BS ISO/IEC 16512-2:2016

BSI Standards Publication

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

bsi.

...making excellence a habit.™

Document Sharing Hub

Full document details: BS ISO/IEC 16512-2:2016

National foreword

This British Standard is the UK implementation of ISO/IEC 16512-2:2016.

The UK participation in its preparation was entrusted to Technical Committee ICT/-/1, Information systems co-ordination.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2016.
Published by BSI Standards Limited 2016

ISBN 978 0 580 90434 9

ICS 35.100.70

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 April 2016.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 16512-2:2016

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)

Documents
Document Sharing Hub

© ISO/IEC 2016

Full document details: BS ISO/IEC 16512-2:2016

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

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 16512-2:2016

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 16512-2:2016

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 16512-2:2016

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.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 16512-2:2016

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*.

AVA Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

– 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.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

MA	Multicast Agent
MAID	Multicast Agent Identification
MM	Member Multicast
PMA	Parent Multicast Agent
PPROBANS	Parent Probe Answer message
PPROBREQ	Parent Probe Request message
RELANS	Relay Answer message
RELREQ	Relay Request message
RMA	Receiver Multicast Agent
RMCP	Relayed Multicast Protocol
RTT	Round Trip Time
SDP	Session Description Protocol
SDU	Service Data Unit
SECAGANS	Security Agreement Answer
SECAGREQ	Security Agreement Request
SECALGREQ	Security Algorithms Request
SECLIST	selected Security LIST
SID	(RMCP-2) Session Identification
SINFO	Session Information
SM	Session Manager
SMA	Sender Multicast Agent
SMNOTI	SM Notification
STANS	Status report Answer message
STCOLANS	Status report Collect Answer message
STCOLREQ	Status report Collect Request message
STREQ	Status report Request message
SUBSANS	Subscription Answer message
SUBSREQ	Subscription Request message
TCP	Transmission Control Protocol
TERMANS	Termination Answer message
TERMREQ	Termination Request message
TLS	Transport Layer Security
UDP	User Datagram Protocol

5 Conventions

Code values for message parameters in clause 9 (RMCP-2 messages) and clause 10 (Parameters) are expressed in hexadecimal notation, e.g., 0x14 for 20 in decimal notation.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

6 Overview

The RMCP-2 is an application-level protocol for providing efficient simplex group communication services over IP-network environment which does not have full deployment of IP multicast. This clause gives an overview of the basic RMCP-2 service, entities, protocol and control/data modules, simplex data delivery model, and message types. In addition to the overview of basic RMCP-2, this clause provides the overview of secure RMCP-2 as well. The basic RMCP-2 refers to the relayed multicast protocol for simplex group applications. The secure RMCP-2 refers to the relayed multicast protocol supporting security features for basic RMCP-2.

6.1 Overview of basic RMCP-2

6.1.1 RMCP-2 service

The RMCP-2 is an application-layer multicast protocol that supports simplex group communication services in IP networks without full deployment of IP multicast. In the simplex group communication services, user data is delivered from a single sender to multiple recipients. To support the simplex group communication, the RMCP-2 uses the relayed multicast mechanism. The RMCP-2 entities configure the data delivery path for simplex group communication. The RMCP-2 entities relay multicast data to other RMCP-2 entities along the constructed data delivery path. The RMCP-2 can support various application services that require simplex group communication, such as multimedia streaming services, file distribution services, e-learning, etc.

Figure 1 shows a typical service model of the RMCP-2 for supporting simplex group communication services in both unicast and multicast network. In RMCP-2, the local network where IP multicast capability is deployed is called a multicast network. One such example of a multicast network is a campus network with the IP multicast capability deployed. For multicast networks, the RMCP-2 constructs a multicast transport connection. In RMCP-2, the network without an IP multicast capability is called a unicast network. For unicast networks, the RMCP-2 constructs a unicast transport connection between MAs. Thus, it is possible for RMCP-2 to deliver multicast data to applications in both a unicast network and multicast network.

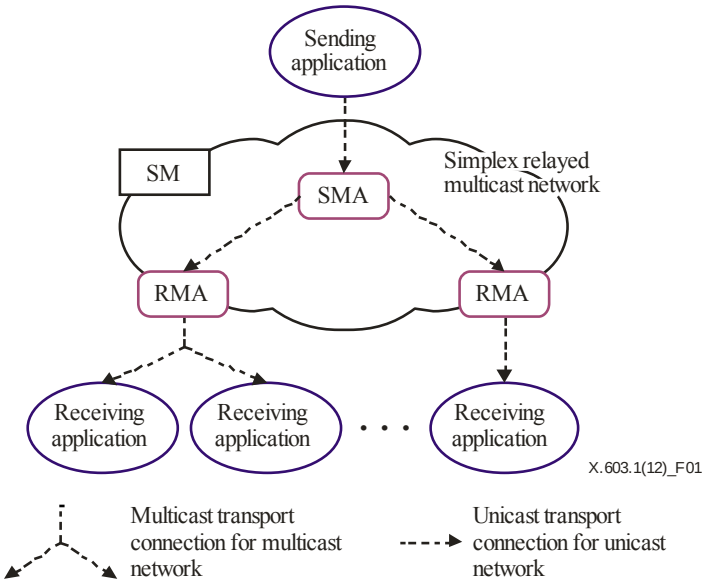

Figure 1 – RMCP-2 service model

The entities of the RMCP-2 are multicast agents (MAs) and a session manager (SM). The SM manages the group membership and RMCP-2 session by providing the configuration-related information to the MA to construct a simplex relayed multicast network, and by monitoring the RMCP-2 session. The MA is an intermediate node that delivers multicast data.

The following features of the RMCP-2 support the simplex group communication:

a) The RMCP-2 constructs a logical control path for each RMCP-2 session by using one or more MAs.

b) The control path is the basis of the data delivery path, which supports the delivery of multicast data in a reliable or real-time manner.

c) The control path consists of logical links between MAs.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

d) The RMCP-2 has the capability of selecting optimal peers to configure logical links. The selection of optimal peers may be based on various metrics. Examples of such metrics include hop count, delay, and/or bandwidth.

e) The RMCP-2 supports group communication using IP multicasting.

f) The RMCP-2 allows MAs to join or leave at any time during the RMCP-2 session.

g) The RMCP-2 manages the MAs of RMCP-2 session by using membership monitoring and expulsion.

h) The RMCP-2 provides an auto-configuration mechanism in constructing the data delivery path for the simplex group communication.

i) The RMCP-2 supports network fault detection and service recovery.

6.1.2 RMCP-2 entities

This clause provides a description of RMCP-2 entities, these are SM and MA. The RMCP-2 entities follow the same definition as defined in Rec. ITU-T X.603 | ISO/IEC 16512-1. The SM manages group membership and RMCP-2 sessions. The MA constructs a multicast data delivery path between senders and receivers and relays the multicast data along the constructed path. The MA is required to support capabilities in both the sending and receiving of multicast data. The MA can be implemented as an agent running on an end-system, server or set-top box. The method of implementation of the MA are out of the scope of this Recommendation | International Standard.

RMCP-2 configures the data delivery path for simplex group communication using the following configuration:

a) one SM;

b) one sender multicast agent (SMA) per sender application;

c) one or more receiver multicast agents (RMAs);

d) one or more sending or receiving group applications.

SM supports the following functions:

a) session initiation;

b) session termination;

c) membership management;

d) session management.

An MA, which refers to both SMA and RMA, supports the following functions:

a) session initiation (applied for SMA only);

b) session subscription;

c) session join;

d) session leave;

e) session maintenance;

f) session status report;

g) application data delivery.

6.1.3 Protocol modules of RMCP-2

The entities in the RMCP-2 use two different types of module, i.e., control module and data module. The control module is used to control the RMCP-2 session. The data module is used to deliver multicast data to the data module of other MAs or to the applications. The SM controls the RMCP-2 sessions and does not participate in data delivery. Therefore, the SM has only the control module.

The MA has the control module and data module to construct paths for control and data delivery. Figure 2 shows the three types of path and interfaces that are used in RMCP-2, listed below.

– The control path between the control modules of the SM and MA and between the control modules of MAs;

– a data path between the data modules of MAs;

– an internal interface between the control module and data module within the MA.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

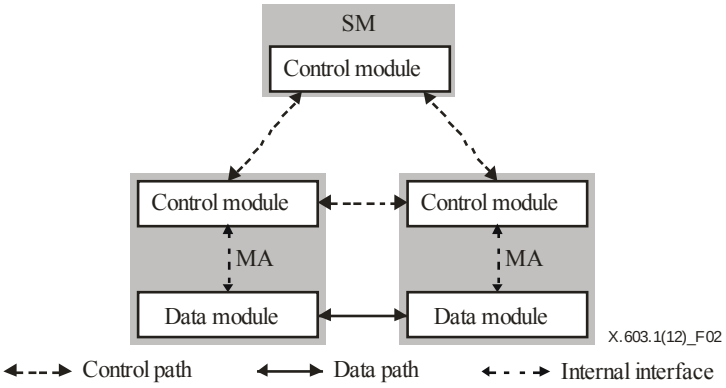

Figure 2 – Three types of interfaces in RMCP-2

The SM is responsible for controlling and managing the RMCP-2 session. The messages used by the SM should be delivered in a reliable manner to provide a stable RMCP-2 session. For reliable delivery, the SM uses the TCP defined in IETF RFC 793 for the transport protocol. Figure 3 shows a protocol stack of an SM.

Control module of SM
TCP
IP (unicast)

Figure 3 – Protocol stack of SM

An MA which refers to both the SMA and the RMA, constructs a relayed multicast delivery path from one sender to many receivers and forwards data along the constructed path. An MA consists of a control module and a data module.

The MA's control module configures the RMCP-2 control tree from the SMA to the leaf MAs. The control module is used for RMCP-2 tree control. The MA's control module uses the TCP in the unicast network and UDP defined in IETF RFC 768 in a multicast network. Figure 4 shows the protocol stack of an MA's control module.

Control module of MA	
TCP	**UDP**
IP (unicast)	**IP (multicast)**

Figure 4 – Protocol stack of an MA's control module

The MA's data module relays application data along the constructed data delivery path. The characteristics of the data delivery channel may vary depending on the application. For example, a real-time data delivery channel is needed for real-time application services, and a reliable data delivery channel is needed for reliable application services. Thus, RMCP-2 is independent of the transport protocols for delivering user data to support various types of applications. The multicast application of an MA can send and receive multicast data from the data module. Figure 5 shows the protocol stack of the MA's data module.

To ensure that RMCP-2 can adopt any kind of data transport mechanism, two MAs (namely, the parent multicast agent (PMA) and the child multicast agent (CMA)) construct a data delivery path on the control tree by exchanging the data profiles.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

Data module of MA
L4 transport protocol
IP (unicast, multicast)

Figure 5 – Protocol stack of an MA's data module

The topologies of the two paths for control and data delivery are usually the same, because a data delivery path is constructed along the RMCP-2 control tree. Along the data delivery path, the application data from the SMA can be delivered to each leaf MAs. For more information, annexes D and E present two feasible real-time and reliable data delivery schemes.

6.1.4 RMCP-2 control model

The RMCP-2 configures a one-to-many tree for control connection. The RMCP-2 tree is suitable for multicast data delivery and is robust to network faults with auto-configuration and self-improvement capability. The RMCP-2 tree is controlled by the SM. The SM can configure, control and monitor the RMCP-2 tree. The SM has the complete list and the connection status information of the MAs of the RMCP-2 session. Figure 6 shows the control connection of the RMCP-2.

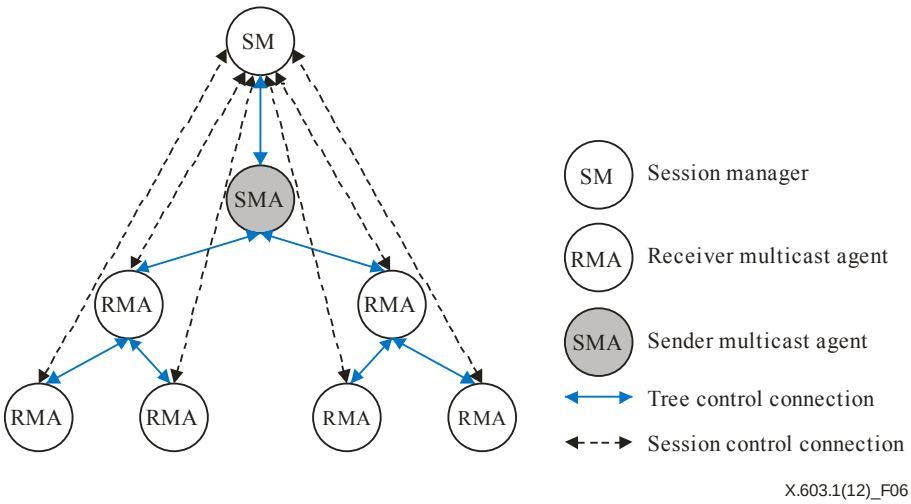

Figure 6 – Control connection of RMCP-2

The control connection of RMCP-2 consists of an SM, an SMA and RMAs. The following are the control connections for RMCP-2 service:

- tree control connection between MAs forming an RMCP-2 control tree;
- session control connection between the SM and MAs.

