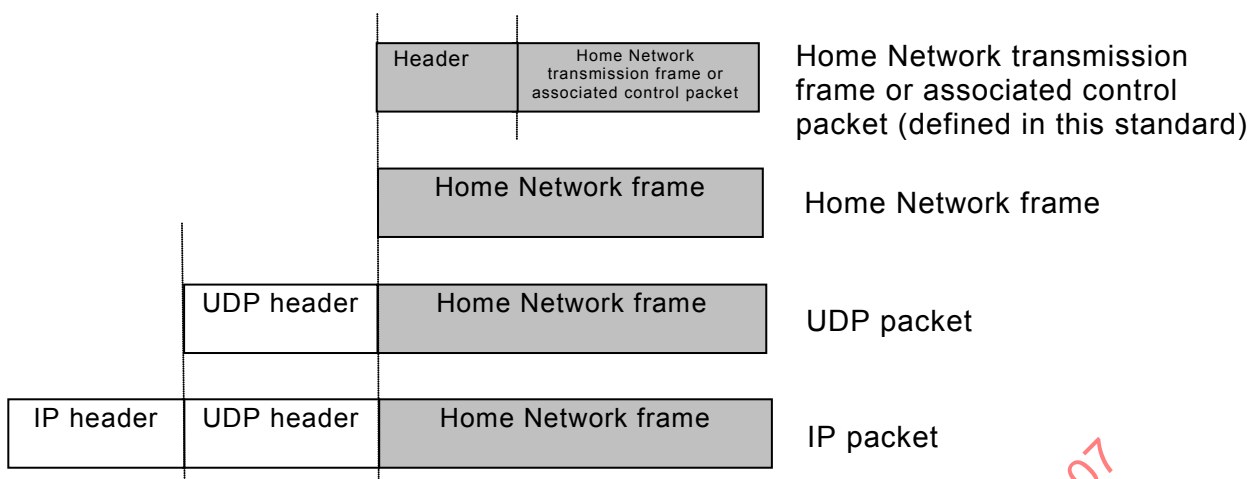
3.2 Abréviations

BNEP	Protocole d'encapsulation de réseau Bluetooth (en anglais, « Bluetooth Network Encapsulation Protocol »)
DHCP	Protocole de configuration de serveur dynamique (en anglais, « Dynamic Host Configuration Protocol »)
GN	Réseaux ad hoc de groupe (en anglais, « Group Ad-hoc Networks »)
Ha	Adresse matérielle (en anglais, « Hardware address »)
IP	Protocole Internet (en anglais, « Internet Protocol »)
Ipme	Adresse de multidiffusion IP (en anglais, « IP multicast address »)
LSB	Bit le moins significatif (en anglais, « Least Significant bit »)
MAC	Commande d'accès au support (en anglais, « Media Access Control »)
MSB	Bit le plus significatif (en anglais: « Most Significant bit »)
Na	Adresse réseau (en anglais, « Network Address »)
NAP	Point d'accès au réseau (en anglais, « Network Access Point »)
Nma	Adresse MAC de réseau (en anglais, « Network MAC address »)
OSI	Interface de systèmes ouverts (en anglais, « Open System Interface »)
PAN	Profil d'interconnexion de réseau personnel (en anglais, « Personal Area Networking Profile »)
PANU	Utilisateur de profil d'interconnexion de réseau personnel (en anglais, « Personal Area Networking Profile User »)
SDP	Protocole de découverte de service (en anglais, « Service Discovery Protocol »)
TCP	Protocole de commande de transmission (en anglais, « Transmission Control Protocol »)
UDP	Protocole de datagramme utilisateur (en anglais, « User Datagram Protocol »)

4 Interface TCP/IP (Protocole de commande de transmission/Protocole Internet, en anglais « Transmission Control Protocol/Internet Protocol ») et exigences

4.1 Vue d'ensemble

Lorsqu'on introduit un support de couche inférieure dans des réseaux résidentiels, certains réseaux résidentiels nécessitent une définition d'un réseau au protocole Internet (IP (en anglais, « Internet Protocol »)) tandis que d'autres ne le nécessitent pas; il convient que la sélection soit effectuée conformément aux exigences de l'application. La présente norme contient des normes internationales pour les protocoles exploités sur IP. Dans le cas où des réseaux résidentiels fonctionnent sur un réseau IP, chaque sous-réseau d'un réseau résidentiel est mappé sur un sous-réseau IP et les trames du réseau résidentiel (trames de transmission du réseau résidentiel ou paquets de commande associés) sont encapsulées dans des paquets IP et transférées sur le réseau IP (voir Figure 4). Les réseaux IP sont classés en réseaux IPv4 et IPv6; la présente norme utilise IPv4. Chaque nœud d'un réseau résidentiel doit avoir une adresse IP, qui doit être une adresse IP globale unique ou une adresse IP privée, en plus d'une adresse matérielle. Bien que la présente norme ne spécifie pas de méthode pour acquérir les adresses IP, l'utilisation d'un nœud comme nœud de réseau résidentiel précède l'acquisition d'une adresse IP. Le protocole de transfert de réseau IP utilisé pour transférer une trame d'un réseau résidentiel doit être le protocole de datagramme utilisateur (UDP (en anglais « User Datagram Protocol »)) sans connexion. Lors du transfert d'une trame du réseau résidentiel, l'UDP doit utiliser en permanence le numéro de port spécifié dans la présente norme. Chaque trame d'un réseau résidentiel est encapsulée dans un paquet UDP. Chaque nœud d'un réseau résidentiel doit également avoir une adresse réseau (Na, en anglais « Network Address ») dans la couche supérieure du réseau résidentiel et une adresse MAC de réseau (NMa, en anglais « Network MAC address ») dans la couche inférieure du réseau résidentiel, en plus de l'adresse IP. Pour les adresses de destination et les adresses d'expéditeur pour les trames de transmission d'un réseau résidentiel, on doit utiliser la Na. Pour les adresses de destination et les adresses d'expéditeur pour les trames d'un réseau résidentiel pour les en-têtes IP, on doit utiliser les adresses IP. Tous les nœuds d'un réseau résidentiel opérant sur un sous-réseau IP doivent être capables d'utiliser les adresses de multidiffusion IP assignées pour le réseau résidentiel. Une trame de réseau résidentiel destinée à être diffusée ou à être diffusée par groupe est mappée sur des paquets de multidiffusion IP adressés à l'adresse de multidiffusion IP spécifiée. Puisqu'il existe un grand nombre de supports autres qu'IEEE 802.15.1, IEEE 802.3, etc. qui ont été définis comme support de couche inférieure, ils ont leurs propres structures en couches, fonctions, schémas d'adressage et topologies. La présente norme définit également les interfaces comme interfaces spécifiques au support qui sont séparées de l'interface TCP/IP (Protocole de commande de transmission/Protocole Internet, en anglais « Transmission Control Protocol/Internet Protocol »).



Légende

Anglais	Français
Header	En-tête
Home Network transmission frame or associated control packet	Trame de transmission du réseau résidentiel ou paquet de commande associé
Home Network transmission frame or associated control packet (defined in this standard)	Trame de transmission du réseau résidentiel ou paquet de commande associé (défini dans la présente norme)
Home Network Frame	Trame du réseau résidentiel
Home Network Frame	Trame du réseau résidentiel
UDP Header	En-tête UDP
Home Network Frame	Trame du réseau résidentiel
UDP packet	Paquet UDP
UDP header	En-tête UDP
IP header	En-tête IP
UDP header	En-tête UDP
Home Network Frame	Trame du réseau résidentiel
IP packet	Paquet IP

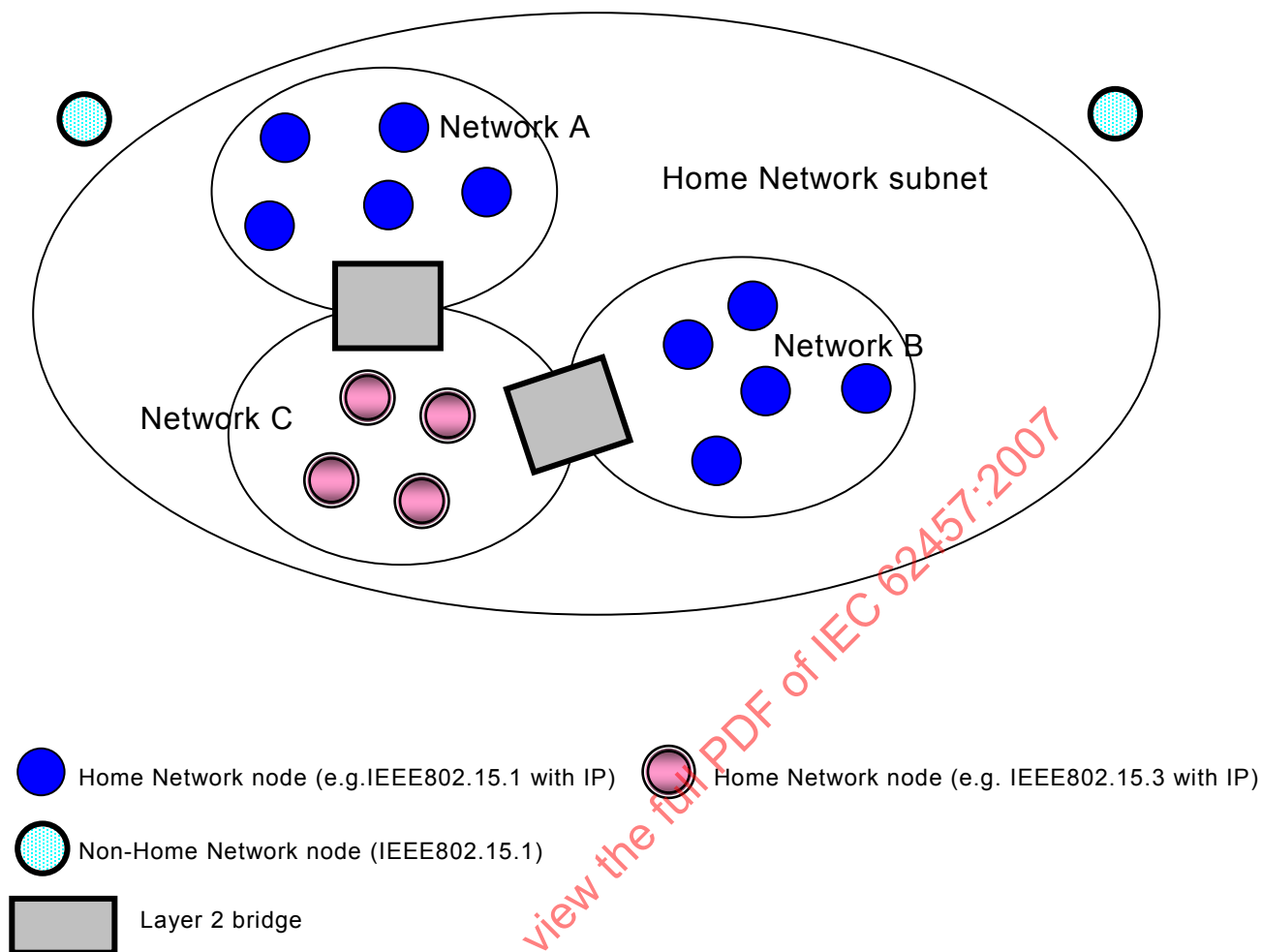
Figure 4 – Encapsulation d'une trame de réseau résidentiel

La séquence d'amorçage d'acquisition de NMA (Adresse MAC de réseau, en anglais « Network MAC address ») est spécifiée dans la présente norme. Chaque nœud du réseau résidentiel possède une Na (Adresse réseau, en anglais « Network Address ») unique qui est contenue dans la couche supérieure du réseau résidentiel, permettant d'identifier le nœud, quel que soit les types de support ou avec IP (Protocole Internet, en anglais « Internet Protocol ») ou avec non-IP. Chacun des composants d'une Na correspond de façon unique à une NMA déterminée par la couche inférieure du réseau résidentiel au moment de l'initialisation. La présente norme stipule trois méthodes de détermination de NMA, la méthode du serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »), la méthode distribuée n'utilisant aucun serveur d'adresses MAC et la méthode de détermination manuelle. Dans la présente norme, trois modes de détermination d'adresse sont acceptables: a) le « Mode nécessitant un serveur » (SR-MODE), où un serveur d'adresses MAC doit toujours être utilisé pour la détermination de la NMA avec un administrateur; b) le « Mode automatique » (A-MODE), où il n'existe aucun serveur d'adresses MAC dans lequel le mécanisme de détermination de la NMA est utilisé d'une manière distribuée; et c) le « Mode manuel » (M-MODE), dans lequel les NMA sont définies manuellement.

4.2 Topologie

Les exigences d'hébergement communes pour tous les types de support IP (Protocole Internet, en anglais « Internet Protocol ») sont les suivantes:

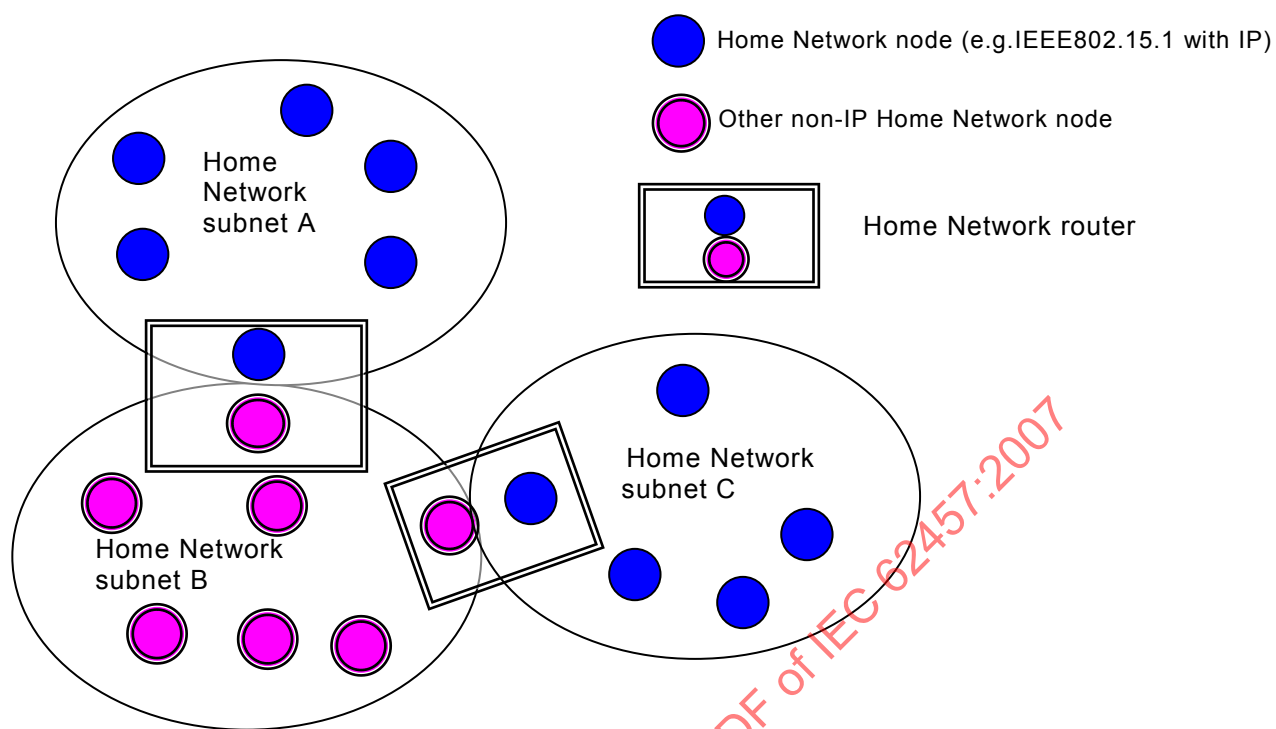
- a) Un sous-réseau IP unique contenant des nœuds utilisant des supports différents raccordés au moyen de ponts de la couche 2 doit être traité comme un sous-réseau du réseau résidentiel. C'est-à-dire que des ensembles de nœuds utilisant des supports différents du réseau résidentiel mais raccordés en utilisant des ponts de la couche 2 sont définis comme un sous-réseau unique du réseau résidentiel. Ceci permet à des ensembles de nœuds utilisant des supports différents d'être raccordés sans utiliser aucun routeur du réseau résidentiel et élimine les modifications d'identifiant de réseau pendant le transport du nœud dans le sous-réseau. Lorsqu'un pont de la couche 2 doit être utilisé, l'exigence de temporisation des paquets du réseau résidentiel spécifiée dans la présente norme doit être satisfaite. La Figure 5 montre un exemple de réseau de raccordement de ponts, A, B, C sur cette figure sont des réseaux de base avec la même couche inférieure et la même couche IP.
- b) Les nœuds du réseau résidentiel doivent être raccordés par des routeurs de réseau résidentiel, sous-réseau par sous-réseau, sans tenir compte de l'existence de la couche IP. Un exemple est représenté à la Figure 6.
- c) Dans un réseau comprenant deux sous-réseaux IP ou plus raccordés au moyen d'un routeur IP ou de routeurs IP, les sous-réseaux du réseau résidentiel doivent être contenus dans le sous-réseau IP respectif. C'est-à-dire qu'il n'est pas autorisé d'utiliser un réseau IP comprenant deux sous-réseaux IP ou plus raccordés au moyen d'un routeur IP ou de routeurs IP comme un sous-réseau du réseau résidentiel. Le raccordement entre des sous-réseaux du réseau résidentiel doit être réalisé au moyen d'un routeur de réseau résidentiel ou de routeurs du réseau résidentiel. Une communication du réseau résidentiel par l'intermédiaire d'un routeur IP n'est pas autorisée. La Figure 7 montre un exemple de ce type de raccordement.



