INTERNATIONAL STANDARD

ISO/IEC 17811-2

First edition
2015-02-15

Information technology — Device control and management —

Part 2:
Specification of Device Control and Management Protocol

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

Partie 2: Spécifications du protocole de commande et gestion de périphériques

Reference number
ISO/IEC 17811-2:2015(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

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

ISO/IEC 17811-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology* SC 6, *Telecommunications and information exchange between systems*.

Introduction

This International Standard provides the architecture for device control and management (DCM). DCM can support the various control and management services, regardless of the network protocols or interfaces. DCM is composed of two protocols; device control and management protocol (DCMP) and reliable message delivery protocol (RMDP).

This International Standard, ISO/IEC 17811, consists of the following parts:

— Part 1: Architecture

— Part 2: Specification of Device Control and Management Protocol

— Part 3: Specification of Reliable Message Delivery Protocol

ISO/IEC 17811-1 describes the architecture of DCM, which includes definition, general concept, requirements, design principles, 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.

ISO/IEC 17811-3 specifies the Reliable Message Delivery Protocol (RMDP), which includes the interworking with DCMP, protocol operations, and message structure associated with RMDP.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this International Standard may involve the use of a patent concerning the message structure of DCMP given in Clause 7.

ISO and IEC take no position concerning the evidence, validity, and scope of this patent right.

The holder of this patent right has assured the ISO and IEC that he is willing to negotiate licences either free of charge or under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from:

Patent Holder: Electronics and Telecommunications Research Institute (ETRI)

Address: 138 Gajeongno, Yuseong-gu, Daejeon, 305-700, Korea

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

ISO (www.iso.org/patents) and IEC (http://patents.iec.ch) maintain on-line databases of patents relevant to their standards. Users are encouraged to consult the databases for the most up to date information concerning patents.

Information technology — Device control and management —

Part 2: Specification of Device Control and Management Protocol

1 Scope

This part of ISO/IEC 17811 provides the specification of Device Control and Management Protocol (DCMP), which is an application-layer protocol used to control and manage the various devices. DCMP supports the device and network status information retrieval, device initialization, firmware and software update, file transmission, and so on. This part of ISO/IEC 17811 specifies the protocol operations and message structure of DCMP.

The network security is out of scope in this part of ISO/IEC 17811. However, the security services can be necessary according to applications of DCMP. DCMP can 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
purposed to control and manage the various smart devices

Note 1 to entry: For this purpose, DCM is composed of the two protocols; Device Control and Management Protocol (DCMP) and Reliable Message Delivery Protocol (RMDP).

[SOURCE: ISO/IEC 17811-1]

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]

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]

2.4
administrative domain
represents a network area where a single administrator can configure and manage a network with the same policy

[SOURCE: ISO/IEC 17811-1]

2.5
device management server
DMS
used to keep track of the various device information and also to manage the devices in an administration domain

Note 1 to entry: There may be one DMS in an administrative domain, if needed.

[SOURCE: ISO/IEC 17811-1]

3 Abbreviation

The following abbreviations are used in this document.

DCMP	Device Control and Management Protocol
DCM	Device Management Architecture and Protocol
DMS	Device Management Server
RMDP	Reliable Message Delivery Protocol
NTP	Network Time Protocol
UUID	Universally Unique Identifier
UPnP	Universal Plug and Play

4 Overview

The DCMP is a protocol used to control and manage a variety of smart devices in the network. The DCMP messages are exchanged between different devices or between device and DMS.

The DCMP operates over RMDP for reliable message delivery. In the networking perspective, RMDP provides one or more devices with an interface to the network. That is, a group of devices are connected to an RMDP node via an internal API interface or a network, and the RMDP performs the reliable delivery of DCMP messages to the different RMDP nodes which are also connected to other devices. For this purpose, RMDP maintains the mapping information between DCM device identifier and physical network identifier such as IP address and port number. After RMDP retrieves the target node information, DCMP messages can be exchanged over RMDP.

Figure 1 gives a general example of DCM operations between a device and DMS. Those operations are divided into RMDP initialization, DCMP initialization, and management service.

