IEC 62457

Edition 1.0 2007-09

INTERNATIONAL STANDARD

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

IEC 62457:2007(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: 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.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

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

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 62457

Edition 1.0 2007-09

INTERNATIONAL STANDARD

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE XB

ICS 33.040; 33.160.01

ISBN 2-8318-9306-2

CONTENTS

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.

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.

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.

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.

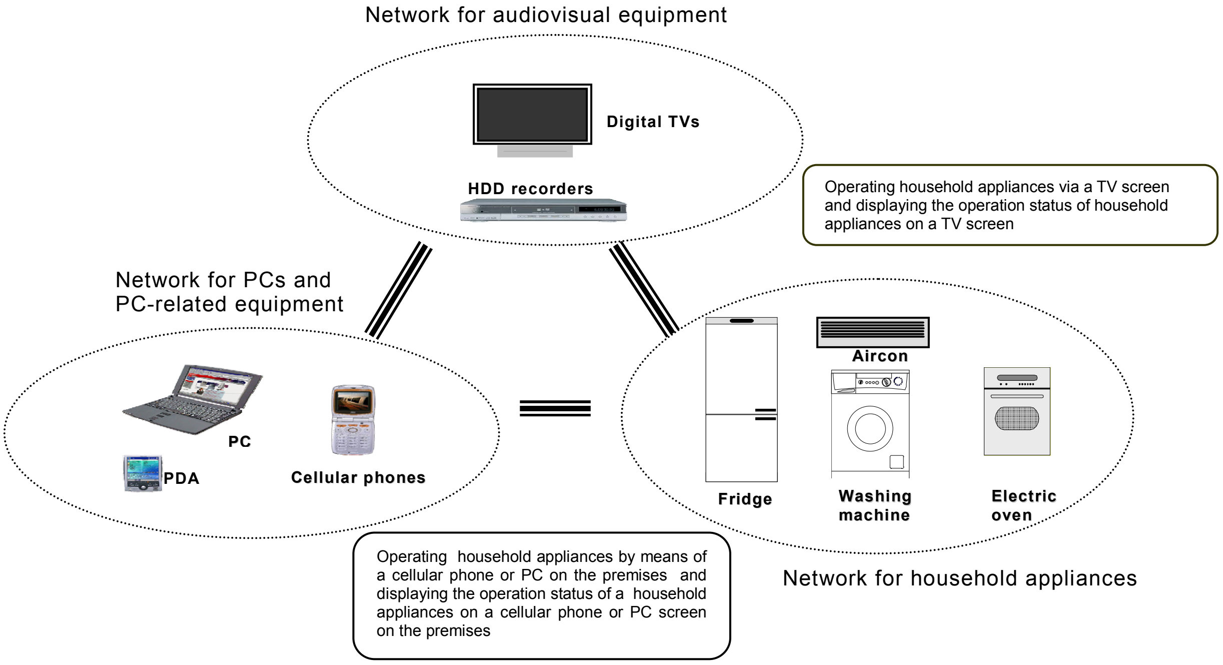
Because data transferred within, into and out of networks of standalone-type household appliances are control data, which are much smaller in volume than data similarly transferred for networks of audiovisual equipment, PCs and PC-related equipment, and because standalone-type household appliances have 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 countries[1)].

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.


Network for audiovisual equipment
Digital TVs
HDD recorders
Network for PCs and PC-related equipment
PC
PDA
Cellular phones
Aircon
Fridge
Washing machine
Electric oven
Network for household appliances

Operating household appliances via a TV screen and displaying the operation status of household appliances on a TV screen

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

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

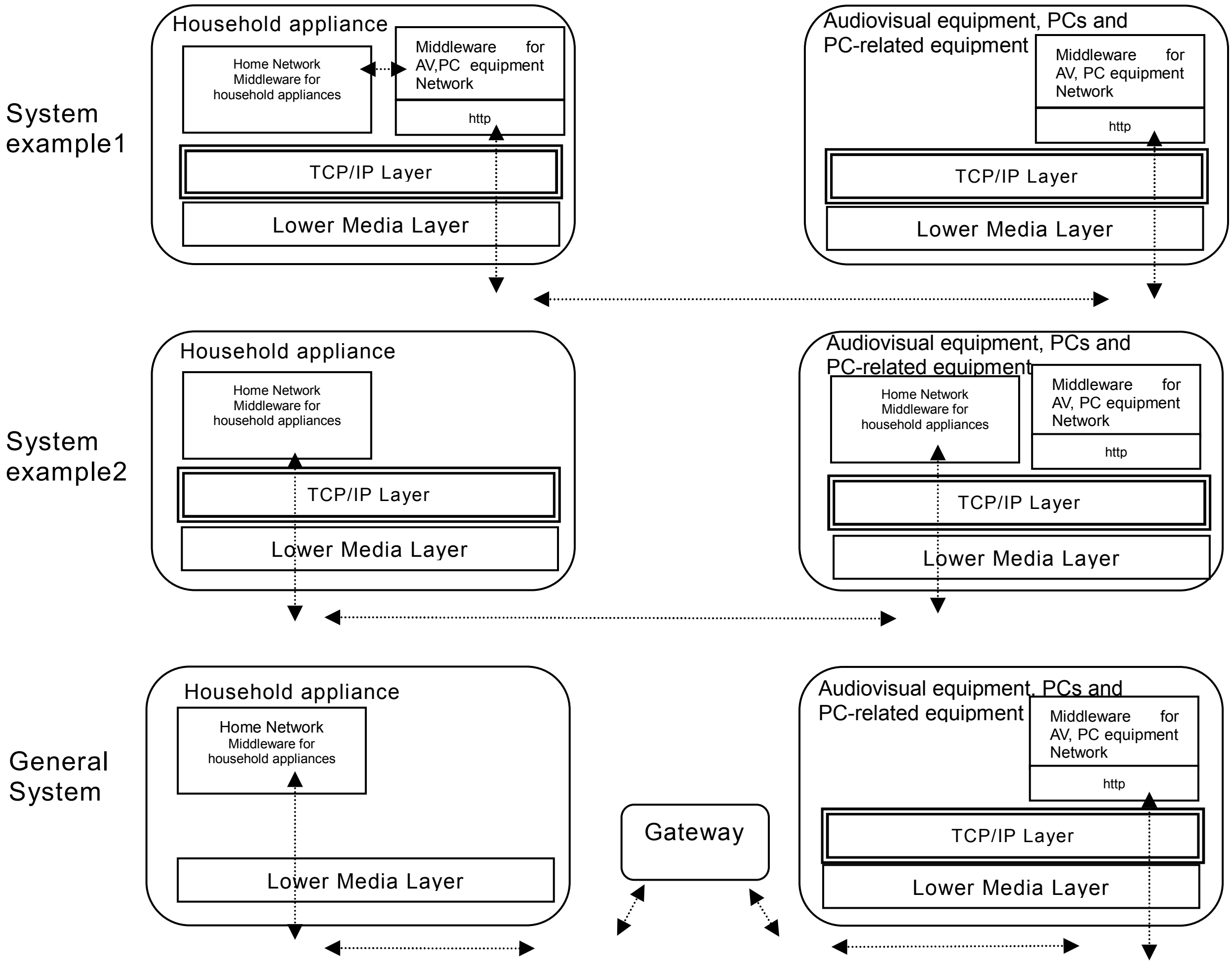
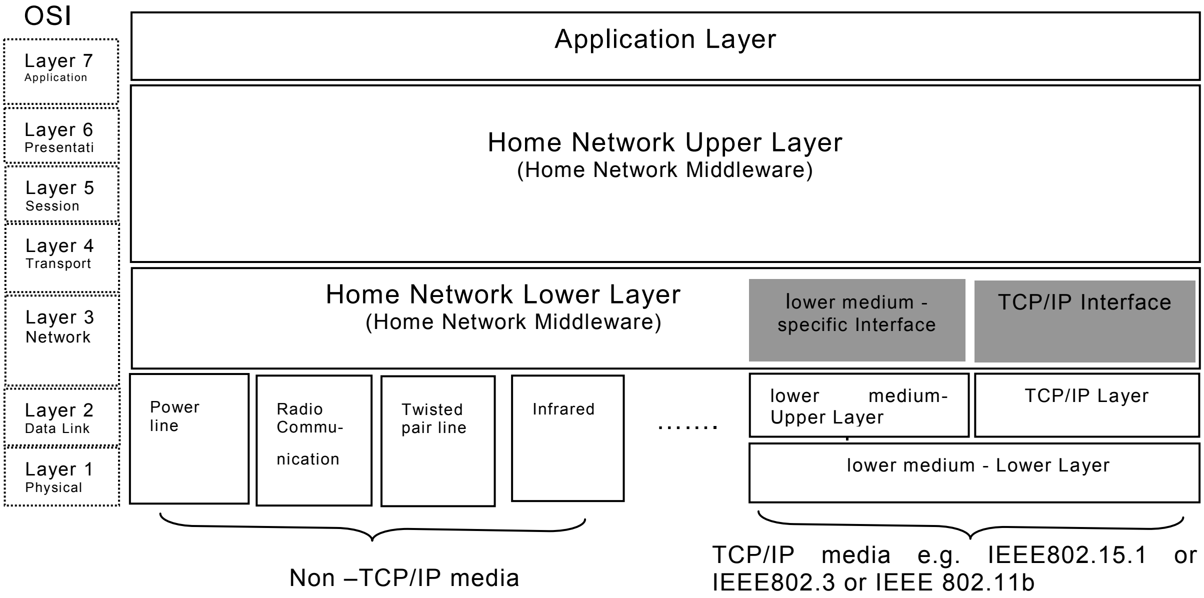

System example1
Household appliance
Home Network Middleware for household appliances
Middleware for AV,PC equipment Network
http
TCP/IP Layer
Lower Media Layer
Audiovisual equipment, PCs and PC-related equipment
Middleware for AV, PC equipment Network
http
TCP/IP Layer
Lower Media Layer
System example2
Household appliance
Home Network Middleware for household appliances
TCP/IP Layer
Lower Media Layer
Audiovisual equipment, PCs and PC-related equipment
Home Network Middleware for household appliances
Middleware for AV, PC equipment Network
http
TCP/IP Layer
Lower Media Layer
General System
Household appliance
Home Network Middleware for household appliances
Lower Media Layer
Gateway
Audiovisual equipment, PCs and PC-related equipment
Middleware for AV, PC equipment Network
http
TCP/IP Layer
Lower Media Layer

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.

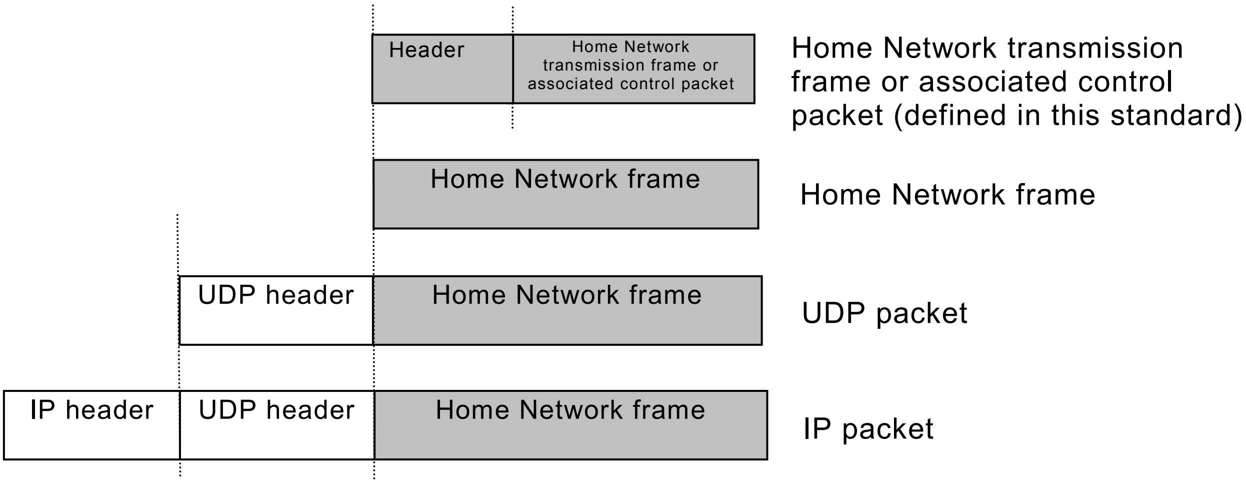

Header
Home Network transmission frame or associated control packet
Home Network transmission frame or associated control packet (defined in this standard)
Home Network frame
Home Network frame
UDP header
Home Network frame
UDP packet
IP header
UDP header
Home Network frame
IP packet

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) 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.

b) 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.

c) 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.

