Part V ECHONET Lite System Design Guidelines

The specifications published by the ECHONET Consortium are established without regard to industrial property rights (e.g., patent and utility model rights). In no event will the ECHONET Consortium be responsible for industrial property rights to the contents of its specifications.

In no event will the publisher of this specification be liable for any damages arising out of use of this specification.

The original language of the ECHONET Lite Specifications is Japanese. This English version is a translation of the Japanese version; in case of any queries about the English version, refer to the Japanese version.

Contents

Chapter 1 Guidelines on the Implementation of ECHONET Lite

Inquiries about the interpretations of specifications received through Plugfest or other means are summarized in Chapter 1 as guidelines.

1.1 Guidelines on the Handling of Property Values

This section provides guidelines on handling cases where a previously set property value is within the ECHONET property definition range but is outside the range in which the corresponding actual device can operate.

(1) In a case where the continuous value range in which the actual device represented by an ECHONET property can operate is narrower than the ECHONET property definition range and a value has been set in the ECHONET property that falls between the upper and lower limit values for the ECHONET property but not between the upper and lower limit values for the actual device, it is recommended that the application software program in the ECHONET Lite node use the following as the property value for the actual device and the ECHONET property value:

The upper limit value for the actual device when the previously set value in the ECHONET property falls between the upper limit value for the ECHONET property and the upper limit value for the actual device; and the lower limit value for the actual device when the previously set value in the ECHONET property falls between the lower limit value for the ECHONET property and the lower limit value for the actual device.

For example, when the ECHONET property definition range is 0x00 to 0xFD (0°C to 253°C) and the operation range of the actual device represented by the ECHONET property is 0x0A to 0x32 (10°C to 50°C) and a value (e.g. 60°C) has been set in the ECHONET property that falls between the upper limit value for the actual device and the upper limit value for the ECHONET property, it is recommended that the upper limit value for the actual device (0x32 (50°C)) be used as the ECHONET property value. When a value (e.g. 5°C) has been set in the ECHONET property that falls between the lower limit value for the actual device and the lower limit value for the ECHONET property under the same range conditions, it is recommended that the lower limit value for the actual device (0x0A (10°C)) be used as the ECHONET property value.
Fig. 1.1 illustrates these examples.

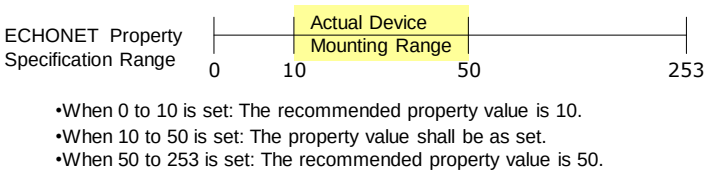

Fig. 1.1 Property Value Setting Example 1

(2) In a case where the number of step values that can be used for step adjustment of the operation of the actual device represented by an ECHONET property is smaller than the number of step values included in the ECHONET property definition range, and one of the values within the ECHONET property definition range that has been set in the ECHONET property is other than the step values for the actual device, it is recommended that the application software program in the ECHONET Lite node use, as the property value for the actual device and the ECHONET property value, the value that can be used for the actual device and is closest to the value previously set in the ECHONET property.

For example, when the ECHONET property definition range includes eight step values between 0x31 and 0x38 but only 0x31, 0x35 and 0x38 (three step values) can be used for step adjustment of the operation of the actual device represented by the ECHONET property, and one of the eight values within the ECHONET property definition range has been set in the ECHONET property, it is recommended that the application software program in the ECHONET Lite node use, as the property value for the actual device and the ECHONET property value, the value among the three values that is closest to the value previously set in the ECHONET property, based on mapping of the 8-value range onto the 3-value range, as shown in Fig. 1.2.