The SM is a dedicated entity that is pre-deployed by the RMCP-2 service provider. This entity provides control and data delivery paths for applications served by MAs. The MA is a dynamic entity that can join and leave the RMCP-2 session.

6.1.5 Simplex delivery model of RMCP-2

The target services of RMCP-2 are simplex broadcasting services, such as Internet live TV and software dissemination. In these service models, building an optimal data delivery path from a sender to multiple receivers is important. RMCP-2 can support a simplex data delivery model by using the MA's control and data modules.

The data delivery path that the RMCP-2 considers is a per-source relayed multicast tree. Along the per-source relayed multicast path, a unidirectional real-time or reliable data channel can be constructed. Figure 7 shows one of the possible relayed multicast trees configured by RMCP-2 for simplex real-time or reliable applications.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

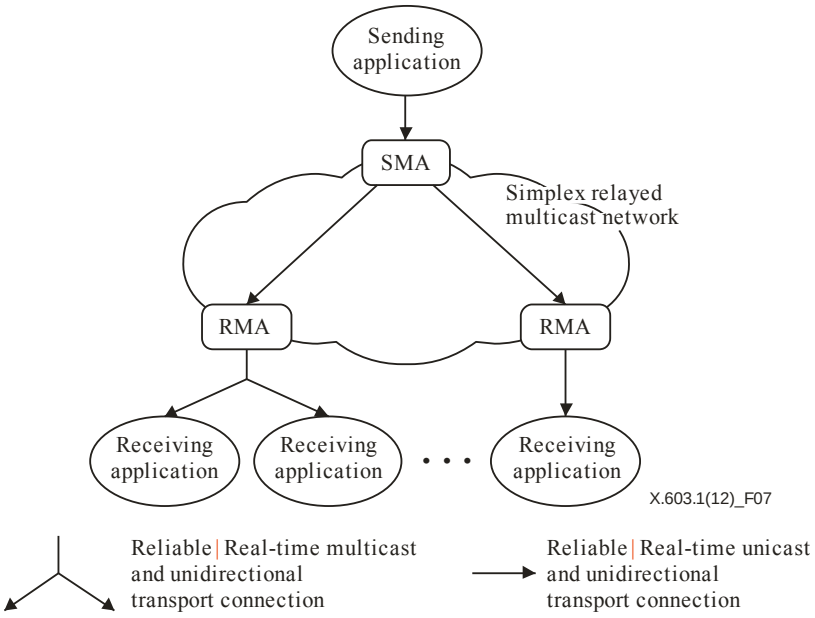

Figure 7 – Relayed multicast tree configured by RMCP-2

6.2 Overview of secure RMCP-2

6.2.1 Secure RMCP-2 entities

The secure RMCP-2 supports security functions of the RMCP-2 used for relayed multicast data transport through unicast communication over the Internet.

The secure RMCP-2 entities correspond to those described in the basic RMCP-2 except that a new type of MA, a dedicated multicast agent (DMA), has been introduced. A dedicated multicast agent is an intermediate MA pre-deployed as a trust server by the SM. For secure communication, each session consists of an SM, an SMA, DMAs and RMAs, together with a single sending application and multiple receiving applications. Their topology, as shown in Figure 8, corresponds with that in the basic RMCP-2 (see clause 6.1).

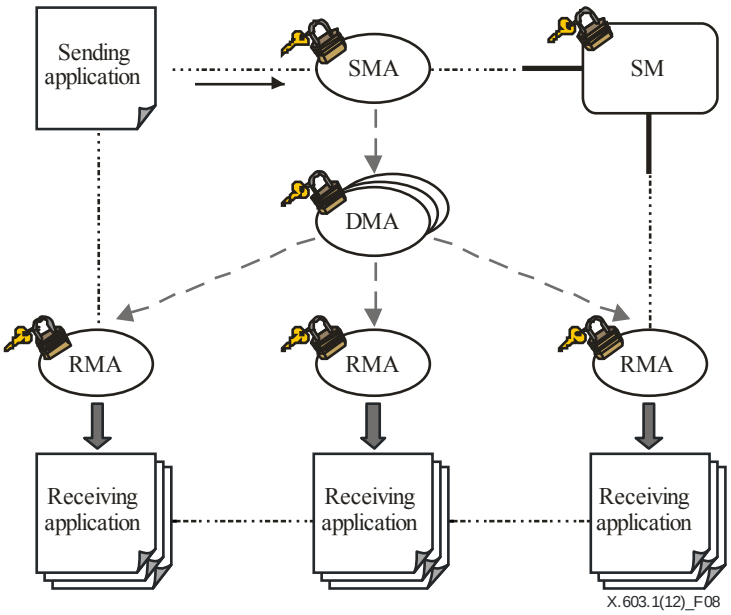

Figure 8 – RMCP-2 service topology with security

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

6.2.2 Session manager

The SM is responsible for maintaining session security, which includes the management of service membership, the management of key and ACL for DMA and RMA, and message encryption/decryption together with the SM functions of basic RMCP-2. Figure 9 shows an abstract protocol stack for the operation of SM functions. The SM has TLS and multicast session security modules for the provision of security. TLS is used for the initial authentication of DMAs and RMAs when they join the session. The multicast session security module performs the following security functions after the completion of TLS authentication:

a) security policy;

b) session admission management;

c) session key management;

d) access control list management;

e) secure group and membership management;

f) message encryption/decryption.

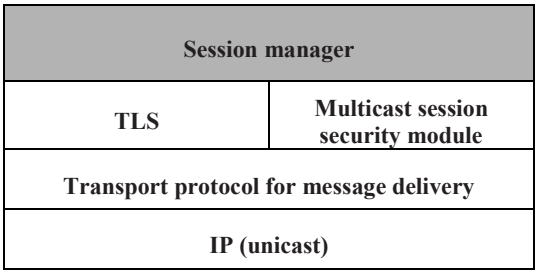

Figure 9 – Internal structure of the SM of secure RMCP-2

6.2.3 Dedicated multicast agents

DMAs are in charge of the secure establishment and maintenance of the RMCP-2 tree, support of membership authentication and data confidentiality. Figure 10 shows the internal structure of the DMAs with modules for key/message security management and group/member security management. These modules support the following security functions:

Key/message security management module

a) group key management;

b) message encryption/decryption;

c) content encryption key management.

Group/member security management module

a) secure tree configuration;

b) session key management;

c) secure group and membership management.

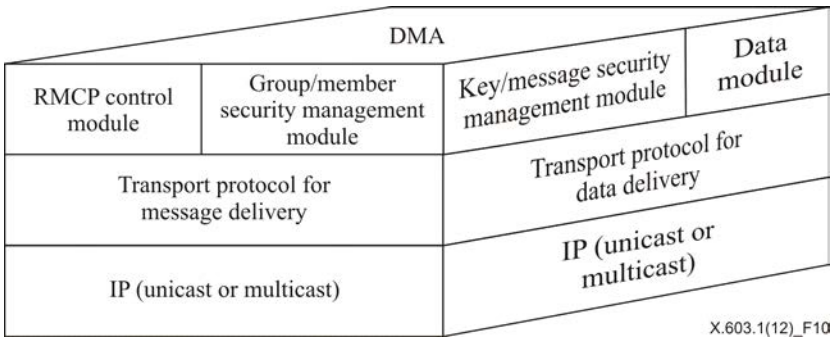

Figure 10 – Internal structure of the DMA of secure RMCP-2

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

6.2.4 Sender and receiver multicast agents

The internal structure of the SMA and RMAs is shown in Figure 11. The structure is the same as for DMAs except that the group security management module is not included.

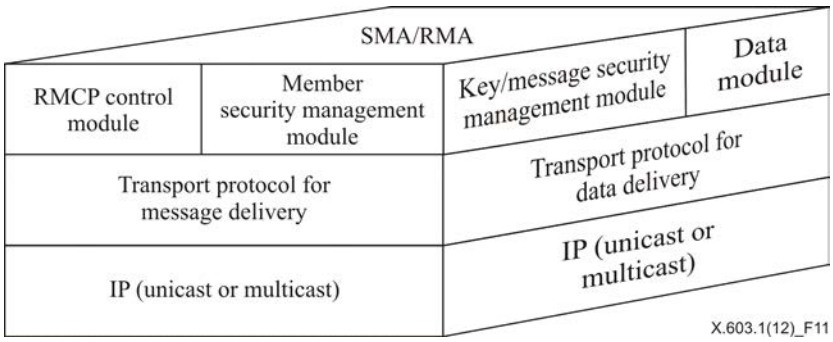

Figure 11 – Internal structure of the SMA and RMA of a secure RMCP-2

6.2.5 Protocol modules of secure RMCP-2

The protocol modules for the SM, group/member security management of MAs and key/message security management of MAs are shown in Figures 12, 13 and 14. They correspond to the protocol stacks in the basic RMCP-2 in clause 6.1.2 (see Figures 3, 4 and 5) but also include the TLS protocol and the multicast session security module.

The secure RMCP-2 supports the general encryption/decryption algorithms of TLS for a variety of common applications. The SM and MAs (SMA, DMAs and RMAs) share the security information described in the security policy. The multicast session security module contains common symmetric encryption/decryption algorithms, authentication mechanisms and multicast security modules related to RMCP-2 security functions.

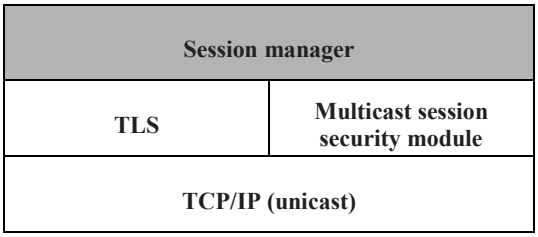

Figure 12 – Protocol module of the SM of a secure RMCP-2

The SM messages and the group/member security management messages of MAs are transmitted reliably through the TCP.

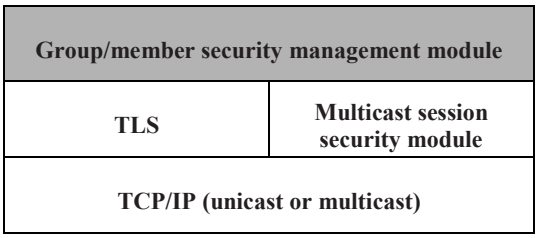

Figure 13 – The group/member security management module of an MA of a secure RMCP-2

Key/message security management messages may be transferred using any transport protocol. The transport protocol may be selected according to the nature of the transferred data types. TLS provides secure communication for TCP over unicast communication. The multicast security encryption/decryption and authentication modules protect the multicast packets. These modules contain common symmetric encryption algorithms, hash algorithms, and multicast security modules defined in this Recommendation | International Standard to protect multicast packets.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

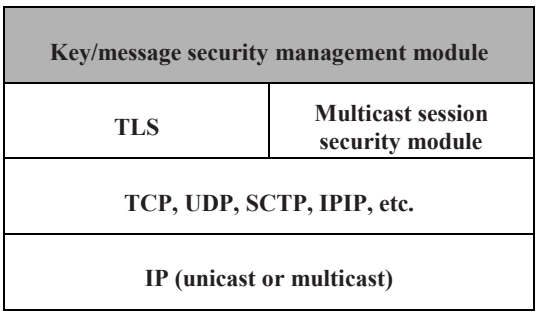

Figure 14 – The key/message security management module of an MA of a secure RMCP-2

6.2.6 Structure of regional security management

For scalable security management, the secure RMCP-2 supports security functions in two independent regions: a relayed multicast (RM) region and a member multicast (MM) region; see Figure 15.

The RM region is a management zone of the session key (Ks). It consists of the SM, the SMA and DMAs in a unicast network.