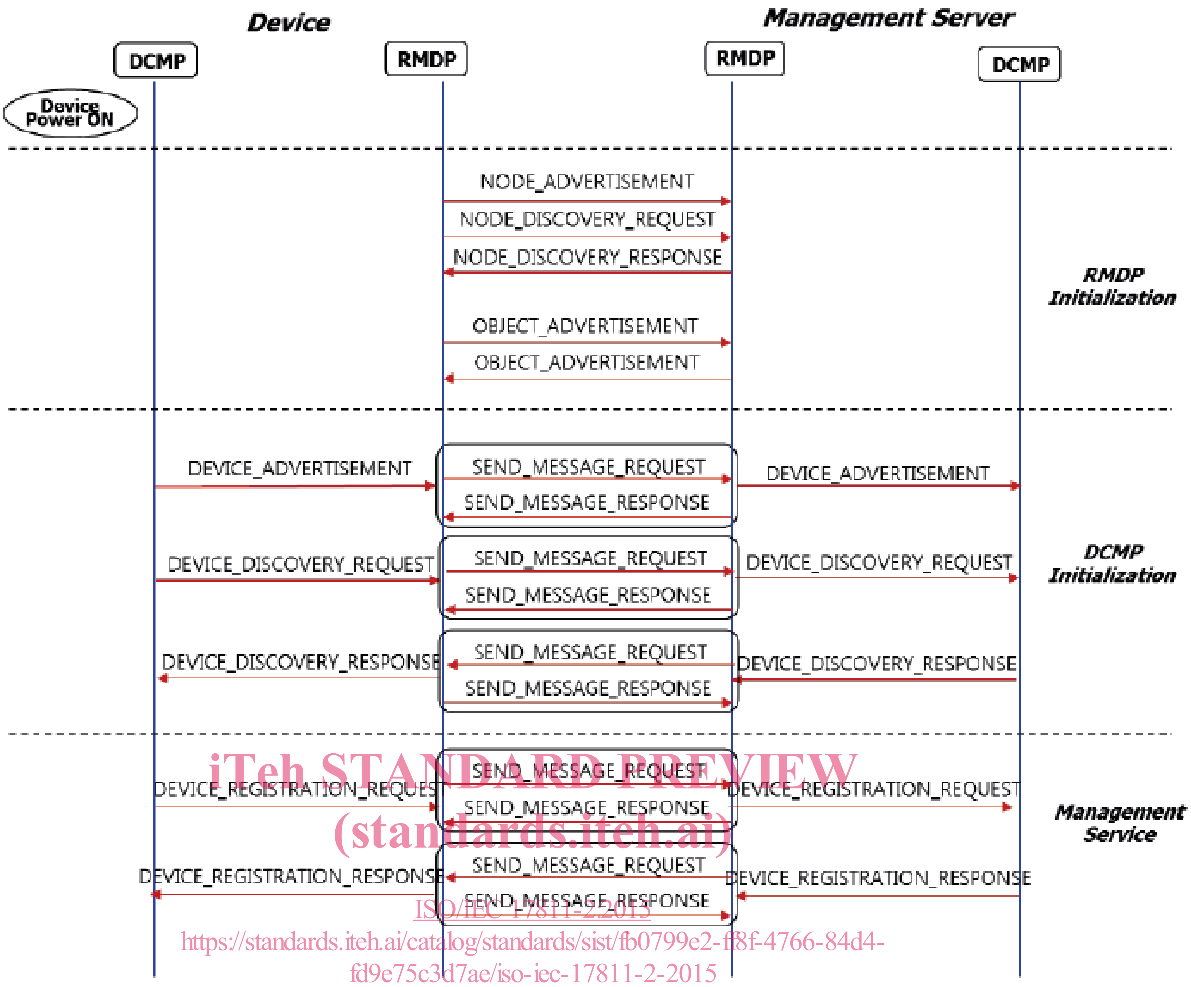

Figure 1 — DCM Operations

The RMDP manages the mapping information between the device identifier and physical network identifier. For an advertisement of the physical network identifier information in the RMDP initialization phase, a “NODE_ADVERTISEMENT” and “NODE_DISCOVERY_REQUEST/RESPONSE” messages are broadcast by the RMDP. To advertise the device identifier information, an OBJECT_ADVERTISEMENT message is then broadcast by the RMDP. The physical address information of the DMS can be added in the RMDP module of a device using the API of RMDP. The RMDP module of the device sends a NODE_ADVERTISEMENT message using a broadcast to the other devices connected in the local network, but the RMDP module of the device uses a unicast when sending the NODE_ADVERTISEMENT message to the DMS. The RMDP module of the DMS can manage the physical address information of the device using the socket information, that is, the IP address and port information of the access point (AP) or router. In the DCMP initialization phase, the DCMP modules of DMS and device can retrieve the basic information of the concerned devices (e.g. device name, device ID and device type) by using the “DEVICE_ADVERTISEMENT” and “DEVICE_DISCOVERY_REQUEST/RESPONSE” messages. In these processes, the DCMP module