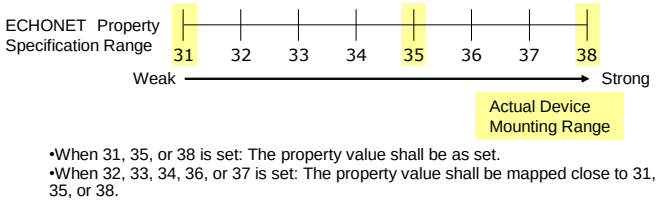

Fig. 1.2 Property Value Setting Example 2

(3) In a case where the previously set value in an ECHONET property specifies a function that is included in the ECHONET property definition range but is not implemented in the actual device represented by the ECHONET property, it is recommended that the application software program in the ECHONET Lite node

ignore the setting and use, as the ECHONET property value, the current value specified for the actual device, as shown in Fig. 1.3.

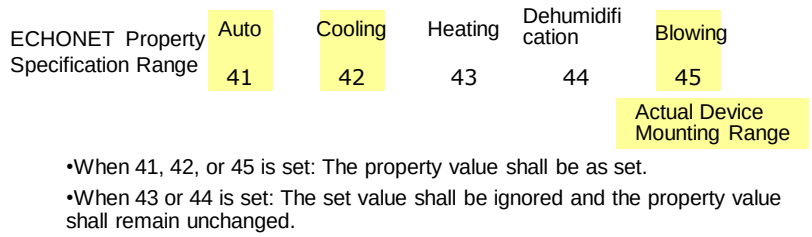

Fig. 1.3 Property Value Setting Example 3

1.2 Guidelines on the Handling of Responses

For a response to a property value write request (ESV=0x60, 0x61) or property value write-read request (ESV = 0x6E) of the values specified below, it is recommended to assume that the processing should have been accepted. In other words, there is no response for ESV=0x60. For ESV = 0x61, 0x6E, a property value write response (ESV = 0x71) or property value write-read response (ESV = 0x7E) is returned.

In case of an implementation that returns a response after confirming the support range of actual equipment or setting up actual equipment, a response of processing impossible (ESV=0x50, 0x51, 0x5E) may be returned.

- In a case where a value outside the ECHONET property definition range was specified.
- In a case where the continuous value range in which the actual device represented by an ECHONET property can operate is narrower than the ECHONET property definition range and a value has been set in the ECHONET property that falls between the upper and lower limit values for the ECHONET property but not between the upper and lower limit values for the actual device.
- In a case where the number of step values that can be used for step adjustment of the operation of the actual device represented by an ECHONET property is smaller than the number of step values included in the ECHONET property definition range, and one of the values within the ECHONET property definition range that has been set in the ECHONET property is other than the step values for the actual device.
- In a case where the previously set value in an ECHONET property specifies a function that is included in the ECHONET property definition range but is not implemented in the actual device represented by the ECHONET property.

1.3 Guidelines on OPC

A controller or similar equipment sends a property value write request (ESV = 0x60, 0x61), property value read request (ESV = 0x62), property value write-read request (ESV=0x6E), or property value notification request (ESV=0x63) to other ECHONET Lite equipment. If this kind of equipment receives a response of processing impossible (B smaller than A is set to OPC) to a sent request (A of 2 or greater is set to OPC), it is recommended to set B (or less) to OPC at later request send.

1.4 Guidelines on General Broadcast

Some use of general broadcasts may cause ECHONET Lite node processing overload or network congestion. The following are guidelines on sending or receiving of a general broadcast message.

- It is preferable not to send a message whose address is for a general broadcast and ESV is a property value notification request (0x63). This kind of message causes a further general broadcast because of the responses from all nodes that receive the message.
- Response concentration may be caused by messages whose addresses are for a general broadcast and ESVs are a property value write request (requiring response) (0x61), read request (0x62), notification request (0x63), or write-read request (0x6E). To ease this concentration on the sender, each node receiving this kind of message should wait for a different length of time until sending a response message. The wait time is a fixed value different for each node or is a random time.

1.5 Guidelines on the Number of Instances

As a rule, the number of equipment object instances held by one ECHONET Lite node shall be 84 or less.

Even for a node entity having 85 or more instances, it is preferable to notify only up to 84 instances by an instance list notification (EPC = 0xD5) by considering nodes that interpret only 84 or less instances.

For the notification or interpretation of an instance list having 85 or more instances, it is preferable to use a message whose OPC value is 2 or more and each EPC value is 0xD5. However, a message sending node should note the existence of receiving nodes which do not interpret it.