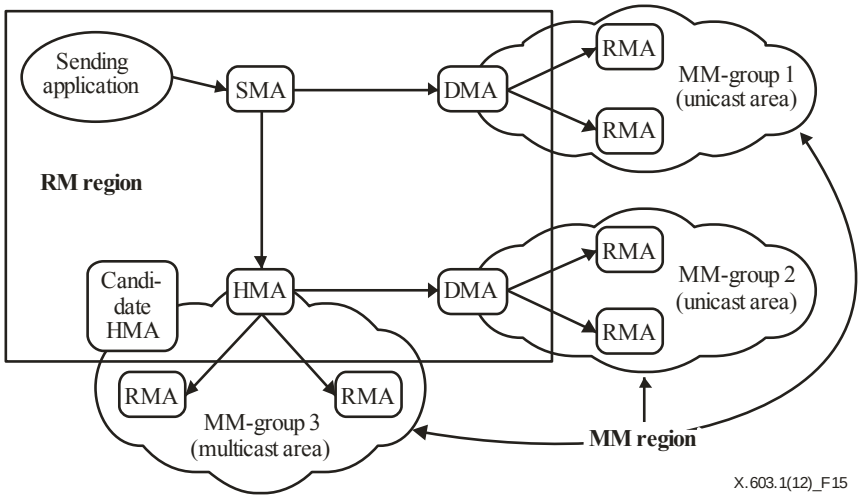

Figure 15 – Security management regions

The MM region is a management zone defined by the use of group keys (Kg). The MM region consists of DMAs and RMAs. They can be connected over a multicast network or a unicast network. The MM region consists of one or more MM groups each using its own Kg group key.

MM groups in a multicast network consist of an HMA, one or more candidate HMAs and multiple RMAs that receive the same multicast messages. Candidate HMAs are DMAs that are not connected to the data delivery tree, but have the capability to assume the role of an HMA if required. MM groups in a unicast network consist of one DMA and multiple RMAs. In both cases, the RMAs are logically connected direct to their parent DMA on the data delivery tree.

Any change in an MM group is localized within the scope of its own MM group.

6.3 Types of RMCP-2 messages

Table 1 lists the RMCP-2 messages with its meaning and the operation that is used.

Table 1 – RMCP-2 messages

Messages	Meaning	Operation
SUBSREQ	Subscription request	Session subscription
SUBSANS	Subscription answer	
PPROBREQ	Parent probe request	Neighbour discovery
PPROBANS	Parent probe answer	

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

Table 1 – RMCP-2 messages

Messages	Meaning	Operation
HSOLICIT	HMA solicit	Management in multicast network
HANNOUNCE	HMA announce	
HLEAVE	HMA leave	
RELREQ	Relay request	Data channel control
RELANS	Relay answer	
STREQ	Status report request	Session monitoring
STANS	Status report answer	
STCOLREQ	Status collect request	
STCOLANS	Status collect answer	
LEAVREQ	Leave request	Session leave/Session tree reconstruction
LEAVANS	Leave answer	
HB	Heartbeat	Session tree maintenance
TERMREQ	Termination request	Session termination
TERMANS	Termination answer	
FAILCHECK	Failure check request	Node failure check
SINFO	Session information	Interworking between SMs which is defined in Annex B
SMNOTI	SM notification	
SECAGREQ	Security agreement request	Establishment of multicast security policy
SECAGANS	Security agreement answer	
SECLIST	Selected security list	
SECALGREQ	Security algorithms request	
KEYDELIVER	Key delivery	Key distribution
HRSREQ	Head required security request	Group member authentication group key distribution ACL management
HRSANS	Head required security answer	

7 Protocol operation for basic RMCP-2

This clause describes the RMCP-2 functions and their operations in detail. All the components described in this clause follow the definitions of Rec. ITU-T X.603 | ISO/IEC 16512-1.

7.1 Session manager's operation

SM manages and controls RMCP-2 sessions through functions of session initialization, termination, membership control and session monitoring.

7.1.1 Session initiation

The SM supports the creation of new RMCP-2 session.

7.1.1.1 Normal procedure

The SMA creates a new session by sending a SUBSREQ message to the SM to create a new RMCP-2 session. The SUBSREQ message contains a session identification (SID) proposed by the SMA. The format of the SID is defined in clause 10.1.1.

The SM creates a new session upon reception of the SUBSREQ message with the proposed SID from the SMA. If the proposed SID is unique, the SM creates an RMCP-2 session with the proposed SID and answers using a SUBSANS message with the SID, MAID of the SMA, and session-related parameters described in clause 10.6. After successful session initiation, the initiated session can be announced through various mechanisms such as a web bulletin board or e-mail. The announcement may include the information on the SM which the RMA should request for session subscription. However, the mechanism of session announcements and the information which a session announcement should include are out of the scope of this Recommendation | International Standard.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

7.1.1.2 Handling SID duplication

The SID includes a multicast address used in multicast applications. Since the use of duplicate multicast addresses can cause the multicast application to receive unwanted multicast data, the SID should be unique for each RMCP-2 session (Figure 16). If the proposed SID is already used by another session, the SM should reject the subscription request and notify the SMA that the SID is already being used. The SM creates a unique SID with a new multicast address and returns a SUBSANS message with the modified SID.

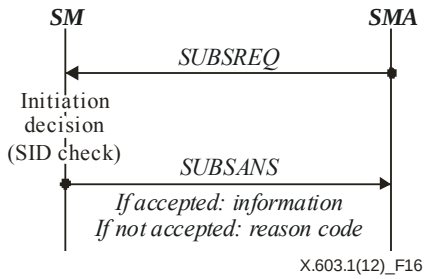

Figure 16 – RMCP-2 session initiation

7.1.2 Membership control

The SM controls the membership of the MA including session subscription and expulsion.

7.1.2.1 Membership subscription

The SM supports the membership subscription from the MA. In order to subscribe to the RMCP-2 session, the MA sends a SUBSREQ message to the SM. Then, the SM makes a decision regarding whether or not to accept the subscription request. If the request is accepted, the SM responds with a SUBSANS message containing the required information on the RMCP-2 session. If not, it returns a SUBSANS message with an adequate reason code.

7.1.2.1.1 MAID allocation

To be identified in the RMCP-2 session, each MA needs to have a unique MA identification (MAID). If the proposed MAID is null or is already in use by another RMCP-2 entity, the SM creates a unique MAID and sends the response message with the created MAID. The MAID can be generated from the IP address and port number of the requesting node. The formats of the MAID are defined in clause 10.1.2.

Figure 17 shows an example of the session subscription procedure. In the example, MA B sends a SUBSREQ message with a proposed MAID. The SM performs a validation check on the proposed MAID and discovers that the proposed MAID is already used by another MA, i.e., MA A. The SM creates a unique MAID and replies with a SUBSANS message with the created MAID. MA B may retry a session subscription with the created MAID sent by the SM.

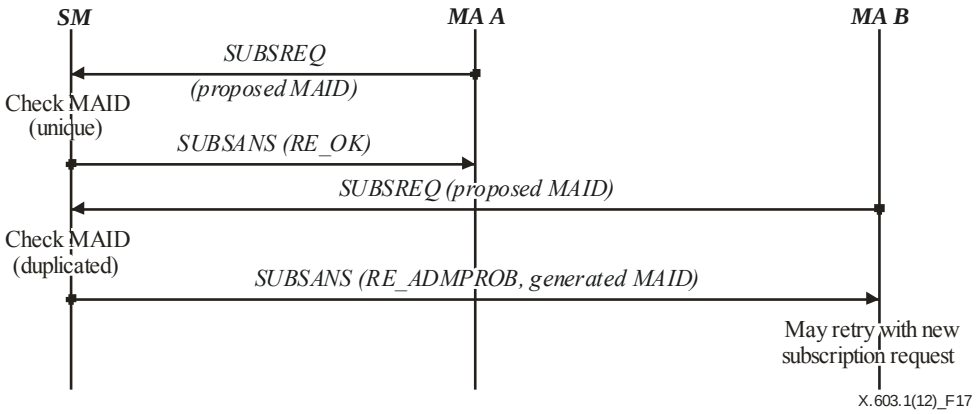

Figure 17 – Session subscription

7.1.2.1.2 Handling extended information

The SUBSREQ message may include a SYSINFO control to specify the information of the subscribing RMCP-2 entity. Such information includes a possible forwarding bandwidth and/or a supportable number of CMAs. The SM can use the received information to classify members for management purposes.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

7.1.2.2 Member expulsion

The SM supports the membership control of MAs to increase manageability of the RMCP-2 service. The membership control is supported through session monitoring as described in clause 7.1.4 and membership control of MAs through expulsion. The SM can expel a specific MA for administrative purposes.

The SM expels a specific MA by sending a LEAVREQ message with the reason code of SM_KICKOUT (see clause 10.4.1). The expelled MA replies with a LEAVANS message and notifies its connected PMA and CMAs before leaving the session. This notification procedure is needed for RMCP-2 tree reconstructions. The detailed procedure for MA leave is described in clause 7.2.4. The message flow of an SM's expulsion of MA B is shown in Figure 18.

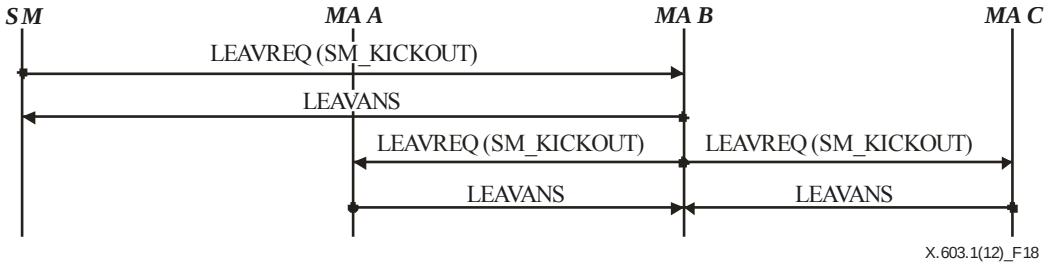

Figure 18 – SM's expulsion of MA B

7.1.3 Heartbeat

The SM checks the status of the RMCP-2 tree by periodically sending a message to the RMCP-2 tree. This message is called an HB message. The heartbeat procedure ensures RMCP-2 tree stability by assisting MAs to synchronize information of the root path.

For the heartbeat procedure, the SM sends an HB message to the SMA of the RMCP-2 tree for each session. The HB message is propagated along the session tree. The SM sends the HB message periodically at every heartbeat message interval (T_HB). The T_HB is defined in clause 10.6.2. Figure 19 shows the periodic heartbeat procedure.

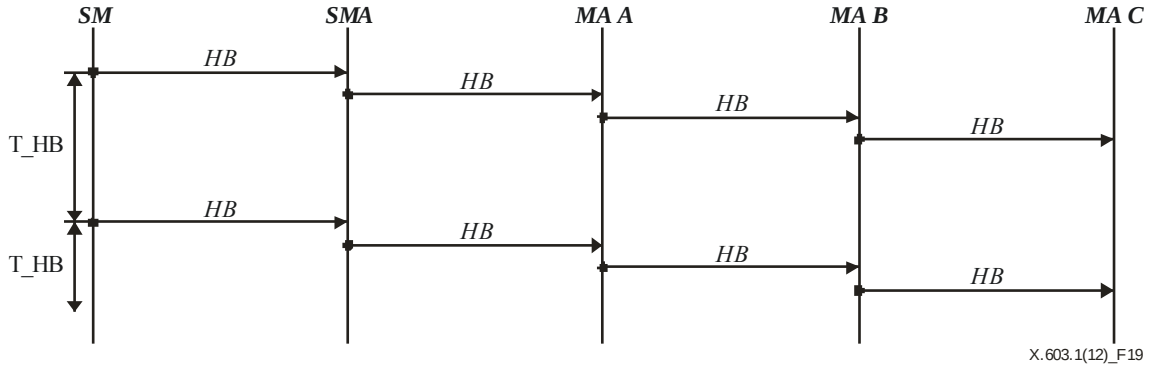

Figure 19 – Periodic heartbeat

7.1.4 Session monitoring

The SM can fetch status information of a specific MA by exchanging a STREQ message and a STANS message. Upon receiving the STREQ message, the MA responds with a STANS message that contains the requested information. Figure 20 shows the procedure of an SM monitoring a specific MA. The "T_REPORT" is the maximum waiting time for STANS message. The T_REPORT is defined in clause 10.6.3. If the STANS message does not arrive within the T_REPORT time, the SM considers that the pertaining MA has left the RMCP-2 session.

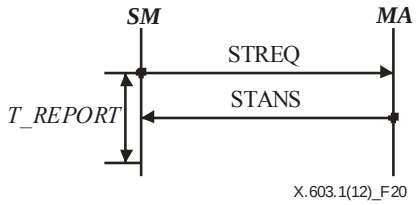

Figure 20 – MA monitoring – Status report

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

The SM can also collect the status information of an entire session or a part of a session. In this case, the SM sends a STREQ message with a TREEEXPLOR control to the most top MA of the part. Upon receiving the STREQ message, the MA should send a STANS message back to the SM with appropriate information on the MA and its children. When the session size is large, the use of this mechanism for the entire session may cause overload to the network and to the system resources. To limit the scope of the monitoring, the status collect message should contain an option for the depth.

