INTERNATIONAL STANDARD

ISO/IEC 17811-1

First edition
2014-06-15

Information technology — Device control and management —

Part 1: Architecture

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

Partie 1: Architecture

Reference number
ISO/IEC 17811-1:2014(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.

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

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 31, *Automatic identification and data capture techniques*.

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*

— *Part 3: Specification of Reliable Message Delivery Protocol*

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: DCMP (Device Control and Management Protocol) and RMDP (Reliable Message Delivery Protocol).

This International Standard consists of the following parts:

— Part 1: Architecture

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

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

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

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

Part 3 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 1: Architecture

1 Scope

This International Standard provides the relationship between DCMP and RMDP with use cases. Also, this International Standard specifies the requirements and design principles.

2 Normative references

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

ISO/IEC 17811-2, *Information technology — Device control and management — Part 2: Specification of Device Control and Management Protocol*

ISO/IEC 17811-3, *Information technology — Device control and management — Part 3: Specification of Reliable Message Delivery Protocol*

3 Terms and definitions

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

3.1
device control and management
DCM
operations are purposed to control and manage the various smart devices. For this purpose, DCM is composed of two protocols; DCMP (Device Control and Management Protocol) and RMDP (Reliable Message Delivery Protocol)

3.2
device control and management protocol
DCMP
used to perform various management operations which are categorized into information retrieval, control, diagnostic, and debugging

3.3
reliable message delivery protocol
RMDP
used to provide uniform and reliable message delivery among devices regardless of the underlying network protocols or interfaces

3.4
administrative domain
represents a network area where a single administrator can configure and manage a network with the same policy

3.5
device management server
DMS
used to keep track of the various device information and also to manage the devices in an administrative domain

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

3.6
DCM device
represents a device that supports the RMDP and DCMP message exchange, parsing, and processing

3.7
node information
information which is managed by RMDP, such as physical address identifier, device identifier, and so on

4 Abbreviations

The following acronyms are used in this International Standard.

DCM	device control and management
DCMP	device control and management protocol
DHCP	dynamic host configuration protocol
DMS	device management server
RMDP	reliable message delivery protocol
UUID	universally unique identifier
UPnP	universal plug and play

5 Overview

DCM provides various functions for the device management. DCM supports the device and network status information retrieval, device and network initialization, firmware and software update, file transmission and so on. In an administrative domain, there may be a device management server that collects, controls, and manages devices using DCMP. To exchange DCMP messages among the devices, RMDP is needed. RMDP is a message exchange protocol among the devices regardless of the network protocols or interfaces. The detailed protocol stack of DCM is illustrated in the Figure 1.

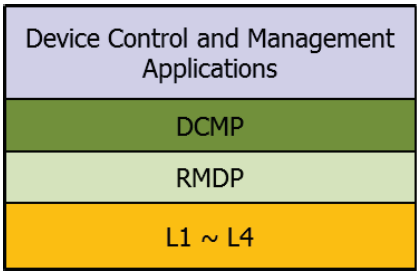

Figure 1 — Protocol Stack for the DCM

Basically, DCMP messages can be exchanged using the RMDP. RMDP has node information, which maintains the mapping information between DCM device identifier and physical network identifier, such as the IP address and port number in IP network. If there is a device management server (DMS) in an administrative domain, the RMDP might be able to obtain the node information about all devices that

are connected in the administrative domain from the DMS. Note : There are several ways to retrieve node information. For example, the RMDP is able to request node information by using the RMDP messages when there is no DMS or when DMS does not response. Therefore the node retrieval mechanisms depend on implementation. When the RMDP retrieves the node information without DMS, the integrity of node information may not be guaranteed

After RMDP retrieves the target node information, DCMP messages, such as 'DEVICE_INFORMATION_REQUEST' or 'DEVICE_CONTROL_REQUEST', can be transferred to the target device using RMDP.

6 DCM Service Environments

6.1 Case 1: Local Network with Device Management Server

Figure 2 shows an example of DCM service environment where all devices and a management server are connected in a local network with device management server (DMS). The DMS retrieves device information in the administrative domain and manages devices with DCMP. In this environment the information device, such as smart phone, is able to control the devices using the DCMP. When smart phone join the administrative domain, RMDP on smart phone could find the DMS and receive the node information about whole devices which are connected in that administrative domain from the DMS. Then DCMP on the smart phone sends the device discovery request message to the other devices and receives the response message by using the RMDP. After that, smart phone is able to see the all devices in the network. If the target device is selected and control information is available by user, DCMP generates and transmits the device control request messages to the target device by using the RMDP.