1.6 Guidelines on the Property Value Write & Read Service

This section gives implementation guidelines for the property value write & read service.

- This service should be implemented so that a node receiving a property value write & read request (ESV = 0x6E) from another node will process the write request first, irrespective of the property combination, then store a value based on the self-node status after completion as a response to the read request. If the processing of an arbitrary property combination in this order cannot be guaranteed (write processing and equipment status change are asynchronous), the node should return a response of processing impossible (ESV = 0x5E) to a property value write & read request by setting OPCSet and OPCGet to 0.

- This service should be implemented so that, if a node sends a property value write & read request (ESV = 0x6E) to a remote node and receives a normal response (ESV = 0x7E), processing should be executed on the assumption that the write request to the remote node should have been processed and a value based on the remote node status after processing should have been acquired as a response to the read request.

Chapter 2 Guidelines for Secure Communications in ECHONET Lite

2.1 Overview

For secure communications in ECHONET Lite, tampering with communications is prevented: illegal access is prevented by authentication, and tapping is prevented by encryption. The ECHONET Lite Communication Middleware ensures security transmissively from ECHONET Lite by applying the existing standard technologies for secure communications to its lower layers. This chapter gives examples of mechanisms for secure communications in lower layers and describes their guidelines.

2.2 Secure Communications in Lower Layers

This section gives examples of mechanisms for secure communications in lower layers that are provided by the ECHONET Lite Communication Middleware. Security may also be ensured by using not the following mechanisms but the unique mechanism of each company. Negotiation by encryption algorithms, the encryption of communications between ECHONET Lite nodes, and authentication between ECHONET Lite nodes shall follow the specifications of each secure communications mechanism.

Table 2.1 Mechanisms for Secure Communications in Lower Layers

Lower Layer	Mechanism for Secure Communications
Transport	DTLS (Datagram Transport Layer Security)
Network	IPsec (Security Architecture for Internet Protocol) RFC5191
Data Link	WEP (Wired Equivalent Privacy) WPA (Wi-Fi Protected Access) WPA2 (Wi-Fi Protected Access2) AES-CCM (Advanced Encryption Standard Counter with CBC-MAC) IEEE802.1X

2.2.1 DTLS

DTLS is a protocol to provide secure communication functions for datagram. The functions are almost the same as those of TLS (Transport Layer Security). The use of DTLS on a UDP is specified in RFC4347. This protocol is applicable when using UDF in the transport layer or when encrypting ECHONET Lite transmission frames and

preventing tampering in the transport layer.

2.2.2 IPsec

IPsec is a protocol to provide functions for keeping data confidential and preventing tampering in units of an IP packet. This protocol is an option for IPv4 but is implemented in IPv6 as a standard feature. This protocol is applicable when using IP in the network layer or when encrypting ECHONET Lite transmission frames and preventing tampering in the network layer.

2.2.3 RFC5191

RFC5191 is a standard to regulate connections by authentication so that only specified devices can join a network. This standard is available in an arbitrary data link layer. A recommended configuration is where an ECHONET Lite node serves as a client issuing an authentication request and a device capable of communicating with an ECHONET Lite node serves as an authentication agent or server receiving an authentication request. A recommended authentication system is PEAP for authentication with an ID or password using a serial key marked on the frame of a device or EAP-TLS for authentication with a digital certificate stored in a device.

2.2.4 AES-CCM

The next-generation encryption system of the U.S. Government established by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce. Counter Mode is used for encryption, Message Integrity Code (MIC) for detecting and preventing tampering, and CBC-MAC for MIC generation.

2.2.5 WEP

An encryption technology for wireless communications. This secret key encryption system, based on the RC4 algorithm, is standardized by IEEE and adopted as a security system of IEEE 802.11b.

2.2.6 WPA

A standard of encryption system for wireless LAN announced by the Wi-Fi Alliance, which is an organization in the wireless LAN industry. The security strength of WEP was improved by compensating for its vulnerable points. For encryption, WPA has a user authentication function, as well as SSID and WEP key, and uses the Temporal Key Integrity Protocol (TTKIP)), which updates the encryption key automatically at fixed time intervals.