Légende

Anglais	Français
Network A	Réseau A
Home Network subnet	Sous-réseau du réseau résidentiel
Network B	Réseau B
Network C	Réseau C
Home Network node (e.g. IEEE802.15.1 with IP)	Nœud du réseau résidentiel (par exemple IEEE802.15.1 avec IP)
Home Network node (e.g. IEEE802.15.3 with IP)	Nœud du réseau résidentiel (par exemple IEEE802.15.3 avec IP)
Non-Home Network node (e.g. IEEE802.15.1)	Nœud du réseau non résidentiel (par exemple IEEE802.15.1)
Layer 2 bridge	Pont couche 2

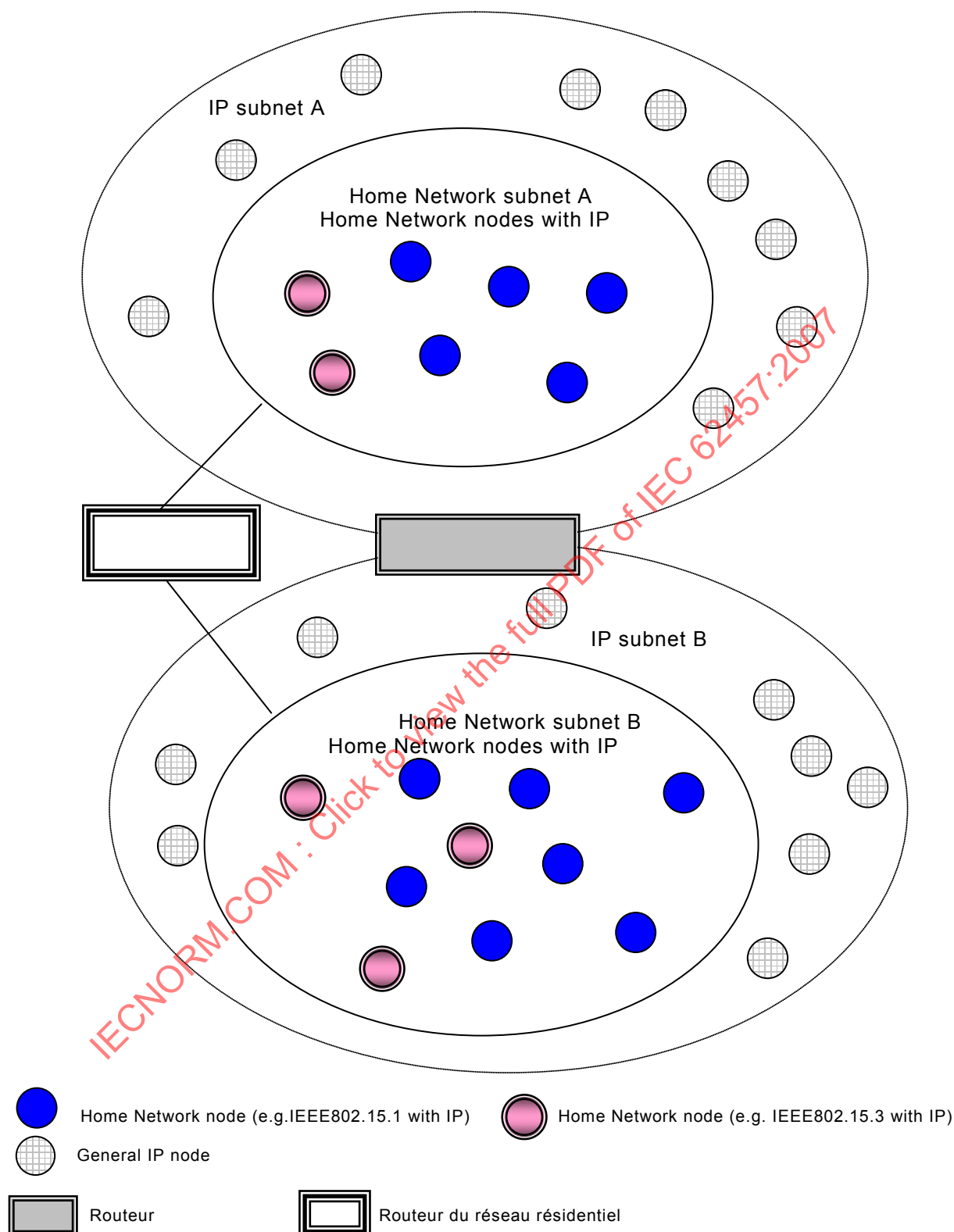
Figure 5 – Exemple de sous-réseau utilisant des ponts de la couche 2



Légende

Anglais	Français
Home Network node (e.g. IEEE802.15.1 with IP)	Nœud du réseau résidentiel (par exemple IEEE802.15.1 avec IP)
Other non-IP Home Network node	Autre nœud du réseau résidentiel non IP
Home Network router	Routeur du réseau résidentiel
Home Network subnet A	Sous-réseau du réseau résidentiel A
Home Network subnet B	Sous-réseau du réseau résidentiel B
Home Network subnet C	Sous-réseau du réseau résidentiel C

Figure 6 - Exemple de raccordement de sous-réseau utilisant des routeurs du réseau résidentiel



Légende

Anglais	Français
IP subnet A	Sous-réseau IP A
Home Network subnet A	Sous-réseau du réseau résidentiel A
Home Network nodes with IP	Noeuds du réseau résidentiel avec IP
IP subnet B	Sous-réseau IP B
Home Network subnet B	Sous-réseau du réseau résidentiel B
Home Network nodes with IP	Noeuds du réseau résidentiel avec IP
Home Network node (e.g. IEEE802.15.1 with IP)	Nœud du réseau résidentiel (par exemple IEEE802.15.1 avec IP)
Home Network node (e.g. IEEE802.15.3 with IP)	Nœud du réseau résidentiel (par exemple IEEE802.15.3 avec IP)
General IP node	Nœud IP général

Figure 7 – Relation entre le sous-réseau IP (Protocole Internet, en anglais « Internet Protocol ») et le sous-réseau du réseau résidentiel

4.3 Interface UDP (Protocole de datagramme utilisateur, en anglais « User Datagram Protocol »)

Pour accéder à UDP/IP par une application UDP/IP, une interface de connexion ou une interface équivalente est normalement utilisée. Ces interfaces dépendent du système d'exploitation et de l'environnement de développement. Pour les détails, voir les normes de l'interface UDP/IP relatives à la plate-forme de développement spécifique.

4.4 Format des paquets d'une trame d'un réseau résidentiel

4.4.1 Généralités

Les trames d'un réseau résidentiel qui sont générées par une interface TCP/IP (Protocole de commande de transmission/Protocole Internet, en anglais « Transmission Control Protocol/Internet Protocol ») doivent être encapsulées dans des paquets UDP (Protocole de datagramme utilisateur, en anglais « User Datagram Protocol ») lorsqu'elles sont transférées sur Internet. Ces paquets doivent être transférés en y attachant le numéro de port UDP 3610. Ce numéro doit concerner le port de réception. Le numéro de port doit être le même quel que soit le type de paquet (monodiffusion, multidiffusion ou diffusion large).

Un paquet de trame du réseau résidentiel préparé pour une trame de transmission du réseau résidentiel et 9 types de paquets de trame du réseau résidentiel pour la gestion du réseau sont spécifiés comme suit:

- transfert d'une trame de transmission d'un réseau résidentiel
- demande/réponse de résolution d'adresse MAC/IP (résolution d'une adresse IP d'après la NMa (Adresse MAC de réseau, en anglais « Network MAC address »))
- demande/réponse de résolution d'adresse IP/MAC (résolution de la NMa d'après l'adresse IP)
- demande/réponse de résolution d'adresse matérielle/MAC (résolution de la NMa d'après la Ha (Adresse matérielle, en anglais « Hardware address »))
- demande/réponse d'initialisation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control »), réponse à l'initialisation du serveur d'adresses MAC
- réponse à l'allocation d'adresse MAC
- demande/réponse de confirmation d'adresse MAC
- demande/réponse d'adresse MAC à tous les nœuds

- demande/réponse de détection de serveur d'adresses MAC, notification de serveur d'adresses MAC
- message de pilotage du réseau (destination invalide/conflit de NMa)

Puisque tous ces types de paquets sont multiplexés sur le même port UDP (Protocole de datagramme utilisateur, en anglais « User Datagram Protocol »), il est nécessaire d'utiliser des numéros de type de paquet pour le multiplexage. Ces paquets sont donc multiplexés sur des paquets UDP en utilisant le format présenté à la Figure 8 ci-dessous. L'entrée dans la section « numéro de version » doit toujours être 0x01.

Numéro de version (0x01)	Numéro de type de paquet	Dépend du numéro de type de paquet
--------------------------	--------------------------	------------------------------------

Figure 8 – Format des paquets d'une trame d'un réseau résidentiel

Les numéros de type de paquet sont présentés dans le Tableau 1. « Obligatoire pour tous les nœuds » dans la colonne « Support » signifie que tous les nœuds du réseau résidentiel doivent prendre en charge des paquets ayant le numéro de type de paquet indiqué. « Obligatoire uniquement pour les serveurs d'adresses » signifie qu'il est exigé des seuls nœuds pouvant devenir un serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») d'avoir le numéro de type de paquet indiqué.

IECNORM.COM : Click to view the full PDF of IEC 62457:2007

Tableau 1 – Numéros de type de paquet de la trame d'un réseau résidentiel

Numéro de type de paquet	Type de paquet	Prise en charge
0	Transfert d'une trame de transmission d'un réseau résidentiel	Obligatoire pour tous les nœuds
1	Demande de résolution d'adresse MAC/IP	Obligatoire pour tous les nœuds
2	Réponse à la résolution d'adresse MAC/IP	Obligatoire pour tous les nœuds
3	Demande de résolution d'adresse IP/MAC	Facultative pour tous les nœuds
4	Réponse à la résolution d'adresse IP/MAC	Obligatoire pour tous les nœuds
5	Demande de résolution d'adresse matérielle/MAC	Facultative pour tous les nœuds
6	Réponse à la résolution d'adresse matérielle/MAC	Obligatoire pour tous les nœuds
7	Demande d'initialisation d'adresse MAC	Obligatoire pour tous les nœuds (non exigé pour les nœuds à mode de détermination manuelle seulement)
8	Réponse à l'initialisation d'adresse MAC	Obligatoire pour tous les nœuds
9	Réponse à l'initialisation de serveur d'adresses MAC	Obligatoire pour tous les serveurs d'adresses
10	Réponse à l'allocation d'adresse MAC	Obligatoire pour tous les nœuds (non exigé pour les nœuds à mode de détermination manuelle seulement)
11	Demande de confirmation d'adresse MAC	Obligatoire pour tous les nœuds (non exigé pour les nœuds à mode de détermination manuelle seulement)
12	Réponse à la confirmation d'adresse MAC	Obligatoire pour tous les nœuds
13	Demande d'adresse MAC à tous les nœuds	Obligatoire pour tous les serveurs d'adresses
14	Réponse à l'adresse MAC à tous les nœuds	Obligatoire pour tous les nœuds
15	Demande de détection de serveur d'adresses MAC	Obligatoire pour tous les serveurs d'adresses
16	Notification de serveur d'adresses MAC	Obligatoire pour tous les serveurs d'adresses
17	Réponse à la détection de serveur d'adresses MAC	Obligatoire pour tous les serveurs d'adresses
18	Message de pilotage du réseau (destination invalide)	Facultative pour tous les nœuds
19	Message de pilotage du réseau (conflit de NMa)	Facultative pour tous les nœuds
Autre que ci-dessus	Réservé pour une future utilisation	

Dans la présente norme, le terme « multidiffusion » signifie « multidiffusion vers tous les nœuds du réseau résidentiel dans le sous-réseau du réseau résidentiel » sauf spécification contraire. Les paquets de multidiffusion sont encapsulés dans des paquets IP (Protocole Internet, en anglais « Internet Protocol ») adressés à l'adresse de multidiffusion IP assignée (appelée également « IPme ») et envoyés aux nœuds du réseau résidentiel.

Le « Type de matériel » et la « longueur de l'adresse matérielle » suivent dans le Tableau 2.

Tableau 2 – Type de matériel

Type matériel	de	Non du matériel	Type d'adresse matérielle	Longueur d'adresse matérielle
0x00		IEEE 802.15.1	IEEE 802	48 bits
0x01		Ethernet ou IEEE 802.3	IEEE 802	48 bits
0x02		IEEE 802.11	IEEE 802	48 bits
Autre que ci-dessus		Réservé pour une future utilisation		

Pour les champs comportant le commentaire « Entrée nulle » ou « Bourrage », « 0x00 » doit être utilisé dans tout le reste de la présente norme. Dans l'explication des formats de paquets de la présente norme, le MSB (Bit le plus significatif, en anglais « Most Significant bit ») doit se référer au bit le plus à gauche et le LSB (Bit le moins significatif, en anglais « Least Significant bit ») au bit le plus à droite. Dans le champ indicateur dans certains tableaux de formats de paquets, le bit 7 doit se référer au MSB et le bit 0 au LSB, comme représenté à la Figure 9. Les champs sur plusieurs octets doivent être transmis, le MSB en premier et le LSB en dernier (« Big-endian »).

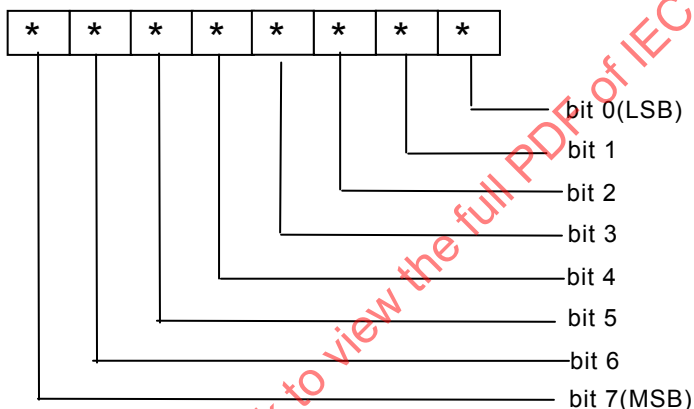


Figure 9 – Notation des bits dans le champ indicateur

L'unité de dimension utilisée dans la présente norme est l'octet.

Un exemple d'ordre des bits dans le cas de l'adresse IEEE 802.15.1 utilisée comme Ha (Adresse matérielle, en anglais « Hardware address ») est présenté à la Figure 10. Dans ce cas, 0x « acde48000080 » est entré dans le paquet.

MSB		LSB
company_id		company_assigned
NAP	UAP	LAP
1010110011011110	01001000	000000000000000010000000

Figure 10 – Adresse IEEE 802.15.1 décrite en bits

Les adresses IP (Protocole Internet, en anglais « Internet Protocol ») représentées par une notation avec virgule décimale sont traitées de façon similaire. Par exemple, « 192.168.10.5 » est entrée dans le paquet sous la forme « 0xc0a80a05 ».

4.4.2 Transfert d'une trame de transmission d'un réseau résidentiel

La définition et le format sont décrits ci-dessous.

- a) Enregistrement d'une trame de transmission du réseau résidentiel qui a été reçue depuis la couche supérieure du réseau résidentiel ou la couche UDP (Protocole de datagramme utilisateur, en anglais « User Datagram Protocol »).
- b) Le nœud transmettant la trame de transmission du réseau résidentiel doit être appelé nœud de transmission et le nœud qui reçoit la trame de transmission du réseau résidentiel doit être appelé nœud de réception.
- c) La trame de transmission d'un réseau résidentiel doit être transférée avec le type de matériel du nœud de transmission, la longueur de Ha (Adresse matérielle, en anglais « Hardware address »), la Ha, la NMa (Adresse MAC de réseau, en anglais « Network MAC address »), et la NMa attachée du nœud de réception.
- d) Lorsque la trame de transmission du réseau résidentiel à transmettre est une trame de diffusion large ou de diffusion de groupe, la valeur de la NMa du nœud de transmission doit être entrée dans la colonne relative à la NMa du nœud de réception.

NOTE La détection de la trame à partir du protocole (CEBus, ECHONET, Konnex, LonTalk, autres) ne fait pas partie du domaine d'application de la présente norme.

Le Tableau 3 ci-dessous indique le format des paquets de « Transfert de trame de transmission du réseau résidentiel ».

Tableau 3 – Format des paquets de « Transfert de trame de transmission du réseau résidentiel »

Élément	Taille (octets)	Explication
Version	1	Entrer « 0x01 » (Version 1)
Type	1	Entrer « 0x00 » (Transfert d'une trame de transmission du réseau résidentiel)
DMAC	1	NMa du nœud de réception
SMAC	1	NMa du nœud de transmission
SHType	1	Type de matériel du nœud de transmission
SHLen	1	Longueur de la Ha du nœud de transmission
SHAddr	SHLen	Ha du nœud de transmission
Msg		Enregistrement direct de la trame de transmission du réseau résidentiel

4.4.3 Demande/réponse de résolution d'adresse MAC/IP

La définition et le format sont décrits ci-dessous.

- a) Utilisée pour obtenir l'adresse IP (Protocole Internet, en anglais « Internet Protocol ») d'un nœud du réseau résidentiel possédant une NMa (Adresse MAC de réseau, en anglais « Network MAC address »).
- b) Le nœud qui souhaite résoudre la NMa (c'est-à-dire, qui souhaite connaître l'adresse IP) doit être appelé « nœud demandeur » et le nœud qui notifie la relation entre les adresses dans la réponse à la demande doit être appelé « nœud cible ».
- c) Le nœud demandeur effectue une multidiffusion vers le sous-réseau du réseau résidentiel d'un paquet de demande de résolution d'adresse IP contenant la NMa à résoudre. Lors de la réception de la demande, le nœud cible envoie un paquet de réponse à la résolution d'adresse IP contenant l'adresse correspondante si TMac et THLen sont exactement les mêmes que pour le nœud cible.

Le Tableau 4 ci-dessous indique le format des paquets de demande de résolution d'adresse MAC/IP.

Tableau 4 – Format des paquets de « demande de résolution d'adresse MAC/IP »

Élément	Taille (octets)	Explication
Version	1	Entrer « 0x01 » (Version 1)
Type	1	Type de paquet (demande de résolution d'adresse MAC/IP; entrer « 0x01 »)
Bourrage	1	Bourrage
RMAC	1	NMa du nœud demandeur
RIPAddr	4	Adresse IP du nœud demandeur
RHType	1	Type de matériel du nœud demandeur
RHLen	1	Longueur de la Ha du nœud demandeur
RHAddr	RHLen	Ha du nœud demandeur
Bourrage	1	Bourrage
TMAC	1	NMa du nœud cible
TIPAddr	4	Adresse IP du nœud cible (Entrer « null »)
THType	1	Type de matériel du nœud cible (Entrer « null »)
THLen	1	Longueur de la Ha du nœud cible (Entrer « RHLen »)
THAddr	THLen	Ha du nœud cible (Entrer « null »)

Le Tableau 5 ci-dessous indique le format des paquets de réponse à la résolution d'adresse MAC/IP.

Tableau 5 – Format des paquets de « réponse à la résolution d'adresse MAC/IP »

Élément	Taille (octets)	Explication
Version	1	Entrer « 0x01 » (Version 1)
Type	1	Type de paquet (réponse à la résolution d'adresse MAC/IP; entrer « 0x02 »)
Bourrage	1	Bourrage
RMAC	1	NMa du nœud demandeur
RIPAddr	4	Adresse IP du nœud demandeur
RHType	1	Type de matériel du nœud demandeur
RHLen	1	Longueur de la Ha du nœud demandeur
RHAddr	RHLen	Ha du nœud demandeur
Bourrage	1	Bourrage
TMAC	1	NMa du nœud cible
TIPAddr	4	Adresse IP du nœud cible
THType	1	Type de matériel du nœud cible
THLen	1	Longueur de la Ha du nœud cible
THAddr	THLen	Ha du nœud cible

4.4.4 Demande/réponse de résolution d'adresse IP/MAC

La définition et le format sont décrits ci-dessous.

- Utilisée pour obtenir la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») d'un nœud du réseau résidentiel possédant une adresse IP (Protocole Internet (en anglais, « Internet Protocol »)).
- Le nœud qui souhaite résoudre l'adresse IP (c'est-à-dire, qui souhaite connaître la NMa) doit être appelé « nœud demandeur » et le nœud qui notifie la relation entre les adresses dans la réponse à la demande doit être appelé « nœud cible ».
- Le nœud demandeur envoie à l'adresse IP destination un paquet de demande de résolution d'adresse IP/MAC contenant l'adresse IP cible à résoudre. Lors de la réception de la demande, le nœud cible envoie un paquet de réponse à la résolution d'adresse IP/MAC contenant l'adresse correspondante si TIPAddr et THLen sont exactement les mêmes que pour le nœud cible.