asks its RMDP module with the device ID of the target (corresponding) device by using a DCMP message, and then the RMDP module will transmit the received DCMP message to the target RMDP module of the target device. In the management service phase, a device can register its basic information (e.g., model name, model number and serial number) on the DMS server by using the “DEVICE_REGISTRATION_REQUEST/RESPONSE” message of DCMP.

The protocol operations of DCMP are classified as follows:

— Device Discovery;

— Device Advertisement;

- Device Information Retrieval;
- Device Control;
- Event Notification;
- Event Subscription;
- Get File Information;
- File Download;
- File Upload;
- Apply;
- Device Registration; and
- Service Registration.

5 Protocol Operation

5.1 Device Discovery

For device discovery, a DEVICE_DISCOVERY_REQUEST and DEVICE_DISCOVERY_RESPONSE messages are exchanged between devices, as shown in Figure 2. A source device broadcasts a DEVICE_DISCOVERY_REQUEST message to the target devices. In response to the DEVICE_DISCOVERY_REQUEST message, all devices which fit into the requested information shall respond with a DEVICE_DISCOVERY_RESPONSE message.

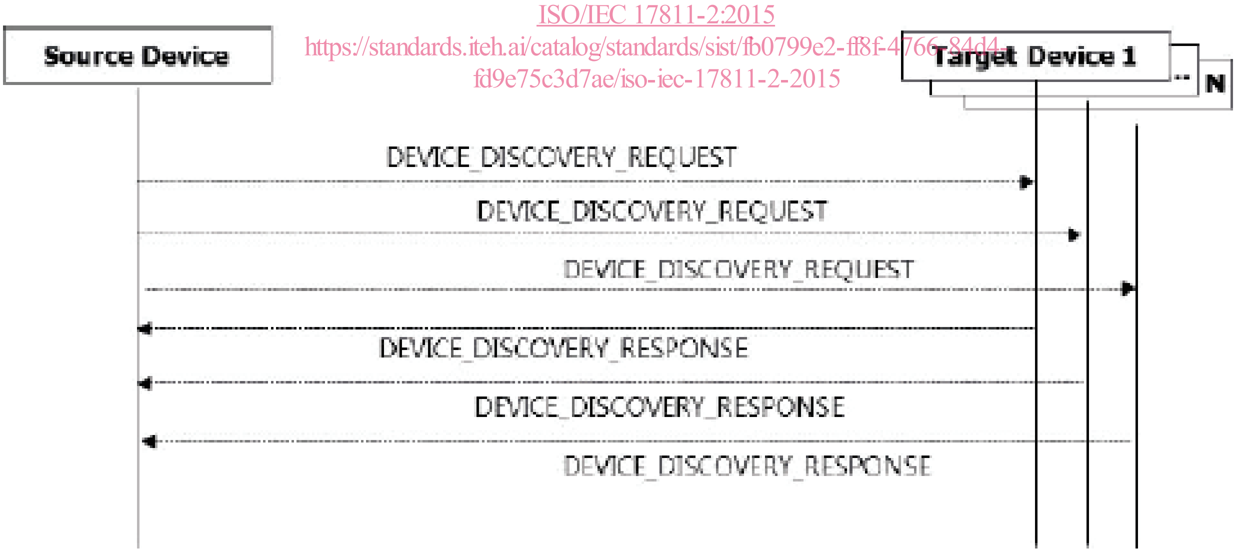

Figure 2 — Device Discovery Operation

The device 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.

