INTERNATIONAL STANDARD

ISO/IEC 17811-3

First edition
2014-10-01

Information Technology — Device control and management —

Part 3: Specification of Reliable Message Delivery Protocol

Technologies de l'information — Commande et gestion de périphériques —

Partie 3: Spécification du protocole de livraison fiable de messages

Reference number
ISO/IEC 17811-3:2014(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 17811-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommitte SC 6, *Telecommunications and information exchange between systems*.

ISO/IEC 17811 consists of the following parts, under the general title *Information technology — Device control and management*:

— *Part 1: Architecture*

— *Part 2: Specification of Device Control and Management Protocol (DCMP)*

— *Part 3: Specification of Reliable Message Delivery Protocol (RMDP)*

Introduction

As the IT industry continues to grow, a large number of smart devices have been deployed in the market. Major consumer electronics companies have already provided a variety of smart devices and appliances; thus, it is expected that the number of smart devices will exceed more than 50% of PCs in the near future. With the growth of smart devices, there is a crucial need for “smart” applications in the market. A smart application represents an application/service that is used to control and manage a lot of smart devices with its own purpose over the network, as shown in the examples of smart home appliances, e-health, smart car, and smart works.

To provide smart applications or services, the essentially required functionality is to control and manage many devices through the network. However, it is not easy to design the device control and management functions, since the specific requirements for those functions can be very different and affected by various device features, such as device types, capabilities, or manufacturers. In addition, the diverse network environments are also considered in the design of the device control and management function.

This International Standard is purposed to make the architecture and protocols for Device Control and Management (DCM). The DCM standard is designed to effectively control and manage various smart devices, regardless of the device features and underlying network environments. It is expected that the DCM is applicable to a wide range of smart applications.

DCM can support the various control and management services, regardless of the network protocols or interfaces. DCM is composed of two protocols: DCMP (Device Control and Management Protocol) and RMDP (Reliable Message Delivery Protocol).

This International Standard consists of the following parts:

— ISO/IEC 17811-1;

— ISO/IEC 17811-2;

— ISO/IEC 17811-3.

ISO/IEC 17811-1 describes the architecture of DCM which includes definition, general concept, requirements, design principles, and service scenarios for device management control and management.

ISO/IEC 17811-2 specifies the Device Control and Management Protocol (DCMP) which includes the functional entities, protocol operations, message structure, and detailed parameter format associated with DCMP.

This part of ISO/IEC 17811 specifies the Reliable Message Delivery Protocol (RMDP) which includes the interworking with DCMP, protocol operations, and message structure associated with RMDP.

Information Technology — Device control and management —

Part 3: Specification of Reliable Message Delivery Protocol

1 Scope

This part of ISO/IEC 17811 provides the specification of Reliable Message Delivery Protocol (RMDP), which is an application-layer protocol used to provide uniform and reliable message delivery among devices regardless of the underlying network protocols or interfaces.

The network security is out of scope in this part of ISO/IEC 17811. However, the security services might be necessary according to applications of RMDP. RMDP might suffer from many network-specific threats. To countermeasure those threats, some security mechanism can be deployed.

2 Terms and definitions

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

2.1
device control and management
DCM
operations are purposed to control and manage the various smart devices. For this purpose, DCM is composed of the two protocols: DCMP (Device Control and Management Protocol) and RMDP (Reliable Message Delivery Protocol)

[SOURCE: ISO/IEC 17811-1:2014, 3.1]

2.2
device control and management protocol
DCMP
used to perform various management operations which are categorized into information retrieval, control, diagnostic and debugging

[SOURCE: ISO/IEC 17811-1:2014, 3.2]

2.3
reliable message delivery protocol
RMDP
used to provide uniform and reliable message delivery among devices regardless of the underlying network protocols or interfaces

[SOURCE: ISO/IEC 17811-1:2014, 3.3]

3 Symbols and abbreviated terms

The following acronyms are used in this part of ISO/IEC 17811.

DCMP Device Control and Management Protocol

DCM Device Management Architecture and Protocol

RMDP Reliable Message Delivery Protocol

NTP Network Time Protocol

UUID Universally Unique Identifier

UPnP Universal Plug and Play

4 Overview

RMDP is a protocol for the message exchange among the devices. Since each device is connected to a different network, the data transport and network protocols are also different. In addition, some devices are connected directly with different interfaces. Therefore, the RMDP provides a uniform and reliable message exchange protocol among devices regardless of the network protocols or interfaces. Each node has an address translation table, which maintains the mapping information between DCM device identifier (object ID) and physical network identifier such as IP address in IP network. Also, it supports different types of connectivity interfaces such as HDMI and USB. An example of an address translation table is shown in Figure 1.