2.2.7 WPA2

A new version of WPA. This system uses the encryption standard AES specified by the U.S. National Institute of Information and Communications Technology (NICT) for

powerful encryption using keys of variable length from 128 to 256 bits.

2.2.8 IEEE802.1X

IEEE802.1X is a standard to regulate connections by authentication so that only specified devices can join a network. This standard is available both for cable and wireless communications. A recommended configuration is where an ECHONET Lite node serves as a supplicant (authentication client) and a device capable of communicating with an ECHONET Lite node serves as an authenticator (authentication device) or authentication server (server which judges whether to allow a supplicant to participate). A recommended authentication system is PEAP for authentication with an ID or password using a serial key marked on the frame of a device or EAP-TLS for authentication with a digital certificate stored in a device.

Chapter 3 Guidelines on Handling Transmission-only Devices

ECHONET Lite defines transmission-only devices to make not only always-live communication devices but also battery-driven devices of low power consumption compatible with ECHONET Lite. Guidelines are available on the handling of these special devices.

- When a transmission-only device joins a network, other devices that are not transmission-only in the system shall be set manually to recognize the transmission-only device.
- When a controller joins a system that has a transmission-only device, information of the transmission-only device shall be set manually in the controller.
- It is recommended that transmission-only devices should periodically broadcast the instance list notification announcement described in Section 4.3.1 of Part II.

Chapter 4 Guidelines on Node Detection and Finding Procedure

4.1 Concept

Except for regular communications with fixed parties, an ECHONET Lite node to control other ECHONET Lite nodes or acquire their statuses (hereinafter, referred to as “controller” in this chapter) acquires communications addresses by node detection and finding before starting communications.

ECHONET Lite does not define a node detection or finding message. However, this can be realized by combining a general broadcast and the acquisition and notification of essential properties to be mounted. This chapter gives guidelines on the procedure.

4.2 Detection by Message Send from Node to Controller

When joining a network (including a change of communication address), an ECHONET Lite node must send an instance list notification message by a general broadcast according to "Part II 4.3.1 Basic Sequence for ECHONET Lite Node Startup." To detect the joining of a new node immediately, the controller may wait for and process the message.

If all nodes start simultaneously after recovery from a power failure, simultaneous transmission may cause network congestion. To ease this congestion, each node should wait for a different length of time after newly joining a network until sending an instance list notification message. The wait time is a fixed value different for each node or is a random time.

4.3 Finding by Message Send from Controller to Node

To find ECHONET Lite nodes within the network, a controller may send a node finding message by a general broadcast at an arbitrary timing. All ECHONET Lite nodes wait for the message, except transmit-only equipment. A node must return a response if the message is related to its own object or property. For a node finding message, it is preferable to use the following parameters:

- Destination address: General broadcast
- TID: Arbitrary value
- SEOJ: One of the objects held by the controller
- DEOJ: Node profile object (0x0EF001)
- ESV: Property value read request (0x62)
- OPC: 1
- EPC: Self-node instance list S (0xD6)

To find a specific model (node having specific equipment objects), the following parameters may be used:

- Destination address: General broadcast
- TID: Arbitrary value
- SEOJ: One of the objects held by the controller
- DEOJ: Equipment object held by a node to find
- ESV: Property value read request (0x62)
- OPC: 1
- EPC: Properties held by DEOJ-specified objects (preferable to specify the operation status (EPC = 0x80) and other essential properties)

It is preferable not to use a property value notification request (0x63) for ESV of a node finding message. A message whose destination is an address for a general broadcast and ESV is a property value notification request causes a further general broadcast because of the responses from all nodes that receive the message. This may result in node processing overload or network congestion. Therefore, the controller waits for a certain time after sending the node finding message. The wait time may be a fixed value or a variable value depending on the network status.

Chapter 5 Guidelines on TCP

- The behavior of a node sending a response message to another node shall be implementation-dependent (no response necessary) if the connection is already cleared at send processing.

- A node sending a request message to another node should send the message again by UDP unicast when necessary in case of a TCP connection failure since the remote party may not be able to use TCP.