5.2 Device Advertisement

The device advertisement operation can be used to inform device's plug-in or plug-out, as shown in Figure 3. The associated device 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.

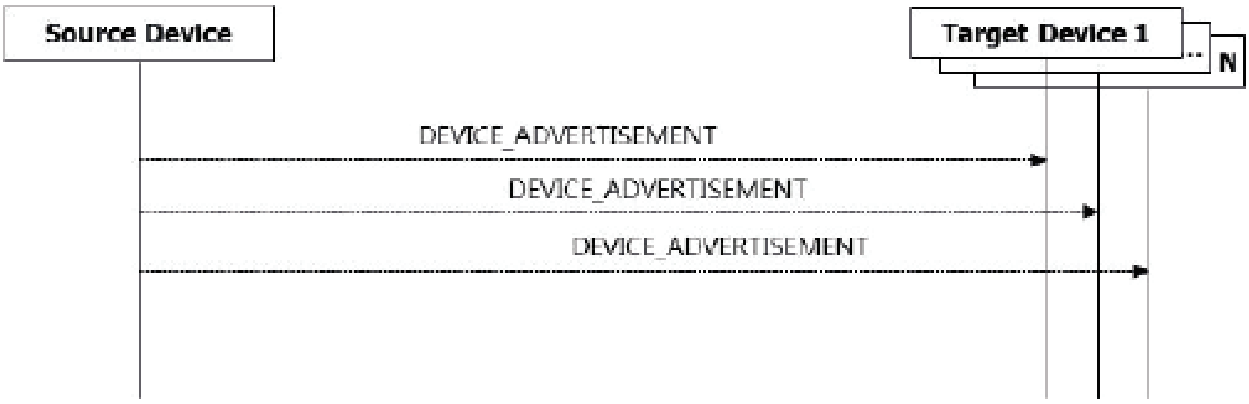

Figure 3 — Device Advertisement Operation

5.3 Device Information Retrieval

The device information retrieval operation can be used when a device needs to know the various device information such as device ID, device name, device property, device status and so on. The volume of the device information is various and depends on the type of device and its capability. To accommodate different level of devices, we may categorize the relevant information into device basic information, device configuration, and system and network information. The basic information represents the fixed information for all devices, whereas the other information is variable for each device.

The operation of device information retrieval is composed of two-message transaction, as shown in Figure 4. This operation requires a request message at source and a response message at destination. When a response message is not received within a specific time interval, the source may cancel the transaction or re-issue the transaction.