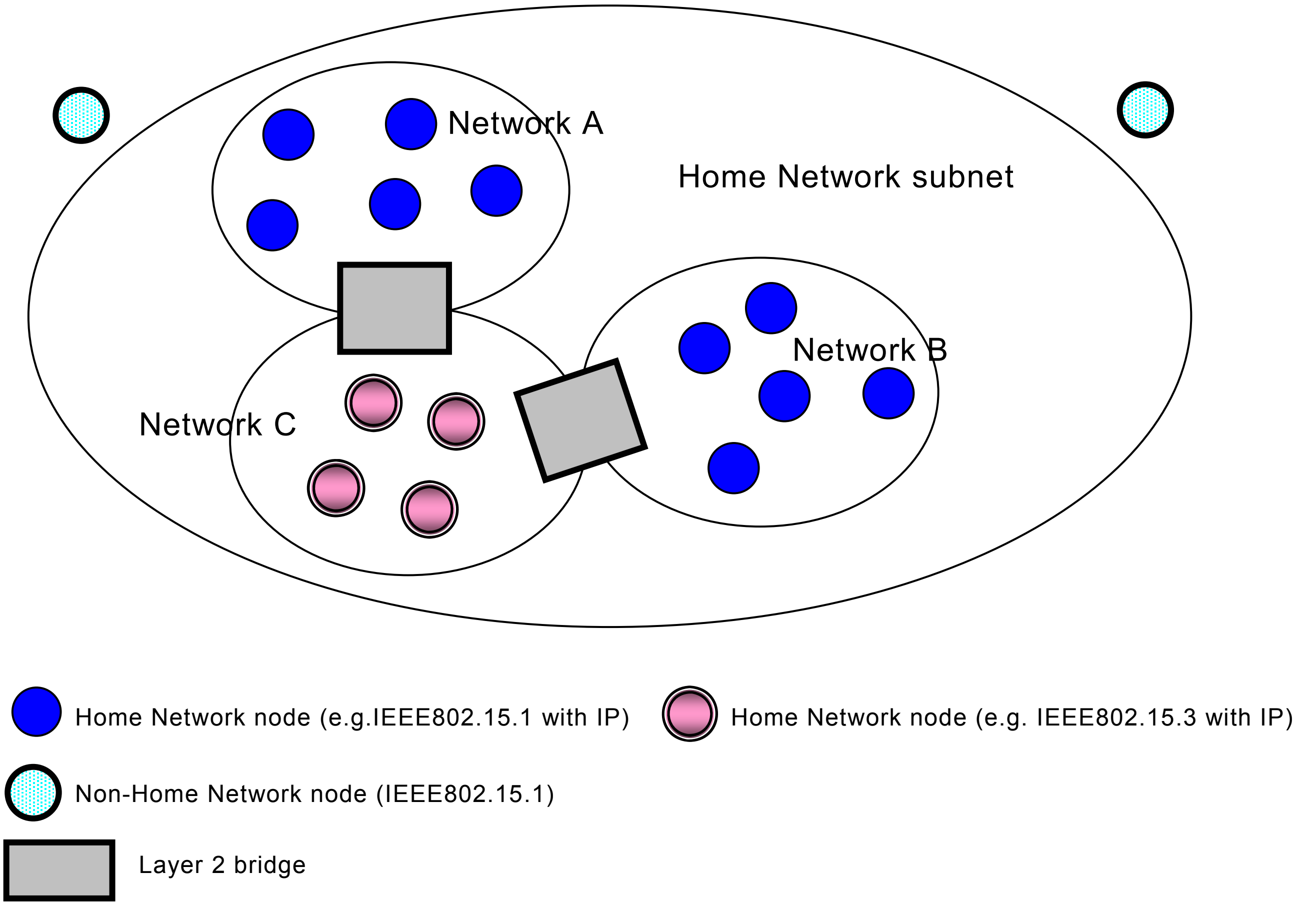

Network A
Home Network subnet
Network B
Network C
Home Network node (e.g.IEEE802.15.1 with IP)
Home Network node (e.g. IEEE802.15.3 with IP)
Non-Home Network node (IEEE802.15.1)
Layer 2 bridge

Figure 5 – Example of a subnet using Layer 2 bridges

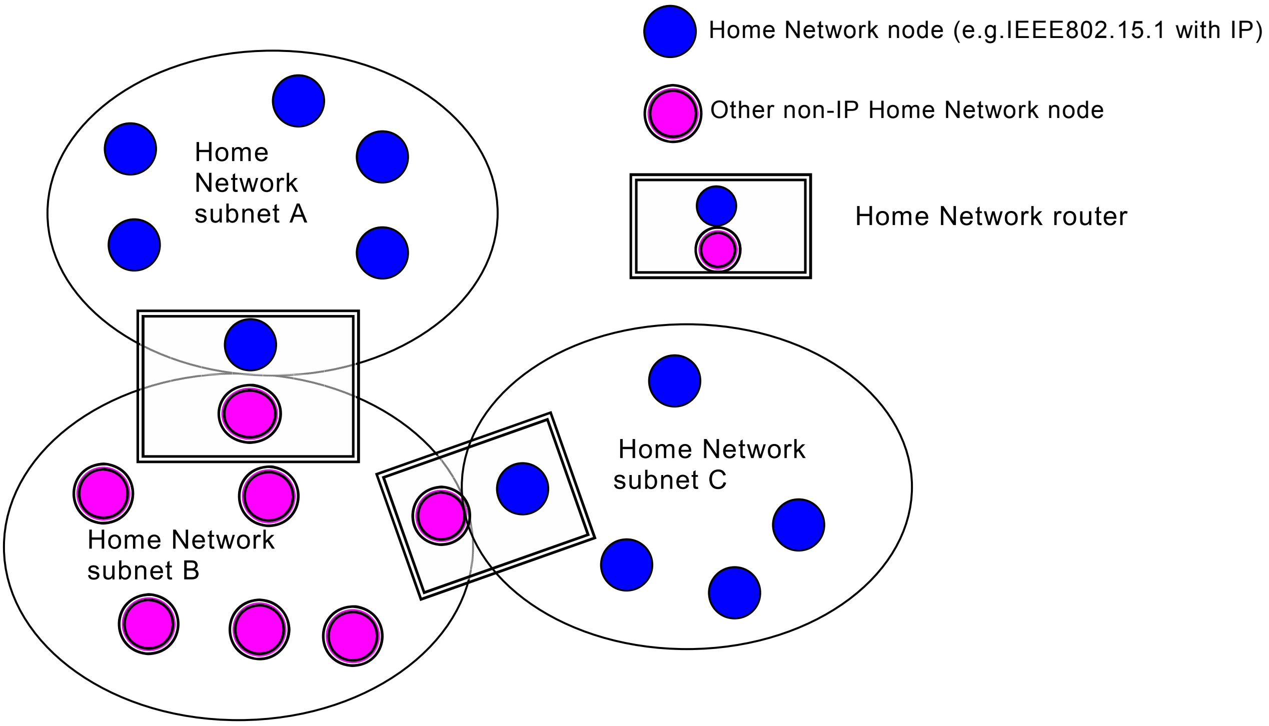


Figure 6 – Example of a subnet connection using Home Network routers

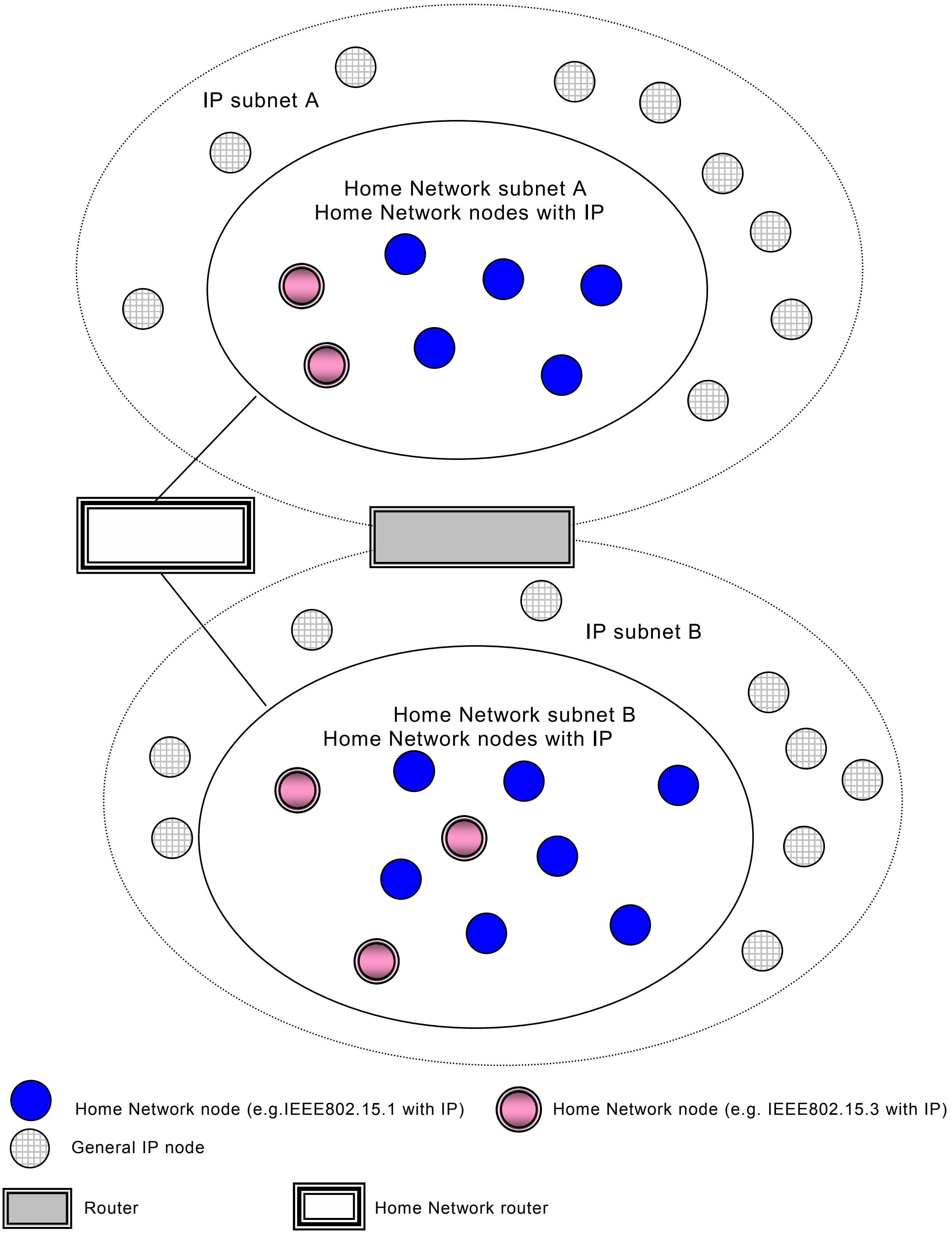

IP subnet A
Home Network subnet A
Home Network nodes with IP
IP subnet B
Home Network subnet B
Home Network nodes with IP
Home Network node (e.g.IEEE802.15.1 with IP)
Home Network node (e.g. IEEE802.15.3 with IP)
General IP node
Router
Home Network router

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).

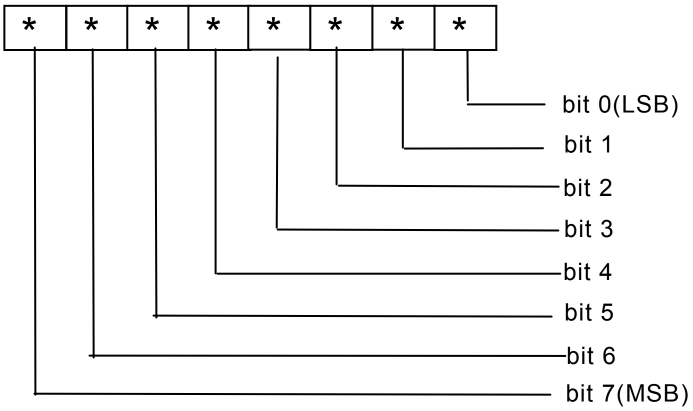


Figure 9 – Notation for bits in the flag field

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
10101100**1101**1110	**0100**1000	**0000**0000**0000**0000**1000**0000

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.

a) Stores a Home Network transmission frame, which was received from the Home Network upper layer or UDP Layer.

b) 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.

c) 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.

d) When the Home Network transmission frame to be transmitted is abroadcasting 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.

a) Used to obtain the IP address of a Home Network node that has a NMa.

b) 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”.

c) 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.

a) Used to obtain the NMa of a Home Network node that has an IP address.

b) 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".

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 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.

a) Used to obtain the NMa of a Home Network node that has a Ha.

b) 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".

c) 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.

a) 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.

b) The booting node (i.e., the node requesting a NMa initialization) shall be referred to as the “requesting node”.

c) 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.

d) 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.

a) 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.

b) 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.

c) 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) 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.

b) 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) 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.

b) 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".

c) 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.

d) 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.

a) 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.

b) 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".

c) 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.

a) 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.

b) The node that transmits the "NMa overlap" network control message shall be referred to as the "transmission node".

c) This message shall be broadcast throughout the subnet.

d) 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.

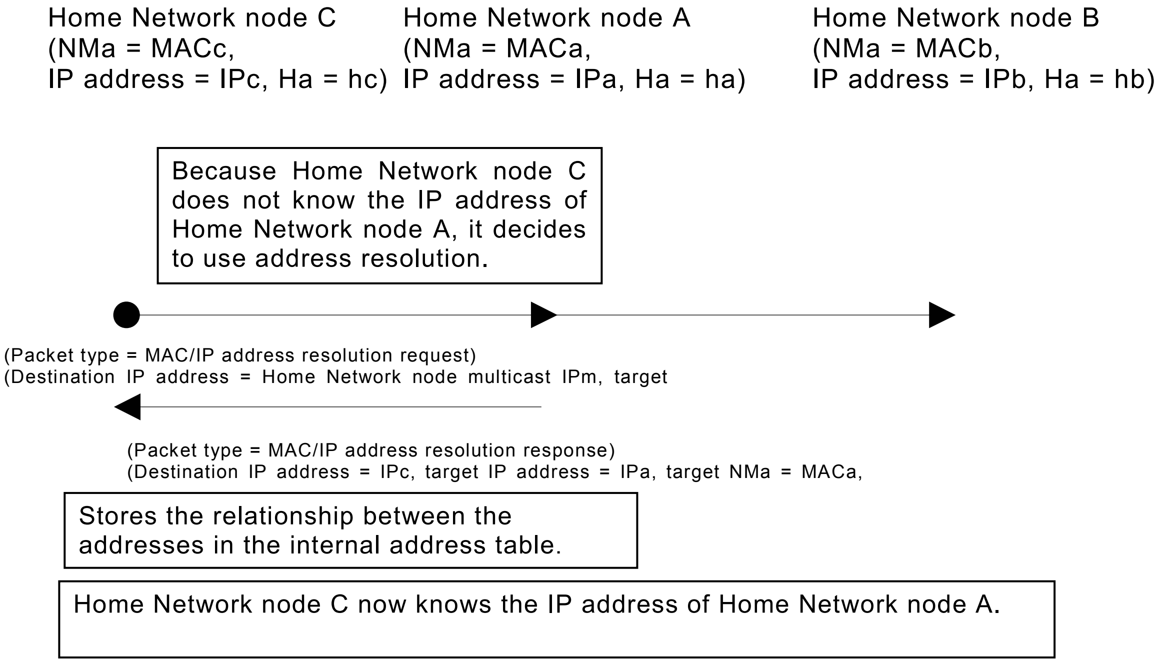
d) The timeout period between the transmission of the IP address resolution request and the receipt of the IP address resolution response packet shall be T3 as described in Table 26. If no IP address resolution response packet is received within the timeout period, an error shall occur.

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 .



Because Home Network node C does not know the IP address of Home Network node A, it decides to use address resolution.

(Packet type = MAC/IP address resolution request)
(Destination IP address = Home Network node multicast IPm, target

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

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

Home Network node C now knows the IP address of Home Network node A.

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.