7.1.5 Session termination

A session can be terminated due to one of the following two reasons:

1) administrative request;
2) SMA's leave or failure.

Figure 21 shows the SM's session termination procedure.

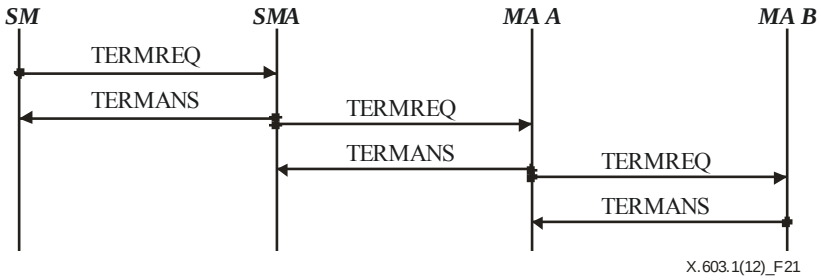

Figure 21 – Session termination issued by an SM

Because an RMCP-2 session can continue only when the SMA is alive, the SMA must notify the SM when it leaves. Having been notified of the SMA's leave, the SM should terminate the session promptly. The session termination caused by SMA's leave is described in clause 7.2.4.4.

7.2 Multicast agent's operation

An MA is an intermediate node or a leaf node in the RMCP-2 tree. An MA can dynamically join or leave the RMCP-2 session anytime. An MA can be categorized into SMA and MA. An SMA is a special form of an MA, which is the sender of the following multicast data as the root of the RMCP-2 tree:

– session subscription;
– dynamic joins and leaves of subscribed session;
– auto-configuration to form an RMCP-2 tree;
– fault detection and recovery.

Unless specified otherwise, an MA means both the MA and SMA.

7.2.1 Session subscription

The MA subscribes to the RMCP-2 session by sending a SUBSREQ message to the SM. The subscription process of the MA and SMA has different meanings and the following describes both types of process.

7.2.1.1 Subscription of an SMA

The subscription of an SMA is part of the session initiation as described in clause 7.1.1. The subscription of an SMA means not only the session subscription but also the session initiation (i.e., creation). An SMA must subscribe to an RMCP-2 session before other MAs. An SMA acts as a root node in the RMCP-2 tree hierarchy.

Figure 22 shows both the procedure of RMCP-2 session initiation and the session subscription of the SMA. The SMA initiates a new RMCP-2 session by sending a SUBSREQ message with a proposed SID which is defined in clause 10.1.1. In Figure 22, the first attempt has failed since the proposed SID has already been used by another session. Thus, the SM sends a SUBSANS message with an indication of session initiation failure and includes a modified SID, which can be used in the new session. The SMA retransmits the SUBSREQ message with a different SID. A different SID can be the modified SID proposed by the SM. Upon receiving the new SUBSREQ message, the SM may decide to accept the request and create a new session. After session creation, the SM sends a SUBSANS message including session-related information, e.g., confirmed SID of the session and session-related parameters. The session-related

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

parameters are information to be used by the SMA and MA for maintaining an RMCP session which is defined by the SM for the pertaining session. The SM provides these parameters in the PARAMETER control in the received SUBSANS message. The details of the PARAMETER control are described in clauses 9.4.14 and 10.6.

After a successful RMCP-2 session initiation, the user of the SMA can announce the RMCP-2 session along with the confirmed SID via a webpage, e-mail, etc. Other MAs can subscribe to the newly established session. The SMA can start the service based on the RMCP-2.

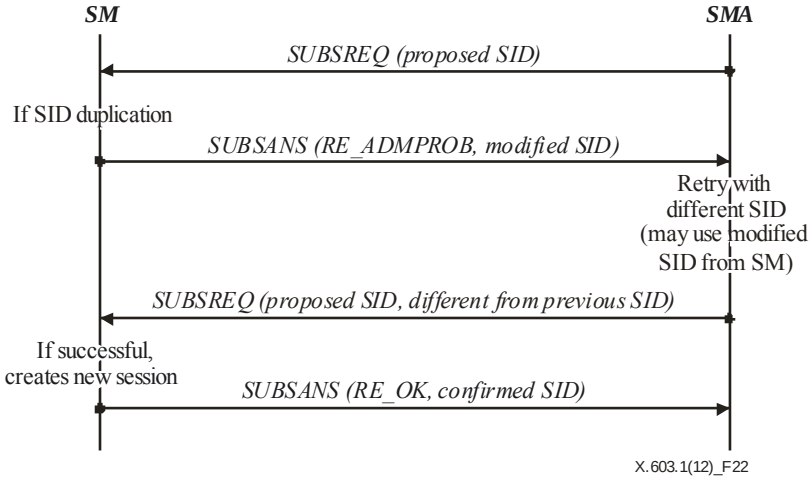

Figure 22 – Session initiation – duplicated SID

7.2.1.2 Subscription of an MA

The subscription of an MA is equivalent to the membership subscription described in clause 7.1.2.1. Figure 17 shows the procedure of an MA subscription (for MA A and MA B). The MA sends a SUBSREQ message to subscribe to a session. If the MA receives a successful SUBSANS message, the MA uses the MAID and the neighbour list within the SUBSANS message to start the neighbour discovery process. The SUBSANS message contains session-related parameters for the MA to maintain the RMCP session which is defined in the PARAMETER control in the received SUBSANS message. The details of the PARAMETER control are described in clauses 9.4.14 and 10.6.

7.2.2 Neighbour discovery

The neighbour discovery procedure enables an MA to discover the most appropriate neighbouring MAs to make a connection with. The MA can exist either in a unicast network or in a multicast network. The neighbour discovery procedure differs according to the network type, which is described next. In a multicast network, only one MA needs to join the RMCP-2 tree for a particular RMCP-2 session. The node that joins the session tree in the multicast network is called head MA (HMA). An example of a multicast network may be a small-sized LAN where the IP multicast is enabled. In a unicast network, each MA needs to perform RMCP-2 operations to represent itself in the RMCP-2 network. Examples of such a network include LAN and WAN where IP multicast is disabled.

Since all MAs are logically interconnected, it would be difficult for an MA to know the entire network condition. However, by using neighbour discovery procedures, each MA can explore the other MAs in the RMCP-2 network and measures the distance between itself and the corresponding MAs. The neighbour discovery mechanism consists of two steps. One is used in a multicast area, such as subnet LAN, and the other is used in a unicast network such as WAN.

7.2.2.1 Neighbour discovery in a multicast network

This capability enables an MA to find neighbouring MA(s) in a local multicast network. The RMCP-2 makes efficient use of the IP multicast. Thus, finding a neighbour in a multicast network is conducted before finding a neighbour in the unicast network.

7.2.2.1.1 Role of an HMA

In a multicast network, only one MA, which is defined as the HMA, participates in the RMCP-2 session. The HMA relays multicast data to the local multicast network. Other MAs in the multicast network do not need to perform the RMCP-2 operation, since it will be receiving multicast data from the HMA. However, those MAs need to be aware of the operational status of the HMA, since the HMA can leave the RMCP-2 session.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

7.2.2.1.2 HMA discovery

A new MA in a multicast network needs to find the HMA of the network. The HMA solicitation and announcement enables the MA to discover the HMA in a multicast network. Figure 23 shows the procedure of a new MA (i.e., MA C) in finding the HMA in a multicast network. MA C multicasts an HSOLICIT message using the predefined multicast address. The multicast address is used inside the local multicast network for exchanging HSOLICIT, HANNOUNCE, and HLEAVE messages.

If an HMA exists, the HMA multicasts an HANNOUNCE message as a response to the multicast network. MA C will receive the HANNOUNCE message and stops the neighbour discovery and acknowledges the existence of the HMA.

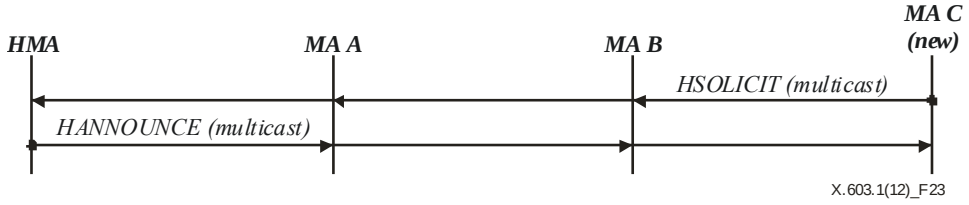

Figure 23 – HMA solicitation and announcement

7.2.2.1.3 New HMA election

The new HMA election can occur when there is no HMA in a multicast network or when the HMA leaves the subscribed RMCP-2 session. There are two occasions for HMA election, the first occasion is when a single MA exists in the multicast network and second occasion is when the HMA leaves the RMCP-2 session.

Initially, there may be no HMA in a multicast network. If a new MA joins the RMCP-2 session, it goes through the HMA election procedure. The HMA election starts with the multicast of an HSOLICIT message to the multicast network. Since the MA is the only node in the multicast network, it fails to receive any HANNOUNCE message within the HANNOUNCE message timeout. The HANNOUNCE message timeout is defined in clause 10.6.4.

If a single MA exists in a multicast network, the MA does not perform the HMA functions. The reason for this is that no other MAs need to receive multicast data in the multicast network. The MA functions as the MA in a unicast network. However, if a new MA in the same multicast network joins the RMCP-2 session, the original MA becomes the HMA by answering to the HSOLICIT message sent from the new MA.

Another occasion for the HMA election process is when the HMA decides to leave the RMCP-2 session. Upon receiving the HLEAVE message from the HMA, the remaining MA(s) competes in the HMA election.

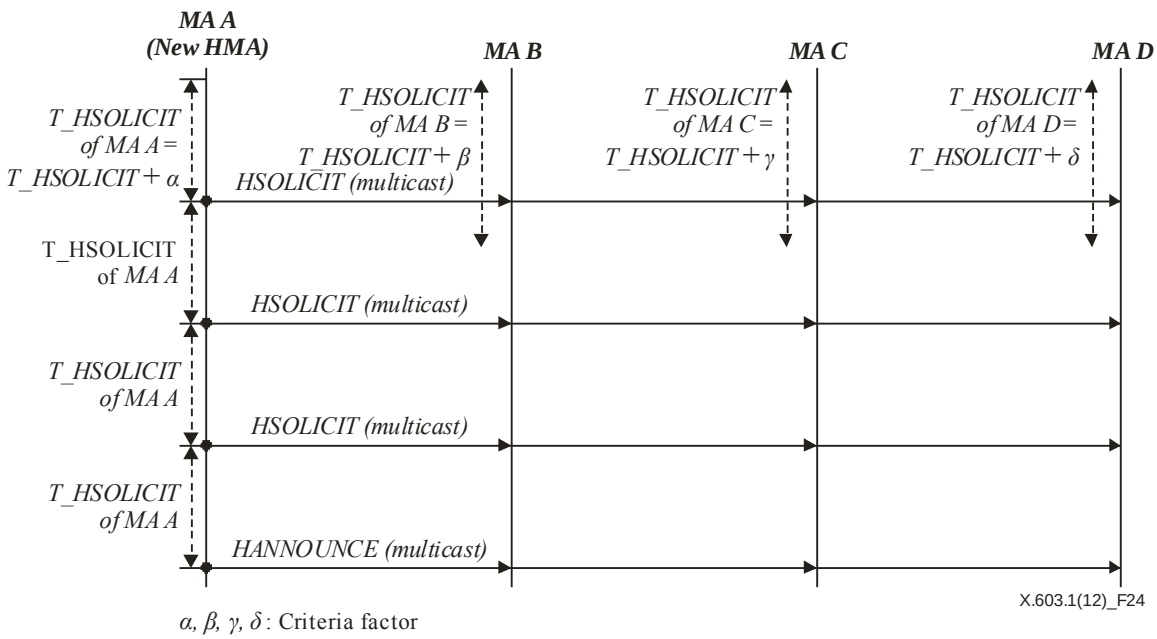

Figure 24 – HMA election

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

Figure 24 shows how MA A becomes a new HMA in a local multicast network. Each MA has its own HSOLICIT message retransmission interval (T_HSOLICIT), which is T_HSOLICIT defined in clause 10.6.4 plus a criteria factor. The criteria factor is used to prevent flooding of the HSOLICIT message. The criteria factor can be derived from various factors such as the distance from the SMA, IP address, etc.