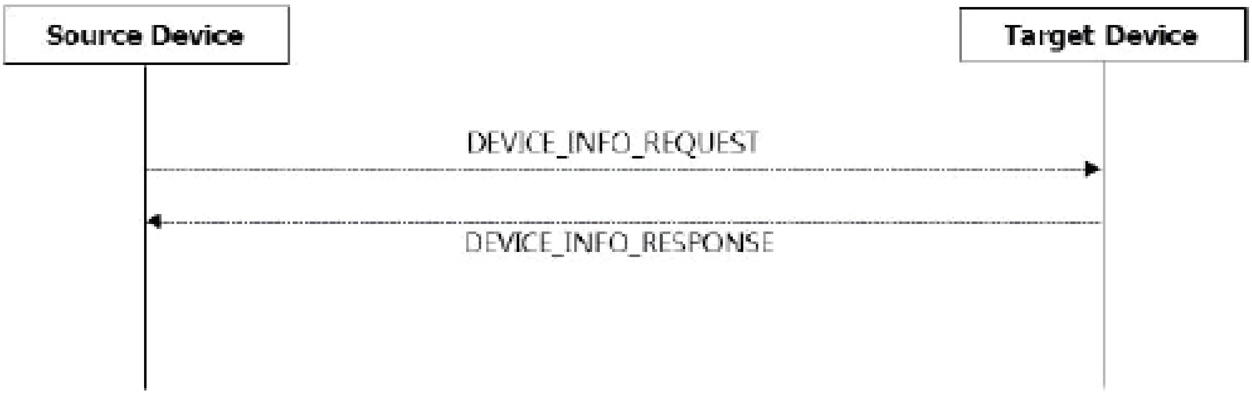

Figure 4 — Device Information Retrieval Operation

5.4 Device Control

Device control is used to perform device specific operations. For device control, a source device shall provide the control code and parameters associated with the device control operation. When a target device receives a DEVICE_CONTROL_REQUEST message, it checks if it the message contains a valid control code for the device and if the control code can be supported. If so, it executes the control operation requested and returns the result to the source device with a DEVICE_CONTROL_RESPONSE message, as shown in Figure 5.

The operation of device control 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 device may cancel the transaction or re-issue the transaction.

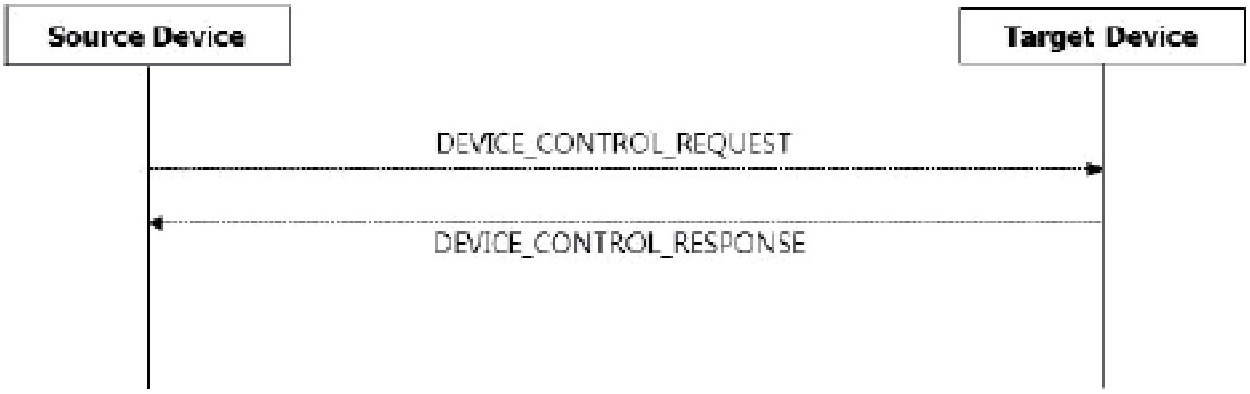

Figure 5 — Device Control Operation

5.5 Event Notification

When an event occurs in a device, the event can be reported to the interested devices by EVENT_NOTIFICATION message, as shown in Figure 6. Event notification transaction is one-way transaction. This means that only one message is required to finish a transaction, and any response message is not required.

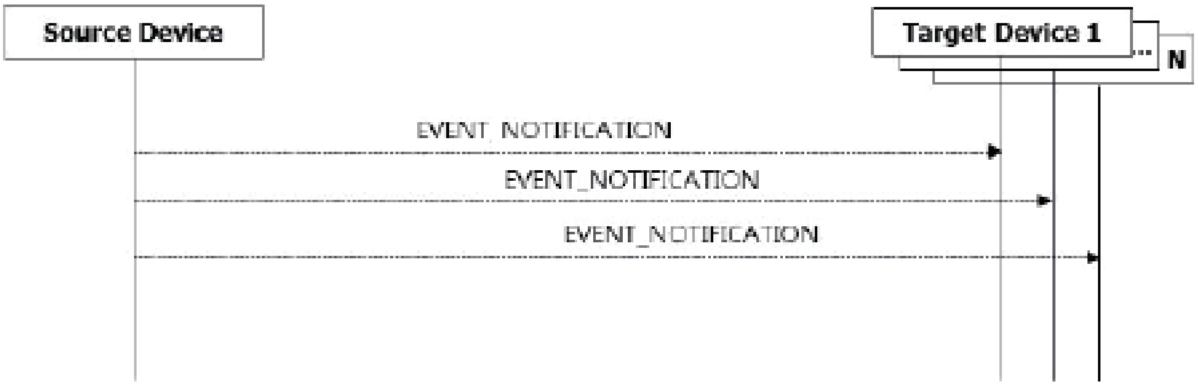

Figure 6 — Event Notification Operation

5.6 Event Subscription

When an event occurs in a device, the event can be reported to all devices in a network. However, whenever an event is broadcast to all devices in network, the event messages are overwhelmed in the network. So, the event information shall be reported to only the interested devices. For this purpose, the event handling related operations include event notification as well as the associated event subscription/un-subscription operations. This is helpful to reduce traffic overhead within a local network.