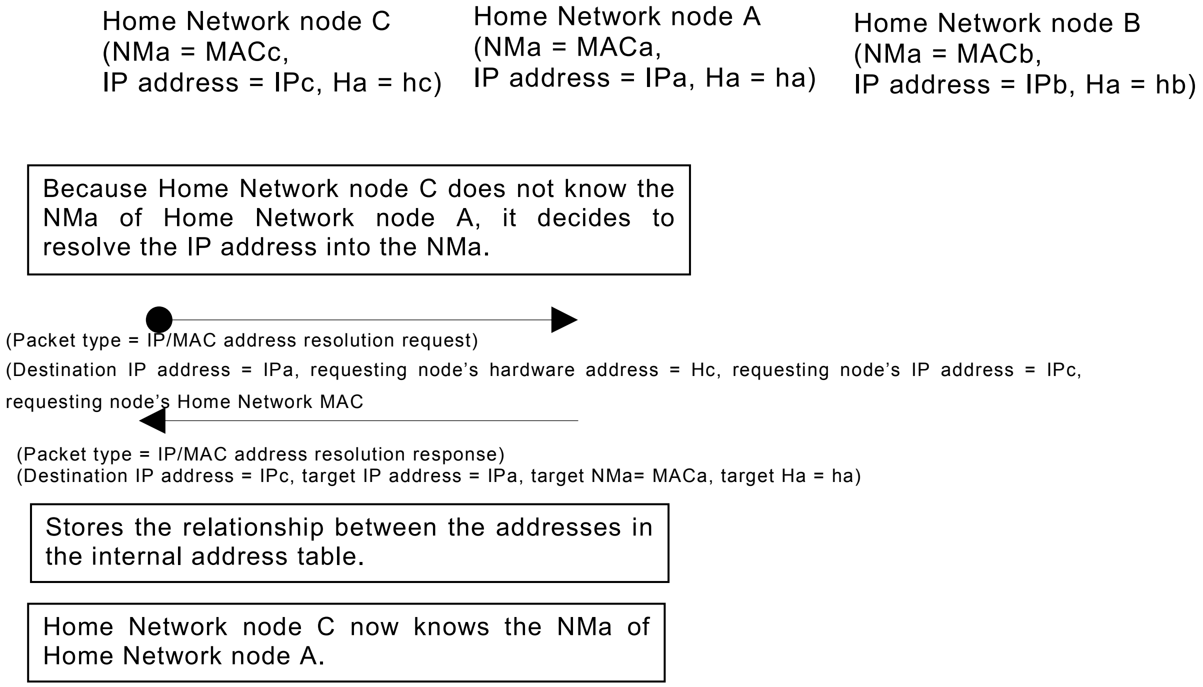

Home Network node C
(NMa = MACc,
IP address = IPc, Ha = hc)
Home Network node A
(NMa = MACa,
IP address = IPa, Ha = ha)
Home Network node B
(NMa = MACb,
IP address = IPb, Ha = hb)
Because Home Network node C does not know the NMa of Home Network node A, it decides to resolve the IP address into the NMa.
(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.

Figure 12 – Basic IP/MAC address resolution sequence

4.5.4 Hardware/MAC address resolution request/response

The details are described below.

a) 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”.

b) 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.

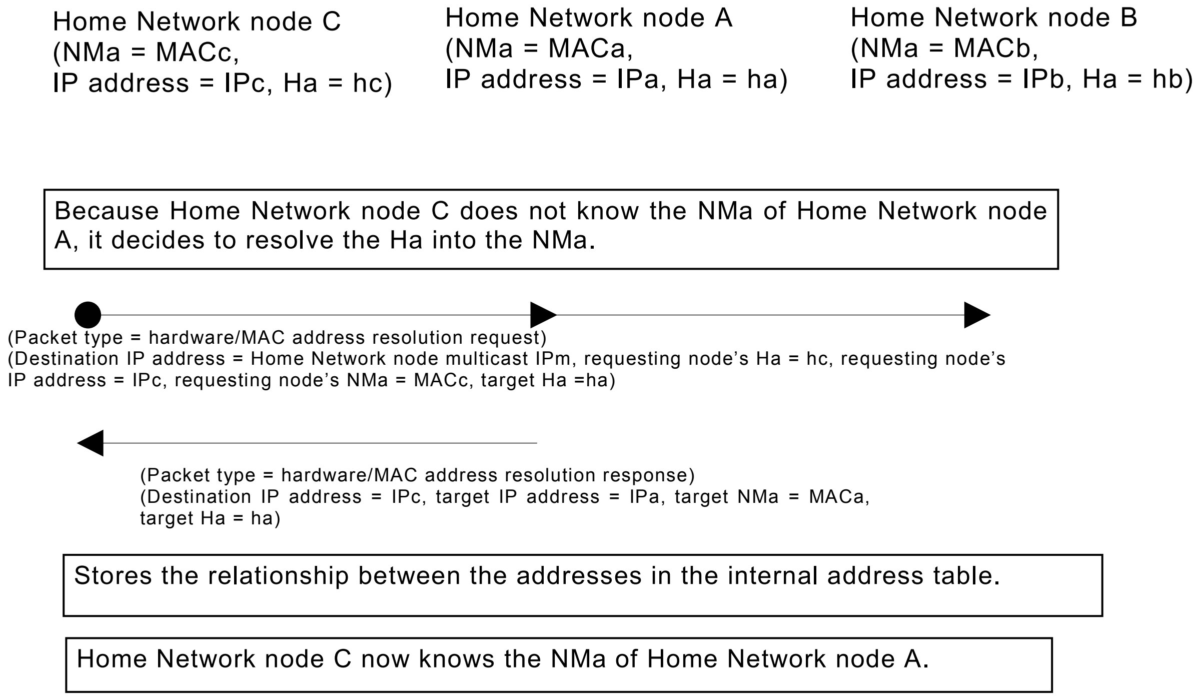
c) The requesting node multicasts to the Home Network subnet a hardware/MAC address resolution request packet that contains the target Hardware type, Ha length, and Ha to be resolved. Upon receipt of the request, the target node sends a hardware/MAC address resolution response packet containing its NMa, IP address, transmission medium Hardware type, Ha length, and Ha.

d) 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.

e) The content of the hardware/MAC address resolution response packet should be reflected in the address relation.

f) 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.


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)
(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)

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

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

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

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:

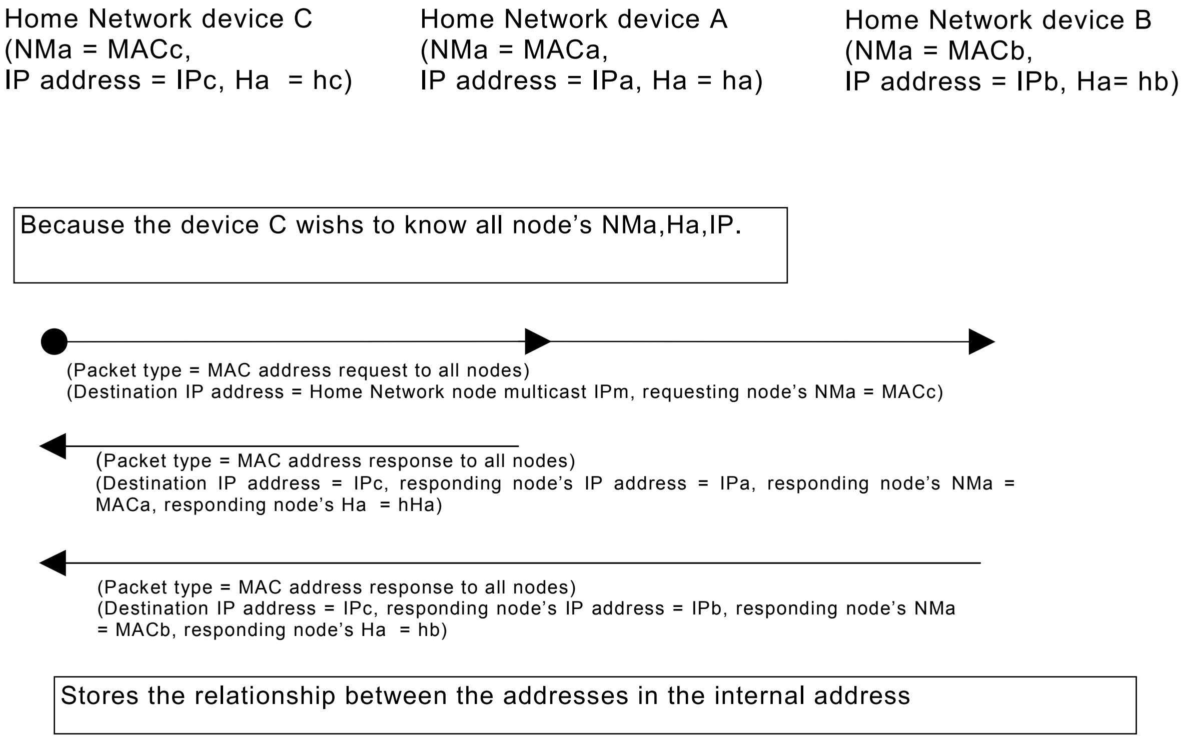

Home Network device C
(NMa = MACc,
IP address = IPc, Ha = hc)
Home Network device A
(NMa = MACa,
IP address = IPa, Ha = ha)
Home Network device B
(NMa = MACb,
IP address = IPb, Ha= hb)
Because the device C wishs to know all node's NMa,Ha,IP.
(Packet type = MAC address request to all nodes)
(Destination IP address = Home Network node multicast IPm, requesting node's NMa = 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)
(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)
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.

a) 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.

b) 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.

c) 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:

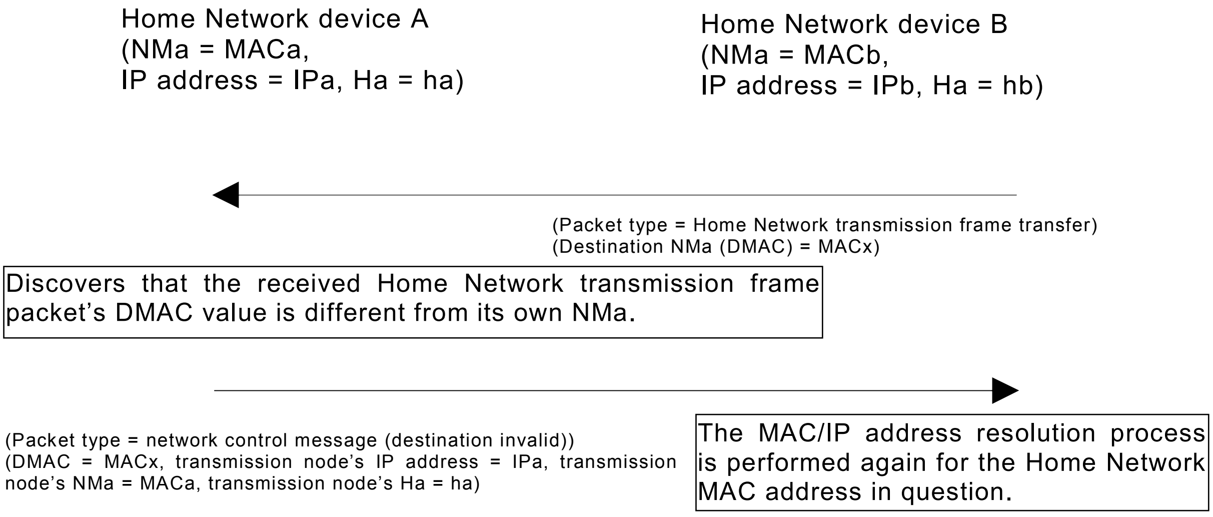

Home Network device A
(NMa = MACa,
IP address = IPa, Ha = ha)
Home Network device B
(NMa = MACb,
IP address = IPb, Ha = hb)
(Packet type = Home Network transmission frame transfer)
(Destination NMa (DMAC) = MACx)
Discovers that the received Home Network transmission frame packet's DMAC value is different from its own 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)
The MAC/IP address resolution process is performed again for the Home Network MAC address in question.

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.

a) 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.

b) 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 .

c) 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.

d) 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:

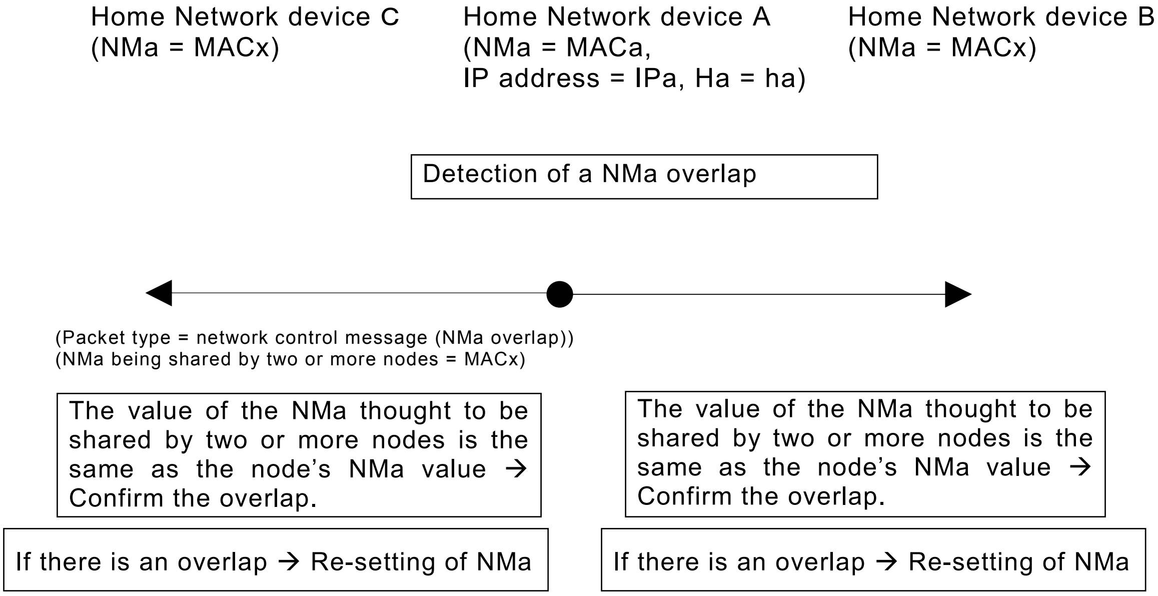

Home Network device C
(NMa = MACx)
Home Network device A
(NMa = MACa,
IP address = IPa, Ha = ha)
Home Network device B
(NMa = MACx)
Detection of a NMa overlap
(Packet type = network control message (NMa overlap))
(NMa being shared by two or more nodes = MACx)
The value of the NMa thought to be shared by two or more nodes is the same as the node’s NMa value → Confirm the overlap.
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.
If there is an overlap → Re-setting of NMa
If there is an overlap → Re-setting of NMa

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)	Booting 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.