As shown in Figure 24, four MAs compete to be the HMA in a local multicast network. Four MAs start the timer with their own T_HSOLICIT timer. The MA with the shortest timer value sends an HSOLICIT message, first. In Figure 24, MA A has the shortest timer and multicasts an HSOLICIT message to the local multicast network. Upon receiving the HSOLICIT message sent by MA A, the other MAs (i.e., MA B, MA C and MA D) suppress sending the HSOLICIT message and restart the HSOLICIT timer. MA A awaits an HANNOUNCE message from HMA for T_HANNOUNCE time. Since there is no answer, MA A sends an HSOLICIT message again. After sending the HSOLICIT message for N_HANNOUNCE time(s) (see clause 10.6.4), MA A knows that there is no HMA in the network and decides to be the HMA by multicasting an HANNOUNCE message to the local multicast network.

7.2.2.1.4 Handling HANNOUNCE message contention

The HMA contention can occur when more than two MAs multicast the HANNOUNCE message to the same multicast network. In such cases, one MA has to be selected as the HMA. Figure 25 shows an example of HANNOUNCE message contention. In this example, it is assumed that both MA A and MA C have same T_HANNOUCE value, which may result in HANNOUNCE message contention. To resolve this, a second criterion is defined for HMA election, which is the use of MAID. In the figure, MA A and MA C have different MAIDs with MA A having a smaller MAID than MA C.

Since MA A and MA C have the same T_HANNOUNCE value, both MAs issue an HANNOUNCE message after sending an HSOLICIT message for N_HSOLICIT time(s). Upon receiving the HANNOUNCE message from other MA(s), each MA makes a decision on the HMA election according to the second criterion, which is MAID. As a result, MA A is selected as an HMA.

Although the rule for electing HMAs may vary, this Recommendation | International Standard recommends the following HMA election rules:

a) The MA with the smaller T_HANNOUCE time will be elected as HMA.

b) The MA with the lower MAID will be elected as HMA.

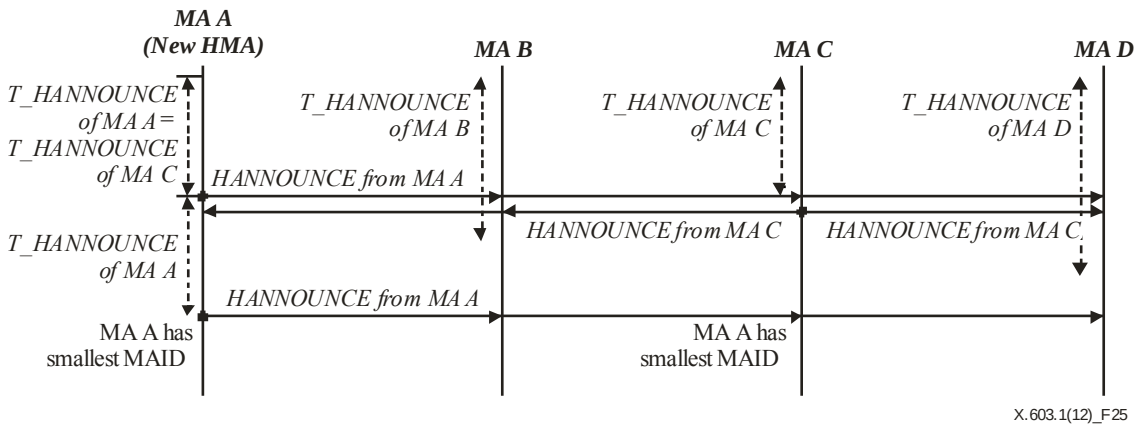

Figure 25 – HANNOUNCE message contention

7.2.2.1.5 HMA continuity

Once the MA is elected as an HMA, it continues its role as an HMA in a multicast network until it leaves the session or the session is terminated. Figure 26 shows how the HMA can continue its role as an HMA. As mentioned above, each MA has its own timer defined by a T_HSOLICIT value and sends an HSOLICIT message after timer expiration.

Another MA(s) suppresses sending an HSOLICIT message after receiving the HSOLICIT message from another MA. The HMA responds by multicasting an HANNOUNCE message. This procedure continues periodically.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

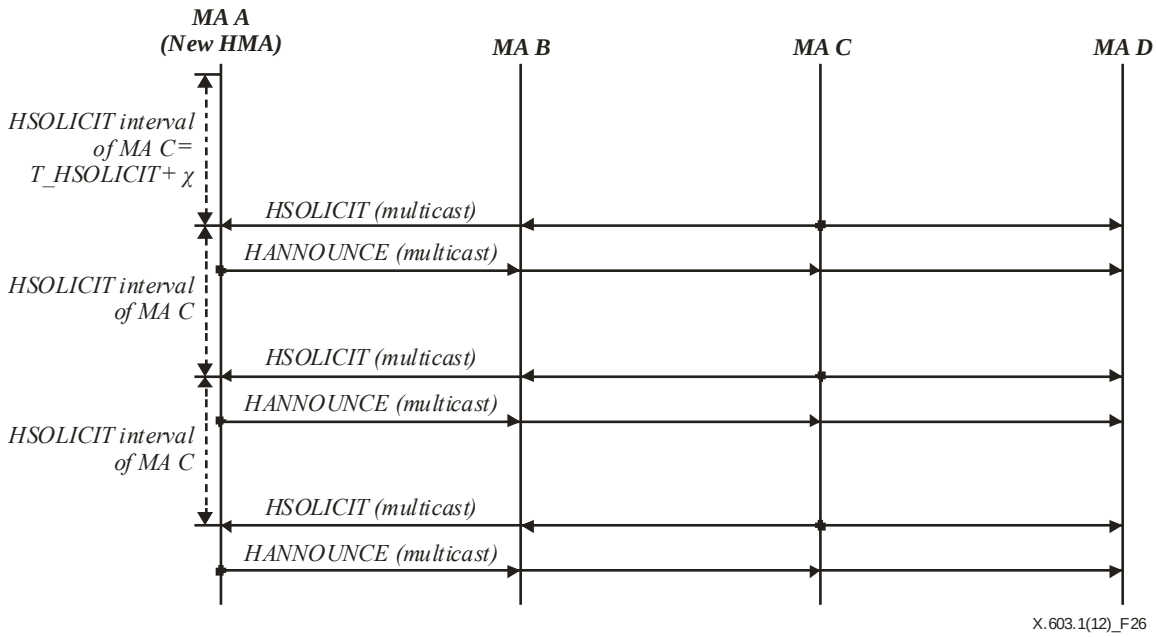

Figure 26 – Periodic HMA announcement

If an HMA fails to receive the HSOLICIT message within the HSOLICIT message timeout (see clause 10.6.4), it recognizes that there is no other MA in the multicast network. The HMA does not perform an HMA function and only performs the MA functions in a unicast network.

A new MA can have a smaller T_HSOLICIT than the current HMA's timer or has a lower MAID than that of the HMA. In this case, the HMA should not be changed. The new MA with the shorter T_HSOLICIT and lower MAID can compete to be the next HMA, if the current HMA leaves the session.

7.2.2.2 Neighbour discovery in the unicast network

If the new MA fails to find neighbours in the multicast network, it becomes the HMA and tries to find neighbour(s) in the unicast network to join the RMCP-2 tree of the subscribed RMCP-2 session.

7.2.2.2.1 Neighbour discovery

Neighbour discovery in a unicast network enables an MA to find other MA(s) subscribing to the same session in other networks.

Figure 27 shows the procedure of neighbour discovery conducted by the MA in a unicast network. MA D sends a PPROBREQ message to the MA(s) listed in the neighbour list given by the SM during the session subscription. MA D will receive a PPROBANS message from each MA. MA D needs to make the decision of which PMA candidate is to join, based on the received PPROBANS messages.

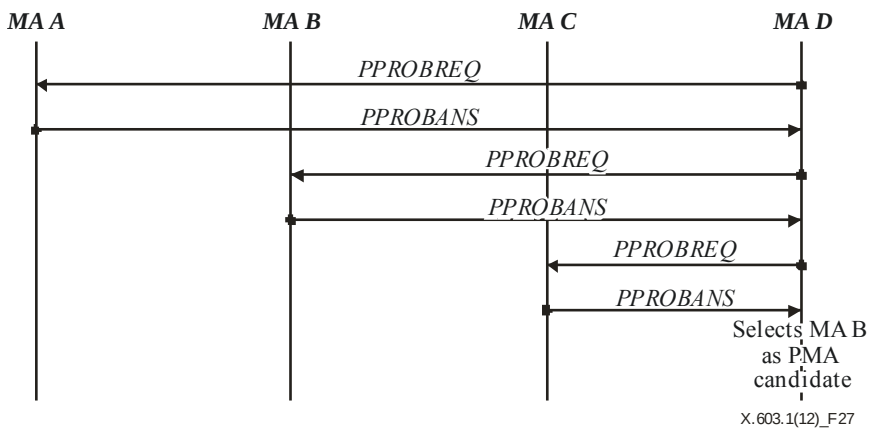

Figure 27 – Neighbour discovery in a unicast network

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

7.2.2.2.2 Exploring more

The PPROBREQ message and the PPROBANS message contain a NEIGHBORLIST control (see clause 9.4.4), which is a list of neighbouring MA(s) that are known by the MA sending the PPROBANS message. Through the exchange of PPROBREQ and PPROBANS messages, the MA can learn of other MA(s). Therefore, the MA can send a PPROBREQ message to the newly discovered MA(s). The MA makes a decision on selecting the most adequate MA, by comparing them with already known MA(s), and newly learned MA(s).

7.2.2.2.3 Selecting a PMA candidate using system information

The neighbour discovery procedure is used to choose the PMA to join. The SYSINFO control (see clause 9.4.8) is included in the PPROBANS message to help probing the MA in making a decision on the PMA candidate. By using the system information within the PPROBANS message, it can contribute to performance enhancement by placing a low-capability node in a low position on the tree hierarchy. TIMESTAMP control (see clause 9.4.9) is also used to choose the PMA to join. Upon receiving PPROBREQ message, the responding MA appends the two types of time values in the first and second fields of TIMESTAMP control. The first type is the time when the PPROBREQ message appears to the receiver, and the second type is the time before sending the PPROBANS message. These two values are used to presume the processing load of the replying MA.

7.2.2.2.4 Selecting a PMA candidate through distance measurement

In order to choose the most adequate MA as a PMA, the MA also uses a distance measuring method. Since MAs are logically interconnected, it would be difficult for MAs to know the actual configuration of a physical network. However, the network distance between MAs can be measured by various metrics, such as per-hop delay, the number of hops, bandwidth, etc. For example, the round trip time (RTT) between MAs can be used. Upon receiving the PPROBANS message, the probing MA can measure the distance using two time values; the time when the PPROBREQ message is sent, and the time when the PPROBANS message is received; the first time value is stored in the TIMESTAMP control within the PPROBREQ message. Thus, through the neighbour discovery procedure, an MA can make decisions on the most adequate MA to join.

7.2.3 Session join

The session join procedure enables each MA to establish a connection with a PMA for the subscribed RMCP-2 session. Figure 28 shows how an MA establishes a PMA-CMA relationship after selecting a PMA candidate based on the neighbour list given by the SM. The joining MA (MA E) conducts the neighbour discovery and decides that MA D is the most appropriate for PMA. After the PMA candidate is selected, MA E sends a RELREQ message including a DATAPROFILE control (see clause 9.4.3) to MA D. The DATAPROFILE control is used to specify the information needed to establish data channels between the PMA and CMA.

If the relay request is acceptable, the MA D responds with a RELANS message including a RESULT control indicating a successful join. Otherwise, MA D returns the RELANS message with the RESULT control indicating a denial of request. If MA D can accept the request but cannot provide the service according to the data profile in DATAPROFILE control, it denies the request and inserts the proposed data profile into the RELANS message. MA E can send a request with the new data profile to be accepted.