The operation of event subscription is a two-message transaction, as shown in Figure 7. This operation requires a request message at source and a response message at destination. When a response message is not received within a specific time interval, the source may cancel the transaction or re-issue the transaction.

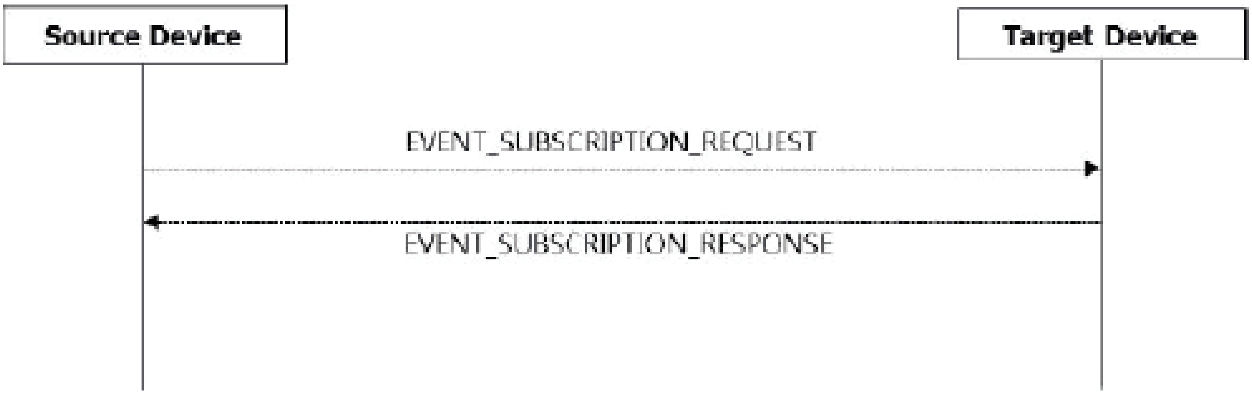

Figure 7 — Event Subscription Operation

5.7 Get File Information

The file upload and download capability is the essential functions for device management, since the software or firmware update requires the updated file to be transferred to the target device. Sometimes it is useful to send quite a large size of message instead of using a simple message transfer. So, the file upload/download operation is defined as a part of common device operations. The processing of the files is various in a large system. So, we classify each file by a file type and provide this information with the file.

The operation of 'get file information' is a two-message transaction, as shown in Figure 8. This operation requires a request message at source and a response message at destination. When a response message is not received within a specific time interval, the source device may cancel the transaction or re-issue the transaction.