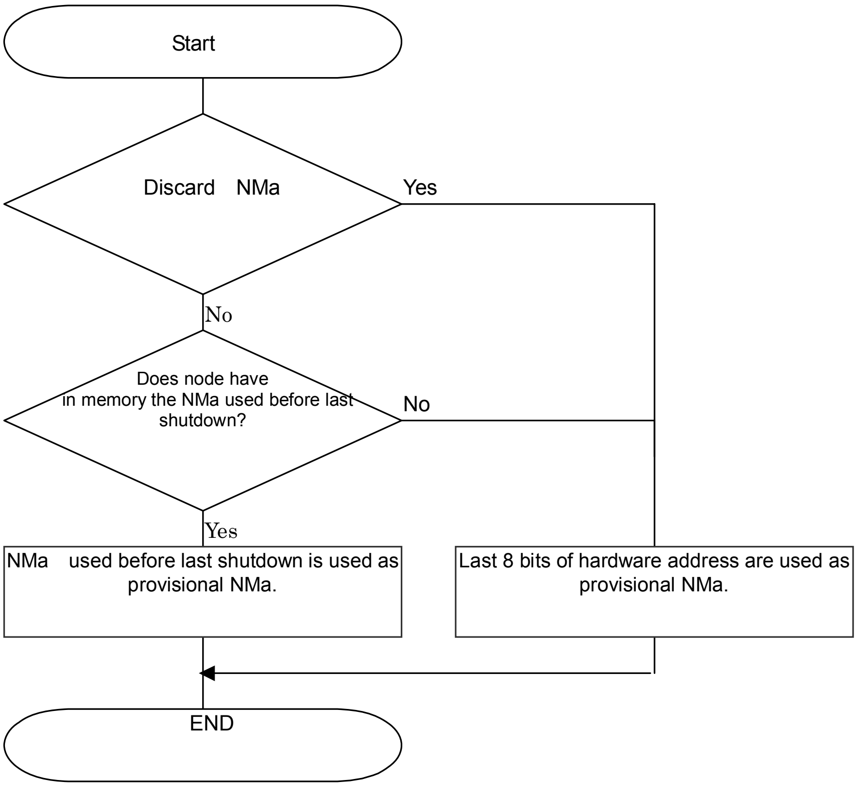

Start
Discard NMa
Yes
No
Does node have in memory the NMa used before last shutdown?
No
Yes
NMa used before last shutdown is used as provisional NMa.
Last 8 bits of hardware address are used as provisional NMa.
END

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.

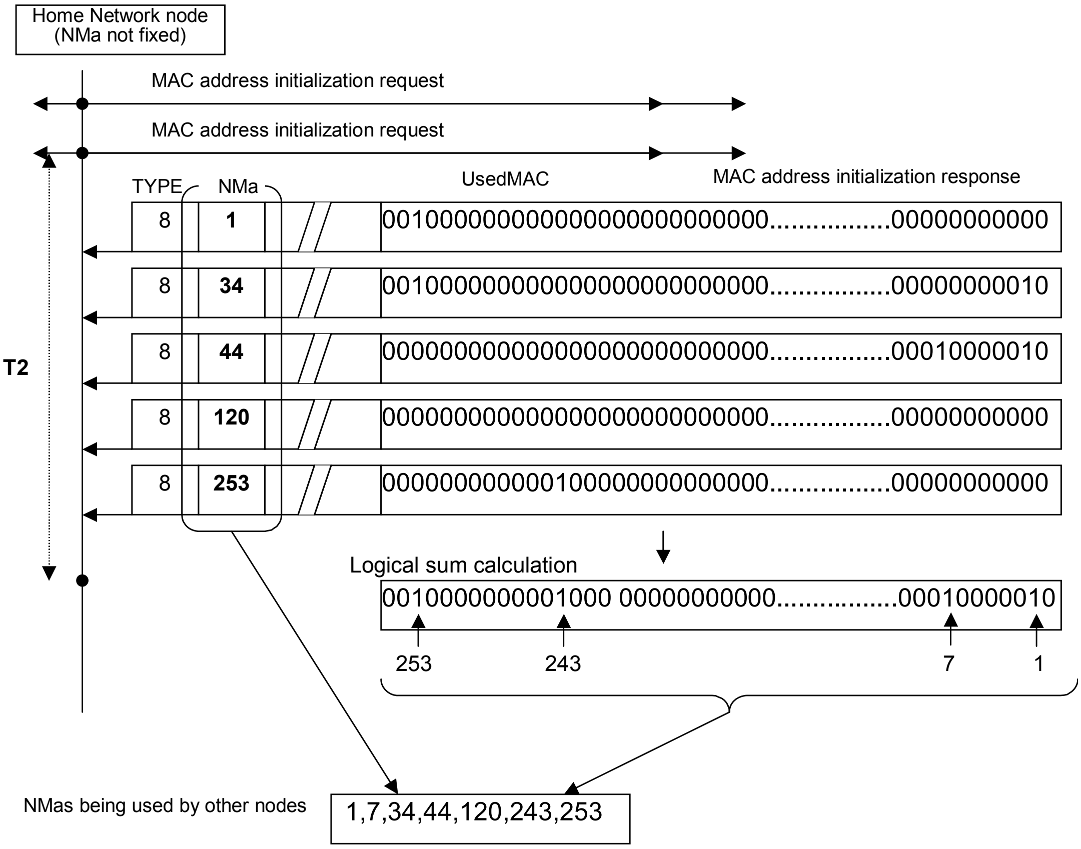


Figure 18 – Check for NMas in use by other nodes

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.

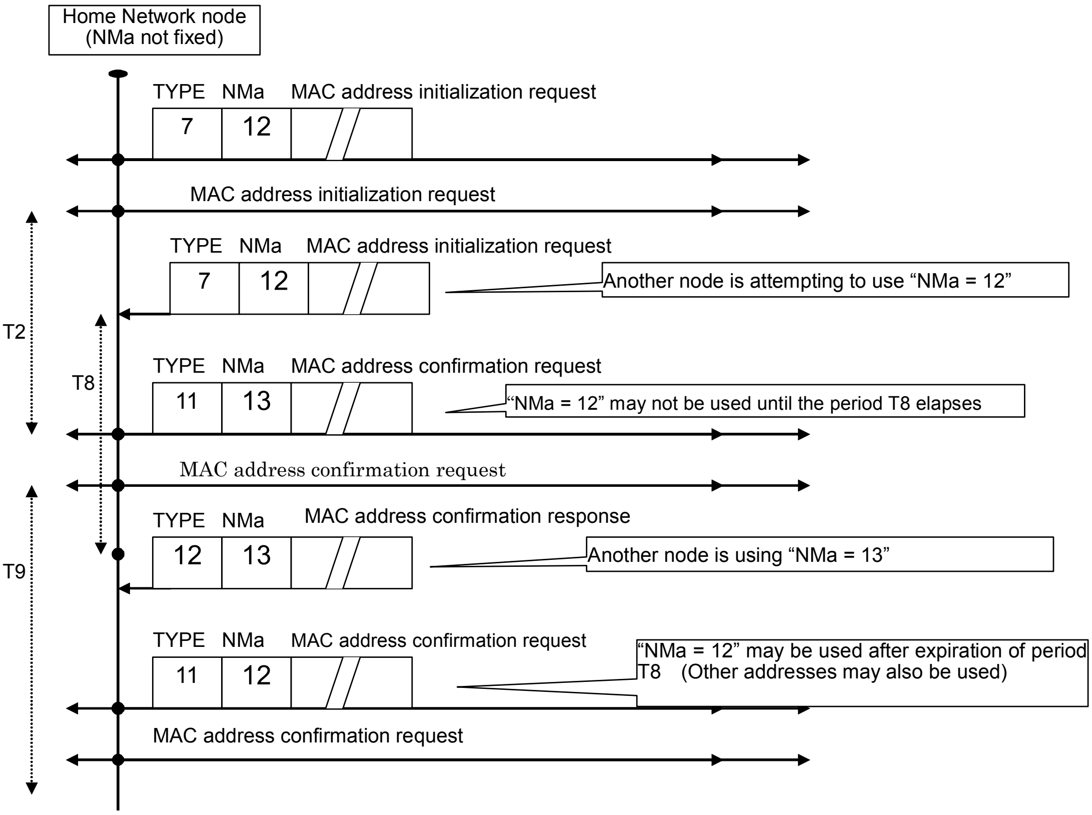

Home Network node
(NMa not fixed)
TYPE NMa MAC address initialization request
7 12
MAC address initialization request
TYPE NMa MAC address initialization request
7 12
Another node is attempting to use "NMa = 12"
T2
T8
TYPE NMa MAC address confirmation request
11 13
"NMa = 12" may not be used until the period T8 elapses
MAC address confirmation request
TYPE NMa MAC address confirmation response
12 13
Another node is using "NMa = 13"
T9
TYPE NMa MAC address confirmation request
11 12
"NMa = 12" may be used after expiration of period T8 (Other addresses may also be used)
MAC address confirmation request

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 Step8.

- 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.

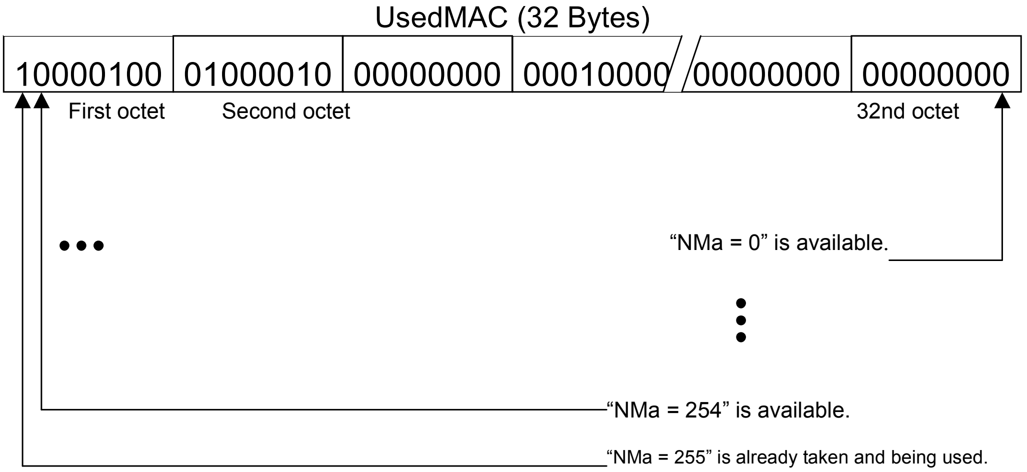
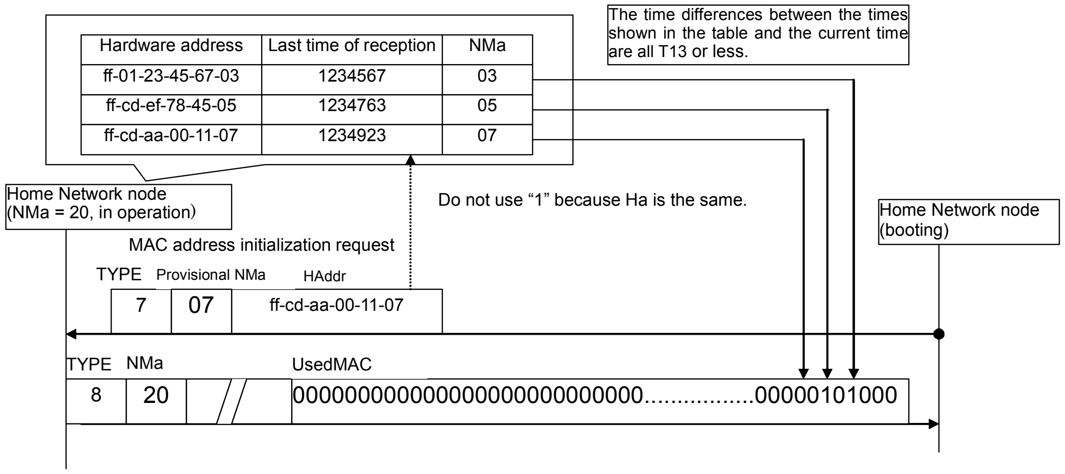


Figure 20 – Format for UsedMAC

In UsedMAC, "1" can be entered for bit n (which corresponds to the NMa n) if the bit satisfies the following condition:

- 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.


Hardware address	Last time of reception	NMa
ff-01-23-45-67-03	1234567	03
ff-cd-ef-78-45-05	1234763	05
ff-cd-aa-00-11-07	1234923	07

The time differences between the times shown in the table and the current time are all T13 or less.
Home Network node (NMa = 20, in operation)
Do not use "1" because Ha is the same.
Home Network node (booting)
MAC address initialization request
TYPE
Provisional NMa
HAddr
7
07
ff-cd-aa-00-11-07
TYPE
NMa
UsedMAC
8
20
000000000000000000000000000.................00000101000

Figure 21 – Example of UsedMAC

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.

4.8 Time period parameters

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

Table 26 – Time period parameters

Para-meter	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 value] x [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.