Figure 2 — DCM service environment case 1: Local network with device management server

6.2 Case 2: Local Network without Device Management Server

Figure 3 shows the example of DCM service environment where all devices are connected in the local network without device management server. The information device, such as smart phone, can control the DCM devices by using the DCM based application. When a node discovery request message is broadcasted by RMDP on the smart phone, RMDPs on the other devices which receive the node discovery request message would response with their node information. Then DCMP on the smart phone sends the device discovery request message to the other devices and receives the response message by using the RMDP. After that, smart phone is able to see the all devices in the network. If the target device is selected and control information is entered by user, DCMP generates the device control request message and sends that control message to the target device by using the RMDP.

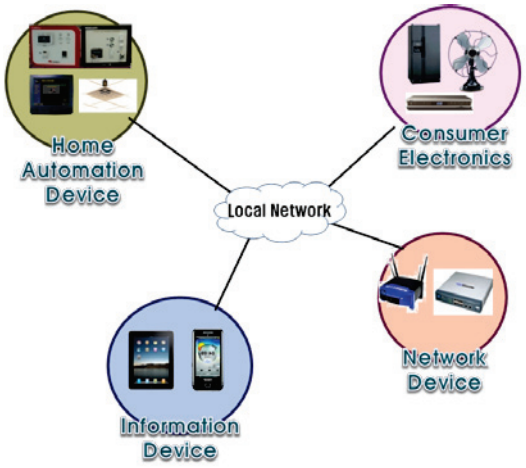

Figure 3 — DCM service environment case 2: Local network without device management server

6.3 Case 3: Public Network with Device Management Server

Recently, more devices are connected to the internet directly and provide various services to users as shown in Figure 4. For example, one of the health care product manufacturers sells the scales that are connected to the internet and upload the user's weight and fat data to the manufacturer server automatically. Then, users can check the changes of their own body weight and fat easily by using the smart phone application. For this service, each scale sends the node advertisement message to the device management server using the RMDP that is installed when the device is manufactured. Then, also DCMP on scale sends the device advertisement message, device registration message and user registration message to the device management server using the RMDP. After these processes, DCMP on scale is able to upload their own data to device management server using RMDP.

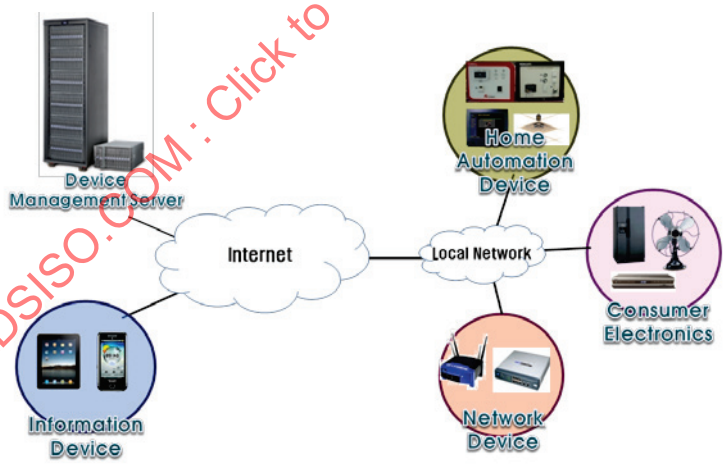

Figure 4 — DCM service environment case 3: Public network with device management server

7 Requirements

7.1 Self-Configuration

When a device is connected to a network, the device is automatically plugged in and is used by many different users. The auto configuration can be achieved in two levels. First is the network auto configuration. When a device is connected to the network, the network configuration shall be set up

automatically. For example, when a device is connected to the IP network, IP address could be assigned by the DHCP (Dynamic Host Configuration Protocol) or Auto IP.

In addition, all service available in a network are detected and advertised automatically. Each device has different capabilities and thus available services are different. Therefore users know a set of available services for each device. Then user detects available services and start services among them. The service detection and running is performed automatically without any intervention.

