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 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*

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

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.

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.

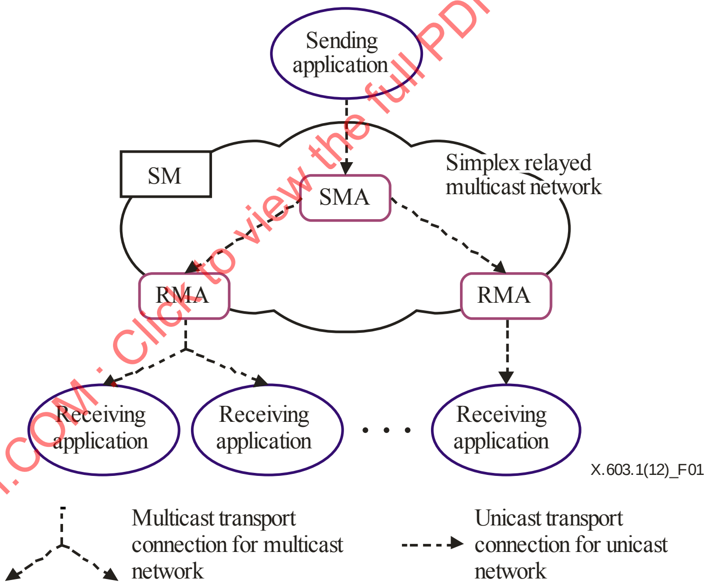

Sending application
SM
SMA
Simplex relayed multicast network
RMA
RMA
Receiving application
Receiving application
. . .
Receiving application
X.603.1(12)_F01
Multicast transport connection for multicast network
Unicast transport connection for unicast network

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.

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.

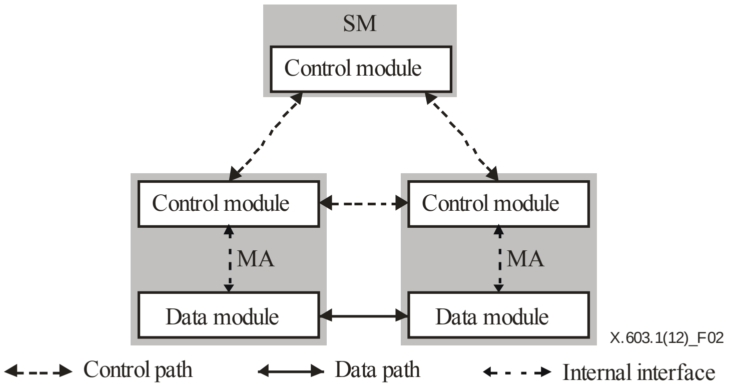


Figure 2 – Three types of interfaces in RMCP-2

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.

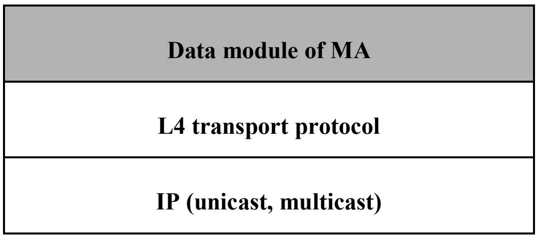


Figure 5 – Protocol stack of an MA's data module

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.