Upon receiving a successful RELANS message, a data channel between the MA D and MA E is established according to the negotiated data profile. Otherwise, MA E should select another MA to join.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

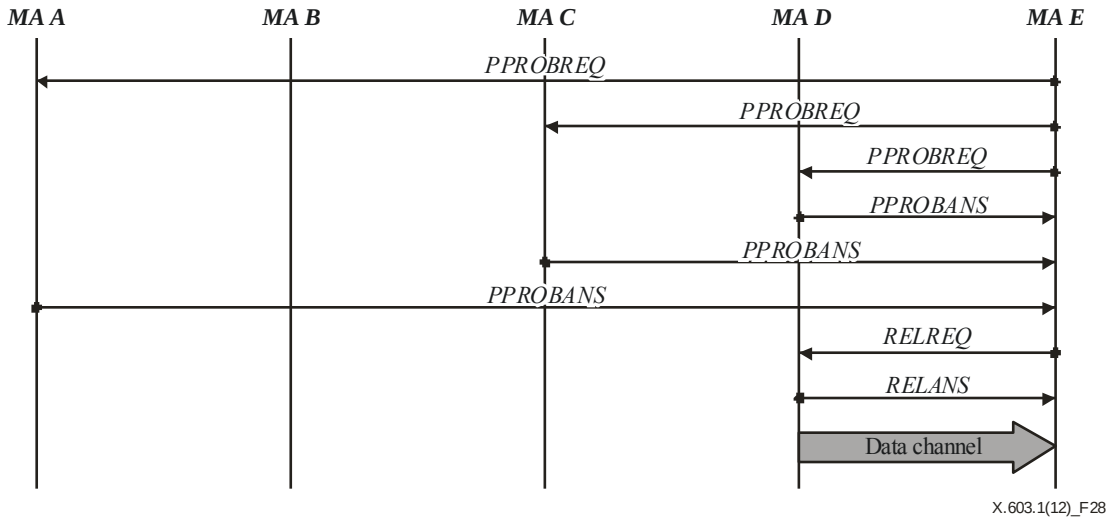

Figure 28 – Successful session join

7.2.4 Leave

An MA may leave a session or change its PMA during the session. To make an RMCP-2 tree robust, each MA should notify its PMA and CMA(s) of its departure. Upon receiving this notification, both the PMA and CMA should follow the appropriate procedure. In addition, a departing MA should also notify the SM of its departure.

The RMCP-2 considers four types of departure:

- leave at own will;
- leave to switch parent;
- expulsion from a PMA or SM;
- departure of an SMA or session termination.

The detailed operations for each case are described as follows.

7.2.4.1 Leave at own will

MAs may leave a session anytime. Before leaving, an MA must notify its PMA and CMA(s) of its departure. The PMA deletes the MA from its CMA list for the session and reserves a space for a new CMA. In addition to the notification to both the PMA and CMA(s), the leaving MA should also notify the SM of its departure. The SM checks whether the requesting MA is subscribed to the session which the MA requests to leave. If the MA is subscribed to the session, the SM modifies the information related to the departing MA. Otherwise the SM ignores the request.

7.2.4.1.1 MA leave in a unicast network

To leave a session, an MA sends a LEAVREQ message to its CMA(s). Each CMA who receives the LEAVREQ message should promptly start to connect to an alternative PMA by sending a RELREQ message to the PMA candidate. If successful, the CMA sends a LEAVANS message to the PMA leaving. When a departing MA receives the LEAVANS messages from all of its CMAs, it sends a LEAVREQ message to its PMA. The PMA responds with a LEAVANS message and modifies the information of the departing MA. Before departing the session, the MA should send a LEAVREQ message to the SM to notify its departure.

NOTE – Data delivery from a leaving MA to each CMA should be continued until each CMA closes connection. It means that data delivery from a PMA to a leaving MA should also be continued until connection between two MAs is disconnected.

Figure 29 shows how an MA leaves a session in a unicast network.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

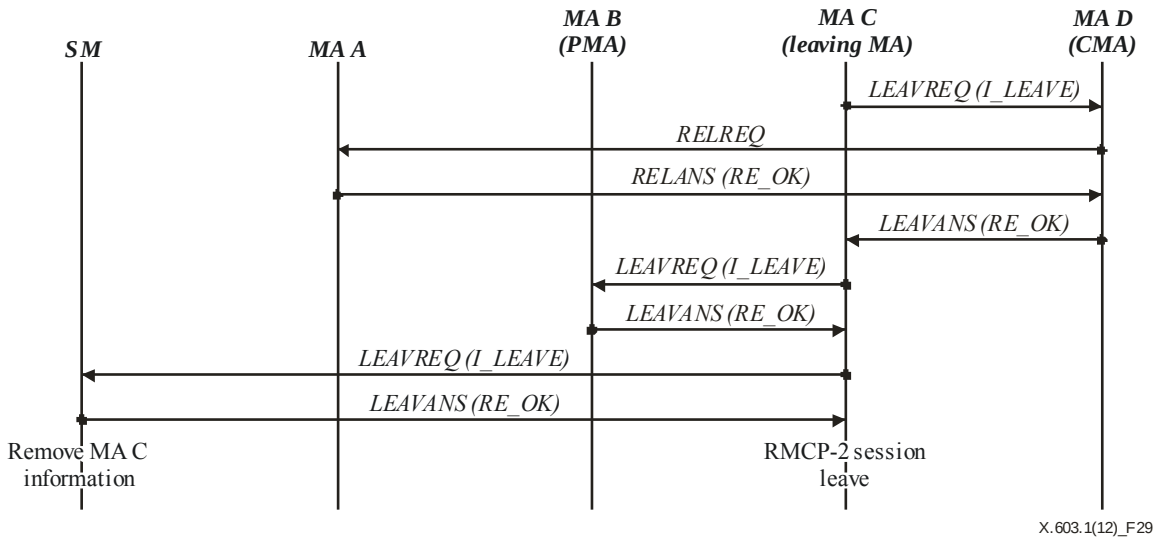

Figure 29 – MA leave in a unicast network

7.2.4.1.2 MA leave in a multicast network

In a multicast network, there are two cases of an MA's leave. The first case is an HMA's leave. Whenever the HMA leaves the subscribed RMCP-2 session, it should notify its departure to the CMA(s) in the local multicast network as well as to the CMA(s) and the PMA in the other network.

Figure 30 shows how the MA B, i.e., HMA, leaves a session. The HMA (MA B) sends a LEAVREQ message to its CMA (MA E) in another network. Upon receiving the LEAVREQ message, MA E starts to switch PMA and responds to MA B with a LEAVANS message. In order to announce its departure, MA B multicasts an HLEAVE message into the local network.

Upon receiving the HLEAVE message from the HMA, both MA C and MA D in Figure 30 wait for a certain back-off time, T_HANNOUNCE, before multicasting the HANNOUNCE message. MA C sends an HANNOUNCE message for the first time and becomes a new HMA. This step occurs because MA C has a shorter back-off time than that of MA D as described in clause 7.2.2.1.3. Because MA B was a point connected to an outside network, MA C should undertake the role of MA B by connecting to the PMA outside the network. Figure 30 shows how MA C selects its parent, MA A, which is the PMA of MA B. In order to connect to MA A, MA C refers to the ROOTPATH control (see clause 9.4.7) in the received HLEAVE message. Before MA B leaves the session, it should send a LEAVREQ message to the SM. The SM modifies the information related to MA B.

NOTE – The departing HMA should stop multicasting the multicast data and send a LEAVREQ message when it receives an HANNOUNCE message from the new HMA because the data it sends can collide with the data sent by the new HMA.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

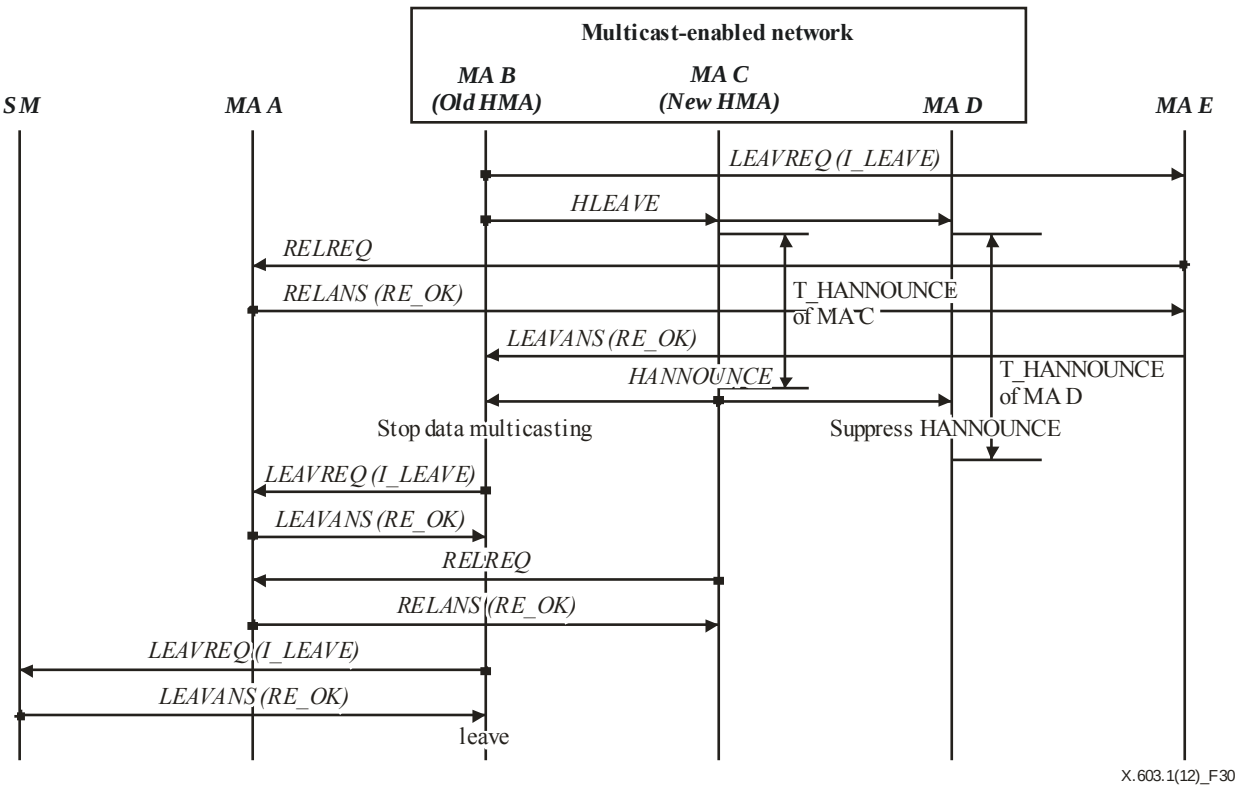

Figure 30 – HMA leave in a multicast network

Whenever the non-HMA of a multicast network wants to leave a session, it silently leaves the session. MA D in Figure 30 does not need to notify other MAs of its departure. However, a leaving MA should send a LEAVREQ message to the SM. The SM modifies the information related to the leaving MA.

7.2.4.2 Parent switching

An MA may need to find a better PMA to get better services. This procedure is called parent switching. Through the procedure of parent switching, it is possible to create a near optimal RMCP-2 tree in terms of performance. For parent switching, an MA interacts with an old PMA to leave the RMCP-2 tree and with a new PMA to join the RMCP-2 tree. It does not need to inform the CMA of the parent switching. Thus, CMAs do not need to know about the parent switching of its PMA if it does not have any problem in receiving the RMCP-2 service. Thus, an MA does not need to send a LEAVREQ message to its CMA(s), when it tries to change its PMA. During parent switching, the MA sends a pseudo HB message to prevent its CMA(s) from conducting a partition recovery operation as described in clause 7.2.5.3.2. The MA sends a RELREQ message to the PMA candidate. In Figure 31, since MA C changes the PMA from MA A to MA B, the root path of MA C should also be changed. Thus, MA B gives its root path to MA C when it sends a RELANS message. The old PMA (MA A) that receives a LEAVREQ message deletes the leaving MA from its CMA list.

NOTE 1 – An MA can switch parent only when it receives an HB message to keep the RMCP-2 tree stable. The heartbeat mechanism is described in clause 7.2.5.1 and parent switching is described in clause 7.2.5.4.

NOTE 2 – HB* in Figure 31 means pseudo-HB message.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

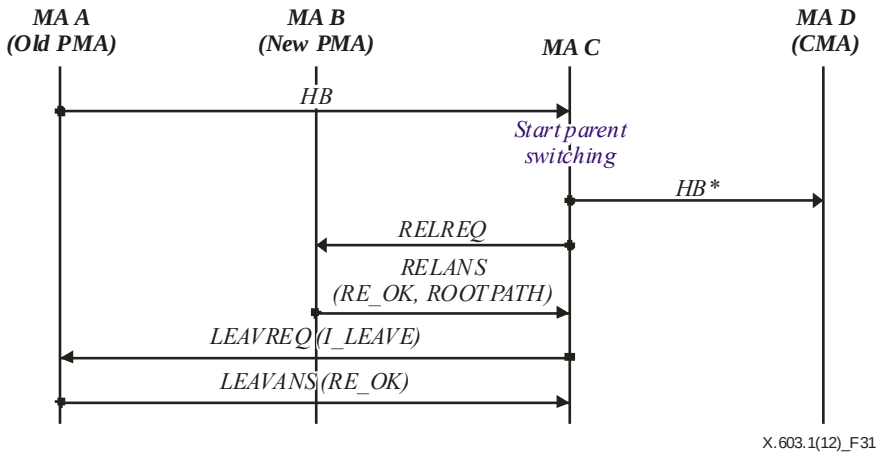

Figure 31 – Parent switching

7.2.4.3 MA expulsion

RMCP-2 has a mechanism for discarding a particular MA. For example, when the SM needs to remove a specific MA, and when an MA expels its CMA.