Object ID	Node ID	MP Type	MC Type	MAddress	MPort	SP Type	SAddress	SPort
0005	000H	UDP	Uni	214.31.5.2	Fixed	UDP	214.31.5.2	Fixed
0002	000B	UDP	Broad	Fixed	Fixed	UDP	192.168.0.8	Fixed
0003	000C	UDP	Uni	19.25.8.5	Fixed	UDP	19.25.8.15	Fixed
0004	000D	TCP	Uni	29. 25.8.5	Fixed	TCP	29. 25.8.15	Fixed

Figure 1 — Example address translation table of the RMDP

MPType is a protocol type for the multi-target message reception (i.e. UDP or TCP), MCType is a casting type for multi-target message reception (i.e. unicast, broadcast, or multicast), MAddress is a network address for multi-target message reception, MPort is a network port for multi-target message reception, SPType is a protocol type for single-target message reception (i.e. UDP or TCP), SAddress is a network address for single-target message reception, and SPort is a network port for single-target message reception.

When a node is initialized first, that node sends a NODE_ADVERTISEMENT message using the broadcast address. Node Information, such as IP address, port number, and so on is included in the NODE_ADVERTISEMENT message. After sending the NODE_ADVERTISEMENT message, that node can send a NODE_DISCOVERY_REQUEST message using the broadcast address and the corresponding nodes shall return the NODE_DISCOVERY_RESPONSE message. After sending the NODE_DISCOVERY_RESPONSE message, the corresponding nodes will exchange an OBJECT_ADVERTISEMENT message which includes the information of device identifier. After these processes, each node can send the DCMP message to the other nodes.