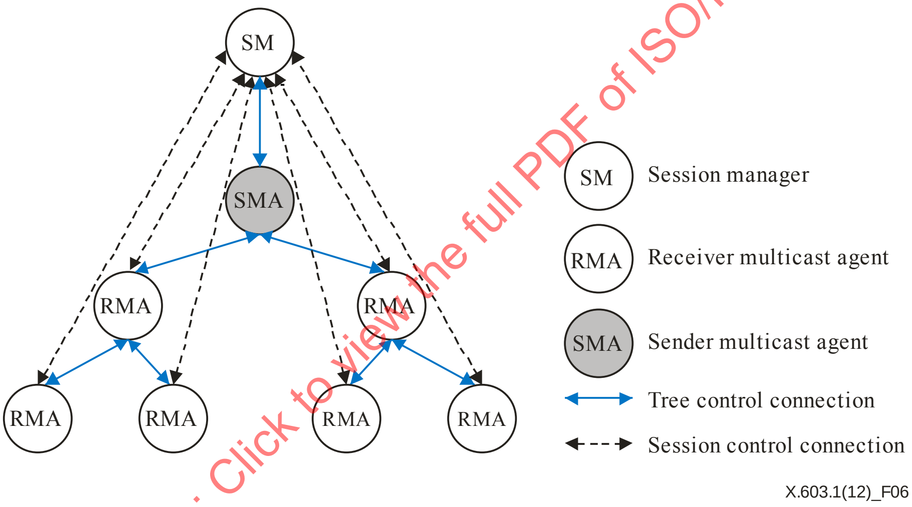

SM
SMA
RMA
RMA
RMA
RMA
RMA
RMA
SM Session manager
RMA Receiver multicast agent
SMA Sender multicast agent
Tree control connection
Session control connection
X.603.1(12)_F06

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.

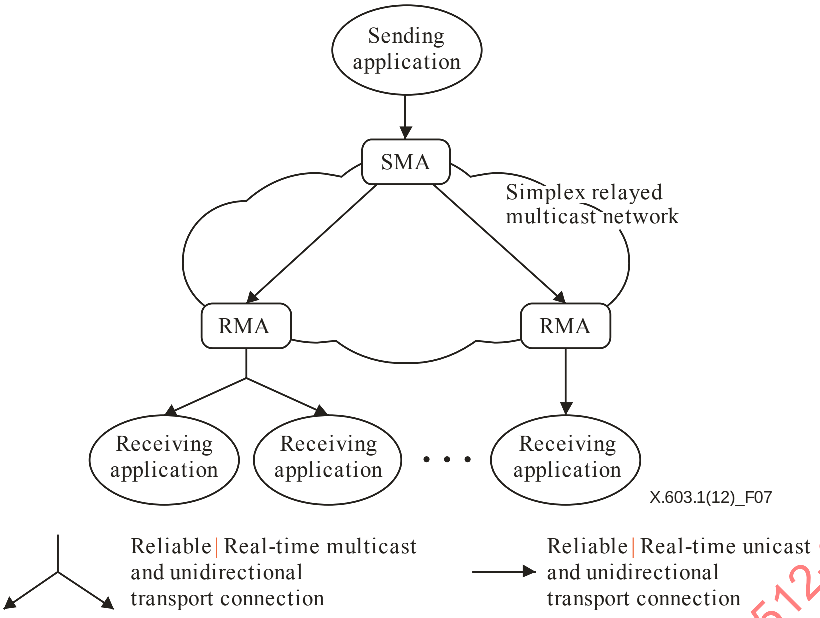

Sending application
SMA
Simplex relayed multicast network
RMA
RMA
Receiving application
Receiving application
. . .
Receiving application
X.603.1(12)_F07
Reliable | Real-time multicast and unidirectional transport connection
Reliable | Real-time unicast and unidirectional transport connection

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).