Le Tableau 6 ci-dessous indique le format des paquets de demande de résolution d'adresse IP/MAC.

Tableau 6 – Format des paquets de « demande de résolution d'adresse IP/MAC »

Élément	Taille (octets)	Explication
Version	1	Entrer « 0x01 » (Version 1)
Type	1	Type de paquet (demande de résolution d'adresse IP/MAC; entrer « 0x03 »)
Bourrage	1	Bourrage
RMAC	1	NMa du nœud demandeur
RIPAddr	4	Adresse IP du nœud demandeur
RHType	1	Type de matériel du nœud demandeur
RHLen	1	Longueur de la Ha du nœud demandeur
RHAddr	RHLen	Ha du nœud demandeur
Bourrage	1	Bourrage
TMAC	1	NMa du nœud cible (Entrer « null »)
TIPAddr	4	Adresse IP du nœud cible
THType	1	Type de matériel du nœud cible (Entrer « null »)
THLen	1	Longueur de la Ha du nœud cible (Entrer « RHLen »)
THAddr	THLen	Ha du nœud cible (Entrer « null »)

Le Tableau 7 ci-dessous indique le format des paquets de réponse à la résolution d'adresse IP/MAC.

Tableau 7 – Format des paquets de « réponse à la résolution d'adresse IP/MAC »

Élément	Taille (octets)	Explication
Version	1	Entrer « 0x01 » (Version 1)
Type	1	Type de paquet (réponse à la résolution d'adresse IP/MAC; entrer « 0x04 »)
Bourrage	1	Bourrage
RMAC	1	NMa du nœud demandeur
RIPAddr	4	Adresse IP du nœud demandeur
RHType	1	Type de matériel du nœud demandeur
RHLen	1	Longueur de la Ha du nœud demandeur
RHAddr	RHLen	Ha du nœud demandeur
Bourrage	1	Bourrage
TMAC	1	NMa du nœud cible
TIPAddr	4	Adresse IP du nœud cible
THType	1	Type de matériel du nœud cible
THLen	1	Longueur de la Ha du nœud cible
THAddr	THLen	Ha du nœud cible

4.4.5 Demande/réponse de résolution d'adresse matérielle/MAC

La définition et le format sont décrits ci-dessous.

- Utilisée pour obtenir la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») d'un nœud du réseau résidentiel possédant une Ha (Adresse matérielle, en anglais « Hardware address »).
- Le nœud qui souhaite résoudre la Ha (adresse IEEE 802.15.1, etc.) (c'est-à-dire, qui souhaite connaître la NMa) doit être appelé « nœud demandeur » et le nœud qui notifie la relation entre les adresses dans la réponse à la demande doit être appelé « nœud cible ».
- Le nœud demandeur effectue une multidiffusion vers le sous-réseau du réseau résidentiel d'un paquet de demande de résolution d'adresse matérielle/MAC contenant le type de

matériel cible, la longueur de la Ha et la Ha à résoudre. Lors de la réception de la demande, le nœud cible envoie un paquet de réponse à la résolution d'adresse matérielle/MAC si THType, THLen et THAddr sont exactement les mêmes que pour le nœud cible.

Le Tableau 8 ci-dessous indique le format des paquets de demande de résolution d'adresse matérielle/MAC.

Tableau 8 – Format des paquets de « demande de résolution d'adresse matérielle/MAC »

Élément	Taille (octets)	Explication
Version	1	Entrer « 0x01 » (Version 1)
Type	1	Type de paquet (demande de résolution d'adresse matérielle/IP; entrer « 0x05 »)
Bourrage	1	Bourrage
RMAC	1	NMa du nœud demandeur
RIPAddr	4	Adresse IP du nœud demandeur
RHType	1	Type de matériel du nœud demandeur
RHLen	1	Longueur de la Ha du nœud demandeur
RHAddr	RHLen	Ha du nœud demandeur
Bourrage	1	Bourrage
TMAC	1	NMa du nœud cible (Entrer « null »)
TIPAddr	4	Adresse IP du nœud cible (Entrer « null »)
THType	1	Type de matériel du nœud cible
THLen	1	Longueur de la Ha du nœud cible
THAddr	THLen	Ha du nœud cible

Le Tableau 9 ci-dessous indique le format des paquets de réponse à la résolution d'adresse matérielle/MAC.

Tableau 9 – Format des paquets de « réponse à la résolution d'adresse matérielle/MAC »

Élément	Taille (octets)	Explication
Version	1	Entrer « 0x01 » (Version 1)
Type	1	Type de paquet (réponse à la résolution d'adresse matérielle/MAC; entrer « 0x06 »)
Bourrage	1	Bourrage
RMAC	1	NMa du nœud demandeur
RIPAddr	4	Adresse IP du nœud demandeur
RHType	1	Type de matériel du nœud demandeur
RHLen	1	Longueur de la Ha du nœud demandeur
RHAddr	RHLen	Ha du nœud demandeur
Bourrage	1	Bourrage
TMAC	1	NMa du nœud cible
TIPAddr	4	Adresse IP du nœud cible
THType	1	Type de matériel du nœud cible
THLen	1	Longueur de la Ha du nœud cible
THAddr	THLen	Ha du nœud cible

4.4.6 Demande/réponse d'initialisation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control »)

La définition et le format sont décrits ci-dessous.

- Utilisée par les nœuds du réseau résidentiel pour initialiser leurs NMa (Adresses MAC de réseau, en anglais « Network MAC addresses ») au moment de l'amorçage.

- b) Le nœud d'amorçage (c'est-à-dire le nœud nécessitant une initialisation de la NMa) doit être appelé « nœud demandeur ».
- c) Lorsqu'un nœud du réseau résidentiel est amorcé (que ce soit un démarrage à chaud ou un démarrage à froid), il effectue une multidiffusion vers le sous-réseau du réseau résidentiel d'un paquet de demande d'initialisation d'adresse MAC pour initialiser le processus d'initialisation de la NMa. Tout nœud du réseau résidentiel qui s'amorce en mode automatique (A-MODE, voir 4.6.2) ou en mode nécessitant un serveur (SR-MODE, voir 4.6.2) doit envoyer ce paquet au moment de l'amorçage.
- d) Un paquet de demande d'initialisation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») agit pour:
 - 1) confirmer si un serveur d'adresses MAC existe dans le sous-réseau du réseau résidentiel;
 - 2) demander à tous les autres nœuds situés dans le sous-réseau du réseau résidentiel d'envoyer leurs paquets de réponse à l'initialisation d'adresse MAC (un paquet de réponse à l'initialisation d'adresse MAC contient des informations concernant la relation entre la NMa, l'adresse IP (Protocole Internet, en anglais « Internet Protocol ») et les autres adresses pertinentes sur le nœud en question); et
 - 3) confirmer si le sous-réseau comporte un nœud de NMa (Adresse MAC de réseau, en anglais « Network MAC address ») qui est le même que la NMa que le nœud demandeur prévoit d'utiliser (c'est-à-dire la NMa provisoire déterminée par le nœud demandeur).
- e) Lors de la réception du paquet de demande d'initialisation d'adresse MAC les autres nœuds du réseau résidentiel (à l'exclusion du serveur d'adresses MAC) doivent envoyer leurs paquets de réponse à l'initialisation d'adresse MAC.

Le Tableau 10 ci-dessous indique le format des paquets de demande d'initialisation d'adresse MAC.

Tableau 10 – Format des paquets de « demande d'initialisation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») »

Élément	Taille (octets)	Explication
Version	1	Entrer « 0x01 » (Version 1)
Type	1	Type de paquet (demande d'initialisation d'adresse MAC; entrer « 0x07 »)
Indicateur	1	Dans le mode nécessitant un serveur, la valeur du champ du bit 7 est « 1 », et dans un autre mode que le mode nécessitant un serveur, la valeur est « 0 ». Les bits 0 à 6 sont réservés et « 0 » doit être entré dans les champs pour ces bits.
RMAC	1	NMa provisoire du nœud demandeur
RIPAddr	4	Adresse IP du nœud demandeur
RHType	1	Type de matériel du nœud demandeur
RHLen	1	Longueur de la Ha du nœud demandeur
RHAddr	RHLen	Ha du nœud demandeur

Le Tableau 11 montre le format des paquets de réponse à l'initialisation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control »).

**Tableau 11 – Format des paquets de « réponse à l'initialisation d'adresse MAC
(Commande d'accès au support, en anglais « Medium Access Control ») »**

Élément	Taille (octets)	Explication
Version	1	Entrer « 0x01 » (Version 1)
Type	1	Type de paquet (réponse à l'initialisation d'adresse MAC; entrer « 0x08 »)
Indicateur	1	Pour un nœud qui est un routeur maître du réseau résidentiel, « 1 » doit être entré dans le champ pour le bit 7. Sinon utiliser « 0 ». Les bits 0 à 6 sont réservés et « 0 » doit être entré dans les champs pour ces bits.
TMAC	1	NMa du nœud répondeur
TIPAddr	4	Adresse IP du nœud répondeur
THType	1	Type de matériel du nœud répondeur
THALen	1	Longueur de la Ha du nœud répondeur
THAddr	THALen	Ha du nœud répondeur
UsedMAC	32	Indicateur « NMa in use » (si la NMa n est en cours d'utilisation, le bit n est à « 1 »). (Le LSB correspond à une NMa de « 0 » et le MSB correspond à une NMa de « 255 ».)

4.4.7 Réponse à l'initialisation de serveur d'adresses MAC/réponse à l'allocation d'adresse MAC

La définition et le format sont décrits ci-dessous.

- Lors de la réception d'un paquet de demande d'initialisation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») depuis un nœud d'amorçage, le serveur d'adresses MAC envoie un paquet de réponse à l'initialisation de serveur d'adresses MAC au nœud d'amorçage. Le nœud recevant ce paquet envoie un paquet de réponse à l'allocation d'adresse MAC au serveur d'adresses MAC pour confirmer la réception du paquet.
- Le nœud d'amorçage (c'est-à-dire le nœud nécessitant une initialisation de NMa (Adresse MAC de réseau, en anglais « Network MAC address »)) doit être appelé « nœud demandeur ».
- Le paquet de réponse à l'initialisation de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») envoyé par le serveur d'adresses MAC au nœud demandeur en réponse au paquet de demande d'initialisation d'adresse MAC contient la NMa à utiliser par le nœud demandeur. Le nœud demandeur recevant ce paquet doit utiliser la NMa spécifiée.
- Lors de la réception du paquet de réponse à l'initialisation de serveur d'adresses MAC, le nœud du réseau résidentiel envoie un paquet de réponse à l'allocation d'adresse MAC au serveur d'adresses MAC.

Le Tableau 12 ci-dessous indique le format des paquets de réponse à l'initialisation de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »).

Tableau 12 – Format des paquets de « réponse à l'initialisation de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») »

Élément	Taille (octets)	Explication
Version	1	Entrer « 0x01 » (Version 1)
Type	1	Type de paquet (réponse à l'initialisation de serveur d'adresses MAC; entrer « 0x09 »)
Indicateur	1	Pour un nœud routeur maître du réseau résidentiel, « 1 » doit être entré dans le champ pour le bit 7. Sinon utiliser « 0 ». Les bits 0 à 6 sont réservés et « 0 » doit être entré dans les champs pour ces bits.
Bourrage	1	Bourrage
RMAC	1	NMa à utiliser par le nœud demandeur
SMAC	1	NMa du nœud serveur d'adresses
SIPAddr	4	Adresse IP du nœud serveur d'adresses
SHType	1	Type de matériel du nœud serveur d'adresses
SHALen	1	Longueur de la Ha du nœud serveur d'adresses
SHAddr	SHALen	Ha du nœud serveur d'adresses

Le Tableau 13 ci-dessous indique le format des paquets de réponse à l'allocation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control »).

Tableau 13 – Format des paquets de « réponse à l'allocation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») »

Élément	Taille (octets)	Explication
Version	1	Entrer « 0x01 » (Version 1)
Type	1	Type de paquet (réponse à l'allocation d'adresse MAC; entrer « 0x0a »)
SMAC	1	NMa du serveur d'adresses MAC
RMAC	1	NMa à utiliser par le nœud demandeur
RPAddr	4	Adresse IP du nœud demandeur
RHType	1	Type de matériel du nœud demandeur
RHALen	1	Longueur de la Ha du nœud demandeur
RHAddr	RHALen	Ha du nœud demandeur

4.4.8 Demande/réponse de confirmation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control »)

La définition et le format sont décrits ci-dessous.

- Lorsque le nœud demandeur apprend par le processus de demande/réponse d'initialisation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») décrit ci-dessus qu'il est prévu d'utiliser la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») (c'est-à-dire que la NMa provisoire déterminée par le mode de demande) est déjà utilisée par un autre nœud, le nœud demandeur utilise un paquet de demande de confirmation de NMa pour déterminer une NMa provisoire différente et confirmer s'il y a un nœud dans le sous-réseau du réseau résidentiel qui utilise déjà la nouvelle NMa provisoire.
- Les nœuds du réseau résidentiel recevant le paquet de demande de confirmation d'adresse MAC vérifient si leurs NMa (Adresses MAC de réseau, en anglais « Network MAC addresses ») coïncident avec la NMa provisoire contenue dans le paquet. Un nœud

du réseau résidentiel avec une NMa identique à la NMa provisoire envoie un paquet de réponse à la confirmation d'adresse MAC au nœud demandeur.

- c) S'il n'y a pas de réponse au paquet de demande de confirmation d'adresse MAC au bout d'un certain temps, le nœud demandeur détermine qu'aucun nœud dans le sous-réseau du réseau résidentiel n'utilise la NMa provisoire et prend la NMa provisoire comme sa NMa formelle.

Le Tableau 14 ci-dessous indique le format des paquets de demande de confirmation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control »).

Tableau 14 – Format des paquets de « demande de confirmation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») »

Élément	Taille (octets)	Explication
Version	1	Entrer « 0x01 » (Version 1)
Type	1	Type de paquet (demande de confirmation d'adresse MAC; entrer « 0x0b »)
Bourrage	1	Bourrage
RMAC	1	NMa provisoire du nœud demandeur
RIPAddr	4	Adresse IP du nœud demandeur
RHType	1	Type de matériel du nœud demandeur
RHLen	1	Longueur de la Ha du nœud demandeur
RHAddr	RHLen	Ha du nœud demandeur

Le Tableau 15 ci-dessous indique le format des paquets de réponse à la confirmation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control »).

Tableau 15 – Format des paquets de « réponse à la confirmation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») »

Élément	Taille (octets)	Explication
Version	1	Entrer « 0x01 » (Version 1)
Type	1	Type de paquet (réponse à la confirmation d'adresse MAC; entrer « 0x0c »)
Indicateur	1	Pour un nœud routeur maître du réseau résidentiel, « 1 » doit être entré dans le champ pour le bit 7. Sinon utiliser « 0 ». Les bits 0 à 6 sont réservés et « 0 » doit être entré dans les champs pour ces bits.
TMAC	1	NMa du nœud répondeur
TIPAddr	4	Adresse IP du nœud répondeur
THType	1	Type de matériel du nœud répondeur
THLen	1	Longueur de la Ha du nœud répondeur
THAddr	THLen	Ha du nœud répondeur

4.4.9 Demande/réponse d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») à tous les nœuds

La définition et le format sont décrits ci-dessous.

- a) Un nœud dans un sous-réseau du réseau résidentiel peut demander à d'autres nœuds du sous-réseau d'envoyer leurs paquets de réponse à l'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») à tous les nœuds (un paquet de réponse à l'adresse MAC à tous les nœuds contient des informations concernant la relation entre l'adresse MAC, l'adresse IP (Protocole Internet, en anglais « Internet Protocol ») et les autres adresses pertinentes du nœud en question) en effectuant une multidiffusion d'un paquet de demande d'adresse MAC à tous les nœuds vers le sous-réseau.

- b) Lors de la réception du paquet de demande d'adresse MAC à tous les nœuds, les nœuds du réseau résidentiel envoient leur paquet de réponse à l'adresse MAC à tous les nœuds contenant les adresses pertinentes vers le nœud demandeur.

Le Tableau 16 ci-dessous indique le format des paquets de demande d'adresse MAC à tous les nœuds.

Tableau 16 – Format des paquets de « demande d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») à tous les nœuds »

Élément	Taille (octets)	Explication
Version	1	Entrer « 0x01 » (Version 1)
Type	1	Type de paquet (demande d'adresse MAC à tous les nœuds; entrer « 0x0d »)
RMAC	1	NMa du nœud demandeur
RIPAddr	4	Adresse IP du nœud demandeur
RHType	1	Type de matériel du nœud demandeur
RHLen	1	Longueur de la Ha du nœud demandeur
RHAddr	RHLen	Ha du nœud demandeur

Le Tableau 17 ci-dessous indique le format des paquets de réponse à l'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») à tous les nœuds.

Tableau 17 – Format des paquets de « réponse à l'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») à tous les nœuds »

Élément	Taille (octets)	Explication
Version	1	Entrer « 0x01 » (Version 1)
Type	1	Type de paquet (réponse d'adresse MAC à tous les nœuds; entrer « 0x0e »)
Bourrage	1	Bourrage
TMAC	1	NMa du nœud répondeur
TIPAddr	4	Adresse IP du nœud répondeur
THType	1	Type de matériel du nœud répondeur
THLen	1	Longueur de la Ha du nœud répondeur
THAddr	THLen	Ha du nœud répondeur

4.4.10 Demande/réponse de détection de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »), notification de serveur d'adresses MAC

La définition et le format sont décrits ci-dessous.

- Un nœud dans un sous-réseau du réseau résidentiel sans serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») souhaitant devenir le serveur d'adresses MAC peut utiliser les paquets de demande/réponse de détection de serveur d'adresses MAC et de notification de serveur d'adresses MAC.
- Après confirmation de l'absence de serveur d'adresses MAC, un nœud souhaitant devenir le serveur d'adresses MAC doit être appelé « nœud demandeur ».
- Le nœud demandeur effectue une multidiffusion d'un paquet de demande de détection de serveur d'adresses MAC vers le sous-réseau du réseau résidentiel. S'il n'y a pas de réponse au bout d'un certain temps, le nœud demandeur détermine qu'il n'y a pas de serveur d'adresses MAC dans le sous-réseau et effectue une multidiffusion d'un paquet de notification de serveur d'adresses MAC vers le sous-réseau du réseau résidentiel pour déclarer qu'il doit servir de serveur d'adresses MAC.

- d) Si le serveur d'adresses MAC existe déjà dans le sous-réseau, un paquet de réponse à la détection de serveur d'adresses MAC est envoyé en réponse au paquet de demande de détection de serveur d'adresses MAC.

Le Tableau 18 ci-dessous indique le format des paquets de demande de détection de serveur d'adresses MAC.

Tableau 18 – Format des paquets de « demande de détection de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») »

Élément	Taille (octets)	Explication
Version	1	Entrer « 0x01 » (Version 1)
Type	1	Type de paquet (demande de détection de serveur d'adresses MAC; entrer « 0x0f »)
RMAC	1	NMa du nœud demandeur

Le Tableau 19 ci-dessous indique le format des paquets de notification de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »).