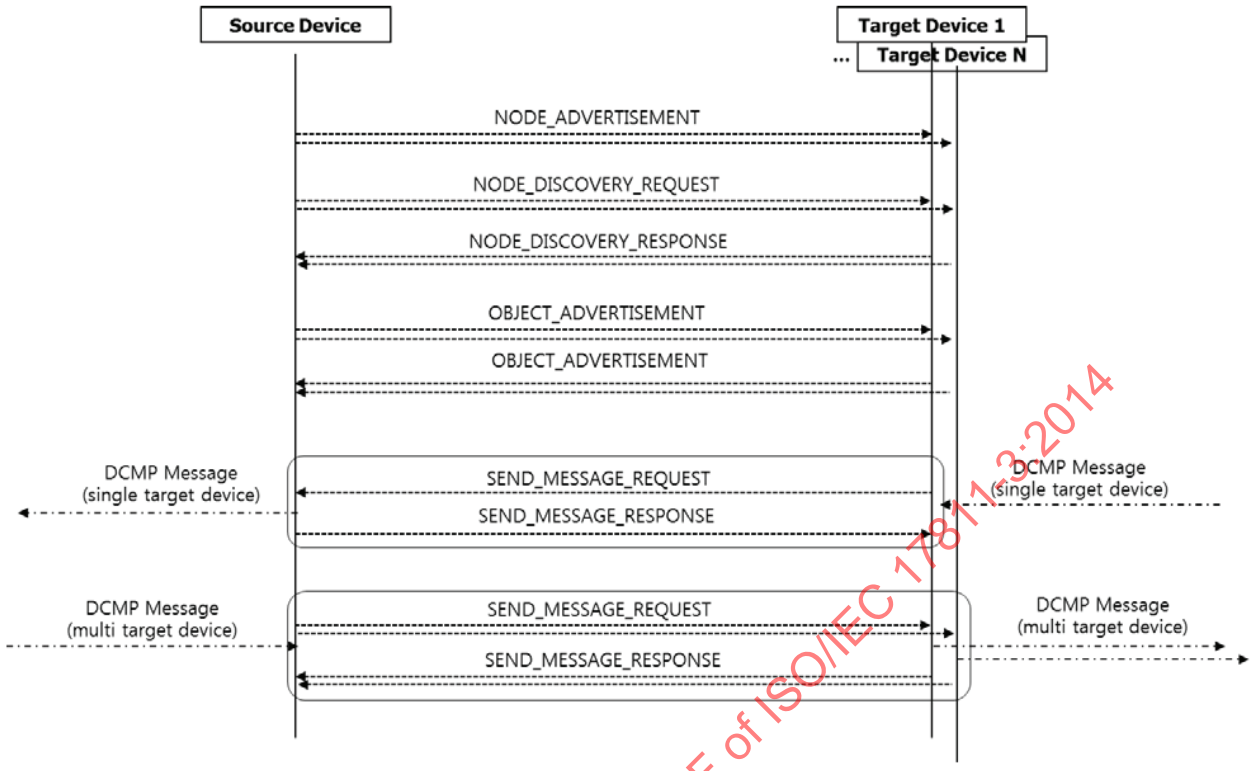

Figure 2 — An Example of Reliable Message Delivery Protocol Operation

5 Protocol Operation

5.1 Node Advertisement

When a network is enabled or re-configured, a node advertisement operation can be used to inform node's plug-in or plug-out, as shown in Figure 3. The associated node advertisement transaction is one-way transaction. This means that only one message is required to finish a transaction, and any response message is not required.

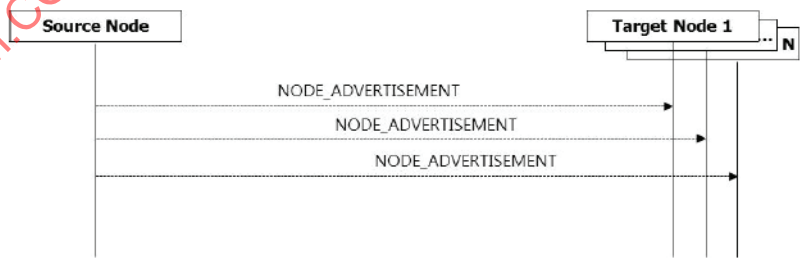

Figure 3 — Node Advertisement Operation

5.2 Node Discovery

For node discovery, NODE_DISCOVERY_REQUEST and NODE_DISCOVERY_RESPONSE messages are exchanged between the nodes, as shown in Figure 4. A source node sends a NODE_DISCOVERY_REQUEST message to target nodes by broadcast. In response to the NODE_DISCOVERY_REQUEST message, all nodes which fit into the requested information shall respond with a NODE_DISCOVERY_RESPONSE message.

The node discovery operation is performed with a two-message transaction. This operation requires a request message at source and a response message at the destination. When a response message is not received within a specific time interval, the source may cancel the transaction or re-issue the transaction.

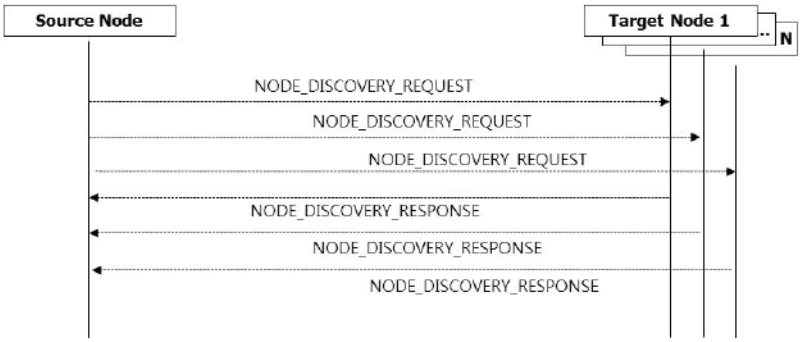

Figure 4 — Node Discovery Operation

5.3 Send Message

The send message operation is used to send some DCMP message to the other node. The send message operation is performed with a two-message transaction. This operation requires a request message at source and a response message at the destination. When a response message is not received within a specific time interval, the source may cancel the transaction or re-issue the transaction.