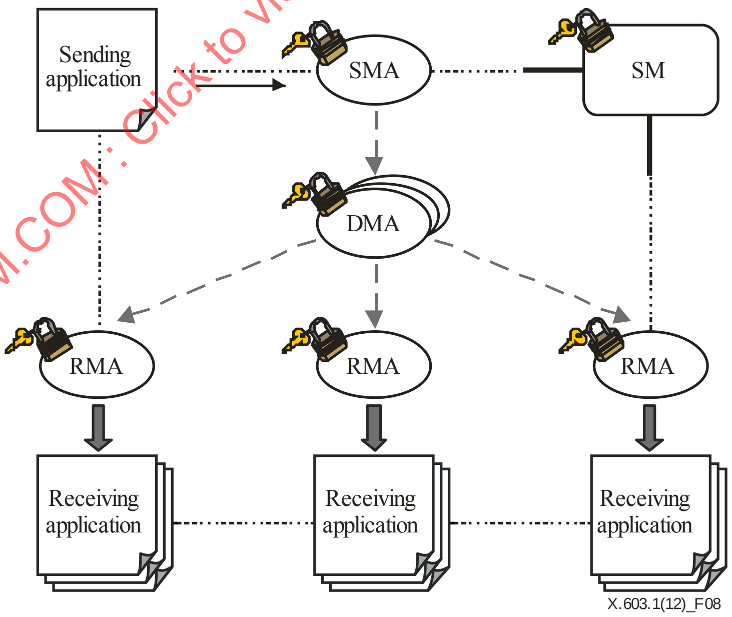


Figure 8 – RMCP-2 service topology with security

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.

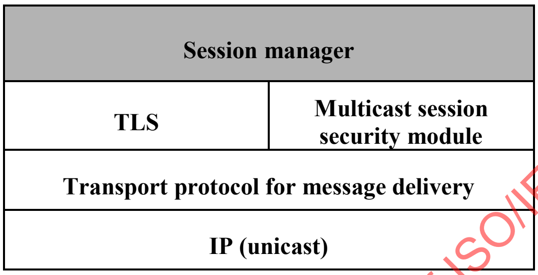

Session manager
TLS
Multicast session security module
Transport protocol for message delivery
IP (unicast)

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.

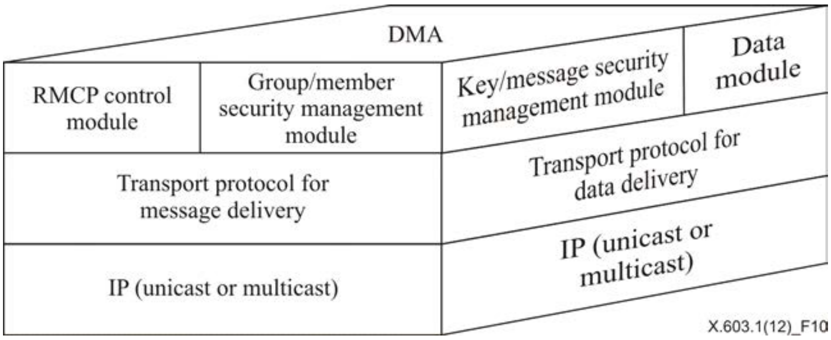

DMA
RMCP control module
Group/member security management module
Key/message security management module
Data module
Transport protocol for message delivery
Transport protocol for data delivery
IP (unicast or multicast)
IP (unicast or multicast)
X.603.1(12)_F10

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

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.

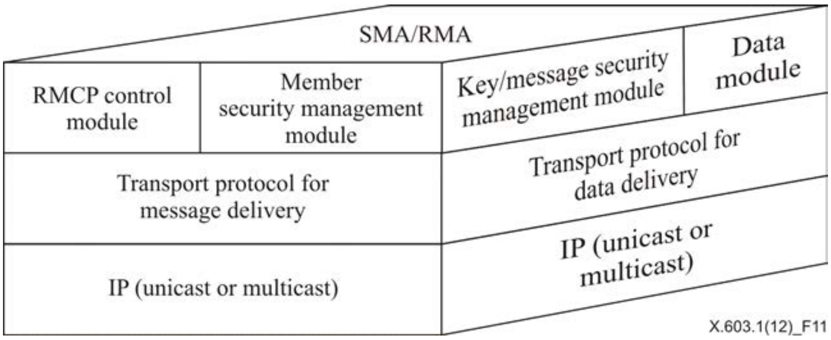

SMA/RMA
RMCP control module
Member security management module
Key/message security management module
Data module
Transport protocol for message delivery
Transport protocol for data delivery
IP (unicast or multicast)
IP (unicast or multicast)
X.603.1(12)_F11

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.