Tableau 19 – Format des paquets de « notifications de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») »

Élément	Taille (octets)	Explication
Version	1	Entrer « 0x01 » (Version 1)
Type	1	Type de paquet (notification de serveur d'adresses MAC; entrer « 0x10 »)
Bourrage	1	Bourrage
SMAC	1	NMa du nœud serveur d'adresses MAC
SIPAddr	4	Adresse IP du nœud serveur d'adresses MAC
SHType	1	Type de matériel du nœud serveur d'adresses MAC
SHALen	1	Longueur de la Ha du nœud serveur d'adresses MAC
SHAddr	SHALen	Ha du nœud serveur d'adresses MAC

Le Tableau 20 ci-dessous indique le format des paquets de réponse à la détection de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »).

Tableau 20 – Format des paquets de « réponse à la détection de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») »

Élément	Taille (octets)	Explication
Version	1	Entrer « 0x01 » (Version 1)
Type	1	Type de paquet (réponse à la détection de serveur d'adresses MAC; entrer « 0x11 »)
Bourrage	1	Bourrage
SMAC	1	NMa du nœud serveur d'adresses MAC
SIPAddr	4	Adresse IP du nœud serveur d'adresses MAC
SHType	1	Type de matériel du nœud serveur d'adresses MAC
SHALen	1	Longueur de la Ha du nœud serveur d'adresses MAC
SHAddr	SHALen	Ha du nœud serveur d'adresses MAC

4.4.11 Message de pilotage du réseau (destination invalide)

La définition et le format sont décrits ci-dessous.

- a) Ce paquet est utilisé lorsque la valeur de DMAC (NMa (Adresse MAC de réseau, en anglais « Network MAC address ») destination) d'un paquet reçu de transfert de trame de

transmission de réseau résidentiel est différente de la valeur de la NMa du nœud de réception, pour avertir le nœud de transmission du paquet de transfert de trame de transmission du réseau résidentiel du désaccord.

- b) Le nœud qui transmet le message de pilotage du réseau (destination invalide) doit être appelé « nœud de transmission » et le nœud qui reçoit le message de pilotage du réseau (destination invalide) doit être appelé « nœud de réception ».
- c) Un nœud qui a reçu ce message (nœud de réception) doit de nouveau exécuter le processus de résolution d'adresse (résolution d'adresse MAC/IP).

Le Tableau 21, ci-dessous, montre le format des paquets de message de pilotage du réseau (destination invalide).

Tableau 21 – Format des paquets de « message de pilotage du réseau (destination invalide) »

Élément	Taille (octets)	Explication
Version	1	Entrer « 0x01 » (Version 1)
Type	1	Type de paquet (entrer « 0x12 » (destination invalide))
Bourrage	1	Bourrage
SMAC	1	NMa du nœud de transmission
SIPAddr	4	Adresse IP du nœud de transmission
SHType	1	Type de matériel du nœud de transmission
SHLen	1	Longueur de la Ha du nœud de transmission
SHAddr	SHLen	Ha du nœud de transmission
DMAC	1	Valeur de DMAC contenue dans le paquet reçu de transfert de trame de transmission du réseau résidentiel

4.4.12 Message de pilotage du réseau (conflit de NMa (Adresses MAC de réseau, en anglais « Network MAC addresses »))

La définition et le format sont décrits ci-dessous.

- a) Ce paquet est utilisé par un nœud qui a découvert un conflit de NMa (Adresses MAC de réseau, en anglais « Network MAC addresses ») (c'est-à-dire qu'il y a deux nœuds ou plus ayant la même NMa), pour avertir ces nœuds du conflit.
- b) Le nœud transmettant le message de pilotage du réseau « conflit de NMa » doit être appelé « nœud de transmission ».
- c) Ce message doit être diffusé dans l'ensemble du sous-réseau.
- d) Les nœuds ayant reçu ce message (c'est-à-dire tous les nœuds partageant la même NMa) doivent exécuter à nouveau le processus de résolution d'adresse après avoir confirmé le conflit de NMa.

Le Tableau 22, ci-dessous indique le format pour le message de pilotage du réseau (conflit de NMa.).

Tableau 22 – Format des paquets de message de pilotage du réseau « conflit de NMa (Adresses MAC de réseau, en anglais « Network MAC addresses ») »

Élément	Taille (octets)	Explication
Version	1	Entrer « 0x01 » (Version 1)
Type	1	Type de paquet (entrer « 0x13 » (conflit de NMa))
Bourrage	1	Bourrage
SMAC	1	NMa du nœud de transmission
SIPAddr	4	Adresse IP du nœud de transmission
SHType	1	Type de matériel du nœud de transmission
SHLen	1	Longueur de la Ha du nœud de transmission
SHAddr	SHLen	Ha du nœud de transmission
DMAC	1	NMa partagée par deux nœuds ou plus

4.5 Séquences de communication de base

4.5.1 Généralités

Un nœud du réseau résidentiel exécute d'abord la procédure d'initialisation de NMa (Adresse MAC de réseau, en anglais « Network MAC address »). À la fin de cette procédure, la NMa du nœud du réseau résidentiel est déterminée et le nœud du réseau résidentiel est alors prêt à être géré par la couche supérieure et la couche inférieure du réseau résidentiel. Dans un réseau IP (Protocole Internet (en anglais, « Internet Protocol »), l'adresse IP d'un nœud peut changer (pour diverses raisons, y compris le fait que l'adresse IP allouée par le serveur DHCP (Protocole de configuration de serveur dynamique, en anglais « Dynamic Host Configuration Protocol ») peut différer d'un moment à un autre). De façon similaire, la NMa d'un nœud peut changer pour des raisons telles qu'une modification de l'emplacement du nœud et un conflit de NMa. Il convient donc que les nœuds du réseau résidentiel possèdent toujours les informations d'adresses les plus récentes (c'est-à-dire, les informations concernant la relation entre le matériel, l'IP et les NMa de chacun des nœuds). Le Tableau 23 ci-dessous montre un exemple de tableau de relations d'adresses.

Tableau 23 – Tableau de relations d'adresses

Type de matériel	Ha	Adresse IP	NMa
0	Ha	IPa	MACa
1	Hb	IPb	MACb
1	Hc	IPc	MACc
2			

Pour cette raison, tous les nœuds du réseau résidentiel doivent recueillir des informations d'adresse concernant les nœuds environnants (en envoyant un paquet d'initialisation de NMa (Adresse MAC de réseau, en anglais « Network MAC address ») et en recevant la réponse) au moment de l'amorçage et doivent informer les nœuds du réseau résidentiel situés dans le domaine de leur adresse établie pour maintenir à jour leurs tables de relations d'adresses. Les périodes de temporisation contenues dans les tableaux dépendent de la mise en œuvre.

Un nœud de réseau résidentiel avec une Na (Adresse réseau, en anglais « Network Address ») établie peut effectuer une communication sur le réseau résidentiel. Un tel nœud peut être confronté à l'un quelconque des cas suivants:

- Il connaît la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») du nœud avec lequel il souhaite communiquer mais ne connaît pas l'adresse IP (Protocole Internet, en anglais « Internet Protocol ») du nœud;
- Il connaît l'adresse IP du nœud avec lequel il souhaite communiquer mais ne connaît pas la NMa du nœud; ou

- Il connaît la Ha (Adresse matérielle, en anglais « Hardware address ») (par exemple, l'adresse IEEE 802.15.1) du nœud avec lequel il souhaite communiquer, mais ne connaît pas la NMa du nœud.

Pour résoudre le problème, le nœud du réseau résidentiel peut utiliser 4.5.2 des paquets de demande/réponse de résolution d'adresse MAC/IP, 4.5.3 des paquets de demande/réponse de résolution d'adresse MAC/IP ou 4.5.4 des paquets de demande/réponse de résolution d'adresse matérielle/MAC. Une explication détaillée de chaque méthode est donnée de 4.5.2 à 4.5.4. Les paquets de demande/réponse d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») à tous les nœuds utilisés pour étudier les NMa (Adresses MAC de réseau, en anglais « Network MAC addresses ») de tous les nœuds du réseau résidentiel dans le sous-réseau du réseau résidentiel sont expliqués en 4.5.5. Les procédures de résolution des problèmes associés aux NMa tels que la réception de 4.5.6, 4.5.7 un paquet de transfert de trame de transmission de réseau résidentiel de « destination invalide » ou 4.5.8 la découverte d'un conflit de NMa pendant une communication sur le réseau résidentiel sont expliquées en 4.5.6, 4.5.7 et 4.5.8.

4.5.2 Demande/réponse de résolution d'adresses MAC/IP (résolution de la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») dans l'adresse IP (Protocole Internet (en anglais, « Internet Protocol »))

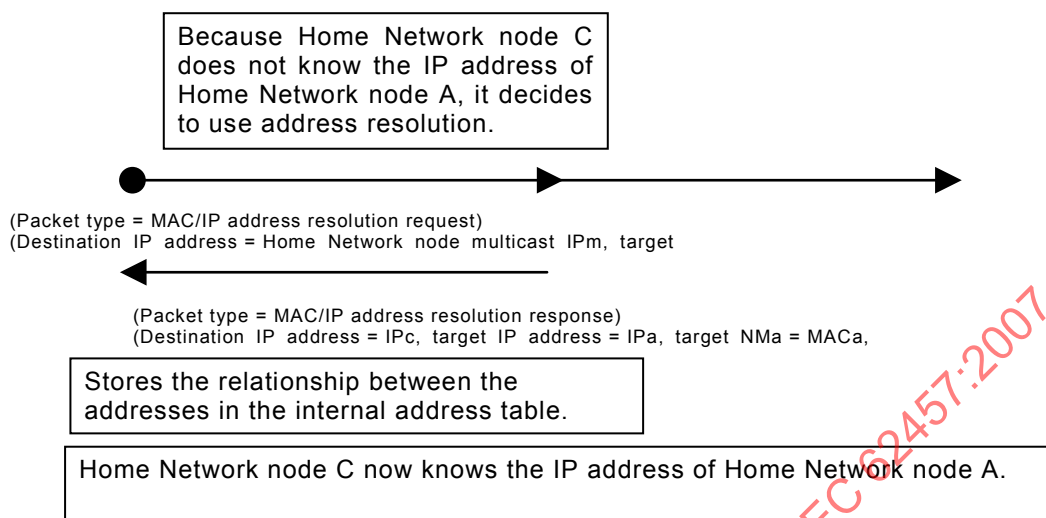
Les détails sont décrits ci-dessous.

- a) Le nœud cherchant à résoudre la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») doit être appelé « nœud demandeur » et le nœud sur lequel la résolution doit être effectuée doit être appelée « nœud cible ».
- b) Un nœud du réseau résidentiel utilise un paquet de demande de résolution d'adresse MAC/IP lorsqu'il souhaite connaître l'adresse IP (Protocole Internet, en anglais « Internet Protocol ») d'un autre nœud du réseau résidentiel avec une NMa.
- c) Le nœud demandeur effectue une multidiffusion vers le sous-réseau du réseau résidentiel d'un paquet de demande de résolution d'adresse contenant la NMa cible à résoudre. Lors de la réception de la demande, le nœud cible envoie un paquet de réponse à la résolution d'adresse MAC/IP contenant sa NMa, son adresse IP, le type de matériel du support de transmission, la longueur de la Ha (Adresse matérielle, en anglais « Hardware address ») et la Ha.
- d) La période de temporisation entre la transmission de la demande de résolution d'adresse IP et la réception du paquet de réponse à la résolution d'adresse IP doit être de T3, comme indiqué dans le Tableau 26. Si aucun paquet de réponse à la résolution d'adresse IP n'est reçu pendant la période de temporisation, une erreur doit se produire.
- e) Il convient que le contenu du paquet de réponse de résolution d'adresse IP soit répercuté dans la relation d'adresse.
- f) Pour empêcher un débordement d'ARP, la fréquence des transmissions de paquets de demande de résolution d'adresse MAC/IP doit être d'un paquet par seconde ou moins. Le nombre maximal de paquets de demande de résolution d'adresse MAC/IP pouvant être envoyés successivement doit être de 5 (l'intervalle entre un paquet de demande de résolution d'adresse MAC/IP et le suivant doit être au moins de 1 s). Si aucun paquet de réponse à la résolution d'adresse MAC/IP n'est reçu après la cinquième tentative, une erreur doit se produire.

Les formats des paquets de demande et de réponse de résolution d'adresse MAC/IP sont respectivement présentés dans le Tableau 4 et le Tableau 5.

La séquence de base est représentée à la Figure 11.

Home Network node C (NMa = MACc, IP address = IPc, Ha = hc) Home Network node A (NMa = MACa, IP address = IPa, Ha = ha) Home Network node B (NMa = MACb, IP address = IPb, Ha = hb)



Légende

Anglais	Français
Home Network node C (NMa = MACc, IP address = IPc, Ha = hc)	Nœud C du réseau résidentiel (NMa = MACc, IP adresse = IPc, Ha = hc)
Home Network node A (NMa = MACa, IP address = IPa, Ha = ha)	Nœud A du réseau résidentiel (NMa = MACa, IP adresse = IPa, Ha = ha)
Home Network node B (NMa = MACb, IP address = IPb, Ha = hb)	Nœud B du réseau résidentiel (NMa = MACb, IP adresse = IPb, Ha = hb)
Because Home Network node C does not know the IP address of Home Network node A, it decides to use address resolution.	Puisque le nœud C du réseau résidentiel ne connaît pas l'adresse IP du nœud A du réseau résidentiel, il décide d'utiliser une résolution d'adresse.
(Packet type = MAC/IP address resolution request) (Destination IP address = Home Network node multicast IPm, target NMa = MACa)	(Type de paquet = demande de résolution d'adresse MAC/IP) (Adresse IP destination = IPm multidiffusion nœud du réseau résidentiel, cible NMa = MACa)
(Packet type = MAC/IP address resolution response) (Destination IP address = IPc, target IP address = IPa, target NMa = MACa, target Ha = ha)	(Type de paquet = réponse à la résolution d'adresse MAC/IP) (Adresse IP destination = IPc, adresse Ip cible = IPa, cible NMa = MACa, cible Ha = ha)
Stores the relationship between the addresses in the internal address table	Mémorise la relation entre les adresses dans le tableau d'adresses internes
Home Network node C now knows the IP address of Home Network node A.	Le nœud C du réseau résidentiel connaît maintenant l'adresse IP du nœud A du réseau résidentiel

Figure 11 – Séquence de résolution d'adresse MAC/IP de base

4.5.3 Demande/réponse de résolution d'adresse IP/MAC (résolution de l'adresse IP (Protocole Internet, en anglais « Internet Protocol ») dans la NMa (Adresse MAC de réseau, en anglais « Network MAC address »))

Les détails sont décrits ci-dessous.

- Le nœud cherchant à résoudre l'adresse IP (Protocole Internet, en anglais « Internet Protocol ») doit être appelé « nœud demandeur » et le nœud sur lequel la résolution doit être effectuée doit être appelée « nœud cible ».

- b) Un nœud du réseau résidentiel utilise un paquet de demande de résolution d'adresse IP/MAC lorsqu'il souhaite connaître la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») d'un autre nœud du réseau résidentiel avec une adresse IP.
- c) Le nœud demandeur envoie à l'adresse IP destination un paquet de demande de résolution d'adresse IP/MAC contenant l'adresse IP cible à résoudre. Lors de la réception de la demande, le nœud cible envoie un paquet de réponse à la résolution d'adresse IP/MAC contenant sa NMa, son adresse IP, le type de matériel du support de transmission, la longueur de la Ha (Adresse matérielle, en anglais « Hardware address ») et la Ha.
- d) La période de temporisation entre la transmission du paquet de demande de résolution d'adresse IP/MAC et la réception du paquet de réponse à la résolution d'adresse IP/MAC doit être de T4 dans le Tableau 26. Si aucun paquet de réponse à la résolution d'adresse IP n'est reçu pendant la période de temporisation, une erreur doit se produire.
- e) Il convient que le contenu du paquet de réponse à la résolution d'adresse IP/MAC soit répercuté dans la relation d'adresse.
- f) Pour empêcher un débordement d'ARP, la fréquence des transmissions de paquets de demande de résolution d'adresse IP/MAC doit être d'un paquet par seconde ou moins. Le nombre maximal de paquets de demande de résolution d'adresse IP/MAC pouvant être envoyés successivement doit être de 5 (l'intervalle entre un paquet de demande de résolution d'adresse IP/MAC et le suivant doit être au moins de 1 s). Si aucun paquet de réponse à la résolution d'adresse IP/MAC n'est reçu après la cinquième tentative, une erreur ne doit se produire.

Les formats des paquets de demande et de réponse de résolution d'adresse IP/MAC sont respectivement présentés dans le Tableau 6 et le Tableau 7. La séquence de base est représentée à la Figure 12 ci-dessous.

Home Network node C
(NMa = MACc,
IP address = IPc, Ha = hc)

Home Network node A
(NMa = MACa,
IP address = IPa, Ha = ha)

Home Network node B
(NMa = MACb,
IP address = IPb, Ha = hb)

Because Home Network node C does not know the NMa of Home Network node A, it decides to resolve the IP address into the NMa.

(Packet type = IP/MAC address resolution request)

(Destination IP address = IPa, requesting node's hardware address = Hc, requesting node's IP address = IPc, requesting node's Home Network MAC

(Packet type = IP/MAC address resolution response)

(Destination IP address = IPc, target IP address = IPa, target NMa= MACa, target Ha = ha)

Stores the relationship between the addresses in the internal address table.

Home Network node C now knows the NMa of Home Network node A.

Légende

Anglais	Français
Home Network node C (NMa = MACc, IP address = IPc, Ha = hc)	Nœud C du réseau résidentiel (NMa = MACc, IP adresse = IPc, Ha = hc)
Home Network node A (NMa = MACa, IP address = IPa, Ha = ha)	Nœud A du réseau résidentiel (NMa = MACa, IP adresse = IPa, Ha = ha)
Home Network node B (NMa = MACb, IP address = IPb, Ha = hb)	Nœud B du réseau résidentiel (NMa = MACb, IP adresse = IPb, Ha = hb)
Because Home Network node C does not know the NMa of Home Network node A, it decides to resolve the IP address into the NMa.	Puisque le nœud C du réseau résidentiel ne connaît pas la NMa du nœud A du réseau résidentiel, il décide de résoudre l'adresse IP dans la NMa.
(Packet type = IP/MAC address resolution request) (Destination IP address = IPa, requesting node's hardware address = Hc, requesting node's IP address = IPc, requesting node's Home Network MAC address = MACc, target IP address IPa)	(Type de paquet = demande de résolution d'adresse IP/MAC) (Adresse IP destination = IPa, adresse matérielle du nœud demandeur = Hc, adresse IP du nœud demandeur = IPc, adresse MAC réseau résidentiel du nœud demandeur = MACc, adresse IP cible IPa)
(Packet type = IP/MAC address resolution response) (Destination IP address = IPc, target IP address = IPa, target NMa = MACa, target Ha = ha)	(Type de paquet = réponse à la résolution d'adresse IP/MAC) (Adresse IP destination = IPc, adresse IP cible = IPa, cible NMa = MACa, cible Ha = ha)
Stores the relationship between the addresses in the internal address table	Mémoire la relation entre les adresses dans le tableau d'adresses internes
Home Network node C now knows the NMa of Home Network node A.	Le nœud C du réseau résidentiel connaît maintenant la NMa du nœud A du réseau résidentiel.