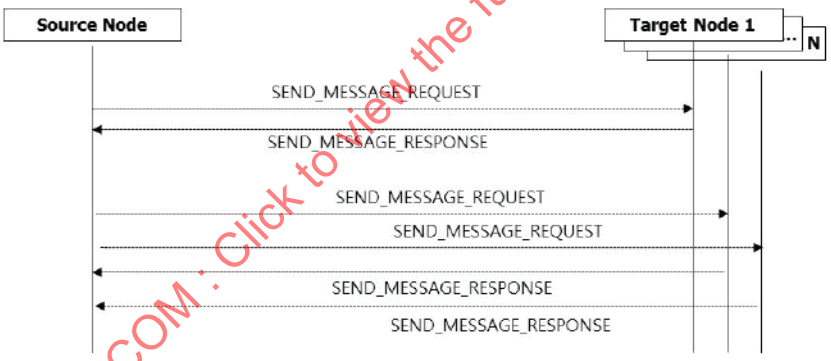

Figure 5 — Send Message Operation

5.4 Send Event

A SEND_EVENT message is used to send some DCMP Message to the other node without any response, as shown in Figure 6. The send event transaction is one-way transaction. This means that only one message is required to finish a transaction and any response message is not required.

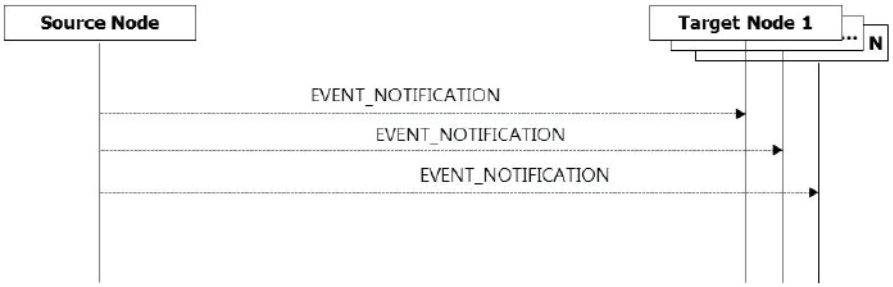

Figure 6 — Send Event Operation

5.5 Object Advertisement

Each node has an address translation table, which maintains the mapping information between device identifier and physical network identifier such as IP address in IP network. If a device is registered in the node, that node shall advertise that fact. The associated object advertisement transaction is one-way transaction. This means that only one message is required to finish a transaction, and any response message is not required.

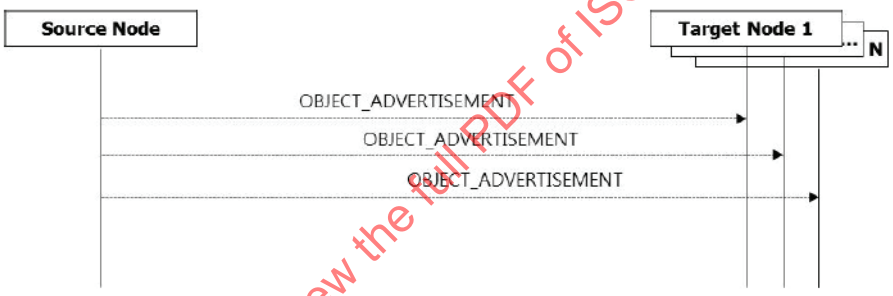

Figure 7 — Object Advertisement Operation

6 Messages

6.1 RMDP Message Structure

RMDP message can provide uniform and reliable message exchange protocol among devices regardless of the network protocols or interfaces. RMDP message is composed of header and payload. Message header includes the information about 'Protocol Version', 'Source Node ID', 'Target Node ID' and 'Message Type' and so on. 'Message Type', especially, defines the various operations, which can be provided by RMDP, and the payload message is determined according to the 'Message Type'. Table 1 and Figure 8 show more details about header message structure of RMDP.

