INTERNATIONAL STANDARD

ISO/IEC 16512-2

Third edition
2016-04-01

Information technology — Relayed multicast protocol: Specification for simplex group applications

Technologies de l'information — Protocole de multidiffusion relayé: Spécification relative aux applications de groupe simplex

Reference number
ISO/IEC 16512-2:2016(E)

© ISO/IEC 2016



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

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.

This third edition cancels and replaces the second edition (ISO/IEC 16512-2:2011), which has been technically revised.

ISO/IEC 16512-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in collaboration with ITU-T. The identical text is published as ITU-T X.603.1 (03/2012).

ISO/IEC 16512 consists of the following parts, under the general title *Information technology — Relayed multicast protocol*:

— *Part 1: Framework*

— *Part 2: Specification for simplex group applications*

© ISO/IEC 2016 – All rights reserved

CONTENTS

Page

1 Scope 1
2 References 1
2.1 Identical Recommendations | International Standards 1
2.2 Additional references 1
3 Definitions 2
3.1 Terms defined elsewhere 2
3.2 Terms defined in this Recommendation 2
4 Abbreviations and acronyms 3
5 Conventions 4
6 Overview 5
6.1 Overview of basic RMCP-2 5
6.2 Overview of secure RMCP-2 9
6.3 Types of RMCP-2 messages 12
7 Protocol operation for basic RMCP-2 13
7.1 Session manager's operation 13
7.2 Multicast agent's operation 16
8 Protocol operation for secure RMCP-2 31
8.1 Session manager's operation 31
8.2 Multicast agent's operation 35
9 RMCP-2 message format 40
9.1 Common format of RMCP-2 message 41
9.2 Control data format 41
9.3 RMCP-2 messages 42
9.4 RMCP-2 controls 64
10 Parameters 84
10.1 Identifications used in RMCP-2 85
10.2 Code values used in RMCP-2 85
10.3 Code values for sub-control types 87
10.4 Code values used in control 89
10.5 Code values related to the security policy for a secure RMCP-2 90
10.6 Timer related parameters 91
10.7 Data profile used in RMCP-2 93
Annex A – Membership authentication mechanism 95
A.1 Overview 95
A.2 Authentication procedure 95
Annex B – Method for sharing session information among multiple SM domains 97
B.1 Overview 97
B.2 Session information sharing between SMs 97
B.3 Supporting session subscription in RMCP-2 between multiple SMs 98
B.4 Supporting a session leave in RMCP-2 between multiple SMs 99
B.5 Other operations of the RMA in RMCP-2 between multiple SMs 100
B.6 RMCP-2 messages for sharing session information between SMs 100
Annex C – Tree configuration rules 102
C.1 Bootstrapping rule 102
C.2 HMA selection rule 102
C.3 CMA acceptance rule 103
C.4 Parent decision rule 103
C.5 Tree improvement rule 104
C.6 PMA's expulsion rule 104
Annex D – Real-time data delivery scheme 105

Page
D.1 Overview ... 105
D.2 Data delivery scheme using IP-IP tunnel mechanism ... 105
D.3 Data delivery scheme using a non-encapsulation scheme ... 106
Annex E – Reliable data delivery scheme ... 108
E.1 Overview ... 108
E.2 Issues for a reliable data delivery scheme ... 108
E.3 Operation ... 109
E.4 Service data unit (SDU) format ... 111
E.5 Data profile ... 111
Annex F – RMCP-2 API ... 113
F.1 Overview ... 113
F.2 RMCP-2 API functions ... 114
Annex G – RMCP-2 service scenario ... 117
Annex H – Bibliography ... 119

Introduction

This Recommendation | International Standard specifies the relayed multicast protocol part 2 (RMCP-2), which is an application-layer relayed multicast protocol for simplex group applications. RMCP-2 can construct an optimized and robust one-to-many relayed multicast delivery path over IP-based networks. Along the relayed multicast delivery path, several types of data delivery channels can be constructed according to the requirements of the application services.

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Relayed multicast protocol: Specification for simplex group applications

1 Scope

This Recommendation | International Standard specifies the relayed multicast protocol part 2 (RMCP-2), an application-layer protocol that constructs a multicast tree for data delivery from one sender to multiple receivers over an IP-based network, where IP multicast is not fully deployed. RMCP-2 defines relayed multicast data transport capabilities over IP-based networks for simplex group applications.

This Recommendation | International Standard specifies the following:

a) descriptions of the entities, control and data delivery models of RMCP-2;

b) description of the functions and procedures of multicast agents (MAs) to construct a one-to-many relayed data path and to relay data for simplex communication;

c) description of the security features of the basic RMCP-2; and

d) definitions of messages and parameters of the basic RMCP-2 and secure RMCP-2.

Annex A defines a membership authentication procedure for use with the secure RMCP-2. Annex B provides a method for sharing information among session managers (SMs) when multiple SMs are used. Annexes C-G provide informative material related to RMCP-2. Annex H contains an informative bibliography.

2 References

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

– Recommendation ITU-T X.603 (2012) | ISO/IEC 16512-1:2012, Information technology – Relayed multicast protocol: Framework.

2.2 Additional references

– ISO/IEC 9797-2:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function*.

– ISO/IEC 9798-3:1998, *Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques*.

– ISO/IEC 18033-2:2006, *Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers*.

– ISO/IEC 18033-3:2010, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*.

– ISO/IEC 18033-4:2011, *Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers*.

– IETF RFC 768 (1980), *User Datagram Protocol*.

– IETF RFC 793 (1981), *Transmission Control Protocol*.

– IETF RFC 2003 (1996), *IP Encapsulation within IP*.