Figure 12 – Séquence de résolution d'adresse IP/MAC de base

4.5.4 Demande/réponse de résolution d'adresse matérielle/MAC

Les détails sont décrits ci-dessous.

- a) Le nœud cherchant à résoudre la Ha (Adresse matérielle, en anglais « Hardware address ») doit être appelé « nœud demandeur » et le nœud sur lequel la résolution doit être effectuée doit être appelée « nœud cible ».
- b) Un nœud du réseau résidentiel utilise un paquet de demande de résolution d'adresse matérielle/MAC lorsqu'il souhaite connaître la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») d'un autre nœud du réseau résidentiel avec une Ha (Adresse matérielle, en anglais « Hardware address »).
- c) Le nœud demandeur effectue une multidiffusion vers le sous-réseau du réseau résidentiel d'un paquet de demande de résolution d'adresse matérielle/MAC contenant le type de matériel cible, la longueur de la Ha (Adresse matérielle, en anglais « Hardware address ») et la Ha à résoudre. Lors de la réception de la demande, le nœud cible envoie un paquet de réponse à la résolution d'adresse matérielle/MAC contenant sa NMa, son adresse IP (Protocole Internet (en anglais, « Internet Protocol »), le type de matériel du support de transmission, la longueur de la Ha et la Ha.
- d) La période de temporisation entre la transmission du paquet de demande de résolution d'adresse matérielle/MAC et la réception du paquet de réponse à la résolution d'adresse matérielle/MAC doit être de T4 comme indiqué dans le Tableau 26. Si aucun paquet de réponse à la résolution d'adresse IP n'est reçu pendant la période de temporisation, une erreur ne doit se produire.
- e) Il convient que le contenu du paquet de réponse à la résolution d'adresse matérielle/MAC soit répercuté dans la relation d'adresse.
- f) Pour empêcher un débordement d'ARP, la fréquence des transmissions de paquets de demande de résolution d'adresse matérielle/MAC doit être d'un paquet par seconde ou moins. Le nombre maximal de paquets de demande de résolution d'adresse matérielle/MAC pouvant être envoyés successivement doit être de 5 (l'intervalle entre un paquet de demande de résolution d'adresse matérielle/MAC et le suivant doit être au moins de 1 s). Si aucun paquet de réponse à la résolution d'adresse matérielle/MAC n'est reçu après la cinquième tentative, une erreur ne doit se produire.

Les formats des paquets de demande et de réponse de résolution d'adresse de réseau matériel/MAC sont respectivement représentés dans le Tableau 8 et le Tableau 9. La séquence de base est représentée à la Figure 13.

Home Network node C
(NMa = MACc,
IP address = IPc, Ha = hc)

Home Network node A
(NMa = MACa,
IP address = IPa, Ha = ha)

Home Network node B
(NMa = MACb,
IP address = IPb, Ha = hb)

Because Home Network node C does not know the NMa of Home Network node A, it decides to resolve the Ha into the NMa.

(Packet type = hardware/MAC address resolution request)
(Destination IP address = Home Network node multicast IPm, requesting node's Ha = hc, requesting node's IP address = IPc, requesting node's NMa = MACc, target Ha = ha)

(Packet type = hardware/MAC address resolution response)
(Destination IP address = IPc, target IP address = IPa, target NMa = MACa, target Ha = ha)

Stores the relationship between the addresses in the internal address table.

Home Network node C now knows the NMa of Home Network node A.

Légende

Anglais	Français
Home Network node C (NMa = MACc, IP address = IPc, Ha = hc)	Nœud C du réseau résidentiel (NMa = MACc, IP adresse = IPc, Ha = hc)
Home Network node A (NMa = MACa, IP address = IPa, Ha = ha)	Nœud A du réseau résidentiel (NMa = MACa, IP adresse = IPa, Ha = ha)
Home Network node B (NMa = MACb, IP address = IPb, Ha = hb)	Nœud B du réseau résidentiel (NMa = MACb, IP adresse = IPb, Ha = hb)
Because Home Network node C does not know the NMa of Home Network node A, it decides to resolve the Ha into the NMa.	Puisque le nœud C du réseau résidentiel ne connaît pas la NMa du nœud A du réseau résidentiel, il décide de résoudre la Ha dans la NMa.
(Packet type = hardware/MAC address resolution request) (Destination IP address = Home Network node multicast IPm, requesting node's Ha = hc, requesting node's IP address = IPc, requesting node's NMa = MACc, target Ha = ha)	(Type de paquet = demande de résolution d'adresse matérielle/MAC) (Adresse IP destination = IPm mode multidiffusion réseau résidentiel, Ha du nœud demandeur = hc, adresse IP du nœud demandeur = IPc, adresse NMa du nœud demandeur = MACc, Ha cible = ha)
(Packet type = hardware/MAC address resolution response) (Destination IP address = IPc, target IP address = IPa, target NMa = MACa, target Ha = ha)	(Type de paquet = réponse à la résolution d'adresse matérielle/MAC) (Adresse IP destination = IPc, adresse IP cible = IPa, cible NMa = MACa, cible Ha = ha)
Stores the relationship between the addresses in the internal address table	Mémorise la relation entre les adresses dans le tableau d'adresses internes
Home Network node C now knows the NMa of Home Network node A.	Le nœud C du réseau résidentiel connaît maintenant la NMa du nœud A du réseau résidentiel.

Figure 13 – Séquence de résolution d'adresse matérielle/MAC de base

Les trames du réseau résidentiel de monodiffusion sont mappées sur des paquets UDP/IP de monodiffusion. Les trames du réseau résidentiel de multidiffusion/diffusion large sont mappées sur des paquets USP/IP adressés à une adresse de multidiffusion IP (Protocole Internet, en anglais « Internet Protocol ») dédiée assignée au réseau résidentiel.

Dans le réseau résidentiel, le mappage des sous-réseaux du réseau résidentiel sur des sous-réseaux IP (Protocole Internet, en anglais « Internet Protocol ») doit toujours être biunivoque. En conséquence, aucun nœud du réseau résidentiel ne doit envoyer une trame du réseau résidentiel à un nœud situé dans un autre sous-réseau IP (en d'autres termes, aucun nœud du réseau résidentiel ne peut envoyer un paquet IP avec une adresse IP de destination représentant un autre sous-réseau IP). De même, aucun nœud du réseau résidentiel ne doit recevoir une trame du réseau résidentiel provenant d'un nœud situé dans un autre sous-réseau IP. En d'autres termes, un nœud du réseau résidentiel recevant un paquet IP avec une adresse IP d'origine représentant un autre sous-réseau IP doit supprimer le paquet.

4.5.5 Demande/réponse d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») à tous les nœuds

Les détails sont décrits ci-dessous.

- a) Le nœud confirmant la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») de tous les nœuds du réseau résidentiel dans le sous-réseau du réseau résidentiel doit être appelé « nœud demandeur » et les nœuds qui répondent à la demande doivent être appelés « nœuds répondeurs ».
- b) Des paquets de « demande/réponse d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») à tous les nœuds » sont utilisés, par exemple, lorsqu'il est nécessaire qu'un serveur d'adresses MAC confirme les adresses MAC de tous les nœuds du réseau résidentiel situés dans le sous-réseau du réseau résidentiel auquel il appartient, auquel cas le serveur d'adresses MAC devient le nœud demandeur.
- c) Le nœud demandeur effectue une multidiffusion dans l'ensemble du sous-réseau du réseau résidentiel d'un « paquet de demande d'adresse MAC à tous les nœuds » contenant sa NMa. En réponse à ce paquet, chaque nœud du réseau résidentiel dans le sous-réseau du réseau résidentiel envoie une réponse à une adresse MAC à tous les paquets de nœuds contenant sa NMa, son adresse IP (Protocole Internet (en anglais, « Internet Protocol »), le type de matériel du support de transmission, la longueur de la Ha (Adresse matérielle, en anglais « Hardware address ») et la Ha.
- d) La période de temporisation entre la transmission du paquet de demande d'adresse MAC à tous les nœuds et la réception du paquet de réponse à l'adresse MAC à tous les nœuds doit être de T14 comme indiqué dans le Tableau 26. Si aucun paquet de réponse à l'adresse MAC à tous les nœuds n'est reçu pendant cette période de temporisation, ceci signifie qu'il n'y a pas d'autre nœud du réseau résidentiel dans le sous-réseau du réseau résidentiel.
- e) Il convient que le contenu du paquet de réponse à l'adresse MAC à tous les nœuds soit répercuté dans la relation d'adresse.

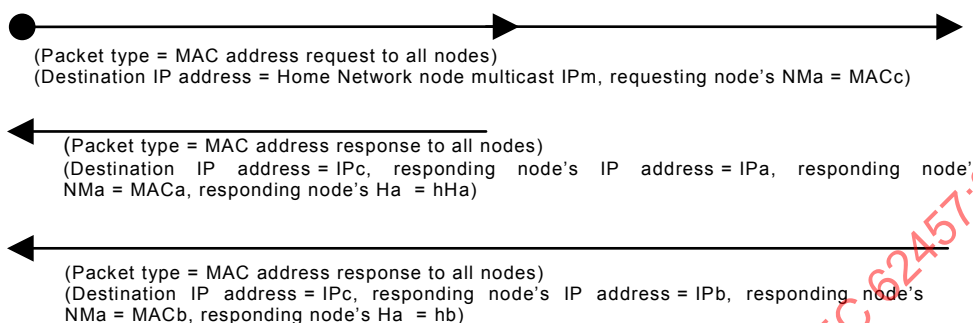
Les formats des paquets de demande d'adresse MAC à tous les nœuds et de réponse à l'adresse MAC à tous les nœuds sont respectivement représentés dans le Tableau 16 et le Tableau 17. La séquence est la suivante:

Home Network device C
(NMa = MACc,
IP address = IPc, Ha = hc)

Home Network device A
(NMa = MACa,
IP address = IPa, Ha = ha)

Home Network device B
(NMa = MACb,
IP address = IPb, Ha = hb)

Because the device C wishes to know all node's NMa,Ha,IP.



Stores the relationship between the addresses in the internal address

Légende

Anglais	Français
Home Network device C (NMa = MACc, IP address = IPc, Ha = hc)	Dispositif C du réseau résidentiel (NMa = MACc, IP adresse = IPc, Ha = hc)
Home Network device A (NMa = MACa, IP address = IPa, Ha = ha)	Dispositif A du réseau résidentiel (NMa = MACa, IP adresse = IPa, Ha = ha)
Home Network device B (NMa = MACb, IP address = IPb, Ha = hb)	Dispositif B du réseau résidentiel (NMa = MACb, IP adresse = IPb, Ha = hb)
Because the device C wishes to know all node's NMa., Ha, IP	Puisque le dispositif C souhaite connaître les NMa, Ha, IP de tous les nœuds
(Packet type = MAC address request to all nodes) (Destination IP address = Home Network node multicast IPm, requesting node's NMa = MACc)	(Type de paquet = demande d'adresse MAC à tous les nœuds) (Adresse IP destination = IPm mode multidiffusion réseau résidentiel, NMa du nœud demandeur = MACc)
(Packet type = MAC address response to all nodes) (Destination IP address = IPc, responding node's IP address = IPa, responding node's NMa = MACa, responding node's Ha = hHa)	(Type de paquet = réponse à l'adresse MAC à tous les nœuds) (Adresse IP destination = IPc, adresse IP nœud répondeur = IPa, NMa nœud répondeur = MACa, Ha nœud répondeur = hHa)
(Packet type = MAC address response to all nodes) (Destination IP address = IPc, responding node's IP address = IPb, responding node's NMa = MACb, responding node's Ha = hb)	(Type de paquet = réponse à l'adresse MAC à tous les nœuds) (Adresse IP destination = IPc, adresse IP nœud répondeur = IPb, NMa nœud répondeur = MACb, Ha nœud répondeur = hb)
Stores the relationship between the addresses in the internal address table	Mémoire la relation entre les adresses dans le tableau d'adresses internes

Figure 14 – Séquence de base de « demande/réponse d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») à tous les nœuds »

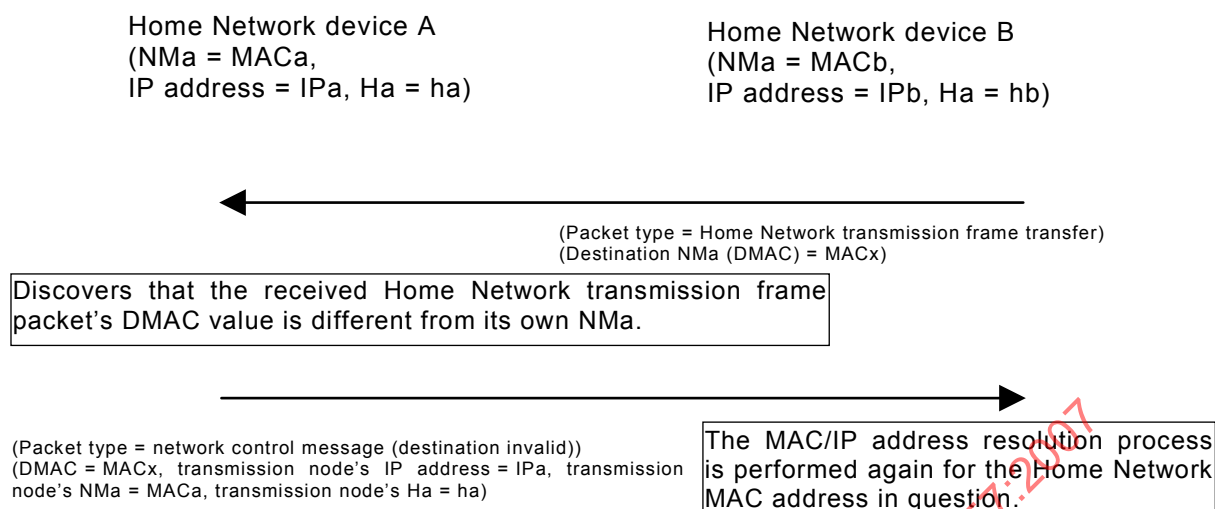
4.5.6 Message de pilotage du réseau (destination invalide)

Les détails sont décrits ci-dessous.

- a) Si la valeur de DMAC (NMa (Adresse MAC de réseau, en anglais « Network MAC address ») du nœud de réception) contenue dans le paquet de transfert de trame de transmission du réseau résidentiel reçu est différente de la valeur de la NMa du nœud, le nœud de réception ne peut pas transmettre le paquet de transfert de trame de transmission du réseau résidentiel à la couche supérieure. En remplacement, le nœud informe le nœud de transmission que la destination du paquet reçu de transfert de trame de transmission du réseau résidentiel est invalide.
- b) Puisque le nœud qui transmet le paquet de transfert de trame de transmission du réseau résidentiel d'origine et le nœud qui reçoit ce paquet sont appelés respectivement « nœud de transmission » et « nœud de réception », le nœud qui transmet ce message de pilotage du réseau et le nœud qui le reçoit sont appelés respectivement « nœud de réception » et « nœud de transmission ».
- c) Un nœud qui a reçu ce message (nœud de transmission) doit de nouveau exécuter le processus de résolution d'adresse (résolution d'adresse MAC/IP).

Le format des messages de pilotage du réseau « destination invalide » est représenté dans le Tableau 21. La séquence est la suivante:

IECNORM.COM : Click to view the full PDF of IEC 62457:2007



Légende

Anglais	Français
Home Network device A (NMa = MACa, IP address = IPa, Ha = ha)	Dispositif A du réseau résidentiel (NMa = MACa, IP adresse = IPa, Ha = ha)
Home Network device B (NMa = MACb, IP address = IPb, Ha = hb)	Dispositif B du réseau résidentiel (NMa = MACb, IP adresse = IPb, Ha = hb)
(Packet type = Home Network transmission frame transfer) (Destination NMa (DMAC) = MACx)	(Type de paquet = Transfert de trame de transmission réseau résidentiel) (NMa destination (DMAC) = MACx)
Discovers that the received Home Network transmission frame packet's DMAC value is different from its own NMa.	Découvre que la valeur DMAC du paquet de la trame de transmission du réseau résidentiel est différente de sa propre NMa.
(Packet type = network control message (destination invalid)) (DMAC = MACx, transmission node's IP address = IPa, transmission node's NMa = MACa, transmission node's Ha = ha)	(Type de paquet = message de pilotage du réseau destination invalide) (DMAC = MACx, adresse Ip du nœud de transmission = IPa, NMa du nœud de transmission = MACa, Ha du nœud de transmission = ha)
The MAC/IP address resolution process is performed again for the Home Network MAC address in question.	Le processus de résolution d'adresse MAC/IP est de nouveau exécuté pour l'adresse MAC du réseau résidentiel en question.

Figure 15 – Séquence de traitement de base de « destination invalide »

Il n'est toutefois pas nécessaire d'effectuer ce traitement si les valeurs de SMAC et DMAC du paquet reçu de transfert de trame de transmission du réseau résidentiel sont les mêmes (c'est-à-dire si le paquet est un paquet de diffusion large ou de diffusion large de groupe). Il peut également se produire un cas où la valeur de SMAC du paquet reçu de transfert de trame de transmission du réseau résidentiel est la même que la valeur de la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») du nœud de réception, auquel cas il peut se produire un conflit de NMa dans le sous-réseau et ainsi, le traitement décrit en 4.5.7 ci-dessous doit être effectué.

4.5.7 Cas particulier concernant les paquets avec des valeurs de destination invalides

Les détails sont décrits ci-dessous.