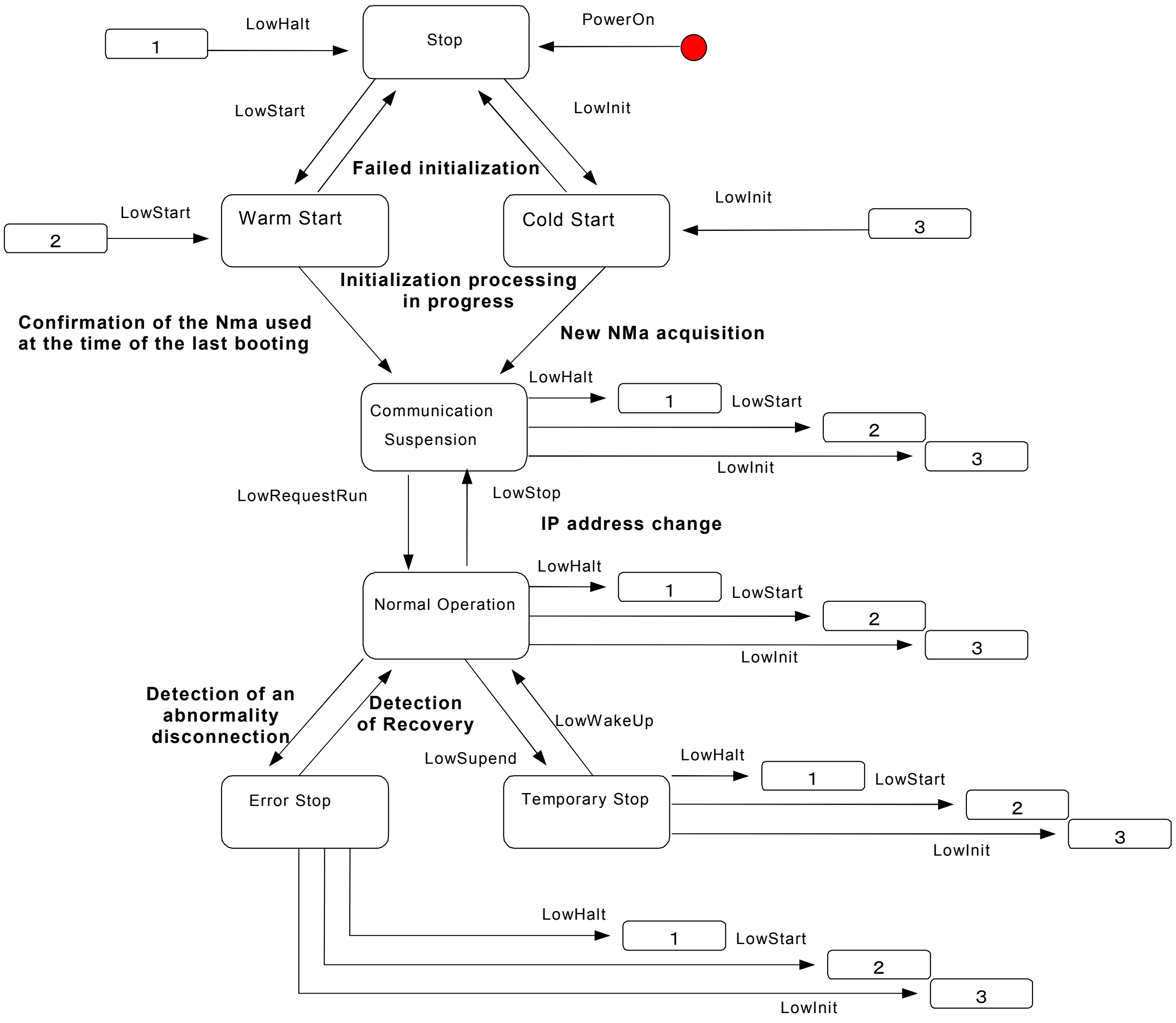


Figure 22 – Internal software status transitions

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 changinginto 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 .

   Booting 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, 0×70 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.

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

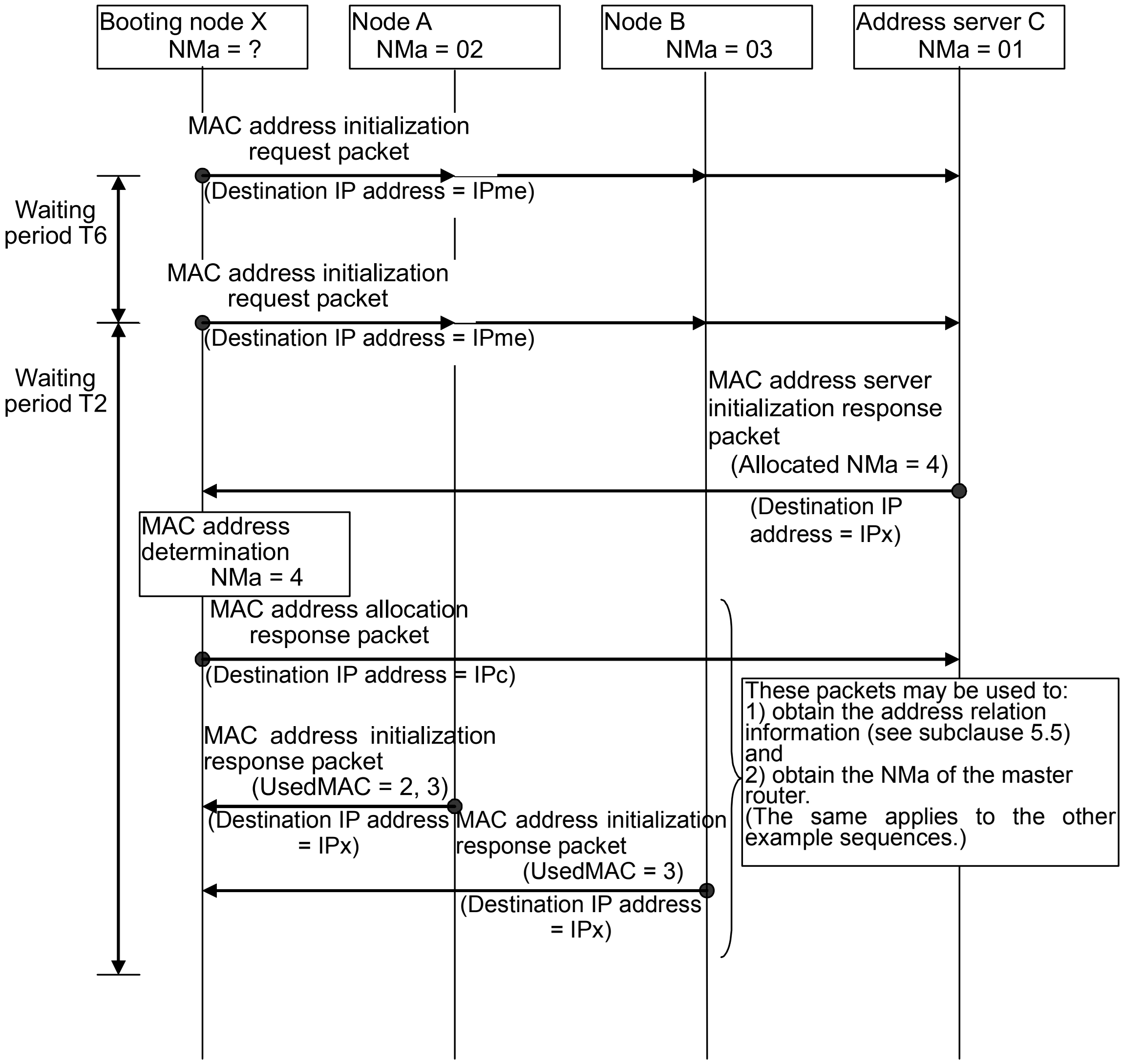

Booting node X
NMa = ?
Node A
NMa = 02
Node B
NMa = 03
Address server C
NMa = 01
MAC address initialization request packet
(Destination IP address = IPme)
Waiting period T6
MAC address initialization request packet
(Destination IP address = IPme)
Waiting period T2
MAC address server initialization response packet
(Allocated NMa = 4)
(Destination IP address = IPx)
MAC address determination
NMa = 4
MAC address allocation response packet
(Destination IP address = IPc)
MAC address initialization response packet
(UsedMAC = 2, 3)
(Destination IP address = IPx)
MAC address initialization response packet
(UsedMAC = 3)
(Destination IP address = IPx)
These packets may be used to:
1) obtain the address relation information (see subclause 5.5) and
2) obtain the NMa of the master router.
(The same applies to the other example sequences.)

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)

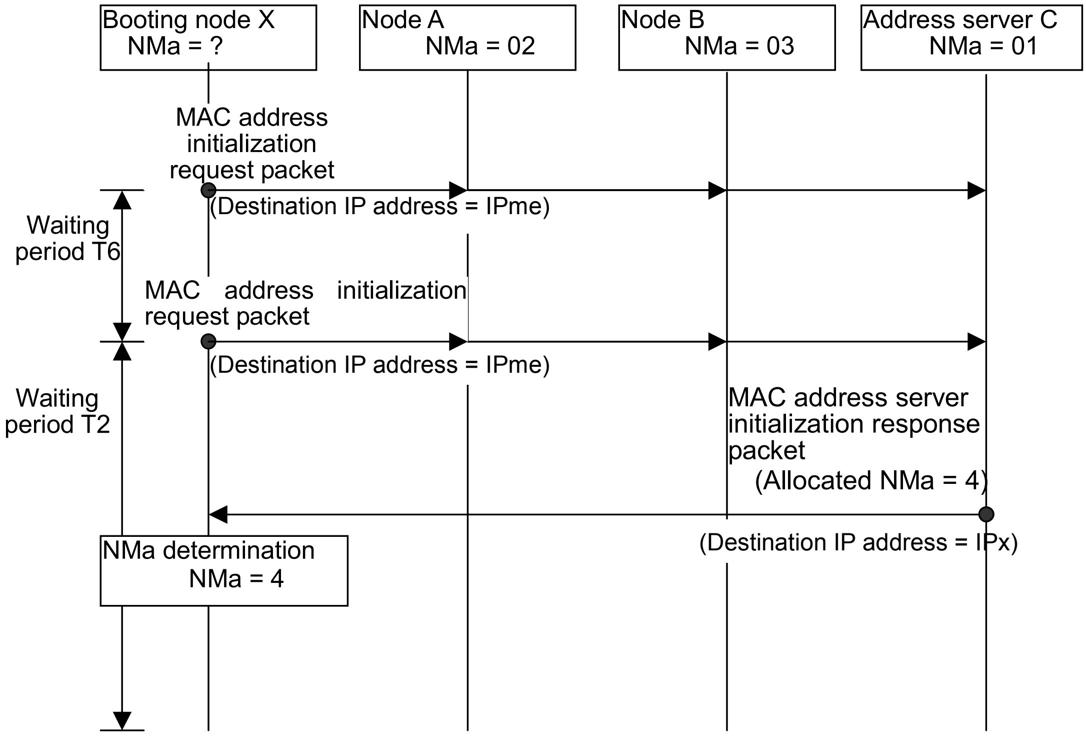

Booting node X
NMa = ?
Node A
NMa = 02
Node B
NMa = 03
Address server C
NMa = 01
MAC address initialization request packet
(Destination IP address = IPme)
Waiting period T6
MAC address initialization request packet
(Destination IP address = IPme)
Waiting period T2
MAC address server initialization response packet
(Allocated NMa = 4)
(Destination IP address = IPx)
NMa determination
NMa = 4

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)

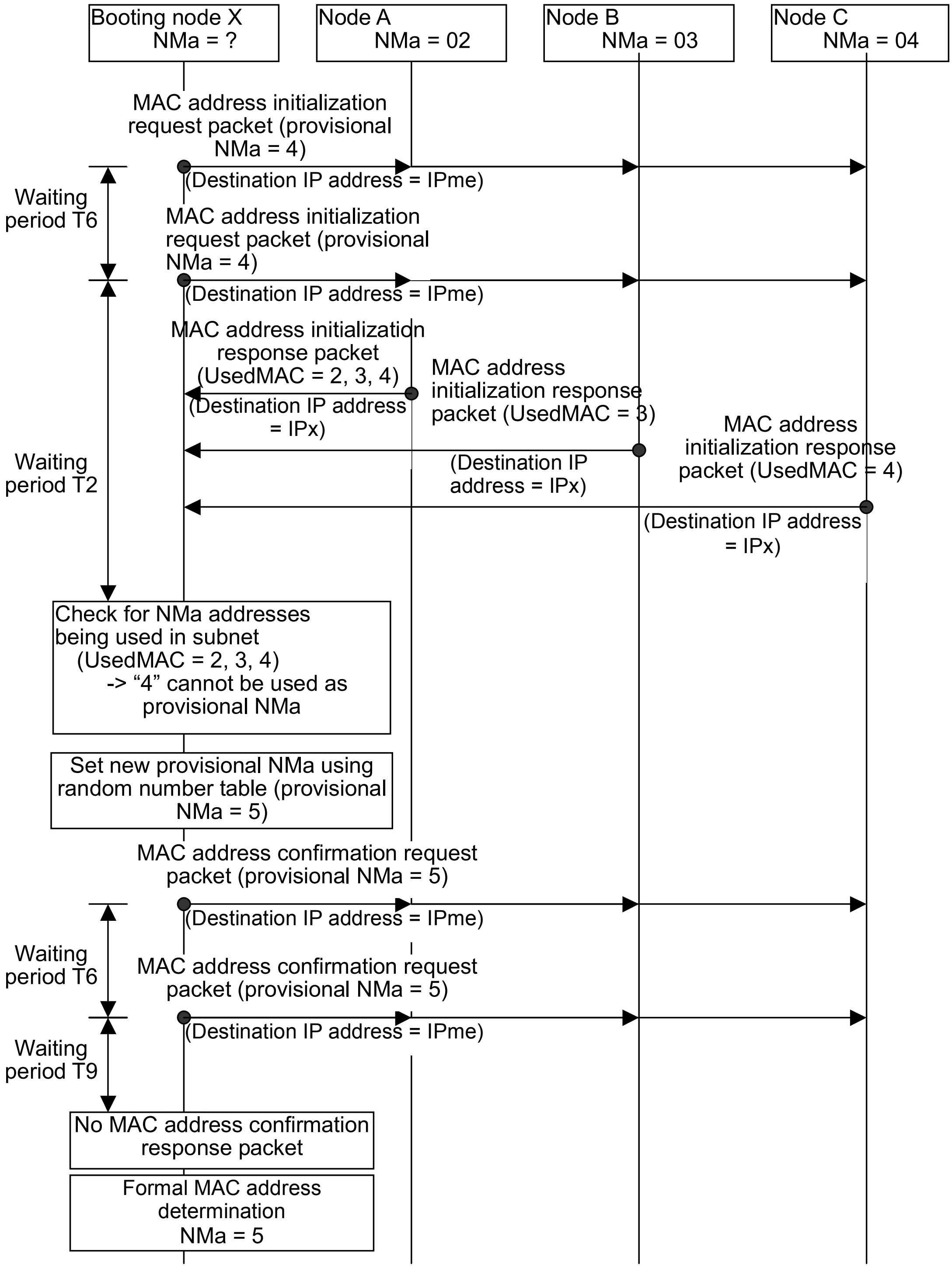

Booting node X
NMa = ?
Node A
NMa = 02
Node B
NMa = 03
Node C
NMa = 04
MAC address initialization request packet (provisional NMa = 4)
(Destination IP address = IPme)
Waiting period T6
MAC address initialization request packet (provisional NMa = 4)
(Destination IP address = IPme)
MAC address initialization response packet (UsedMAC = 2, 3, 4)
(Destination IP address = IPx)
MAC address initialization response packet (UsedMAC = 3)
(Destination IP address = IPx)
MAC address initialization response packet (UsedMAC = 4)
(Destination IP address = IPx)
Waiting period T2
Check for NMa addresses being used in subnet (UsedMAC = 2, 3, 4) -> “4” cannot be used as provisional NMa
Set new provisional NMa using random number table (provisional NMa = 5)
MAC address confirmation request packet (provisional NMa = 5)
(Destination IP address = IPme)
Waiting period T6
MAC address confirmation request packet (provisional NMa = 5)
(Destination IP address = IPme)
Waiting period T9
No MAC address confirmation response packet
Formal MAC address determination NMa = 5