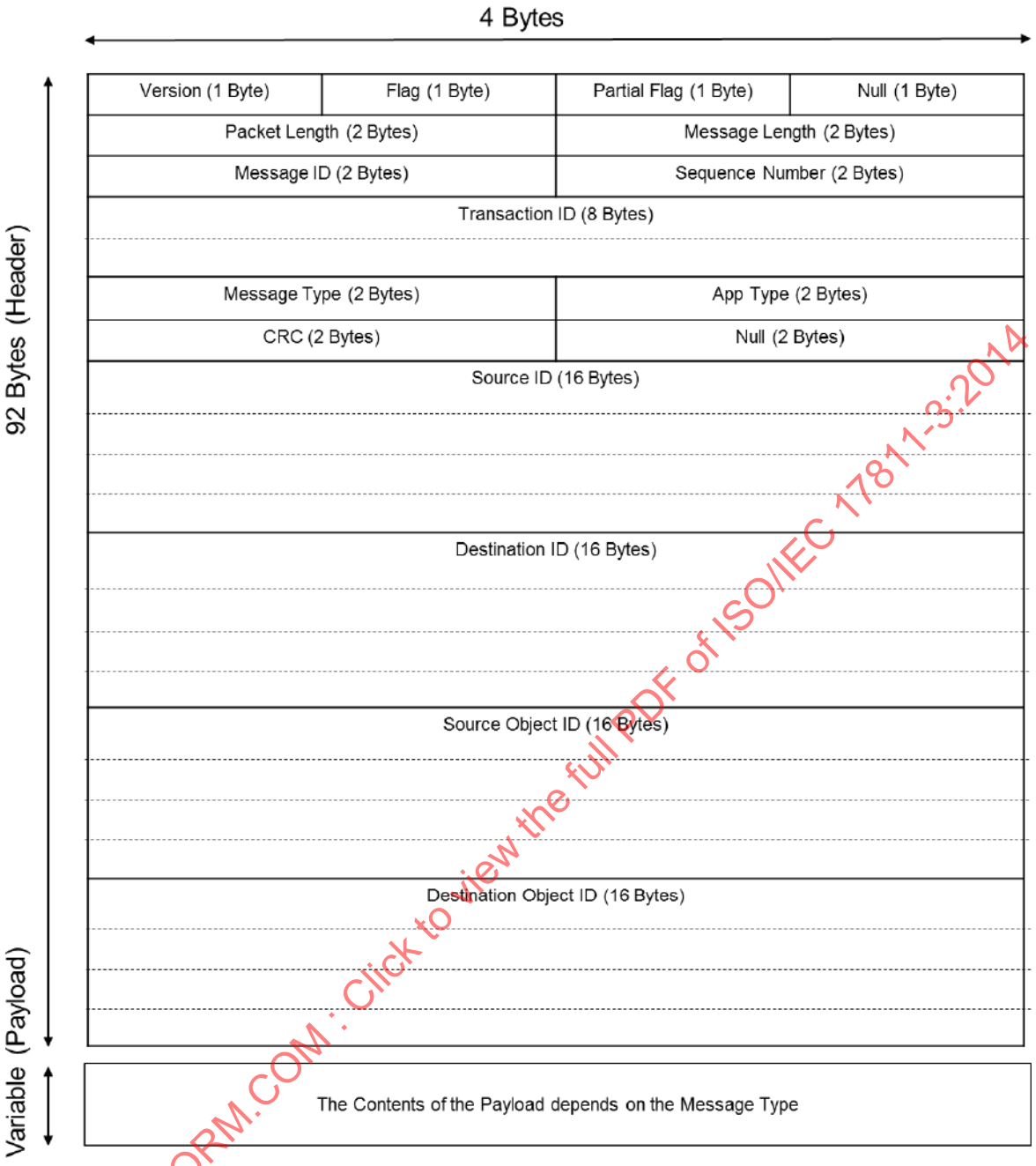

Figure 8 — RMDP Message Header Structure

Table 1 — RMDP Message Header Structure

Field Name	Size (Byte)	Description
Version	1	— Protocol Version — 0x01
Urgent Flag	1	— Urgent flag — Emergency: 0x01/Normal: 0x00
Partial Flag	1	— Indicates whether the current message is the last part of partial message sequence or not — 0x00 : the last or partial message sequence
Packet Length	2	— Message Size (Including Header)
Message Length	2	— Payload message size
Message ID	2	— Payload message ID — If the message is fragmented, random number message ID will be used. — If the value is '0', sequence number is inactive. If the value is not '0', sequence number will be used.
Sequence Number	2	— If the message is fragmented, each fragment has a sequence number starting from '1'
TransactionID	8	— Transaction Identifier — The value will be NTP timestamp — time_t 8bytes
Message Type	2	— Message type code for the RMDP operations
AppType	2	— Payload Message Type — 0x0000(RMDP), 0x0001(DCMP)
CRC	2	— Message Error Check Code — Packet Length(2Bytes), Message Length(2Bytes), MessageID(2Bytes), AppType(2Bytes), SourceID(Low 2Bytes), DestinationID(Low 2Bytes), TransactionID(2Bytes) XOR value
Source ID	16	— Source Node ID — Random generation using the UUID — Can be Installed when a device is manufactured
Destination ID	16	— Destination Node ID (UUID)
Source Object ID	16	— Source Object ID (ex: Device ID)
Destination Object ID	16	— Destination Object ID (ex: Device ID)

6.2 Messages according to the Operations

Major operations, which can be provided by RMDP, are node information management and DCMP message transmission. These operations can be classified by 'Message Type' and more details about 'Message Type' are shown in Table 2.