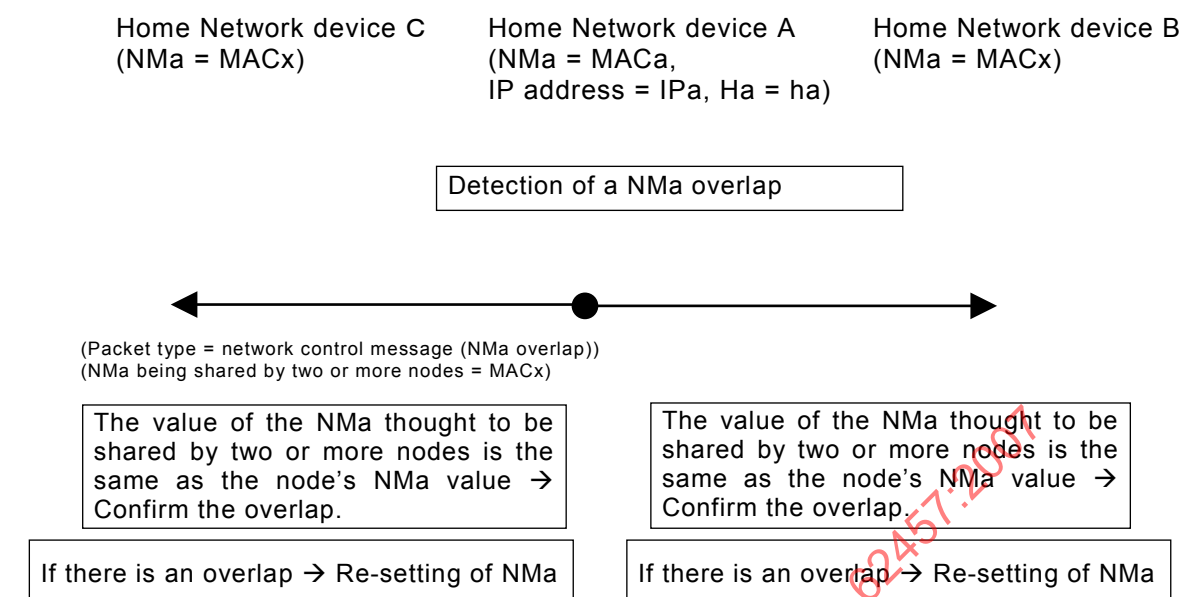
- a) Comme mentionné en 4.5.6, dans certains cas, la valeur d'adresse de l'expéditeur (SMAC) d'un paquet reçu de transfert de trame de transmission du réseau résidentiel avec une valeur de destination invalide peut être la même que la valeur de la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») du nœud de réception, auquel cas, il peut y avoir un conflit de NMa dans le sous-réseau.
- b) Lorsque ceci se produit, le nœud ayant reçu le paquet de transfert de trame de transmission du réseau résidentiel avec la valeur de destination invalide doit effectuer une demande de résolution d'adresse MAC/IP en utilisant l'adresse de l'expéditeur du paquet (SMAC) comme NMa du nœud cible.
- c) Si le nœud ayant reçu le paquet de transfert de trame de transmission du réseau résidentiel avec la valeur de destination invalide reçoit une réponse à la résolution d'adresse MAC/IP depuis le nœud cible (ce qui constitue une confirmation qu'il y a un conflit de NMa), il doit initialiser un démarrage à froid et initialiser sa Na (Adresse réseau, en anglais « Network Address »).
- d) Si aucune réponse de résolution d'adresse MAC/IP n'est reçue du nœud cible, il doit estimer que le paquet de transfert de trame de transmission du réseau résidentiel avec la valeur de destination invalide est un paquet invalide et le supprimer.

4.5.8 Message de pilotage du réseau (conflit de NMa (Adresses MAC de réseau, en anglais « Network MAC addresses »))

Les détails sont décrits ci-dessous.

- a) Un nœud qui a découvert un conflit de NMa (Adresses MAC de réseau, en anglais « Network MAC addresses ») (c'est-à-dire qu'il y a deux nœuds ou plus ayant la même NMa), doit avertir les nœuds partageant la même NMa du conflit. Un nœud est habituellement informé de la présence d'un conflit de NMa lorsque des réponses à la résolution d'adresse MAC/IP sont reçues depuis deux nœuds ou plus pour une demande de résolution d'adresse MAC/IP pour une unique NMa ou lorsqu'il détecte une NMa dans son tableau de relations d'adresses correspondant à deux adresses IP (Protocole Internet, en anglais « Internet Protocol ») ou plus. Lors de la découverte d'un conflit de NMa, il diffuse dans tout le sous-réseau un message de pilotage du réseau (conflit de NMa).
- b) Le nœud qui transmet ce message doit être appelé « nœud de transmission ».
- c) Le message de pilotage du réseau est diffusé dans tout le sous-réseau en utilisant l'adresse de diffusion multiple IP allouée par le réseau résidentiel.
- d) Tous les nœuds ayant reçu ce message (c'est-à-dire tous les nœuds partageant la même NMa) doivent exécuter à nouveau le processus de détermination d'adresse en utilisant un démarrage à froid après avoir confirmé le conflit. Cette confirmation est habituellement effectuée par une demande de résolution d'adresse MAC/IP sur la NMa propre du nœud.

Le format des paquets de messages de pilotage du réseau « conflit de destination » est représenté dans le Tableau 22. La séquence est la suivante:



Légende

Anglais	Français
Home Network device C (NMa = MACx)	Dispositif de réseau résidentiel C (NMa = MACx)
Home Network device A (NMa = MACa, IP address = IPa, Ha = ha)	Dispositif de réseau résidentiel A (NMa = MACa, IP adresse = IPa, Ha = ha)
Home Network device B (NMa = MACx)	Dispositif de réseau résidentiel B (NMa = MACx)
Detection of a NMa overlap	Détection de conflit de NMa
(Packet type = network control message (NMa overlap)) (NMa being shared by two or more nodes = MACx)	(Type de paquet = message de pilotage du réseau (conflit de NMa)) (NMa partagée par deux nœuds ou plus = MACx)
The value of the NMa thought to be shared by two or more nodes is the same as the node's NMa value → Confirm the overlap.	La valeur de la NMa estimée partagée par deux nœuds ou plus est la même que la valeur de la NMa du nœud → Confirmation du conflit.
The value of the NMa thought to be shared by two or more nodes is the same as the node's NMa value → Confirm the overlap.	La valeur de la NMa estimée partagée par deux nœuds ou plus est la même que la valeur de la NMa du nœud → Confirmation du conflit.
If there is an overlap → Re-setting of NMa	S'il y a un conflit → Réinitialisation de la NMa
If there is an overlap → Re-setting of NMa	S'il y a un conflit → Réinitialisation de la NMa

Figure 16 – Séquence de base pour traiter le conflit de NMa (Adresses MAC de réseau, en anglais « Network MAC addresses ») détectée

4.6 Séquence d'amorçage d'acquisition de NMa (Adresse MAC de réseau, en anglais « Network MAC address »)

4.6.1 Vue d'ensemble de la séquence d'amorçage d'acquisition de NMa (Adresse MAC de réseau, en anglais « Network MAC address »)

Le traitement d'amorçage d'acquisition de NMa (Adresse MAC de réseau, en anglais « Network MAC address ») peut être divisé en trois étapes de traitement comme suit:

- Traitement jusqu'à l'établissement du support inférieur (dans le cas du raccordement PANU-NAP/GN IEEE 802.15.1 utilisant BNEP (Protocole d'encapsulation de réseau Bluetooth, en anglais « Bluetooth Network Encapsulation Protocol ») et la formation d'un picoréseau) (couche de support inférieure)
- Traitement jusqu'à l'acquisition/établissement d'une adresse IP (Protocole Internet, en anglais « Internet Protocol ») (couche IP). Pour le traitement jusqu'à l'acquisition/établissement d'une adresse IP avec IPv4, il est recommandé d'utiliser le DHCP (Protocole de configuration de serveur dynamique, en anglais « Dynamic Host Configuration Protocol ») pour l'acquisition de l'adresse IP. La mise en œuvre d'une fonction pour acquérir des adresses, par exemple d'un client DHCP doit être obligatoire. (Couche TCP/IP (Protocole de commande de transmission/Protocole Internet, en anglais « Transmission Control Protocol/Internet Protocol »))
- Traitement après acquisition d'une adresse IP (couche inférieure du réseau résidentiel)

Une vue d'ensemble du traitement après acquisition d'une adresse IP est décrite en 4.6.2 et la description détaillée est donnée en 4.6.3 .

4.6.2 Vue d'ensemble du traitement après acquisition d'une adresse IP (Protocole Internet (en anglais, « Internet Protocol »))

Tous les nœuds doivent déterminer leurs NMa (Adresses MAC de réseau, en anglais « Network MAC addresses ») au moment de l'amorçage en exécutant la séquence spécifiée ci-dessous. Le « mode automatique » (A-MODE), le « mode nécessitant un serveur » (SR-MODE) ou le « mode manuel » (M-MODE) peut être utilisé pour y parvenir, en fonction du paramétrage de l'administrateur, etc. Il est toutefois recommandé d'utiliser le mode automatique (A-MODE) sauf si un autre mode a été configuré dans le paramétrage. Le mode manuel (M-MODE) ou le mode automatique (A-MODE) doivent être prévus. La mise en œuvre du mode nécessitant un serveur (SR-MODE) est facultative. L'utilisation mélangée de nœuds utilisant le mode manuel (M-MODE) pour l'amorçage et de nœuds utilisant un autre mode d'amorçage doit être évitée. La présente norme ne spécifie aucune exigence fonctionnelle pour une telle utilisation mélangée (par exemple, les effets de paramétrages incorrects dans le mode manuel).

Tableau 24 – Modes d'amorçage

Mode d'amorçage	Explication
Mode automatique (A-MODE)	Amorçage des nouveaux nœuds en utilisant la méthode du serveur d'adresses ou la méthode de détermination distribuée. L'acquisition dynamique de la NMa est possible.
Mode nécessitant un serveur (SR-MODE)	Les nouveaux nœuds effectuent une acquisition dynamique des NMa à partir de l'adresse de serveur. Si aucun serveur d'adresses MAC n'est trouvé, une erreur doit apparaître et le traitement doit s'arrêter.
Mode manuel (M-MODE)	Les NMa des nouveaux nœuds sont réglées manuellement.

Étape 1. Contrôle du mode d'amorçage. Si le mode manuel (M-MODE) est utilisé pour l'amorçage, le nœud d'amorçage doit utiliser la valeur déterminée comme étant sa NMa (Adresse MAC de réseau, en anglais « Network MAC address »). Ici, le nœud d'amorçage termine cette séquence.

Étape 2. Le nœud d'amorçage détermine une NMa (Adresse MAC de réseau, en anglais « Network MAC address ») provisoire.

Étape 3. Le nœud d'amorçage effectue une multidiffusion d'un paquet de demande d'initialisation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») utilisant l'adresse IPme (Adresse de multidiffusion IP, en anglais « IP multicast address »). Dans le mode nécessitant un serveur (SR-MODE), « 1 » doit être entré dans le champ du bit 7 de l'indicateur. Dans le mode automatique (A-MODE), « 0 » doit être entré dans le champ du bit 7 de l'indicateur. Lors de la réception d'un paquet de demande d'initialisation d'adresse MAC avec « 1 » dans le champ du bit 7 de l'indicateur, le serveur d'adresses MAC envoie un paquet de réponse à l'initialisation de serveur d'adresses MAC au nœud d'amorçage. Les nœuds autres que le serveur d'adresses MAC envoient leurs paquets de réponse à l'initialisation d'adresse MAC au nœud d'amorçage seulement lorsque le champ du bit 7 de l'indicateur du paquet de demande d'initialisation d'adresse MAC qu'ils ont reçu est à « 0 ».

Étape 4. Si le nœud d'amorçage reçoit le paquet de réponse à l'initialisation de serveur d'adresses MAC, il doit utiliser la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») contenue dans celui-ci comme étant sa NMa formelle. Dans ce cas, le nœud d'amorçage envoie un paquet de réponse à l'allocation d'adresse MAC et termine cette séquence.

Étape 5. Si le nœud d'amorçage ne reçoit pas le paquet de réponse à l'initialisation de serveur d'adresses MAC dans le mode nécessitant un serveur (SR-MODE), la séquence doit échouer et on doit la forcer à s'arrêter.

Étape 6. Le nœud d'amorçage vérifie tous les paquets de réponse à l'initialisation d'adresse MAC qu'il a reçus avant expiration de la période de temporisation pour déterminer si une NMa (Adresse MAC de réseau, en anglais « Network MAC address ») est utilisée dans le sous-réseau, c'est-à-dire la même que la NMa provisoire déterminée à l'Étape 2. Si aucune de ces NMa n'existe dans le sous-réseau, le nœud d'amorçage passe à l'Étape 8.

Étape 7. Si une NMa (Adresse MAC de réseau, en anglais « Network MAC address ») est utilisée dans le sous-réseau, qui est la même que la NMa provisoire déterminée à l'étape 2, le nœud d'amorçage détermine une NMa provisoire différente.

Étape 8. Le nœud d'amorçage effectue une multidiffusion d'un paquet de demandes de confirmation d'adresse MAC utilisant l'adresse IPme (Adresse de multidiffusion IP, en anglais « IP multicast address »). Les nœuds recevant le paquet de demande de confirmation d'adresse MAC vérifient si leurs NMa (Adresses MAC de réseau, en anglais « Network MAC addresses ») sont les mêmes que la NMa provisoire contenue dans le paquet. Un nœud dont la NMa coïncide avec la NMa provisoire envoie un paquet de réponse à la confirmation d'adresse MAC au nœud d'amorçage. Le nœud d'amorçage répète les Étapes 7 et 8 jusqu'à ce qu'il ne reçoive plus de paquet de réponse à la confirmation d'adresse MAC. Les nœuds autres que le serveur d'adresses MAC ne doivent pas envoyer de paquet de réponses à l'initialisation de serveur d'adresses MAC aux nœuds utilisant le mode nécessitant un serveur (SR-MODE) pour l'amorçage, ce qui signifie que le trafic des paquets associé à l'amorçage initial doit être inférieur lorsqu'il y a des nœuds qui utilisent le mode nécessitant un serveur (SR-MODE) pour l'amorçage. Une explication détaillée des séquences de traitement pour les nœuds d'amorçage, le serveur d'adresses MAC et les nœuds d'exploitation suit.

4.6.3 Nœud d'amorçage

Chaque nœud (incluant le serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »)) doit déterminer sa NMa (Adresse MAC de réseau, en anglais « Network MAC address ») au moment de l'amorçage selon la séquence suivante:

Étape 1. Le mode d'amorçage est contrôlé. Dans le mode manuel (M-MODE) le nœud d'amorçage doit utiliser la valeur déterminée comme étant sa NMa (Adresse MAC de réseau,

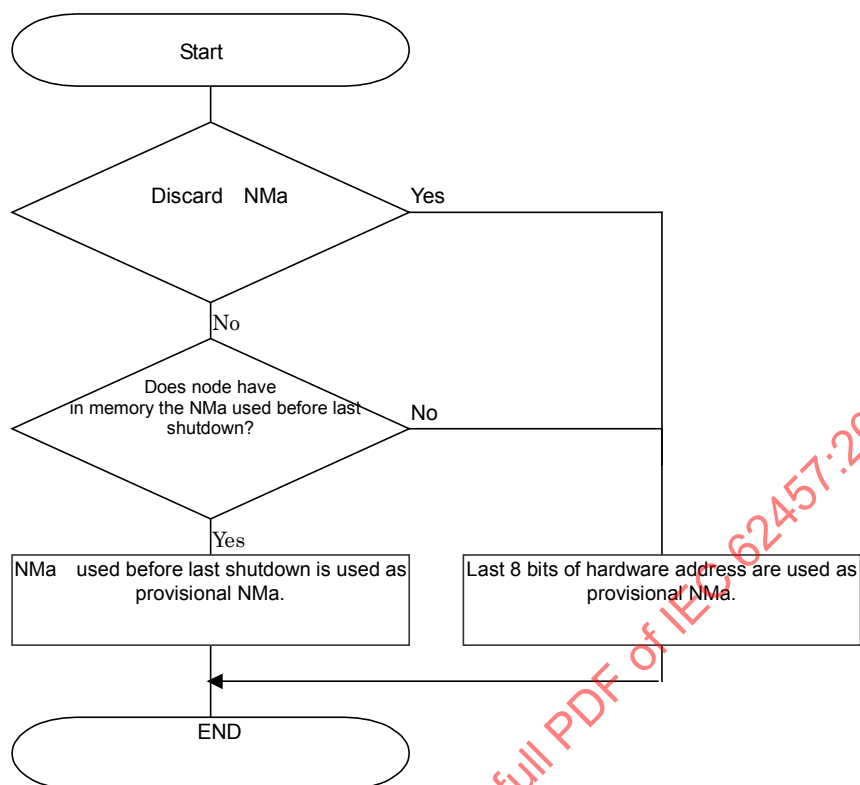
en anglais « Network MAC address »). Dans ce cas, le nœud d'amorçage termine cette séquence. Le nœud d'amorçage passe à l'étape 2 lorsqu'il est dans le mode automatique (A-MODE) ou le mode nécessitant un serveur (SR-MODE).

Étape 2. Le nœud d'amorçage attend que le temps T10 ait expiré (voir Tableau 26).

Étape 3. Le nœud d'amorçage détermine une NMa (Adresse MAC de réseau, en anglais « Network MAC address ») provisoire. Cette adresse doit être déterminée en se basant sur l'algorithme suivant:

- Lorsque la mémoire du nœud d'amorçage comporte la NMa utilisée avant le dernier arrêt, il doit utiliser cette NMa comme NMa provisoire.
- Lorsque la mémoire du nœud d'amorçage ne comporte pas la NMa utilisée, le nœud d'amorçage doit utiliser les 8 derniers bits de la Ha (Adresse matérielle, en anglais « Hardware address ») comme NMa provisoire. Lorsque le nœud d'amorçage doit supprimer la NMa au moment de l'initialisation ou lorsque le nœud d'amorçage démarre pour la première fois.

La prévision d'une fonction pour enregistrer la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») avant le dernier arrêt est obligatoire. La Figure 17 est un organigramme de détermination de la NMa provisoire à utiliser.



Légende

Anglais	Français
Start	Début
Discard NMa	Supprimer NMa
Yes	Oui
No	Non
Does node have in memory the NMa used before last shutdown?	La NMa utilisée avant le dernier arrêt est-elle en mémoire ?
No	Oui
Yes	Non
NMa used before last shutdown is used as provisional NMa	La NMa utilisée avant le dernier arrêt est utilisée comme NMa provisoire
Last 8 bits of hardware address used as provisional NMa	8 derniers bits de l'adresse matérielle utilisée comme NMa provisoire
END	FIN

Figure 17 – Organigramme de détermination de la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») provisoire à utiliser

Étape 4. Le nœud d'amorçage effectue une multidiffusion d'un paquet de demande d'initialisation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») utilisant l'adresse IPme (Adresse de multidiffusion IP, en anglais « IP multicast address »). Le paquet doit être transmis deux fois selon un intervalle T6 (voir Tableau 26). La deuxième transmission peut toutefois être omise si le nœud d'amorçage a reçu le paquet de réponse à l'initialisation de serveur d'adresses MAC expliqué ci-dessous avant expiration de la période T6. Le format des paquets de demande d'initialisation d'adresse MAC est représenté dans le Tableau 10. Dans ce paquet, mettre le bit 7 de l'indicateur à « 1 » pour le mode nécessitant un serveur (SR-MODE) et à « 0 » pour le mode automatique (A-MODE).

Étape 5. Si le nœud d'amorçage reçoit un paquet de réponse d'initialisation de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») dans la période de temporisation T2 (voir Tableau 26) mesurée depuis la transmission du dernier paquet de demande d'initialisation d'adresse MAC, il doit utiliser la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») (RMAC) contenue dans celui-ci comme sa NMa. Dans ce cas, le nœud d'amorçage envoie un paquet de réponse à l'allocation d'adresse MAC à l'expéditeur du paquet de réponse à l'initialisation de serveur d'adresses MAC et termine cette séquence. Si le nœud d'amorçage reçoit de nouveau le paquet de réponse à l'initialisation de serveur d'adresses MAC après avoir déterminé quelle NMa utiliser, il doit envoyer de nouveau le paquet de réponse à l'allocation d'adresse MAC. Par ailleurs, si de quelconques valeurs différentes des champs SMAC dans tous les paquets de réponse à l'initialisation de serveur d'adresses MAC reçus sont découvertes, cette séquence doit échouer comme erreur et on doit la forcer à s'arrêter. Le Tableau 13 fournit le format des paquets de réponse à l'allocation d'adresse MAC. La NMa allouée et la NMa du serveur d'adresses MAC sont respectivement mémorisées dans RMAC et SMAC.