7.2.4.3.1 Expulsion by PMA

A PMA can expel its CMA(s) when it suffers from system resources depletion and can no longer provide a service to its CMAs. The expelled CMA should find another PMA candidate.

Figure 32 shows an example of a message flow for expulsion by the PMA. First, a PMA, namely the MA B, sends a LEAVREQ message with a reason code PMA_KICKOUT to expel MA C. MA C searches for another PMA and sends a RELREQ message to the new PMA. After switching parents to MA A, MA C transmits a LEAVANS message to its old PMA, MA B.

NOTE – MA C in Figure 32 may have CMA(s) but the CMA(s) of MA C do not need to know about the expulsion of the PMA as long as they successfully receive data.

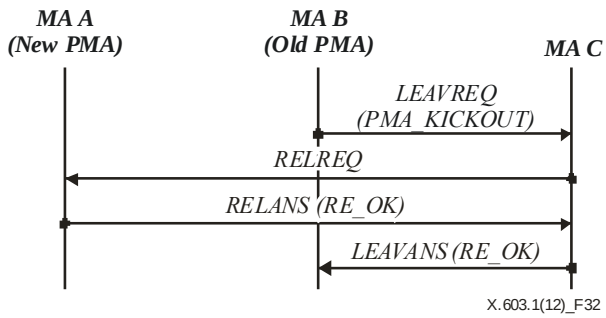

Figure 32 – Expulsion by PMA

7.2.4.3.2 Expulsion by SM

The SM can discard any MA in a certain RMCP-2 session by sending a LEAVREQ message with the reason code SM_KICKOUT. Upon receiving the LEAVREQ message from the SM, an MA must leave the session promptly. After the expulsion, the SM should update the information related to the expelled MA, e.g., session member list, MA list, etc.

In the message flow shown in Figure 33, the SM requests MA B to leave by sending a LEAVREQ message with the reason code SM_KICKOUT. MA B must leave the session but, before leaving the session, MA B must notify its PMA and CMA(s) of its expulsion by sending a LEAVREQ message with a reason code SM_KICKOUT. The PMA, MA A, removes the information related to MA B and the CMA, i.e., MA C, should find a new PMA to continue receiving the multicast data.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

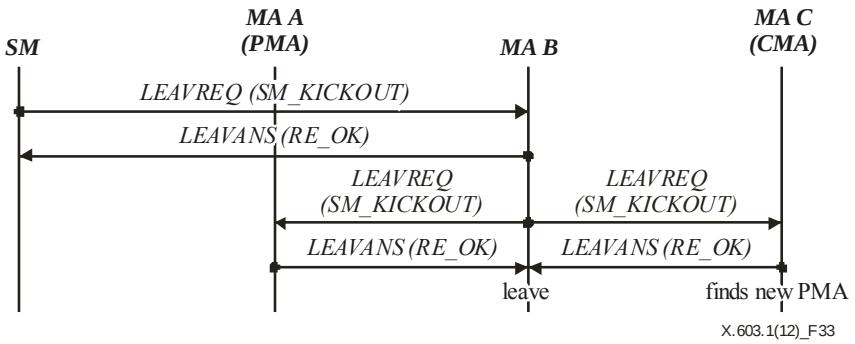

Figure 33 – Expulsion by the SM

7.2.4.4 SMA leave

An RMCP-2 session cannot exist without an SMA. An SMA should not leave a session as it is required for maintaining the session. However, if an SMA does leave the session, the session should be terminated.

Figure 34 shows the session leave of the SMA. The SMA sends a LEAVREQ message to the SM. Upon receiving the LEAVREQ message from the SMA, the SM checks whether the mapping between the SMA and the session it has requested to terminate is correct. If the mapping is correct, the SM removes the session information and then replies with a LEAVANS message, it also initiates session termination as described in clause 7.1.5.

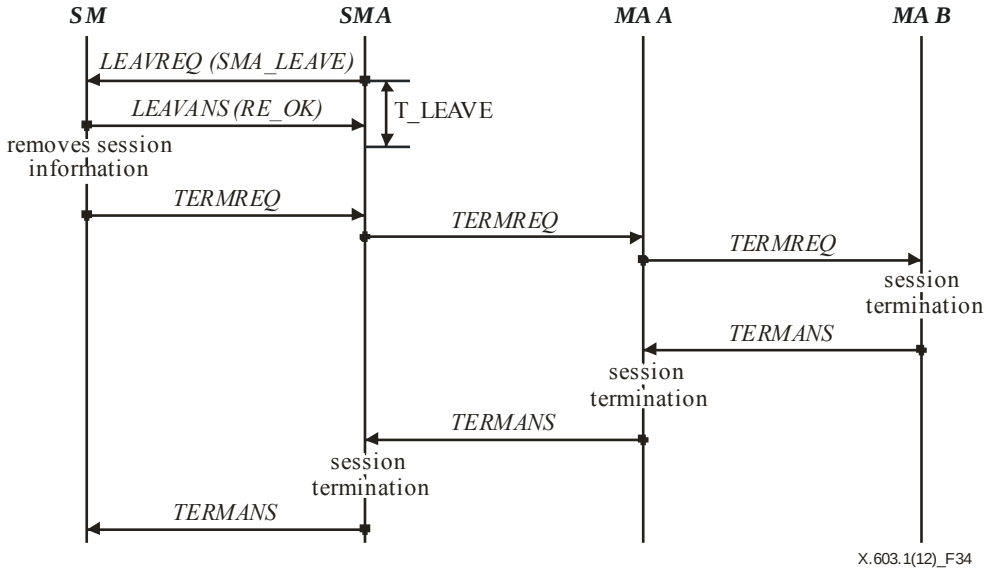

Figure 34 – SMA leave

7.2.5 Maintenance

7.2.5.1 Heartbeat

The purpose of the heartbeat is to keep the constructed RMCP-2 tree robust. The heartbeat, which gives unified synchronizing information to the session, helps each MA to detect whether the session is currently alive. It also contains useful information on the data delivery path, named ROOTPATH. The ROOTPATH includes a relayed data path which follows the tree hierarchy.

7.2.5.2 Monitoring

RMCP-2 has two types of monitoring mechanisms. The first one is about monitoring a specific MA described in clause 7.1.4. The other one, which is shown in Figure 27, is about monitoring a part of the RMCP-2 tree below a specific MA.

Figure 35 shows how RMCP-2 monitors a part of the RMCP-2 tree. As shown in Figure 35, STREQ and STANS messages are exchanged between the SM and MA which is the root of the sub-tree to be reported. However, STCOLREQ and STCOLANS messages are used under the MA received STREQ message. This indicates that STCOLANS messages are aggregated along the path towards the SM. In order to specify the depth of the sub-tree to be monitored, the TREEEXPLOR control is used. Figure 35 shows an example of such a set where MA 0 is the selected

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

MA and the value of "Tree depth" field is 3. The COLLECT control is used to identify the MA reporting the requested information and the SYSINFO control is used to report the requested information as described in clause 9.4.8.

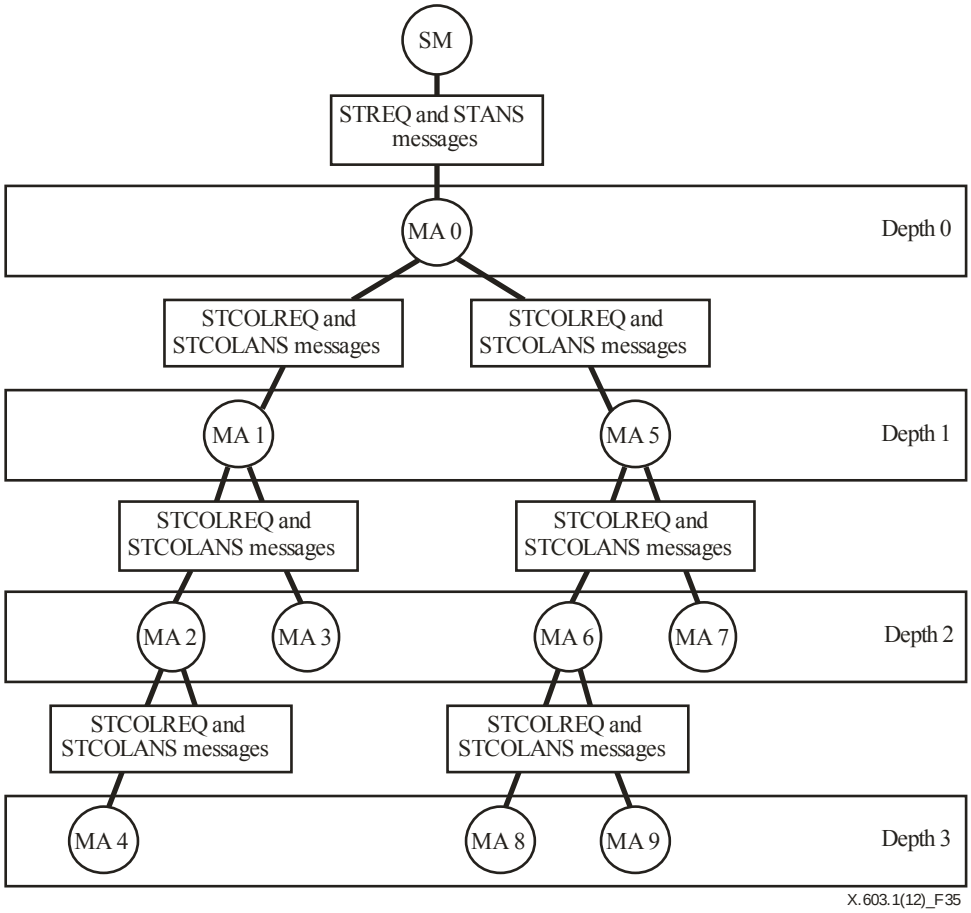

Figure 35 – Example of a delivery tree for STCOLREQ and STCOLANS messages

Figure 36 shows how the SM queries the scoped area of a tree. That is, the SM asks for merged information on the scoped area of a tree, by sending an STREQ message to a specific MA (SMA and MA A each) to collect status information for the scoped area.

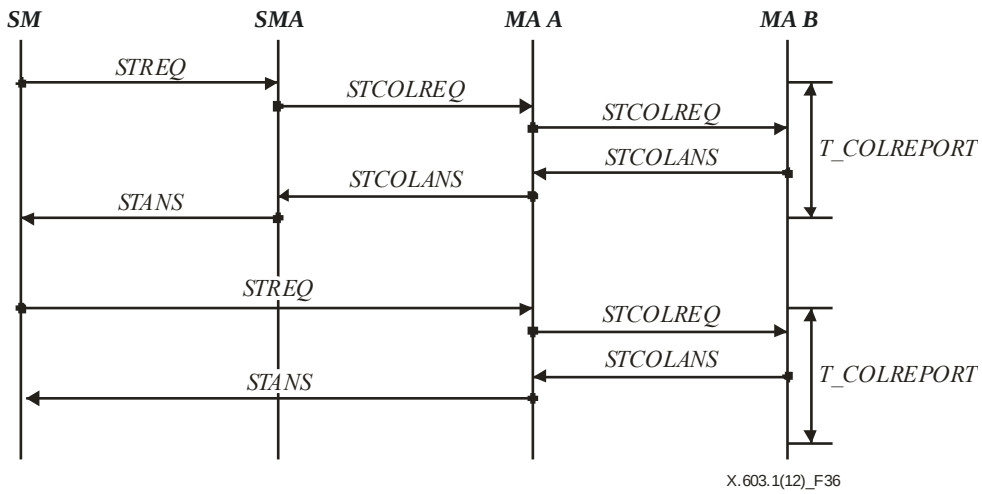

Figure 36 – Tree monitoring by collecting a status report

7.2.5.3 Fault detection and recovery

Network faults such as a loop or partition may be caused by an MA's frequent and careless parent switching. To detect and recover such network faults, RMCP-2 provides the following fault detection and recovery mechanisms.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

7.2.5.3.1 Loop detection and prevention

A loop occurs when an MA becomes the CMA of its descendant on the RMCP-2 tree during parent switching. One such scenario can be as follows:

a) MA A performs neighbour discovery and chooses a certain MA (which is, MA B) as a PMA candidate;

b) the chosen MA B happens to be a descendant of MA A;

c) MA A receives an HB message and changes the PMA from its current PMA to MA B;

d) thus, a loop has occurred.