In case that the REQUEST message is transmitted and the corresponding RESPONSE message is not returned within an appropriate time, the indication that the REQUEST was not successful will be delivered to the user without retransmission. The receiver who received the REQUEST shall respond if the transaction ID is valid.

Transaction ID in RESPONSE message will be same to the transaction ID of the corresponding REQUEST message.

Table 2 — RMDP Message and Message type

Operation	Message	Message Type	Description
Node Advertise-ment	NODE_ADVERTISEMENT	0xF100	— Node Plug in/out
Node Discovery	NODE_DISCOVERY_REQUEST NODE_DISCOVERY_RESPONSE	0xF011 0xF012	— Node Search
Send Message	SEND_MESSAGE_REQUEST SEND_MESSAGE_RESPONSE	0xF021 0xF022	— Message Transmission
Send Event	EVENT_NOTIFICATION	0xF030	— Event Message Transmission
Object Advertisement	OBJECT_ADVERTISEMENT	0xF040	— Device Plug in/out

6.3 Error Types of RMDP

RMDP defines various error types, which can be occurred during the message operation. More details of each error type are listed below and the description of error codes is shown in Table 3.

Table 3 — Error Types

Error Type (Hex)		Description
0000 ~ 09FF (Message Error)	0000	Success
	0100	Header Error
	0100	Header Start Message Error
	0101	Header Version Message Error
	0102	Header Length Message Error
	0103	Header Source ID Error
	0104	Header Destination ID Error
	0105	Header OP Code Error
	0106	Header TransactionID Error
	0107	Header CRC Error
	0108	Header End Message Error
	0200	Payload Error
	0201	No Payload
	0202	Whole Payload data can't be received
	0203	Payload size Mismatch between the received data and the size which is described in the Header
	0204	Payload Syntax Error
0AXX (Transaction Error)	0000	Success
	0A01	Other operation is running
	0A02	Transaction is stopped
	0A03	Deadlock
	0A04	Transaction Time over

6.4 Payload Messages

6.4.1 Related Subclause for each Payload Message Structure

RMDP message is composed of header and payload. The payload data is described according to the Message Type in the header. Table 4 shows the related subclauses for each RMDP message structure.

Table 4 — Related Subclause for each Payload Message Structure

Operation	Message	Related Subclause
Node Advertisement	NODE_ADVERTISEMENT	6.4.2
Node Discovery	NODE_DISCOVERY_REQUEST	6.4.3
	NODE_DISCOVERY_RESPONSE	6.4.4
Send Message	SEND_MESSAGE_REQUEST	6.4.5
	SEND_MESSAGE_RESPONSE	6.4.6
Send Event Message	EVENT_NOTIFICATION	6.4.7
Object Advertisement	OBJECT_ADVERTISMENT	6.4.8

6.4.2 NODE_ADVERTISEMENT

— When a network is enabled or re-configured, then a node advertises its presence.

— To distinguish between start(in) signal and end(out) signal, 'Adtype' is described.

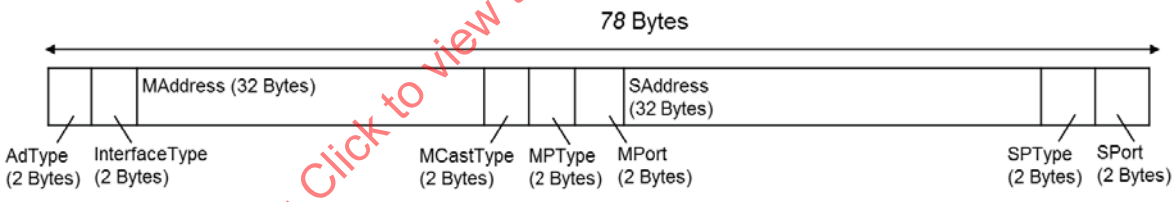

Figure 9 — NODE_ADVERTISEMENT Message Structure

Table 5 — NODE_ADVERTISEMENT Message Structure

Field Name	Field Size	Description
AdType	2 Bytes (uint16_t)	Describes one of following: — 0x0000 In — 0x0001 Out
InterfaceType	2 Bytes (uint16_t)	Physical Interface Type and describes one of following: — 0x0000 IPV4 — 0x0001 IPV6
MAddress	32 Bytes (Char[32])	Network Address for the multi-target message reception ex) 192.168.1.8