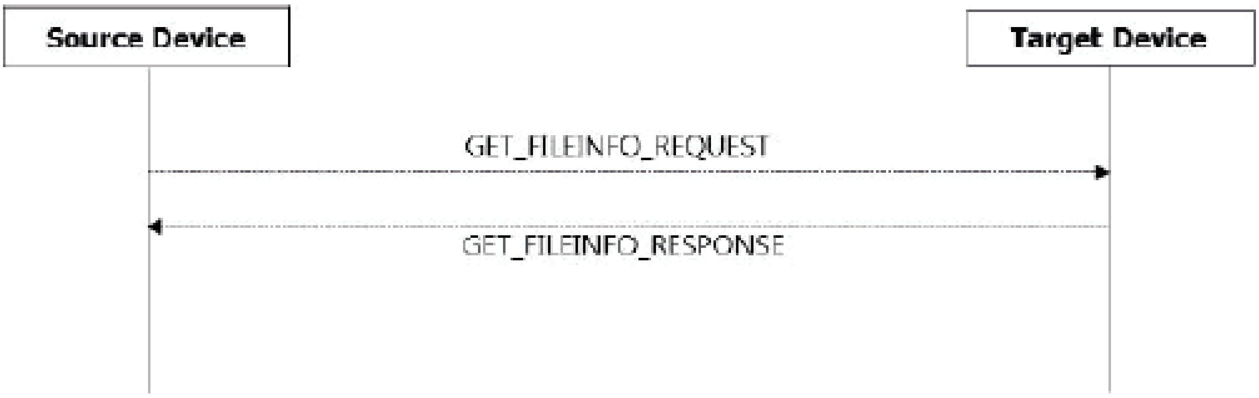

Figure 8 — Get File Information Operation

5.8 File Download

The file download capability is an essential function for device management since the software or firmware update requires the updated file to be transferred to the target device. Sometimes it is useful to send quite a large size of message instead of using a simple message transfer. So, file upload/download operation is defined as a part of common device operations.

The file download transaction can be used to get some file in a remote device and totally the three messages are required, as shown in Figure 9. First, a source device requests the file download by using a GET_FILE_REQUEST message. Then, a destination device decides if the request is accepted or rejected. When the request is accepted, the destination device shall respond with a GET_FILE_RESPONSE message containing a SUCCESS indication code. However, if the destination device rejects the file transfer, the 'get file' transaction is terminated.

After finishing the file transfer, the destination device sends a GET_FILE_RESULT message with a SUCCESS indication code. When a file transfer is aborted by some reasons, the destination device sends the GET_FILE_RESULT message with an appropriate error code.

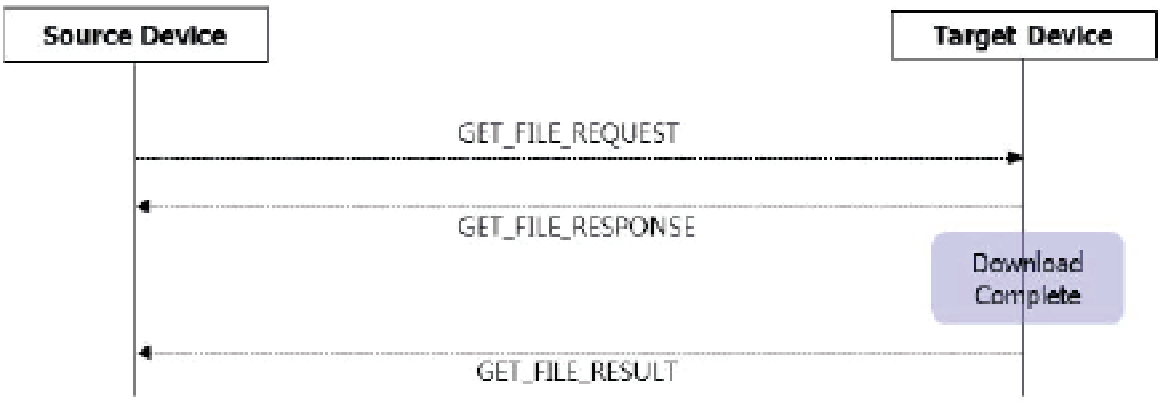

Figure 9 — File Download Operation

5.9 File Upload

The file upload capability is an essential function for device management since the software or firmware update requires the updated file to be transferred to the target device. Sometimes it is useful to send quite a large size of message instead of using a simple message transfer. So, file upload/download operation is defined as a part of common device operations.

The file upload transaction can be used to send some file from the source device to the target device and totally the three messages are required, as shown in Figure 10. First, a source device requests the file upload by using a PUT_FILE_REQUEST message. Then, a destination device decides if the request is accepted or rejected. When the request is accepted, the destination device shall respond with a PUT_FILE_RESPONSE message containing a SUCCESS indication code. However, if the destination device rejects the file transfer, a 'put file' transaction is terminated.

After finishing the file transfer, the source device sends a PUT_FILE_RESULT message with a SUCCESS indication code. When a file transfer is aborted by some reasons, the source device sends the PUT_FILE_RESULT message with an associated error code.