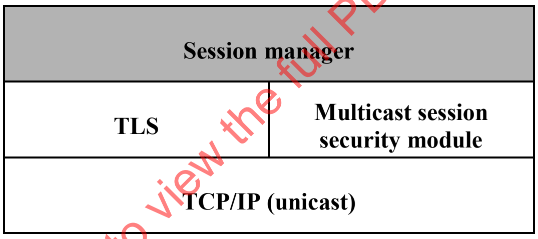


Figure 12 – Protocol module of the SM of a secure RMCP-2

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

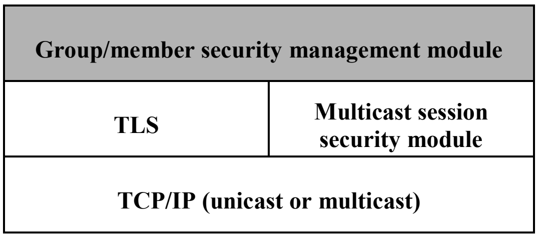

Group/member security management module
TLS
Multicast session security module
TCP/IP (unicast or multicast)

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.

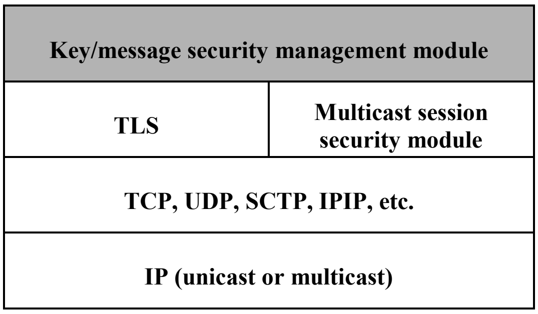

Key/message security management module
TLS
Multicast session security module
TCP, UDP, SCTP, IPIP, etc.
IP (unicast or multicast)

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.

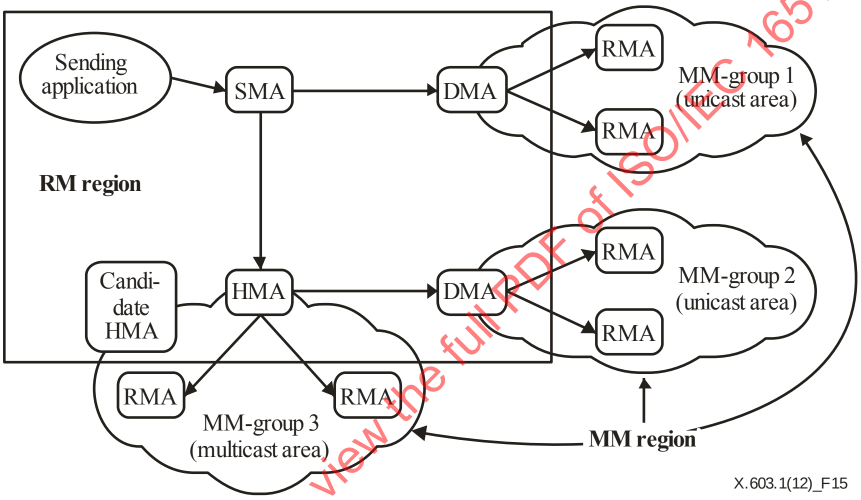


Figure 15 – Security management regions

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	

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.

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.

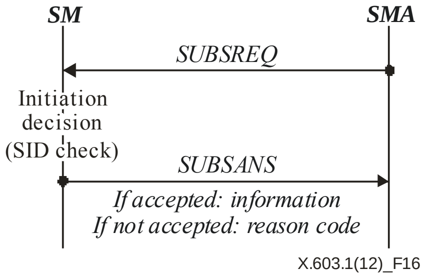


Figure 16 – RMCP-2 session initiation

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.