Étape 6. Si le nœud d'amorçage ne reçoit pas le paquet de réponse à l'initialisation de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») avant expiration de la temporisation T2 (voir Tableau 26) dans le mode nécessitant un serveur (SR-MODE), la séquence doit échouer et on doit la forcer à s'arrêter. Dans le mode automatique (A-MODE), le nœud d'amorçage passe à l'étape 7.

Étape 7. Le nœud d'amorçage vérifie toutes les NMa (Adresses MAC de réseau, en anglais « Network MAC addresses ») utilisées dans le sous-réseau du réseau résidentiel au moyen de tous les paquets de réponse à l'initialisation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») reçus après expiration de la période de temporisation T2. Les NMa utilisées sont les adresses de TMAC ou les NMa représentées par des « 1 » dans l'indicateur UsedMAC dans les paquets de réponse à l'initialisation d'adresse MAC. Un calcul de la somme logique de UsedMAC peut être utilisé pour la mise en œuvre. La Figure 18 montre cette séquence. Si la NMa provisoire satisfait à l'une quelconque des conditions suivantes, le nœud d'amorçage passe à l'étape 8 de cette séquence. Sinon, le nœud d'amorçage ignore l'étape 8 et passe à l'étape 9 de cette séquence.

- La NMa provisoire coïncide avec une adresse TMAC (NMa du nœud répondeur) contenue dans un paquet de réponse à l'initialisation d'adresse MAC reçu (signifiant que la NMa est utilisée dans le sous-réseau du réseau résidentiel) ou la NMa représentée par « 1 » dans l'indicateur UsedMAC d'un paquet de réponse à l'initialisation d'adresse MAC.
- La NMa provisoire coïncide avec une NMa provisoire (RMAC) contenue dans un paquet reçu de demande d'initialisation d'adresse MAC.
- La NMa provisoire coïncide avec une NMa provisoire (RMAC) contenue dans un paquet reçu de demande de confirmation d'adresse MAC.

Des conditions supérieures à la deuxième et à la troisième sont nécessaires pour empêcher qu'un nœud d'amorçage utilise la même NMa que celle que tente d'utiliser un autre nœud d'amorçage.



Anglais	Français
Home Network node (NMa not fixed)	Nœud de réseau résidentiel (NMa non fixe)
MAC address initialization request	Demande d'initialisation d'adresse MAC
MAC address initialization request	Demande d'initialisation d'adresse MAC
MAC address initialization response	Réponse à l'initialisation d'adresse MAC
Logical sum calculation	Calcul de somme logique
NMas being used by other nodes	NMa utilisées par d'autres nœuds

Figure 18 – Vérification des NMA (Adresses MAC de réseau, en anglais « Network MAC addresses ») utilisées par les autres nœuds

Étape 8. Le nœud d'amorçage remplace la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») provisoire par une nouvelle en utilisant un nombre aléatoire. Les adresses suivantes ne doivent pas être utilisées comme NMa provisoire:

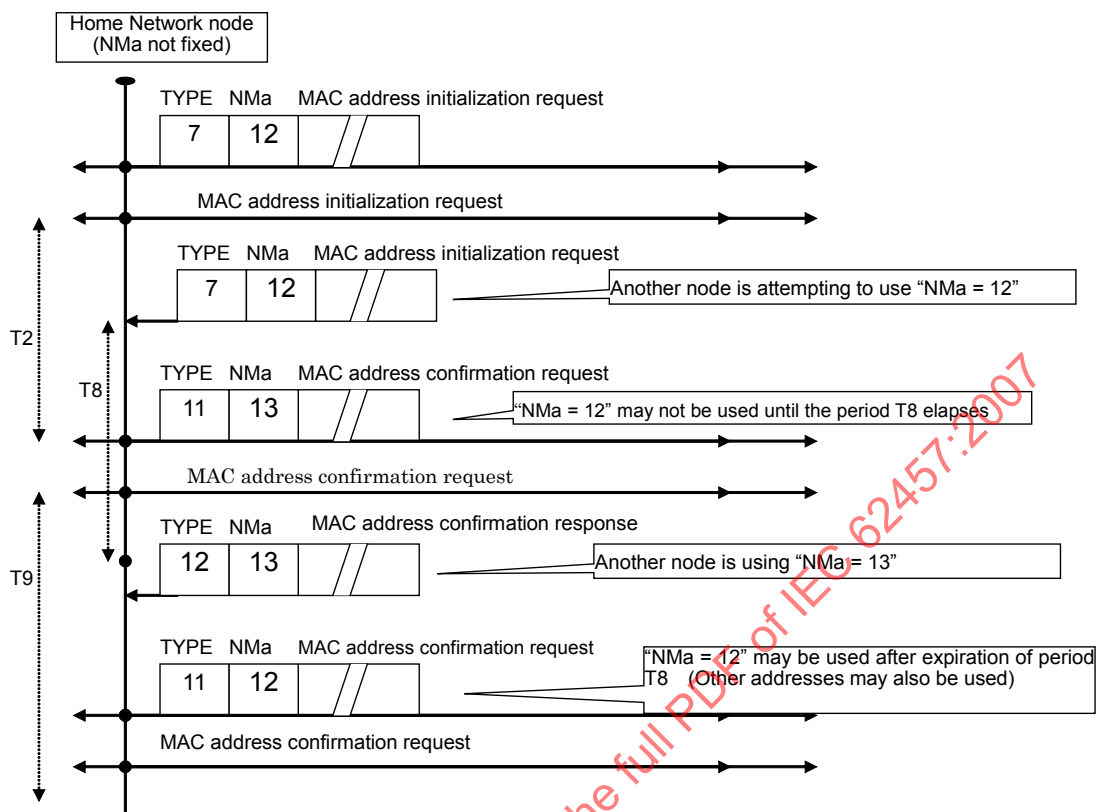
- La NMA des nœuds répondeurs (TMAC) contenue dans les paquets reçus de réponse à l'initialisation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») dans cette séquence.
- Les NMA représentées par des « 1 » dans les indicateurs UsedMAC des paquets de réponse à l'initialisation d'adresse MAC reçus dans cette séquence.
- Les NMA provisoires (RMAC) contenues dans les paquets de demande d'initialisation d'adresse MAC reçus dans cette séquence (voir NOTE ci-dessous).
- Les NMA provisoires (RMAC) contenues dans les paquets de demande de confirmation d'adresse MAC reçus dans cette séquence (voir NOTE ci-dessous).

- La NMa provisoire déjà utilisée par le nœud d'amorçage dans cette séquence (voir NOTE ci-dessous).

La Figure 19 indique le mode opératoire de l'étape 8.

NOTE Il existe une exception aux troisième, quatrième et cinquième conditions ci-dessus. Une NMa (Adresse MAC de réseau, en anglais « Network MAC address ») notée dans le troisième ou le quatrième état peut être utilisée comme NMa après expiration d'une période T8 (voir Figure 19 et Tableau 26) depuis la réception du paquet. Cette exception est facultative et il n'est pas nécessaire de la mettre en œuvre. Dans ce cas, il convient de ne pas utiliser la NMa provisoire. L'exception est prévue pour empêcher une situation dans laquelle deux nœuds ou plus amorçant tentent simultanément d'utiliser la même NMa, rendant impossible à tout nœud d'utiliser l'adresse en question.

IECNORM.COM : Click to view the full PDF of IEC 62457:2007



Légende

Anglais	Français
Home Network node (NMa not fixed)	Nœud de réseau résidentiel (NMa non fixe)
MAC address initialization request	Demande d'initialisation d'adresse MAC
MAC address initialization request	Demande d'initialisation d'adresse MAC
MAC address initialization request	Demande d'initialisation d'adresse MAC
Another node is attempting to use "NMa = 12"	Un autre nœud tente d'utiliser "NMa = 12"
MAC address confirmation request	Demande de confirmation d'adresse MAC
"NMa = 12" may not be used until the period T8 elapses	"NMa = 12" ne peut pas être utilisée avant expiration de la période T8
MAC address confirmation request	Demande de confirmation d'adresse MAC
MAC address confirmation request	Demande de confirmation d'adresse MAC
Another node is using "NMa = 13"	Un autre nœud utilise "NMa = 13"
MAC address confirmation request	Demande de confirmation d'adresse MAC
"NMa = 12" may be used after expiration of period T8 (Other addresses may also be used)	"NMa = 12" peut être utilisée après expiration de la période T8 (D'autres adresses peuvent également être utilisées)
MAC address confirmation request	Demande de confirmation d'adresse MAC

**Figure 19 – Exemple de NMa (Adresse MAC de réseau, en anglais
« Network MAC address ») provisoire dupliquée**

Étape 9. Le nœud d'amorçage effectue une multidiffusion d'un paquet de demande de confirmation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») utilisant l'adresse IPme (Adresse de multidiffusion IP, en anglais « IP multicast

address »). Le paquet de demande de confirmation d'adresse MAC doit être transmis deux fois dans un intervalle T6 (voir Tableau 26). Toutefois, la deuxième transmission peut être omise si le nœud d'amorçage reçoit un paquet de réponse à la confirmation d'adresse MAC. Le Tableau 14 montre le format des paquets de demande de confirmation d'adresse MAC.

Étape 10. Si le nœud d'amorçage reçoit l'un quelconque des paquets suivants avant expiration de la période de temporisation T9 (voir Tableau 26) mesurée à partir de la transmission du dernier paquet de demande de confirmation d'adresse MAC, il doit revenir à l'étape 8:

- Un paquet de réponse à la confirmation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control »)
- Un paquet de demande d'initialisation d'adresse MAC dont la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») provisoire (RMAC) coïncide avec la NMa provisoire de l'étape 8.
- Un paquet de demande de confirmation d'adresse MAC dont la NMa provisoire (RMAC) coïncide avec la NMa provisoire de l'étape 8.

Étape 11. Si le nœud d'amorçage ne reçoit aucun des paquets énumérés à l'étape 10, il doit utiliser la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») provisoire comme sa NMa formelle. Dans ce cas, le nœud d'amorçage termine cette séquence.

Les informations de la NMa (TMAC), les informations de la Ha (Adresse matérielle, en anglais « Hardware address ») (THAddr) et les informations de l'adresse IP (Protocole Internet, en anglais « Internet Protocol ») (TIPAddr) contenues dans les paquets de réponse à l'initialisation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control »), les paquets de réponse à la confirmation d'adresse MAC et les paquets de réponse à l'initialisation de serveur d'adresses MAC reçus dans cette séquence (ou après la fin de cette séquence) peuvent être utilisés comme informations de relation d'adresse auxquelles il est fait référence en « 4.5 Séquences de communication de base ». La NMa (Adresse MAC de réseau, en anglais « Network MAC address ») du routeur maître du réseau résidentiel peut être obtenue d'après les informations de l'indicateur maître (bit 7 de l'indicateur) d'un paquet de réponse à l'initialisation d'adresse MAC ou d'un paquet de réponse à l'initialisation de serveur d'adresses MAC.

4.6.4 Serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »)

Pour la séquence de traitement pour le serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »), se référer à 4.7.

4.6.5 Nœuds fonctionnels

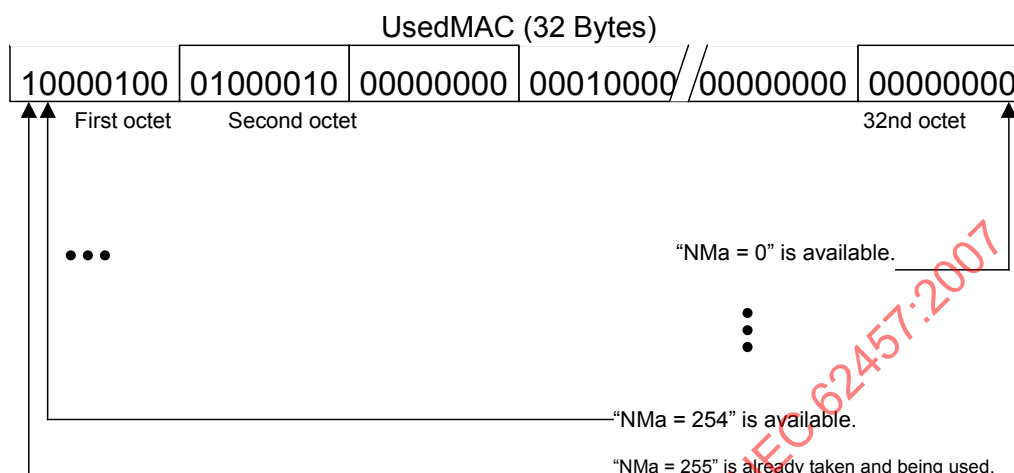
Les nœuds fonctionnels (c'est-à-dire les nœuds ayant achevé la séquence décrite en 4.6.3 et ayant une NMa (Adresse MAC de réseau, en anglais « Network MAC address ») établie, sauf pour le serveur d'adresses expliqué en 4.6.4) doivent exécuter les deux étapes suivantes:

Étape 1. Si un nœud fonctionnel reçoit un paquet de demande d'initialisation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») et que le bit 7 de l'indicateur est à « 0 », il doit envoyer un paquet de réponse à l'initialisation d'adresse MAC à l'expéditeur après expiration de la période T7 (voir Tableau 26). Cette transmission n'est pas nécessaire lorsque le nœud fonctionnel reçoit un paquet de demande d'initialisation d'adresse MAC contenant la même Ha (Adresse matérielle, en anglais « Hardware address ») dans la période T6. T7 doit être calculée comme suit:

$$T7 = [NMa \text{ du nœud fonctionnel}] \times [T1] + [T0]$$

Lorsque le bit 7 de l'indicateur est à « 1 », aucun autre nœud que le serveur d'adresses MAC ne doit répondre car ceci signifie que la transmission provient d'un nœud utilisant le mode

nécessitant un serveur (SR-MODE) pour l'amorçage. Le Tableau 11 indique le format des paquets de réponse à l'initialisation d'adresse MAC. La Figure 20 montre le format pour UsedMAC.



Légende

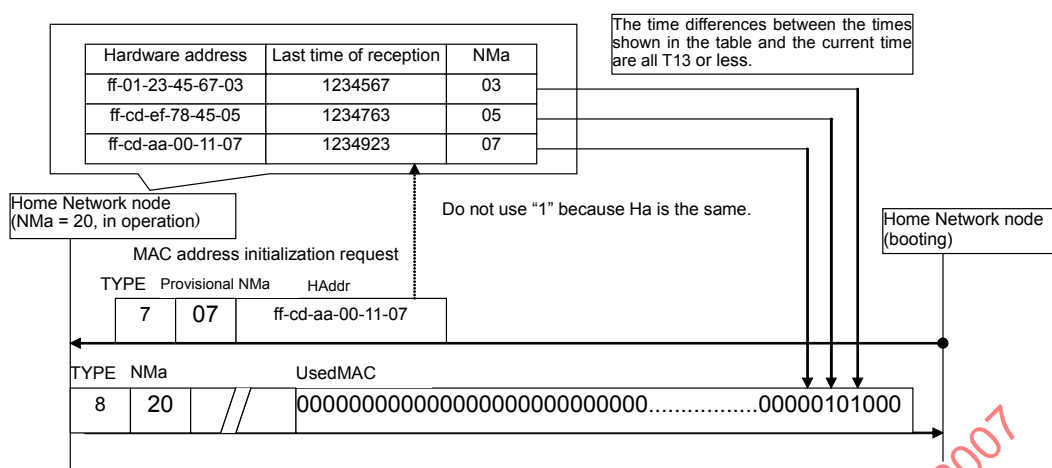
Anglais	Français
(32 bytes)	(32 octets)
First octet	Premier octet
Second octet	Deuxième octet
32nd octet	32ème octet
"NMa = 0" is available	"NMa = 0" est disponible
"NMa = 254" is available	"NMa = 254" est disponible
"NMa = 255" is already taken and being used	"NMa = 255" est déjà prise et est utilisée

Figure 20 – Format pour UsedMAC

Dans UsedMAC, on peut entrer « 1 » pour le bit n (qui correspond à la NMa (Adresse MAC de réseau, en anglais « Network MAC address n ») si le bit satisfait aux conditions suivantes:

- Un paquet a été reçu depuis un nœud dont la NMa est n pendant la période antérieure T13 (voir Tableau 26), sauf lorsque la Ha (Adresse matérielle, en anglais « Hardware address ») contenue dans le paquet coïncide avec celle qui est contenue dans le paquet de demande d'initialisation d'accès à l'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control »).

L'utilisation de « 1 » pour le bit n de UsedMAC empêche les nœuds recevant le paquet d'utiliser la NMa n. Ceci permet à un dispositif communiquant fréquemment avec un dispositif ayant une NMa particulière d'empêcher d'autres dispositifs d'utiliser cette NMa. Dans la mise en œuvre, une fonction peut être utilisée pour: a) enregistrer lors de la réception d'un paquet l'heure de réception et la NMa du paquet en utilisant la Ha (Adresse matérielle, en anglais « Hardware address ») comme clé et b) vérifier au moment de la demande si la période T13 s'est écoulée depuis la réception. Lorsque l'alimentation du nœud fonctionnel a été arrêtée ou coupée pendant la période antérieure T13, tous les paquets reçus avant l'arrêt/la coupure doivent être ignorés.



Légende

Anglais	Français
Hardware address	Adresse matérielle
Last time of reception	Dernière heure de réception
The time difference between the times shown in the table and the current time are all T13 or less	La différence de temps entre les heures indiquées dans le tableau et l'heure courante est toujours inférieure ou égale à T13
Home network node (NMa = 20, in operation)	Nœud du réseau résidentiel (NMa = 20, en fonctionnement)
Do not use "1" because Ha is the same	Ne pas utiliser "1" car Ha est la même
MAC address initialization request	Demande d'initialisation d'adresse MAC
Provisional NMa	NMa provisoire
Home network node (booting)	Nœud du réseau résidentiel (amorçage)

Figure 21 – Exemple de UsedMAC

Le responsable de la mise en œuvre doit prendre beaucoup de précautions pour utiliser « 1 » dans UsedMAC. De façon spécifique, le responsable de la mise en œuvre doit convenablement comparer les Ha (Adresses matérielles, en anglais « Hardware addresses »), et si elles sont identiques, il ne doit jamais utiliser « 1 » car il obligerait inutilement le dispositif utilisant cette NMa (Adresse MAC de réseau, en anglais « Network MAC address ») avant le dernier arrêt de le modifier au moment de l'amorçage. Pour une mise en œuvre simplifiée, il convient que le responsable de la mise en œuvre utilise « 0 » pour tous les bits de UsedMAC ou décide d'utiliser « 0 » ou « 1 » pour certains bits et entrer de manière inconditionnelle « 0 » pour le reste.