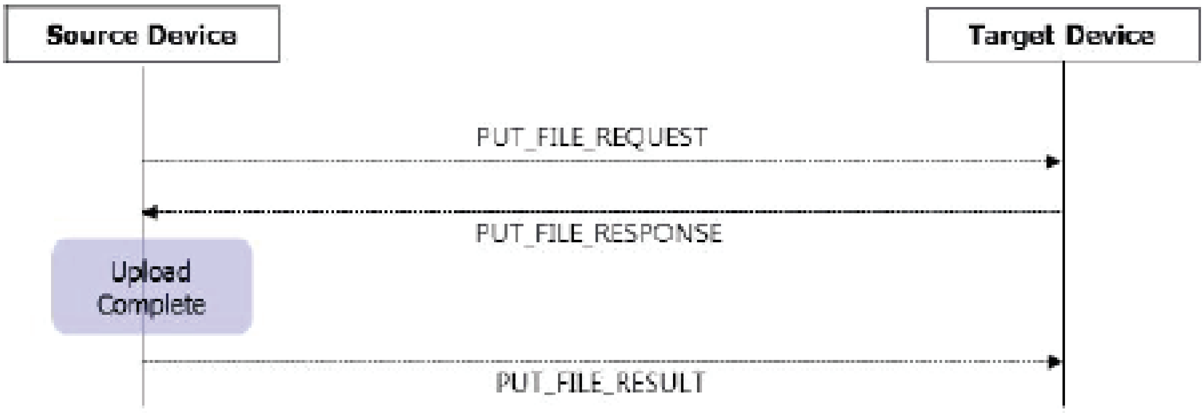

Figure 10 — File Upload Operation

5.10 Apply

Apply transaction can be used to request a critical control action to a device and get the result, as shown in Figure 11. A source device requests an APPLY_REQUEST message specifying the requested operation such as firmware update, reboot, configuration, etc. Then a destination device decides if the request will be accepted or rejected. When the requested operation is accepted, then the device immediately replies with an APPLY_RESPONSE message and performs the requested action. When the requested action is finished, then an apply result message is sent back to the source device.

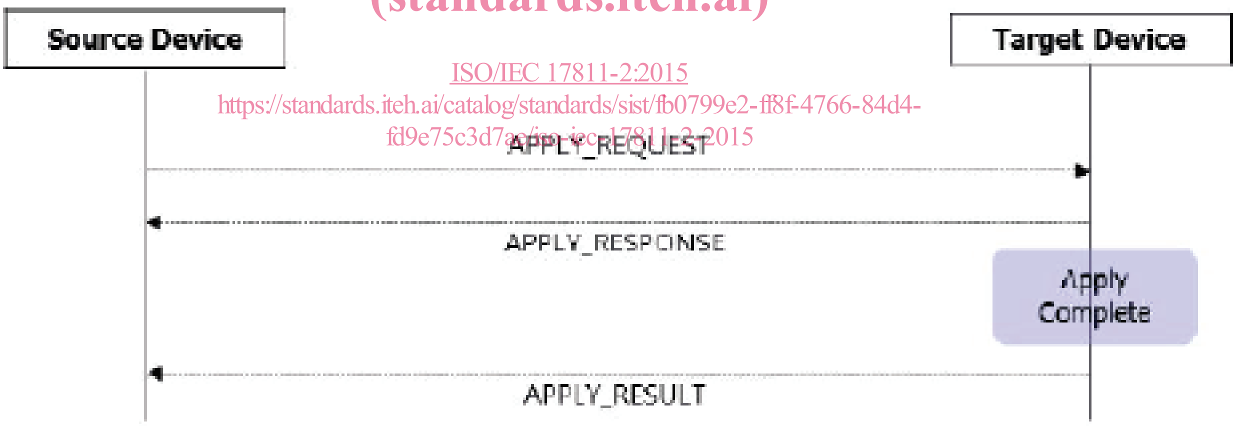

Figure 11 — Apply Operation

5.11 Device Registration

Device registration message can be used when a device wants to register its own information to the DMS. The operation of device registration is a two-message transaction, as shown in Figure 12. This operation requires a request message at source and a response message at destination. When a response message is not received within a specific time interval, the source device may cancel the transaction or re-issue the transaction.