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)

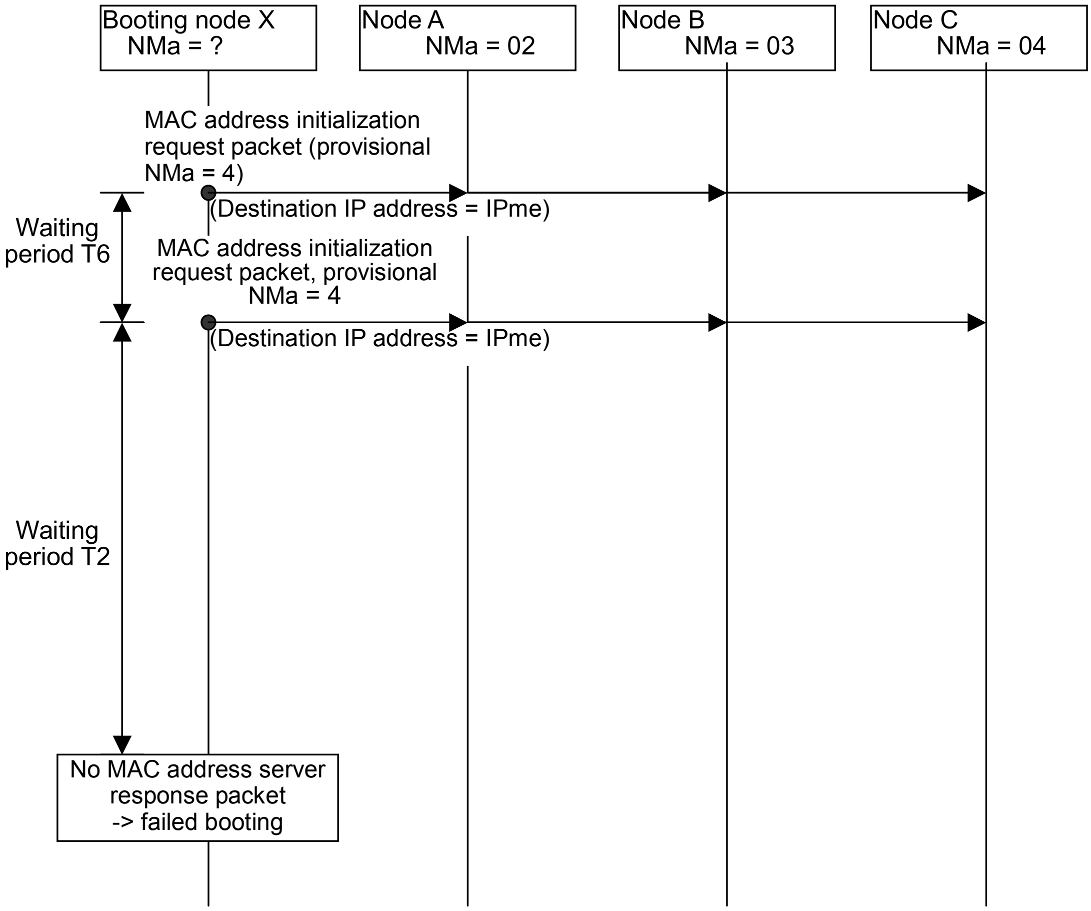

Booting node X
NMa = ?
Node A
NMa = 02
Node B
NMa = 03
Node C
NMa = 04
MAC address initialization request packet (provisional NMa = 4)
(Destination IP address = IPme)
Waiting period T6
MAC address initialization request packet, provisional NMa = 4
(Destination IP address = IPme)
Waiting period T2
No MAC address server response packet -> failed booting

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

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

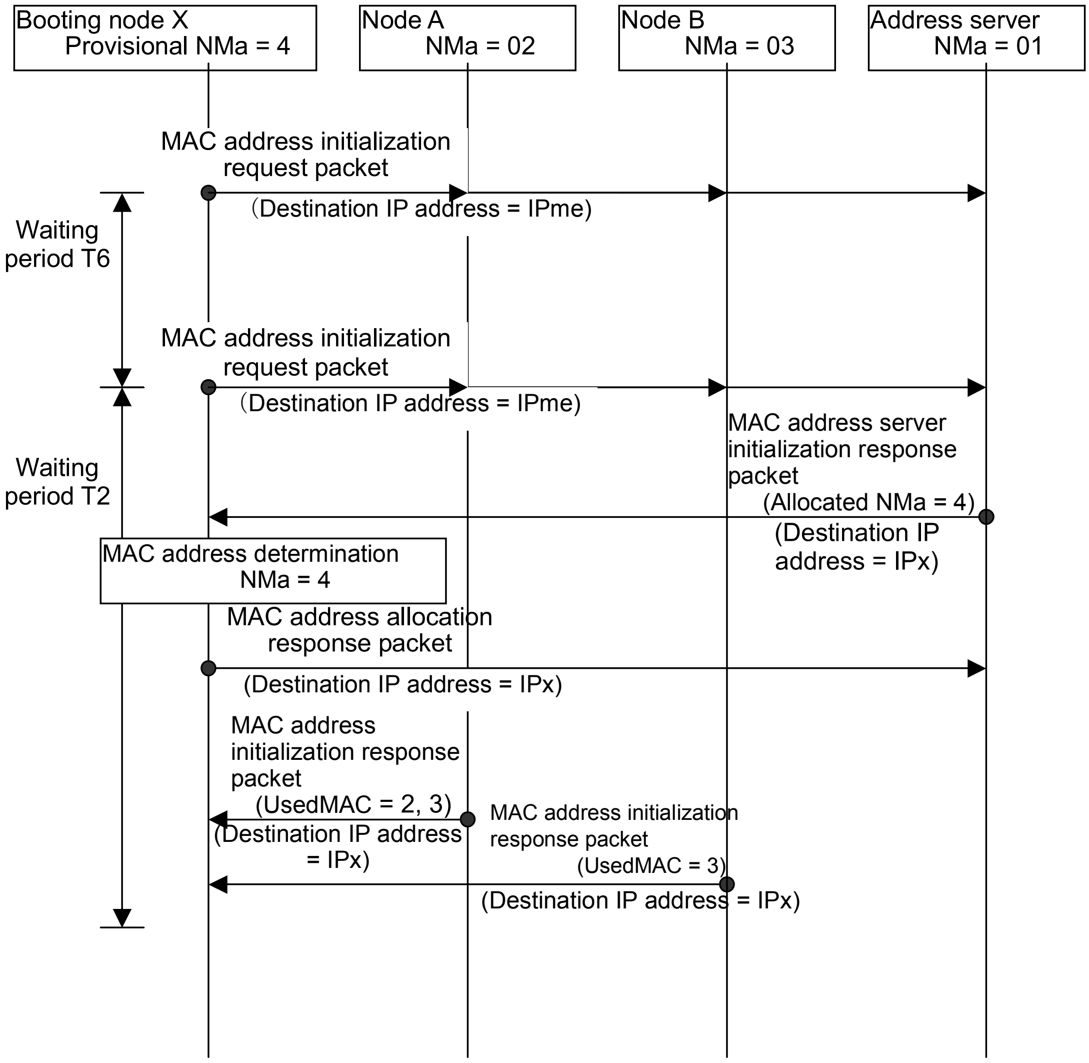

Booting node X
Provisional NMa = 4
Node A
NMa = 02
Node B
NMa = 03
Address server
NMa = 01
MAC address initialization request packet
(Destination IP address = IPme)
Waiting period T6
MAC address initialization request packet
(Destination IP address = IPme)
MAC address server initialization response packet
(Allocated NMa = 4)
(Destination IP address = IPx)
Waiting period T2
MAC address determination
NMa = 4
MAC address allocation response packet
(Destination IP address = IPx)
MAC address initialization response packet
(UsedMAC = 2, 3)
(Destination IP address = IPx)
MAC address initialization response packet
(UsedMAC = 3)
(Destination IP address = IPx)

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

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

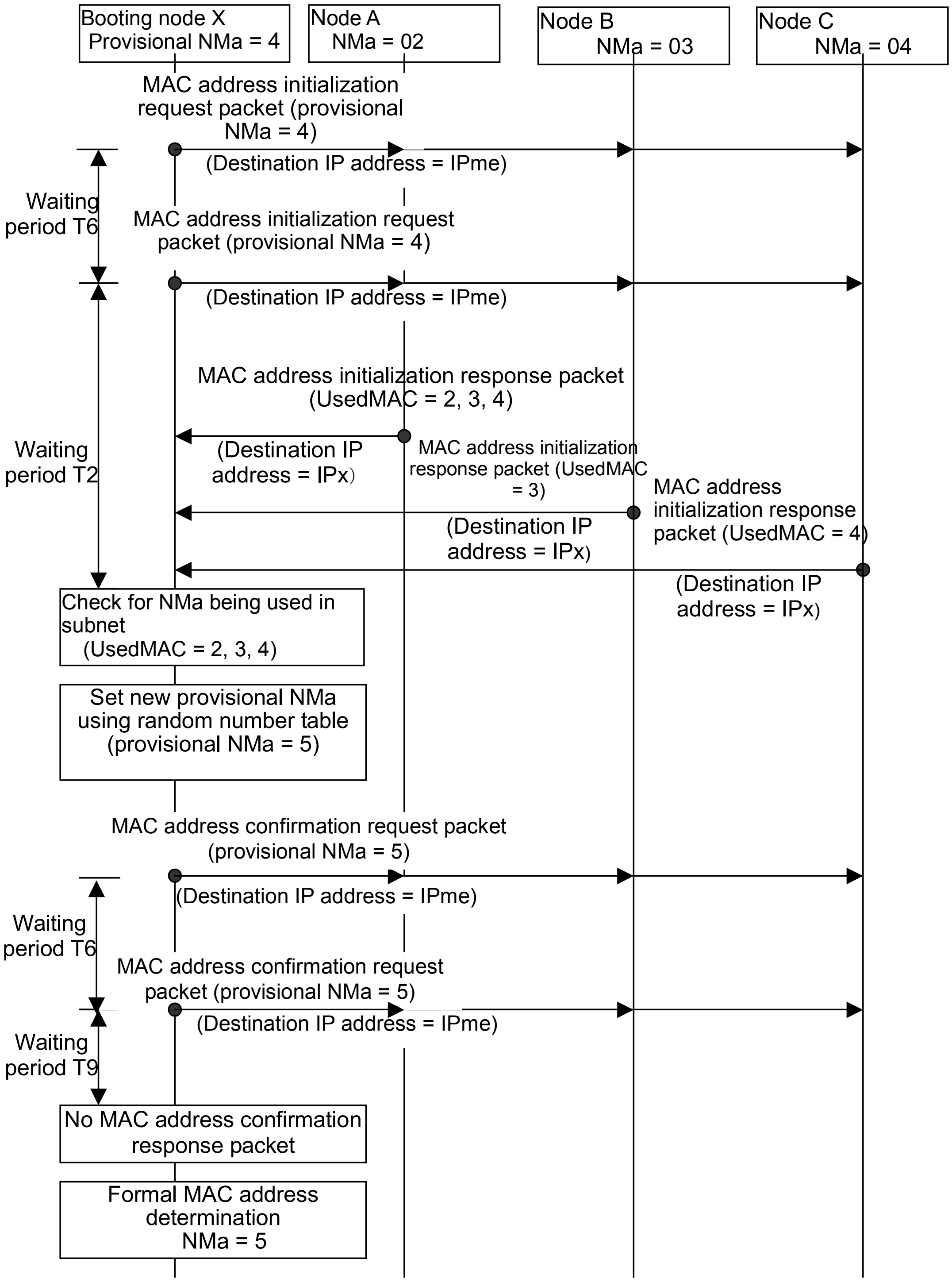

Booting node X
Provisional NMa = 4
Node A
NMa = 02
Node B
NMa = 03
Node C
NMa = 04
MAC address initialization request packet (provisional NMa = 4)
(Destination IP address = IPme)
Waiting period T6
MAC address initialization request packet (provisional NMa = 4)
(Destination IP address = IPme)
Waiting period T2
MAC address initialization response packet (UsedMAC = 2, 3, 4)
(Destination IP address = IPx)
MAC address initialization response packet (UsedMAC = 3)
(Destination IP address = IPx)
MAC address initialization response packet (UsedMAC = 4)
(Destination IP address = IPx)
Check for NMa being used in subnet (UsedMAC = 2, 3, 4)
Set new provisional NMa using random number table (provisional NMa = 5)
MAC address confirmation request packet (provisional NMa = 5)
(Destination IP address = IPme)
Waiting period T6
MAC address confirmation request packet (provisional NMa = 5)
(Destination IP address = IPme)
Waiting period T9
No MAC address confirmation response packet
Formal MAC address determination NMa = 5