Figure 37 shows the procedure of loop detection and prevention. To prevent a loop, MA B checks the root path in the PPROBREQ message sent by MA A, to see whether its MAID is already in the root path. Since MA A is an ancestor of MA B, MA A is already present in the root path. Thus, MA B can detect the potential loop and prevent it by sending the RELANS message indicating a denial of request. MA A cancels the parent switching and sends an HB message including the unchanged root path to its CMA(s).

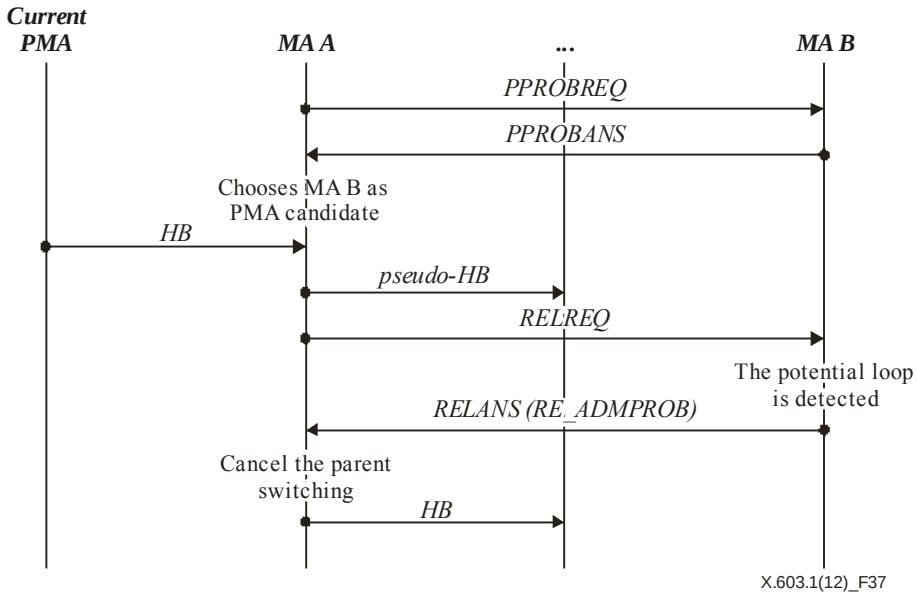

Figure 37 – Loop detection and prevention

7.2.5.3.2 Network partition detection and recovery

Partitions can occur when the connection between a PMA and CMA is disconnected. An MA can detect partition based on the timers for periodic message exchange and resolves this problem by establishing a new connection with the new PMA. Figure 38 shows how MA C detects the tree partition: that is, the tree partition is detected whenever MA C fails to receive the HB message for HB message timeout (see clause 10.6.2). The failure to receive the HB message triggers neighbour discovery for finding a PMA candidate. MA C sends a FAILCHECK message to the SM to check whether MA B is alive.

NOTE – MA C may send a PPROBREQ message toward MA(s) in the neighbour list or MA(s) in the ROOTPATH control except for MA B.

In Figure 38, the SM fails to receive a STANS message from MA B for a certain period of time, the SM considers that MA B has failed. In this case, the SM modifies the information of MA B to indicate that MA B has failed. If MA B responds to the SM with the STANS message, the SM does nothing. In this case, network connectivity may have been lost between MA B and MA C.

During an MA's recovery from network partition, the MA's descendant(s) may also consider that the network has partitioned and start to repair the partition. As a result, a single point of failure can cause an entire RMCP-2 sub-tree to be collapsed. To prevent this problem, RMCP-2 uses two methods, use of a pseudo HB message and allocating T_HB.

An MA, which is trying to establish a connection with a new PMA, sends a pseudo HB message to its descendant(s) to notify that the session is partitioned. For the pseudo HB message, RMCP-2 uses the HB message with PSEUDO_HB control. Upon receiving the pseudo HB message, each MA recognizes that one of its ancestors on its root path is trying to recover from network partition. So each MA does not conduct the recovery procedure, and it resets its timer in the same way when it receives the normal HB message, and forwards the pseudo HB message to its CMA(s), if it exists.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

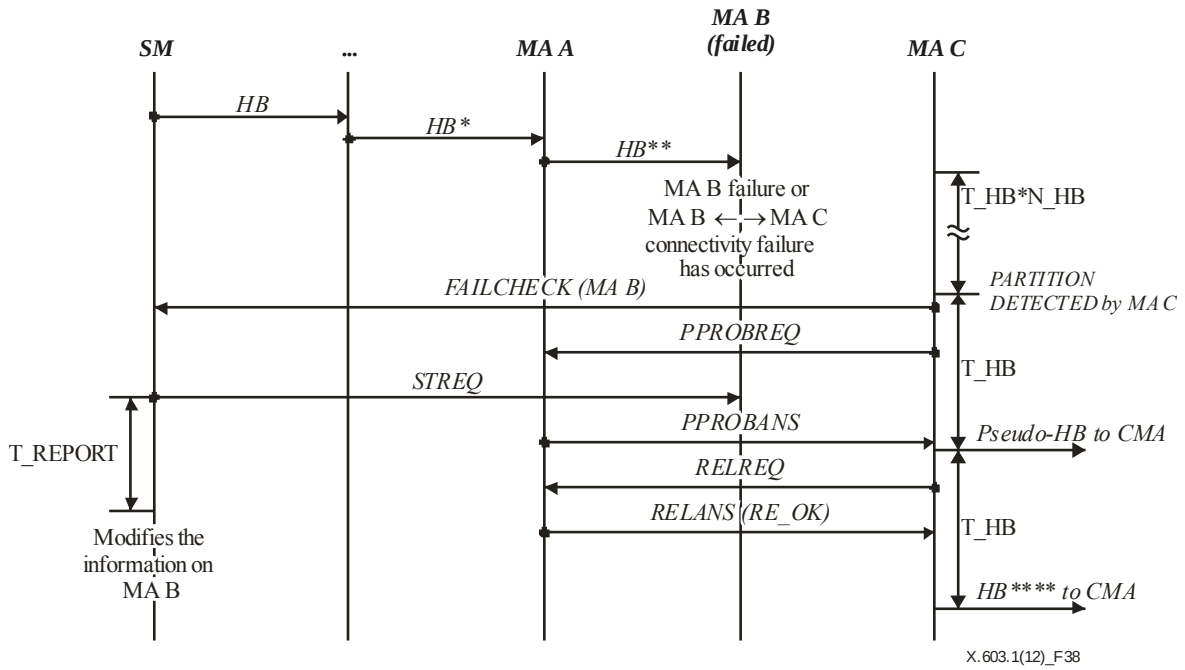

Figure 38 – Network partitioning detection and recovery

Since, the network recovery may vary in time, using a pseudo HB message is not enough. Pseudo HBs may be delayed because of network congestion and as a result, some MAs conduct the recovery procedure simultaneously. Therefore, each MA needs to prevent the fault report chain effect by setting a longer T_HB compared to the preceding MA. Figure 39 shows how the T_HB is set for each MA based on the sequential order in the RMCP-2 tree.

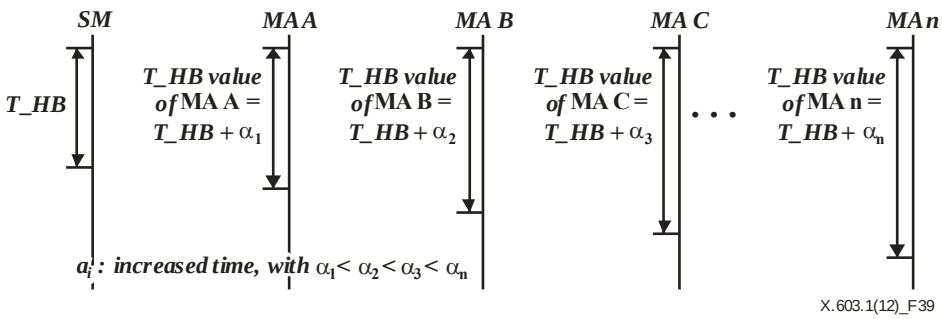

Figure 39 – T_HB setting

Network partition detection includes not only detection of the partition between the PMA and CMA but also detection of the failure of the SM.

An SMA can detect failure of the SM, when an SMA fails to receive the periodic HB message from the SM. In this case, ongoing sessions may continue, however, session subscription and session join are impossible. If the RMCP-2 service should be managed by the SM, the SMA should send a TERMREQ message to its CMA(s) to terminate the session.

Network partition can also be detected through the periodic exchange of RELREQ and RELANS messages.

In the case of MA failure, the MA may be a PMA or a CMA of the failed MA. An MA can recognize failure of its PMA, if it fails to receive a RELANS message and the MA can recognize failure of its CMA, if it fails to receive a RELREQ message within the predefined interval. Figure 40 shows the procedure of PMA failure detection and recovery procedure through the absence of a RELANS message. Since the MA B fails to receive a RELANS message during its timer (T_RELAY), the MA B sends a FAILCHECK message to the SM. The MA B also performs the neighbour discovery simultaneously for recovery of partition.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016

The SM sends a STREQ message to MA A but the MA A does not answer because of the failure. Thus the SM modifies the information related to MA A when the timer for the STANS message expires. If MA A answers the STREQ message with a STANS message, the SM does not remove the information related to MA A and does nothing. In that case, although MA A has not failed, MA B will still change its parent.

In case of SMA failure, the session served by the failed SMA should be terminated. The CMA(s) of an SMA can recognize failure of the SMA. The MA sends a FAILCHECK message to the SM to check whether the SMA is alive. The SM sends a STREQ message to the SMA. If the SMA answers with the STANS message, the SM does nothing. If, however, the SMA does not answer, the SM considers that the SMA has failed and closes the session. The CMA(s) of the failed SMA sends a LEAVREQ message with reason code SMA_LEAVE to all CMAs to terminate the session. The LEAVREQ message is relayed along the RMCP-2 tree of the RMCP-2 session and the session is terminated gradually.

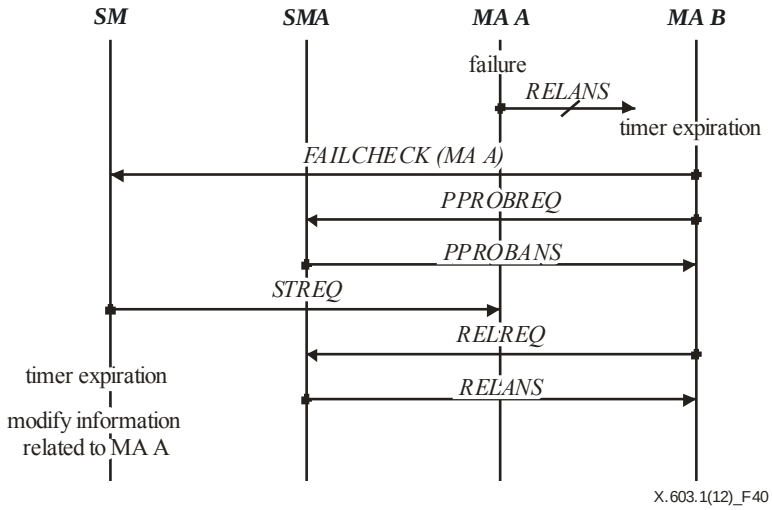

Figure 40 – PMA failure detection and recovery

7.2.5.4 Tree reconstruction

The tree reconstruction procedure occurs when an MA finds that the PMA candidate which can provide a better service than the current PMA and tries to switch parent to the new PMA candidate. By continuing the tree reconstruction procedure during the session, the RMCP-2 tree can be improved gradually.

The procedure for finding better nodes follows the neighbour discovery mechanism described in clause 7.2.2. When an MA finds a better MA than its current PMA, the MA can change its current PMA to a newly discovered PMA candidate according to the parent switching procedure described in 7.2.4.2.

While the tree is being improved, network faults such as a loop or partition can be caused by parent switching. In particular, network faults may occur in the following cases: when multiple MAs in the same branch may try to switch PMA at the same time and when multiple MAs along the branch may try to successively switch PMA.

To maintain RMCP-2 tree stability, each MA can switch its PMA only when it receives an HB message. In addition, a threshold value is used to prevent frequent parent switching. It means that an MA can try to change its PMA only when the difference between the metric of connection with the PMA candidate and that of the connection with the current PMA is larger than the predefined threshold value. The cost may be a hop count, delay, bandwidth, etc. Detailed description of the cost as well as the threshold value is not addressed in this Recommendation | International Standard because it can be varied according to the service policy.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 16512-2:2016