Étape 2. Si un nœud fonctionnel reçoit un paquet de demande de confirmation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») et que la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») provisoire contenue dans celui-ci est la même que la NMa du nœud fonctionnel, le nœud fonctionnel doit envoyer un paquet de réponse à la confirmation d'adresse MAC à l'expéditeur. Le Tableau 15 indique le format des paquets de réponse à la confirmation d'adresse MAC. Les données à enregistrer dans UsedMAC sont décrites à l'alinéa précédent.

Des exemples de séquences d'amorçage de base sont présentés à l'Annexe A. Si ces exemples de séquences ne sont pas cohérents avec cet article, la terminologie de cet article a priorité.

4.7 Serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »)

4.7.1 Exigence concernant le serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »)

Toutes les NMa (Adresses MAC de réseau, en anglais « Network MAC addresses ») dans un sous-réseau du réseau résidentiel doivent être pilotées par un serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »). Chaque nœud d'un sous-réseau d'un réseau résidentiel peut obtenir une NMa auprès du serveur d'adresses MAC au moment de l'amorçage. Le serveur d'adresses MAC doit allouer une NMa appropriée à chaque nœud nouvellement amorcé de façon que la NMa de chaque dispositif du sous-réseau soit différente de celle des autres dispositifs. Le serveur d'adresses MAC doit allouer la même adresse aux nœuds ayant la même Ha (Adresse matérielle, en anglais « Hardware address »). Il est habituellement nécessaire au serveur d'adresses MAC de se souvenir des NMa qu'il a allouées aux Ha. Un sous-réseau ne doit pas comporter plus d'un serveur d'adresses MAC. Lorsqu'il n'y a pas de serveur d'adresses MAC dans un sous-réseau (ou lorsqu'il n'y a pas de nœud cherchant à devenir le serveur d'adresses MAC), tout nœud du sous-réseau peut devenir le serveur d'adresses MAC conformément au mode opératoire de 4.7.2. Toutefois, lorsqu'un nœud est devenu le nœud du serveur d'adresses MAC il doit continuer à être le nœud du serveur d'adresses MAC jusqu'à ce que le sous-réseau auquel il appartient soit reconstruit. Par ailleurs, si un nœud du serveur d'adresses MAC souhaite rejoindre un nouveau sous-réseau, le mode opératoire de 4.7.2 doit être exécuté après l'avoir rejoint en tant que nœud général.

4.7.2 Séquence de traitement pour l'amorçage du serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »)

Lorsqu'il n'y a pas de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») dans un sous-réseau (ou lorsqu'il n'y a pas de nœud tentant de devenir le serveur d'adresses MAC), tout nœud de serveur d'adresses non MAC (nœud général) du sous-réseau peut devenir le serveur d'adresses MAC s'il le désire et quand il le désire. Pour devenir le serveur d'adresses MAC, un nœud général doit exécuter la séquence suivante:

Étape 1. Le nœud général envoie deux fois un paquet de demande de détection de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») en utilisant l'adresse IPme (Adresse de multidiffusion IP, en anglais « IP multicast address ») avec un intervalle T6. La seconde transmission peut être omise s'il reçoit un paquet de réponse à la détection de serveur d'adresses MAC ou un paquet de notification de serveur d'adresses MAC.

Étape 2. Si le nœud général reçoit un paquet de réponse à la détection de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») ou un paquet de notification de serveur d'adresses MAC avant expiration de la période de temporisation T5, cette séquence doit échouer et on doit la forcer à s'arrêter.

Étape 3. Si le nœud général reçoit un paquet de demande de détection de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control »), il doit répéter cette séquence à partir de l'étape 1 après une période d'attente de T12 ou plus. Le traitement de l'étape 2 doit se poursuivre même pendant la période d'attente.

Étape 4. Le serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») commence à fonctionner.

Étape 5. Un paquet de notification de serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») fait l'objet d'une diffusion multiple deux fois ou plus en utilisant l'adresse IPme (Adresse de multidiffusion IP, en anglais « IP multicast address ») par intervalles de T6. Un paquet de notification de serveur d'adresses MAC est représenté dans le Tableau 19.

La période d'attente T12 est une période déterminée de façon aléatoire avant que le nœud puisse exécuter de nouveau cette séquence lorsqu'il a déterminé qu'un autre nœud tente de démarrer cette séquence simultanément (voir Tableau 26). Cette période d'attente empêche deux nœuds ou plus de devenir des serveurs d'adresses MAC. Normalement, cette période d'attente permet à l'autre nœud de devenir le serveur d'adresses MAC, auquel cas la séquence échoue et on la force à s'arrêter. Lorsqu'il y a au moins un nœud fonctionnel lorsque le serveur de NMa (Adresse MAC de réseau, en anglais « Network MAC address ») est amorcé, il convient que le serveur d'adresses MAC n'alloue pas la NMa utilisée par le nœud à un autre dispositif. En conséquence, il convient que le serveur d'adresses MAC obtienne les Ha (Adresses matérielles, en anglais « Hardware addresses ») et NMa des nœuds situés dans le sous-réseau en utilisant les paquets de demande d'adresse MAC à tous les nœuds, etc.

4.7.3 Traitement par serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») fonctionnel

Un serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») fonctionnel doit exécuter ce qui suit:

- a) Lorsque le serveur d'adresses MAC fonctionnel reçoit un paquet de demande de détection de serveur d'adresses MAC:

Le serveur d'adresses MAC doit envoyer à l'expéditeur un paquet de réponse à la détection de serveur d'adresses MAC.

Le Tableau 20 montre le format des paquets de réponse à la détection de serveur d'adresses MAC.

- b) Lorsque le serveur d'adresses MAC fonctionnel reçoit un paquet de demande d'initialisation d'adresse MAC:

Le serveur d'adresses MAC doit déterminer la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») à allouer à l'expéditeur et envoyer à l'expéditeur un paquet de réponse à l'initialisation de serveur d'adresses MAC contenant l'adresse. La NMa allouée à l'expéditeur doit être déterminée comme suit:

- 1) Si le serveur d'adresses MAC a autrefois répondu en utilisant cette séquence au type matériel (RHType), longueur de Ha (Adresse matérielle, en anglais « Hardware address ») (RHLen) et Ha (RHAddr) contenu dans le paquet de demande d'initialisation d'adresse MAC, la NMa allouée à l'expéditeur dans cette réponse doit être utilisée.
- 2) Dans tous les autres cas sauf 1), une NMa qui n'est pas utilisée dans le sous-réseau doit être allouée à l'expéditeur. Ce qui suit ne doit pas être utilisé: une NMa allouée autrefois en utilisant cette séquence, une NMa dont on a déterminé qu'elle était utilisée dans le sous-réseau par l'intermédiaire de paquets reçus, une NMa réservée par l'administrateur, etc., et la NMa du serveur d'adresses MAC. Si la NMa provisoire contenue dans le paquet de demande d'initialisation d'adresse MAC satisfait à cette condition, il convient d'allouer la NMa provisoire comme NMa. Selon la mise en œuvre, une fonction peut être utilisée vérifiant les paquets reçus et permettant aux NMa utilisées avant un certain moment antérieur d'être utilisées comme adresses qui ne sont pas actuellement utilisées dans le sous-réseau.

Si le serveur d'adresses MAC ne reçoit pas de paquet de réponse à l'allocation d'adresse MAC avant expiration de la période de temporisation T11 (voir Tableau 26) mesurée à partir de la transmission du paquet de réponse à l'initialisation de serveur d'adresses MAC, le serveur d'adresses MAC doit envoyer de nouveau le paquet de réponse à l'initialisation de serveur d'adresses (jusqu'à 3 fois au total).

Il est habituellement nécessaire que le serveur d'adresses MAC se souvienne des adresses MAC qu'il a allouées aux Ha (Adresses matérielles, en anglais « Hardware addresses ») pour être exécutées (Le Tableau 25 montre un exemple de tableau pour mémoriser la NMa (Adresse MAC de réseau, en anglais « Network MAC address ») allouée pour référence pour le responsable de la mise en œuvre).

Tableau 25 – Exemple de mémorisation des NMa (Adresses MAC de réseau, en anglais « Network MAC addresses ») allouées

Hardware type	Hardware address	Allocation time	Allocated NMa
1	ff-01-23-45-67-03	1232567	03
1	ff-cd-ef-78-45-05	1231763	05
1	ff-cd-aa-00-11-07	1233923	07

Anglais	Français
Hardware type	Type de matériel
Hardware address	Adresse matérielle
Allocation time	Heure d'allocation
Allocated NMa	NMa allouée

Lorsque le serveur d'adresses MAC (Commande d'accès au support, en anglais « Medium Access Control ») reçoit une nouvelle demande d'allocation (c'est-à-dire une demande d'un nœud avec une Ha (Adresse matérielle, en anglais « Hardware address ») qui n'est pas incluse dans la table d'adresses), il doit allouer une NMa (Adresse MAC de réseau, en anglais « Network MAC address ») qu'il n'a pas allouée antérieurement. Toutefois, lorsque le serveur d'adresses MAC a utilisé toutes les adresses pouvant être allouées, il doit allouer une adresse appropriée en utilisant une méthode d'allocation appropriée à la mise en œuvre. Ceci peut être obtenu par:

- Une fonction pour utiliser la NMa la plus ancienne que le serveur d'adresses MAC a allouée antérieurement; ou
- Une fonction mémorisant tous les paquets entrants, vérifiant tous les paquets reçus et permettant aux NMa allouées aux Ha (Adresses matérielles, en anglais « Hardware addresses ») des nœuds n'ayant pas effectué de communication pendant une certaine période de temps d'être allouées aux nouveaux nœuds demandeurs.

Quelle que soit la méthode choisie, il convient que celle-ci minimise ou élimine la possibilité de conflit d'adresse.

Des exemples de séquences d'amorçage de base sont présentés à l'Annexe B. Si ces exemples de séquences ne sont pas cohérents avec cet article, la terminologie de cet article a priorité.

4.8 Paramètres de période de temps

Le Tableau 26 ci-dessous indique les valeurs obligatoires ou recommandées pour la période de temps.

Tableau 26 – Paramètres de période de temps

Para-mètre	Valeur	Type (obligatoire ou recommandé)	Définition
T0	Moins de 50 ms	recommandé	Période d'attente avant que le paquet de réponse à l'initialisation d'adresse MAC puisse être envoyé après réception du paquet de demande d'initialisation d'adresse MAC lorsque NMa est à « 0 »
T1	0	obligatoire	Unité incrémentale de période d'attente multipliée par la valeur de NMa et additionnée avec T0 pour calculer T7
T2	3,0 s	obligatoire	Intervalle entre la multidiffusion d'un paquet de demande d'initialisation d'adresse MAC et la réception d'un paquet de réponse à l'initialisation d'adresse MAC correspondant
T3	3,0 s	obligatoire	Période de temporisation pour la réception d'un paquet de réponse à la résolution d'adresse MAC/IP après transmission d'un paquet de demande de résolution d'adresse MAC/IP
T4	3,0 s	obligatoire	Période de temporisation pour la réception d'un paquet de réponse de résolution d'adresse IP/MAC après transmission d'un paquet de demande de résolution d'adresse IP/MAC
			Période de temporisation pour la réception d'un paquet de réponse à la résolution d'adresse matérielle/MAC après transmission d'un paquet de demande de résolution d'adresse matérielle/MAC
T5	3,0 s	obligatoire	Période de temporisation pour la réception d'un paquet de réponse à la détection de serveur d'adresses MAC après transmission d'un paquet de demande de détection de serveur d'adresses MAC
T6	pas supérieure à 100 ms	recommandé	Intervalle de transmission de paquet de demande d'initialisation d'adresse MAC
			Intervalle de transmission de paquet de demande de confirmation d'adresse MAC
			Intervalle de transmission de paquet de demande de détection de serveur d'adresses MAC
			Intervalle de transmission de paquet de notification de serveur d'adresses MAC
T7	-	-	Période d'attente avant que le paquet de réponse à l'initialisation d'adresse MAC puisse être envoyé après réception du paquet de demande d'initialisation d'adresse MAC $T7 = [\text{valeur de NMa}] \times [T1] + [T0]$
T8	24 h	recommandé	Période d'attente avant de pouvoir réutiliser la NMa contenue dans le paquet de demande d'initialisation d'adresse MAC reçu. Période d'attente avant de pouvoir réutiliser la NMa contenue dans le paquet de demande de confirmation d'adresse MAC reçu
T9	3,0 s	obligatoire	Période de temporisation pour la réception d'un paquet de réponse à la confirmation d'adresse MAC, d'un paquet de demande d'initialisation d'adresse MAC (lorsque RMAC est identique à l'auto-NMa provisoire) ou d'un paquet (lorsque RMAC est identique à l'auto-NMa provisoire) après transmission d'un paquet de demande de confirmation d'adresse MAC
T10	0 à 100 ms	recommandé	Période d'attente avant que la séquence d'initialisation puisse être exécutée (nombre aléatoire)
T11	200 ms	obligatoire	Période de temporisation pour la réception d'un paquet de réponse à l'allocation d'adresse MAC après transmission d'un paquet de réponse à l'initialisation d'adresse MAC par le serveur d'adresses MAC
T12	20 s	recommandé	Période d'attente avant qu'un paquet de demande de détection de serveur d'adresses MAC puisse être réémis après réception d'un paquet de demande de détection de serveur d'adresses MAC
T13	24 h	recommandé	Période d'attente avant de pouvoir entrer un « 1 » dans le champ UsedMAC après réception d'un paquet
T14	3,0 s	recommandé	Période d'attente pour la réception d'un paquet de réponse à l'adresse MAC à tous les nœuds après transmission d'un paquet de demande d'adresse MAC à tous les nœuds

4.9 Disposition pour la mise à jour des données après acquisition de la NMa (Adresse MAC de réseau, en anglais « Network MAC address »)

Ce paragraphe décrit les mécanismes recommandés pour la mise à jour des données après acquisition de la NMa (Adresse MAC de réseau, en anglais « Network MAC address »).

- a) Même lorsqu'un nœud est fixe dans un sous-réseau, sa NMa peut changer au réamorçage lorsqu'il rejoint le réseau après l'avoir quitté en conséquence d'une commutation d'alimentation ou d'une déconnexion de liaison, en particulier avec la méthode distribuée. Il est donc recommandé de mettre en œuvre dans les couches associées un mécanisme mettant à jour, lorsqu'un nœud rejoint le réseau, les valeurs de la NMa et de la Na (Adresse réseau, en anglais « Network Address ») qu'il maintient et gère sur les bases de données des informations associées conjointement avec sa NMa et sa Na en utilisant un paquet de réponse à l'initialisation d'adresse MAC (Commande d'accès au support, en anglais « Medium Access Control ») et/ou de quelconques paquets de demande de résolution d'adresse.
- b) Il est possible que pendant qu'un nœud est temporairement détaché du réseau, la NMa d'un nœud dans un autre sous-réseau puisse changer. Dans ce cas, le nœud détaché ne peut pas reconnaître la nouvelle adresse de ce nœud. Il est donc recommandé d'introduire un mécanisme similaire à celui décrit en a) de façon que pendant l'initialisation d'un nœud lorsqu'il rejoint le réseau après l'avoir quitté, les bases de données des informations associées incluant la NMa et la Na du nœud soient mises à jour.

5 TCP/IP (Protocole de commande de transmission/Protocole Internet, en anglais « Transmission Control Protocol/Internet Protocol ») et exigences

On doit utiliser l'UDP (Protocole de datagramme utilisateur, en anglais « User Datagram Protocol ») pour la couche transport.

5.1 IP (Protocole Internet (en anglais, « Internet Protocol »)

5.1.1 Protocoles à utiliser

Les protocoles suivants, tels que référencés dans la bibliographie, doivent être mis en œuvre.

IPv4: Protocole Internet IETF RFC 791

ARP: Résolution d'adresse IETF RFC 826

IGMP: Protocole de messages de commande Internet IETF RFC 792, Mode opératoire de mise en sous-réseau normalisé Internet IETF RFC 950

DHCP: Protocole de configuration de serveur dynamique IETF RFC1541, Exigences pour les serveurs Internet IETF RFC1122

Les documents suivants doivent être utilisés pour référence:

IGMP:IETF RFC1112 Internet Group Multicast Protocol

IETF RFC1597 Address Allocation for Private Internets

5.1.2 Adresse IP (Protocole Internet (en anglais, « Internet Protocol »)

Chaque couche IP (Protocole Internet, en anglais « Internet Protocol ») prenant en charge un nœud doit avoir une adresse IPv4. La présente norme ne spécifie pas la plage des adresses IP pouvant être utilisées par des nœuds individuels. On peut utiliser une adresse IP privée ou globale.

5.1.3 Adresse de multidiffusion

L'adresse de multidiffusion **224.0.23.0** (IPme) doit être utilisée pour cette couche. Chaque nœud prenant en charge cette couche doit être capable d'envoyer des paquets à cette adresse et de recevoir les paquets envoyés à cette adresse.

5.1.4 DHCP (Protocole de configuration de serveur dynamique, en anglais « Dynamic Host Configuration Protocol »)

Chaque nœud prenant en charge cette couche doit comporter une fonction pour obtenir les informations de détermination d'adresse en utilisant un serveur DHCP (Protocole de configuration de serveur dynamique, en anglais « Dynamic Host Configuration Protocol »). Pour le fonctionnement, il est recommandé de déployer un serveur DHCP dans le réseau IP (Protocole Internet (en anglais, « Internet Protocol »).

5.1.5 Méthodes d'obtention d'une adresse IP (Protocole Internet, en anglais « Internet Protocol ») par détermination manuelle, etc.

La présente norme ne spécifie aucune méthode de détermination d'adresse IP (Protocole Internet, en anglais « Internet Protocol ») autre que le DHCP (Protocole de configuration de serveur dynamique, en anglais « Dynamic Host Configuration Protocol »).

5.1.6 Routage

Les opérations dans lesquelles les paquets du réseau résidentiel/IP (Protocole Internet, en anglais « Internet Protocol ») sont transférés au-delà d'un routeur IP ne sont pas autorisées. Cette couche ne doit pas envoyer un paquet adressé à un nœud situé dans un autre sous-réseau IP. Tous les paquets reçus depuis un ou plusieurs nœuds situés dans un autre sous-réseau IP doivent être éliminés.

5.2 UDP (Protocole de datagramme utilisateur, en anglais « User Datagram Protocol »)

5.2.1 Protocoles à utiliser

Le protocole suivant, tel que référencé dans la bibliographie, doit être mis en œuvre.

IETF RFC 768 User Datagram Protocol

5.2.2 Numéro de port

Le numéro du port de destination pour les paquets UDP (Protocole de datagramme utilisateur, en anglais « User Datagram Protocol ») doit être **3610**. La présente norme ne spécifie aucun numéro de port d'origine.

6 Interface et exigences spécifiques au support de couche inférieure

6.1 Interface et exigences du support de couche inférieure

L'interface et les exigences sur chaque support de couche inférieure sont spécifiées à l'Annexe C.

6.2 Transition d'état interne logiciel

6.2.1 Vue d'ensemble

Ce paragraphe montre la séquence pour chacun des sept états internes du logiciel de la couche inférieure du réseau résidentiel. Les sept états sont les suivants:

- a) État d'arrêt