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

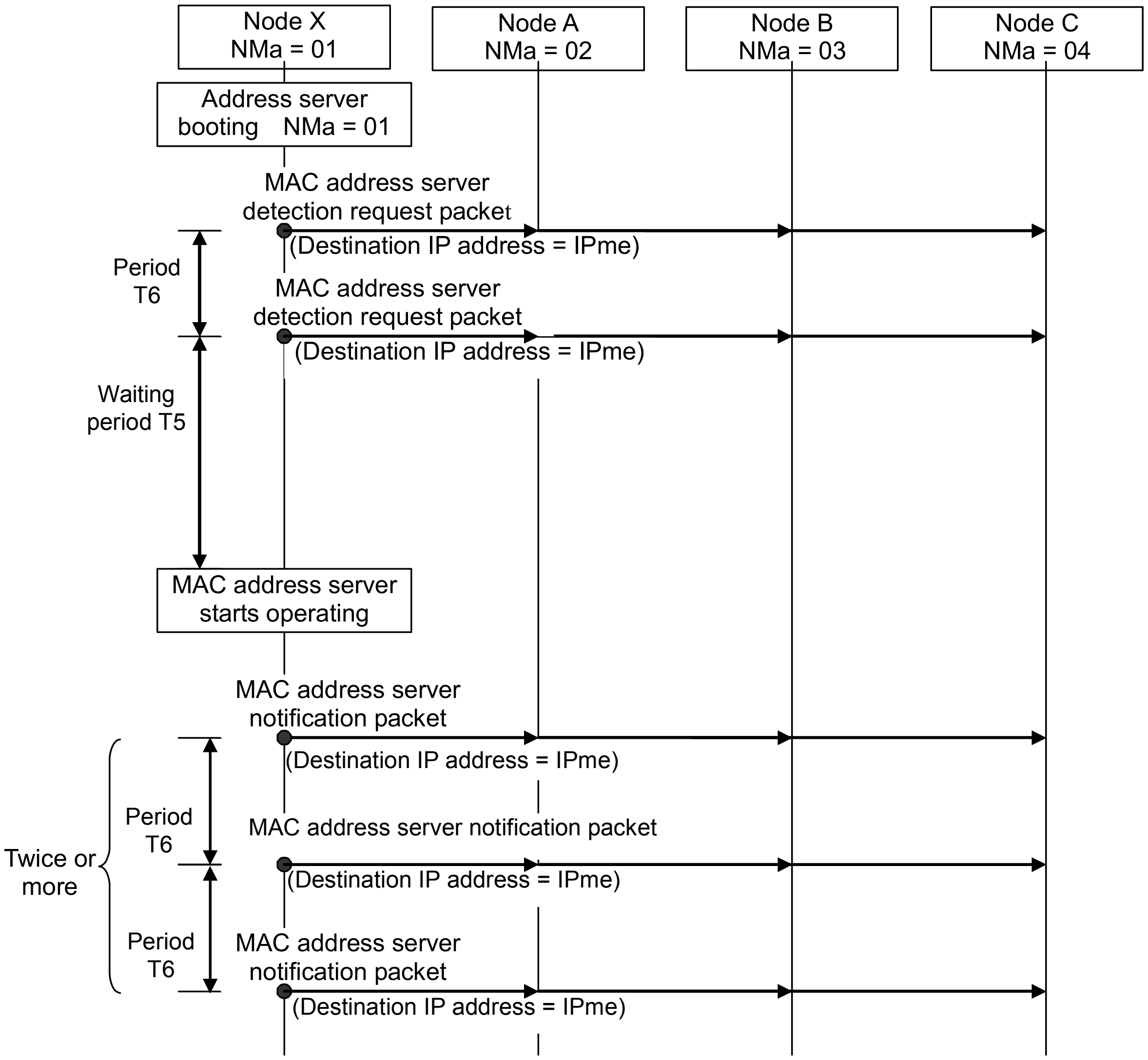


Figure B.1 – Booting of a single MAC address server

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

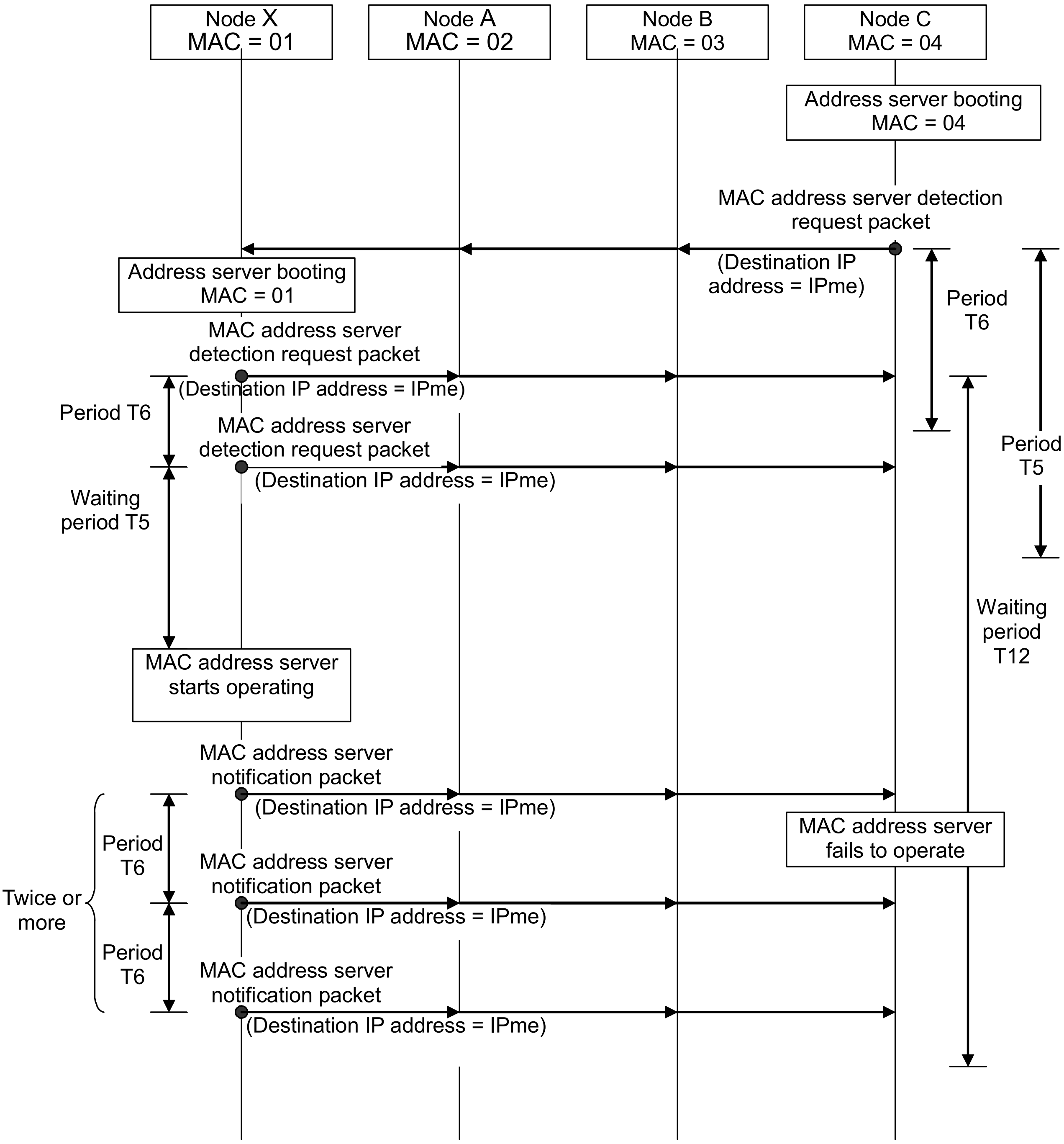

Node X
MAC = 01
Node A
MAC = 02
Node B
MAC = 03
Node C
MAC = 04
Address server booting
MAC = 04
MAC address server detection request packet
(Destination IP address = IPme)
Period T6
Period T5
Address server booting
MAC = 01
MAC address server detection request packet
(Destination IP address = IPme)
Period T6
MAC address server detection request packet
(Destination IP address = IPme)
Waiting period T5
Waiting period T12
MAC address server starts operating
MAC address server notification packet
(Destination IP address = IPme)
MAC address server fails to operate
Period T6
Twice or more
MAC address server notification packet
(Destination IP address = IPme)
Period T6
MAC address server notification packet
(Destination IP address = IPme)

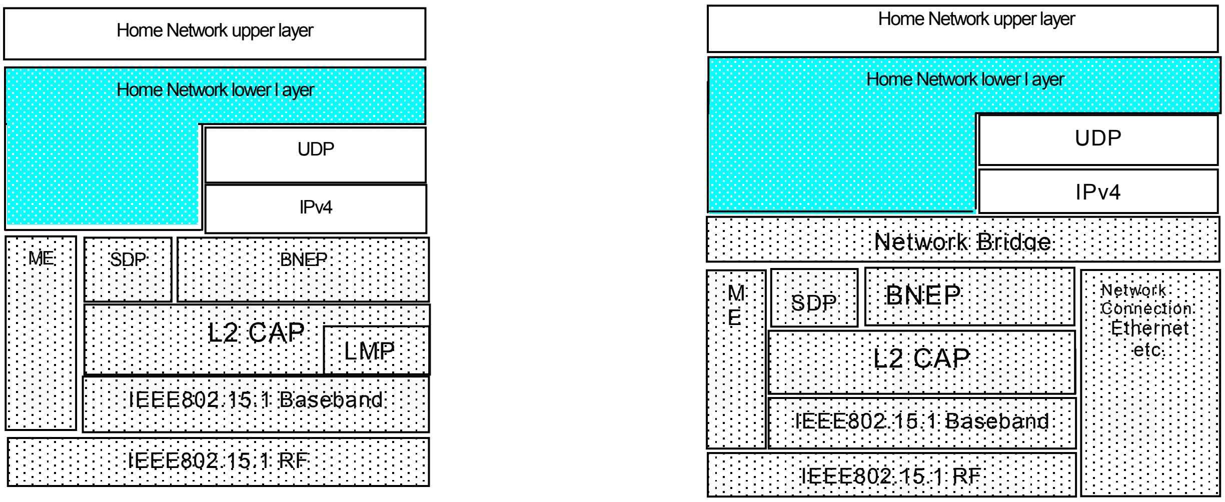
Figure B.2 – Near-simultaneous booting of two or more MAC address servers

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.



Without bridge (PANU, GN) With bridge (NAP)

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:

a) 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.

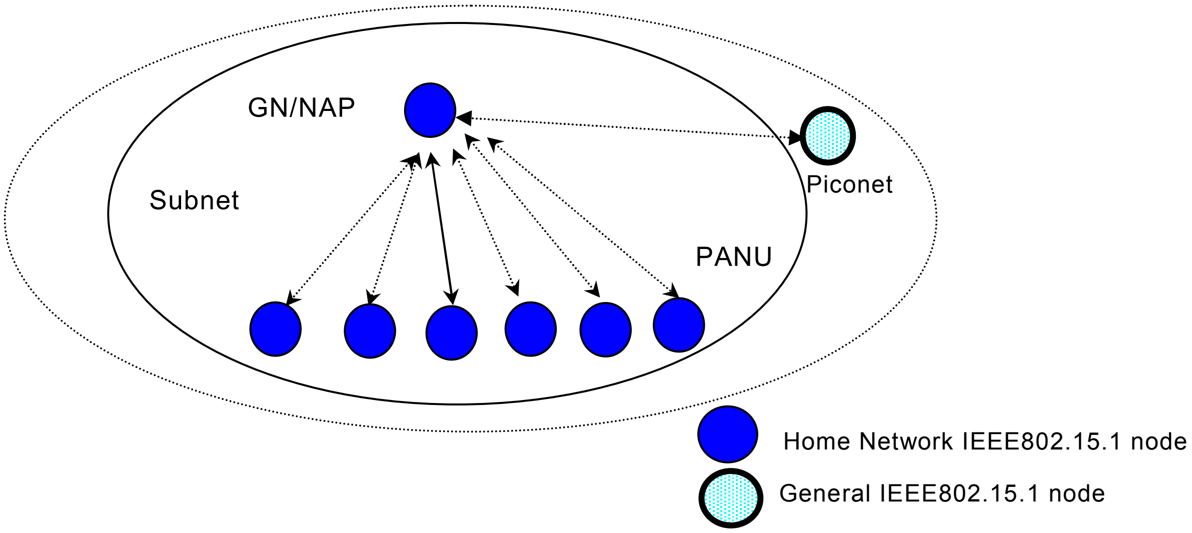


Figure C.2 – Basic form of subnet

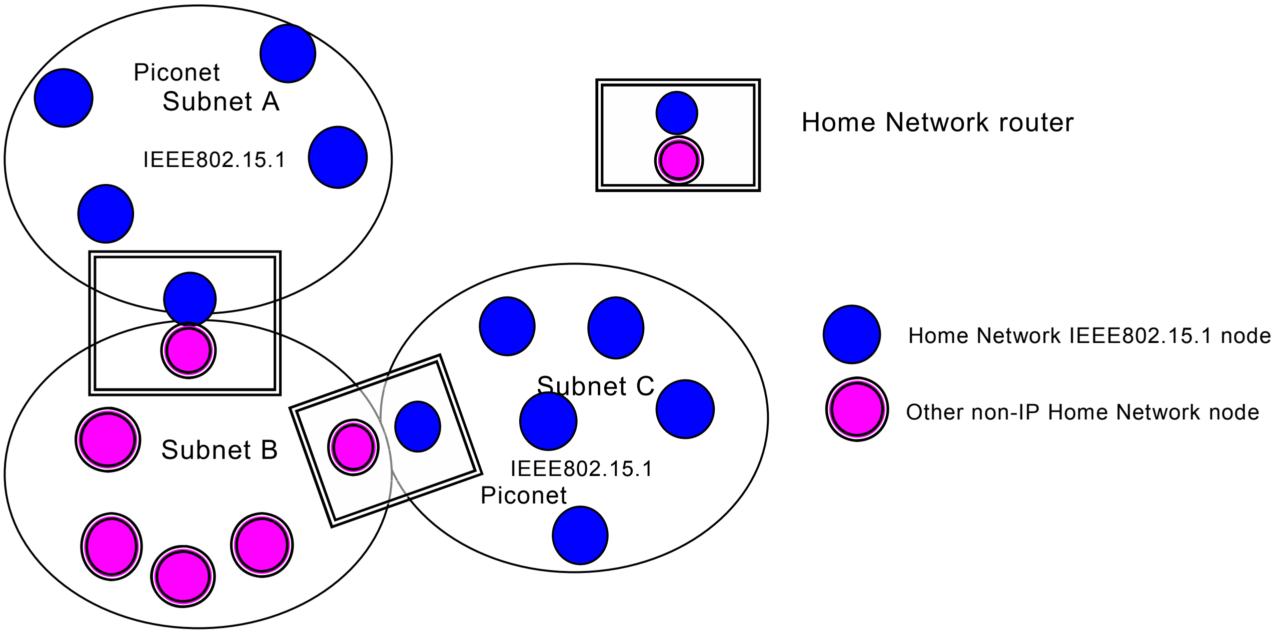


Figure C.3 – Example of a subnet connection using Home Network routers

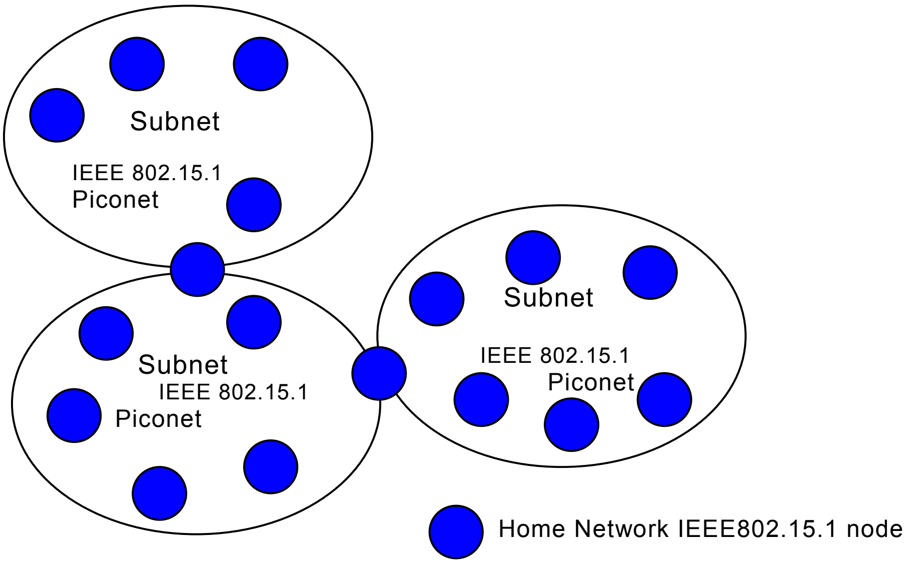


Figure C.4 – Example of an unacceptable subnet connection (scatternet)