7.2 Multiple Administrative networks

Devices are connected to the different networks where it is located. So, the network protocols for the networks shall not be network dependant. This means that network independent device management mechanism is required regardless of where a device is located.

Since a device is access through multiple administrative network depending on the network hierarchy. Different administrative policy may be enforced to each device where it is located. So, the device management scheme is required to deal with the multiple administrative policies.

7.3 Uniform device interface

A user wants to control many different types of device regardless of the manufacturer, device type and device location. However, different types of device provide different device functions while same type of devices is provide some common functions. So, device control and management architecture covers various types of devices. Since the device type, manufacturer, and capabilities are different, it is required to provide uniform device control and management interface. Also, a device will provide an interface to support special device functions such as manufacturer specific control function and user defined functions.

7.4 Common device control and management

Device functions are categorized into information retrieval, control, and management, diagnostic and debugging. Recently, all devices are connected through a network. So, it is possible to control and to manage a device remotely. When a device has some problems or it is required to update or to monitor device status, it is also possible to do it remotely. For this, each device shall provide the functions to exchange remote maintenance commands by the network. So, it is required to define the remote maintenance functions and to define protocols for it. The remote maintenance function includes reboot, firmware update, and application service update. Also, it is required optionally to exchange log and debug information among devices. This may require file upload and download protocols to be defined.

7.5 Open Service Interface

For smart services, the service provider should implement a smart service with different types of smart devices. When device control and management (DCM) provides uniform interfaces for any types of services, then it is easy to implement various smart services. All different types of users directly connect all devices. Therefore, a single management server manages all devices in an administrative domain and all different types of users share its information.

7.6 Security and privacy concerns

Since a device is shared by many users, illegal access by the illegal users shall be prohibited. So, any access attempts to the device are verified. Using the security mechanism, lower level users may control and manage the device with limited functions. But device critical functions such as firmware upgrade and reboot are only limited to the registered users.

8 Design Principles

8.1 Auto Configuration

The devices and their service will be configured automatically without any intervention from users or administrator. For the network auto configuration, the underlying networks should support auto configuration mechanism. For IP networks, IP address shall be automatically configured through DHCP and Auto IP mechanism. When auto configuration is not supported, manual mechanism should be supported.

Service discovery and advertisement mechanism shall be enforced. For the synchronization of the service information, each device shall advertise when it is connected to the network for the first time. Also, the device information is periodically broadcasted to all devices for the synchronization.

8.2 Network Abstraction

Since the device is operating in the different networks, network heterogeneity shall be dealt with. For this, the physical network is abstracted. This means that the device management protocol messages are exchanged and delivered to other objects in the network regardless of what kind of physical network is used.

For the network abstraction, we define a network independent message interface layer and network adaptation layer. The network adaptation layer provides a capability to deliver message in each physical networks such as TCP/IP, RS485, RS422, GSM/CDMA, etc. The message interface layer provides an interface for the network adaptation layer and its consumer. The message consumer sends and receives message without considering underlying physical network.

8.3 Common control and management protocols

Since device type, function and capability is different, the device is also abstracted so as to control and manage device. The device is classified into several categories based on its functions. And, its functions and information for each device type is abstracted. The device information is categorized into device basic information, configuration, and control functions as well as the basic maintenance functions. By classifying the information and functions, we abstract device and has a uniform view for all kinds of devices. With the abstracted device information, device is controlled and managed uniformly.

8.4 Transaction Management

The device management protocols may include the management for the operations. Since the message can be lost and the destination device is not available, then the requester knows about the status of its request. Also, when several requests are issued, then a user wants to know which requests are in trouble and which are successful. For this, we define a transaction, which consists of one or more messages to accomplish one operation in a device.

In this specification, five types of transactions are defined: Event, Request/Response, File Upload, File Download, and Apply. Event transaction is used to notify some events to the registered users. Request/Response transaction is usually used for the information or control request and response. File Upload/Download Transaction is used for the file uploads and downloads. Apply transaction is used when system critical action such as reboot and firmware update is requested and its response takes some time.

8.5 Device Security

Every device may have different level of security. However, not all functions are required to enforce the security. In the global mode, a user authentication is required. Each administrative network has its own security policy. However, the access to the device is available for all access. But, the critical operations shall be prohibited to all users. For the critical operations, administrative policy shall be enforced. Some operations are required to access device with secure code for all devices.