Table 5 *(continued)*

Field Name	Field Size	Description
MCastType	2 Bytes (uint16_t)	Casting Type for the multi-target message reception and describes one of following: — 0x0000 Unicast — 0x0001 Broadcast — 0x0002 Multicast
MPType	2 Bytes (uint16_t)	Protocol Type for the multi-target message reception and describes one of following: — 0x0000 UDP — 0x0001 TCP
MPort	2 Bytes (uint16_t)	Network Port for the multi-target message reception
SAddress	32 Bytes (Char[32])	Network Address for the single-target message reception ex) 192.168.1.8
SPType	2 Bytes (uint16_t)	Protocol Type for the single-target message reception and describes one of following: — 0x0000 UDP — 0x0001 TCP
SPort	2 Bytes (uint16_t)	Network Port for the single-target message reception

6.4.3 NODE_DISCOVERY_REQUEST

— This message is used when a device wants to discover nodes in the network.

— There is no Payload Message in this case.

6.4.4 NODE_DISCOVERY_RESPONSE

— This message is a response message for the NODE_DISCOVERY_REQUEST.

— Result: Describes whether discovery request message is reached to the destination well or not. If an error occurred, error code is described as shown in the Table 3.

— The payload message structure is shown in Table 6.

— NODE_DISCOVERY_RESPONSE message structure is very similar to NODE_ADVERTISEMENT message, but there is no 'Adtype' field.

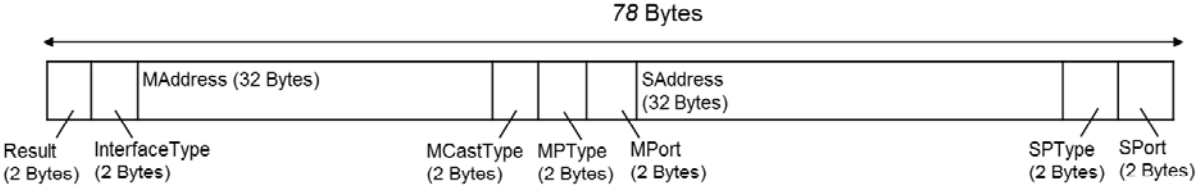

Figure 10 — NODE_ADVERTISEMENT Message Structure

Table 6 — NODE_DISCOVERY_RESPONSE Message Structure

Field Name	Field Size	Description
Result	2 Bytes (uint16_t)	Error Type (Table 3)
InterfaceType	2 Bytes (uint16_t)	Physical Interface Type and describes one of following: — 0x0000 IPV4 — 0x0001 IPV6
MAddress	32 Bytes (Char[32])	Network Address for the multi-target message reception ex) 192.168.1.8
MCastType	2 Bytes (uint16_t)	Casting Type for the multi-target message reception and describes one of following: — 0x0000 Unicast — 0x0001 Broadcast — 0x0002 Multicast
MPType	2 Bytes (uint16_t)	Protocol Type for the multi-target message reception and describes one of following: — 0x0000 UDP — 0x0001 TCP
MPort	2 Bytes (uint16_t)	Network Port for the multi-target message reception
SAddress	32 Bytes (Char[32])	Network Address for the single-target message reception ex) 192.168.1.8
SPType	2 Bytes (uint16_t)	Protocol Type for the single-target message reception and describes one of following: — 0x0000 UDP — 0x0001 TCP
SPort	2 Bytes (uint16_t)	Network Port for the single-target message reception

6.4.5 SEND_MESSAGE_REQUEST

— This message can be used when a node want to send some application protocol message (such as DCMP) to the target node.

— 'Apptype' field in the Header is described according to the Payload Message.

— The payload message structure is shown in Table 7.

Table 7 — SEND_MESSAGE_REQUEST Message Structure

Field Name	Field Size	Description
Message	Variable	Application Protocol Message such as DCMP