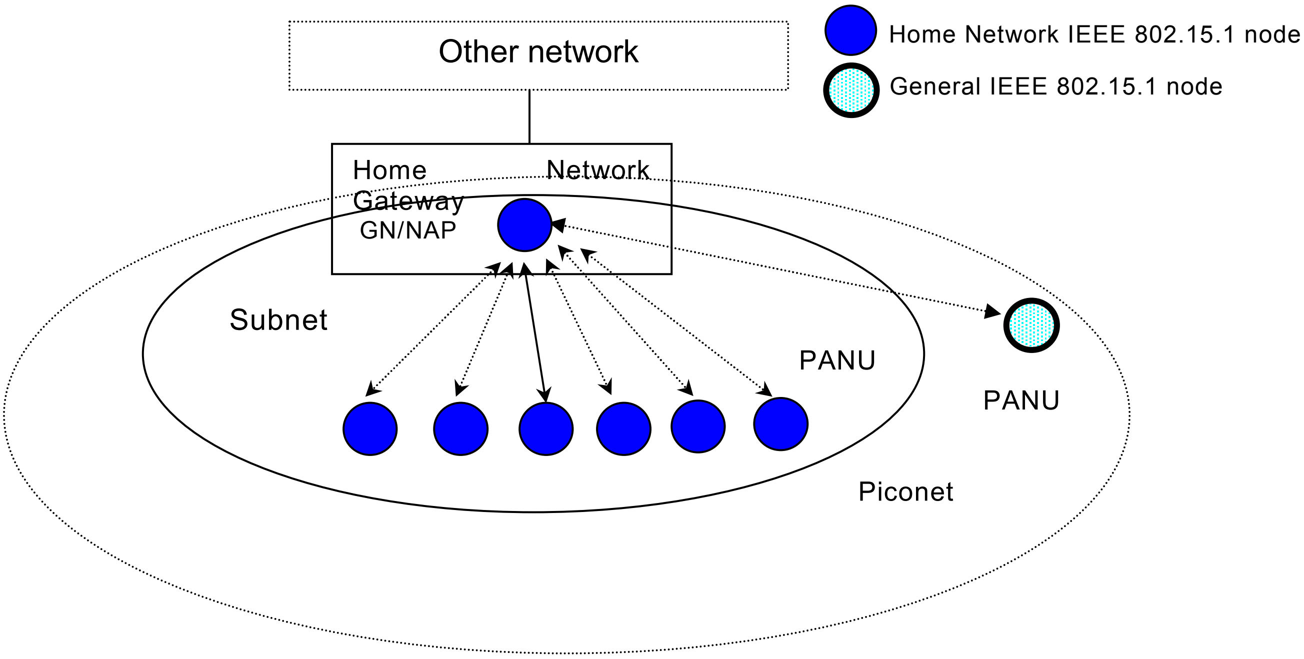


Figure C.5 – Example of a connection using a home network gateway

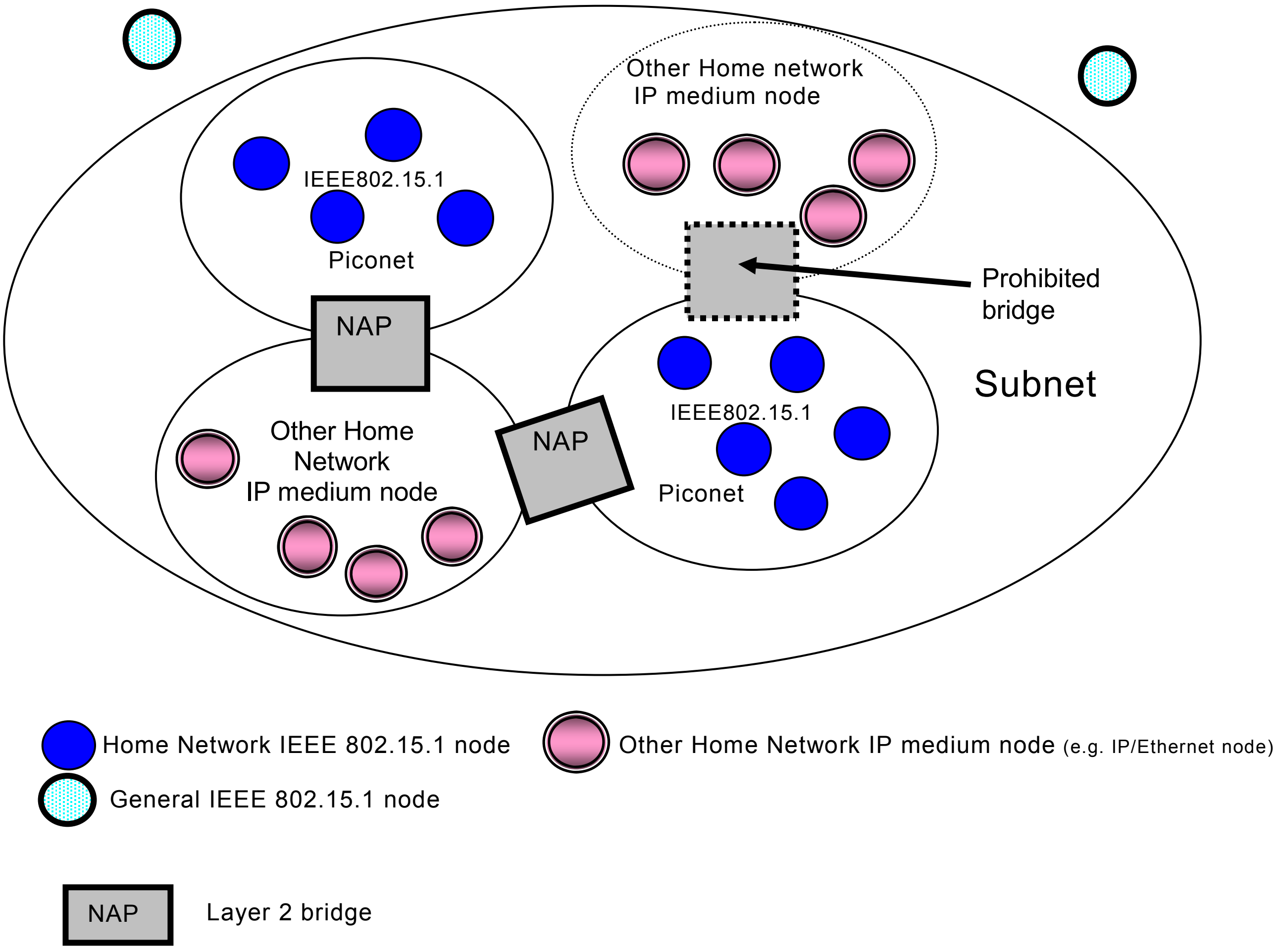


Figure C.6 – Example of a subnet using Layer 2 bridges

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.

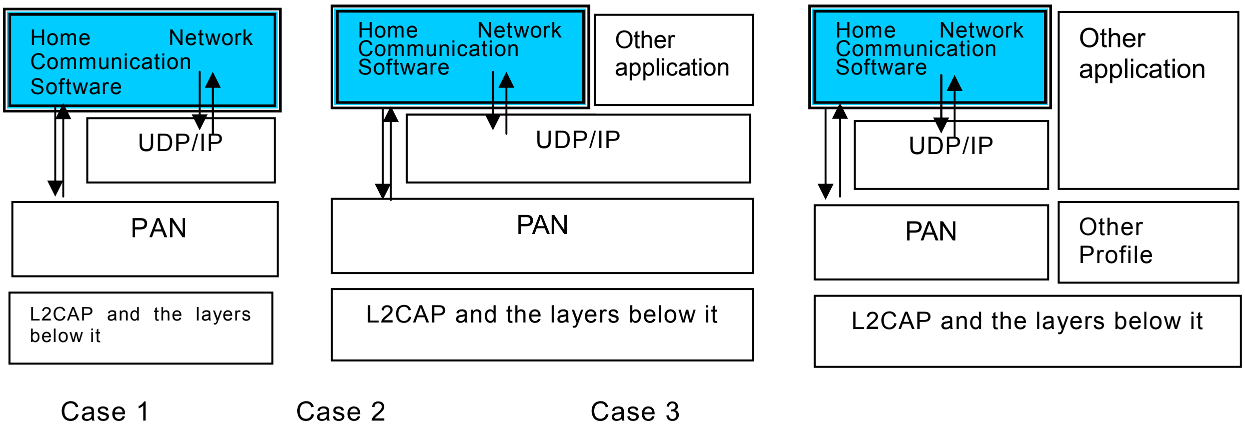

Home Network Communication Software
UDP/IP
PAN
L2CAP and the layers below it
Home Network Communication Software
Other application
UDP/IP
PAN
L2CAP and the layers below it
Home Network Communication Software
Other application
UDP/IP
PAN
Other Profile
L2CAP and the layers below it
Case 1
Case 2
Case 3

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.

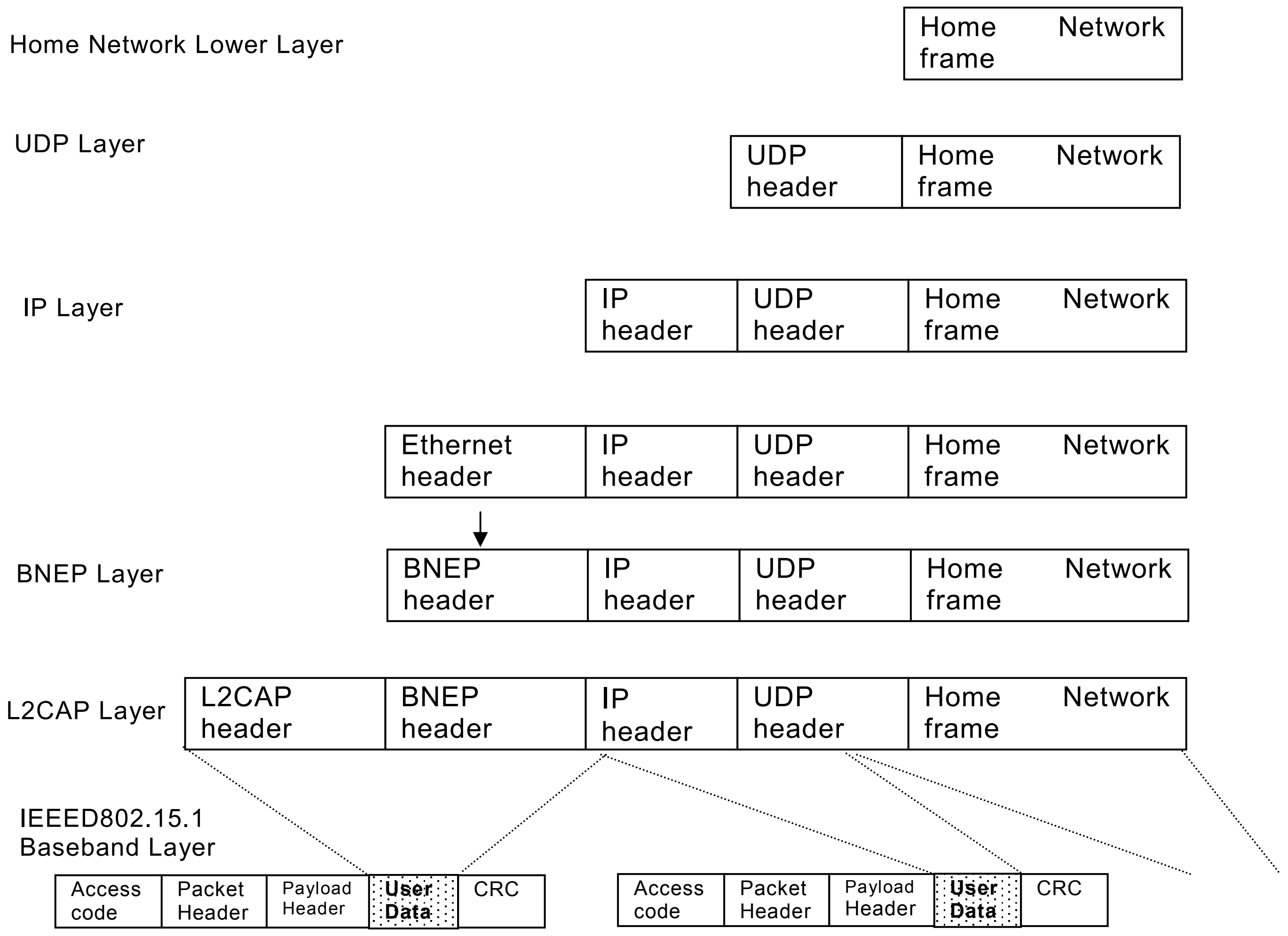


Figure C.8 – Packet structure

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

____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
P.O. Box 131
CH-1211 Geneva 20
Switzerland

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