– IETF RFC 3830 (2004), *MIKEY: Multimedia Internet KEYing*.

– IETF RFC 4279 (2005), *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*.

– IETF RFC 4535 (2006), *GSAKMP: Group Secure Association Key Management Protocol*.

- IETF RFC 4960 (2007), *Stream Control Transmission Protocol*.
- IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.
- IETF RFC 6066 (2011), *Transport Layer Security (TLS) Extensions: Extension Definitions*.

3 Definitions

For the purposes of this Recommendation | International Standard, the following definitions apply.

3.1 Terms defined elsewhere

The following terms are defined in Rec. ITU-T X.603 | ISO/IEC 16512-1:

3.1.1 IP multicast: Realizes a multicast scheme in an IP network with the help of multicast-enabled IP routers.

3.1.2 multicast: A data delivery scheme where the same data unit is transmitted from a single source to multiple destinations in a single invocation of service.

3.1.3 multicast agent (MA): An intermediate node which relays group application data.

3.1.4 relayed multicast protocol (RMCP): A protocol to realize the relayed multicast scheme using end hosts.

3.1.5 simplex: Wherein only one sender is send-only and all others are receive-only.

3.1.6 session manager (SM): A relayed multicast protocol (RMCP) entity that is responsible for the overall RMCP operations.

3.2 Terms defined in this Recommendation

This Recommendation | International Standard defines the following terms:

3.2.1 basic RMCP-2: The relayed multicast protocol for simplex group applications, defined in clause 7.

3.2.2 candidate HMA: The MA that is able to assume the role of an HMA, when the original HMA leaves or is terminated. In the basic RMCP-2, the MA indicates the RMA while it indicates the DMA in a secure RMCP-2.

3.2.3 child multicast agent (CMA): The next downstream MA in the RMCP-2 data delivery path.

3.2.4 closed group: A member multicast (MM) group in which all the RMAs have been allocated a service user identifier from the content provider before subscribing to the secure RMCP-2 session.

3.2.5 dedicated multicast agent (DMA): An intermediate MA pre-deployed as a trust server by the session manager (SM) in an RMCP-2 session.

3.2.6 group attribute (GP_ATTRIBUTE): An attribute that defines whether or not the content provider controls the admission of RMAs to the secure RMCP-2 session.

3.2.7 head multicast agent (HMA): A representative of the MA inside a local network where the multicast is enabled.

3.2.8 member multicast region (MM region): A management zone defined by the use of one or more group keys Kg.

3.2.9 member multicast group (MM group):

1) (in unicast network) a group consisting of one DMA and multiple RMAs sharing the same group key Kg.
2) (in multicast network) a group consisting of one HMA, multiple RMAs together with one or more candidate HMAs sharing the same group key Kg.

3.2.10 multicast agent ID (MAID): A 64-bit value that identifies the MA. MAID consists of the local IP address, port number and serial number.

3.2.11 open group: An MM group in which none of the RMAs require a service user identifier before subscribing to the secure RMCP-2 session.

3.2.12 parent multicast agent (PMA): The next upstream MA in the RMCP-2 data delivery path.

3.2.13 pseudo-HB message: An HB message that indicates a fault in the delivery path of the RMCP-2 tree. The originator of a pseudo-HB message is the MA that discovers this fault.

3.2.14 receiver multicast agent (RMA): The MA attached to the receiving application in the same system or local network.

3.2.15 regular HB message: An HB message that is relayed without interruption along the path of the RMCP-2 tree from the SMA to the receiver of the message. The originator of a regular HB message is the SMA.

3.2.16 relayed multicast: A multicast data delivery scheme that can be used in unicast environments, which is based on the intermediate nodes to relay multicast data from the media server to media players over a logically configured network.

3.2.17 relayed multicast region (RM region): A management zone defined by the use of the session key Ks.

3.2.18 RMCP-2: A relayed multicast protocol for simplex group communication applications.

3.2.19 RMCP-2 session: A session which provides a certain RMCP-2 service.

3.2.20 secure RMCP-2 protocol: The relayed multicast protocol supporting the security features for simplex group applications defined in clause 8.

3.2.21 security policy: The set of criteria for the provision of security services, together with the set of values for these criteria, resulting from agreement of the security mechanisms defined in clause 8.1.4.

3.2.22 sender multicast agent (SMA): The MA attached to the sender in the same system or local network.

3.2.23 session ID (SID): A 64-bit value that identifies the RMCP-2 session. SID is a combination of the local IP address of the session manager (SM) and the group address of the session.

3.2.24 TLS_CERT mode: A mode of transport layer security (TLS) defined in IETF RFC 5246 for the authentication of MAs using a certificate.

3.2.25 TLS_PSK mode: A mode of transport layer security (TLS) defined in IETF RFC 4279 for the authentication of MAs using a pre-shared key for the TLS key exchange.

4 Abbreviations and acronyms

For the purposes of this Recommendation | International Standard, the following abbreviations apply.

ACL	Access Control List
AUTH	Authentication
CEK	Content Encryption Key
CGSPRBG	Cryptographically Secure Pseudo-Random Bit Generator
CMA	Child Multicast Agent
CP	Content Provider
DMA	Dedicated Multicast Agent
FAILCHECK	Failure check request message
HANNOUNCE	HMA announce message
HB	Heartbeat message
HLEAVE	HMA Leave message
HMA	Head Multicast Agent
HRSANS	Head Required Security Answer
HRSREQ	Head Required Security Request
HSOLICIT	HMA Solicit message
IP-IP	IP in IP
KEYDELIVER	Key Delivery
LEAVANS	Leave Answer message
LEAVREQ	Leave Request message