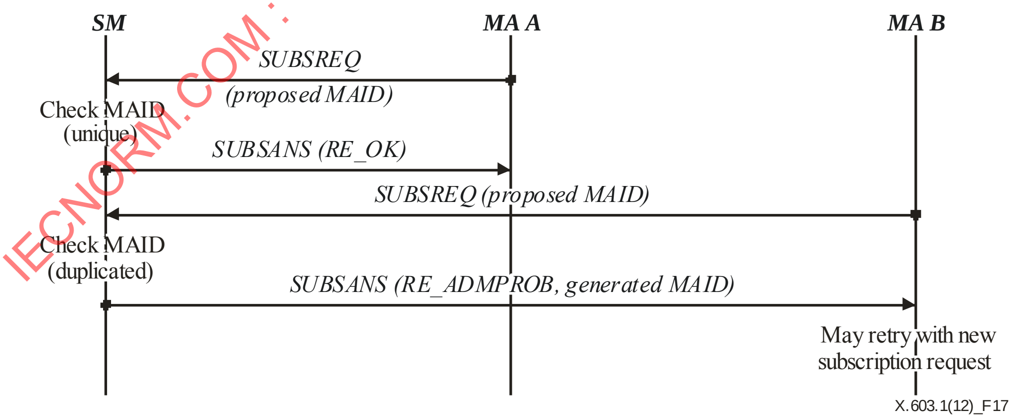


Figure 17 – Session subscription

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.

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.

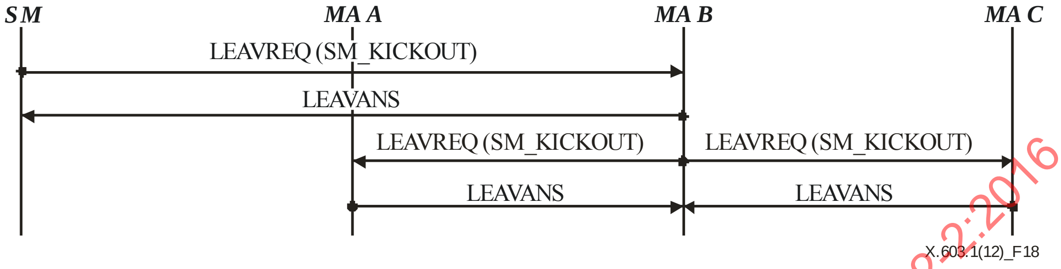


Figure 18 – SM's expulsion of MA B

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.

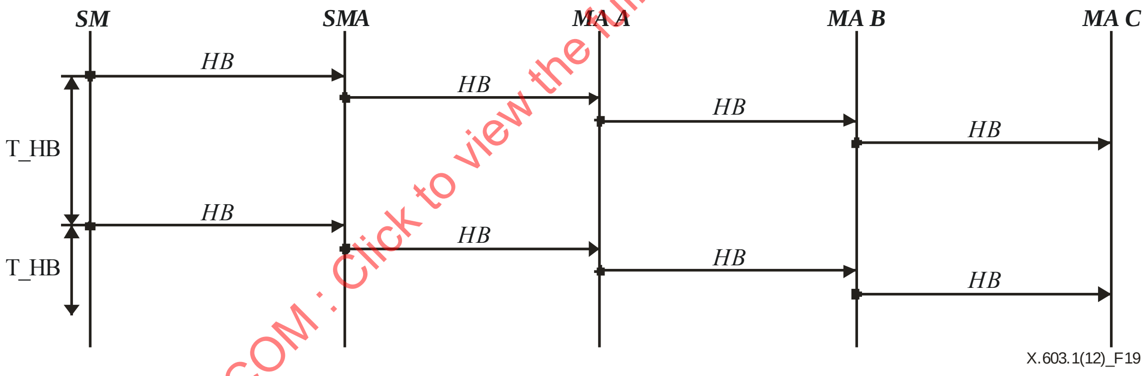


Figure 19 – Periodic heartbeat

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.

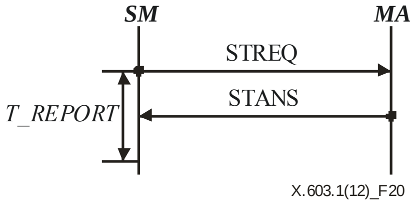


Figure 20 – MA monitoring – Status report

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.

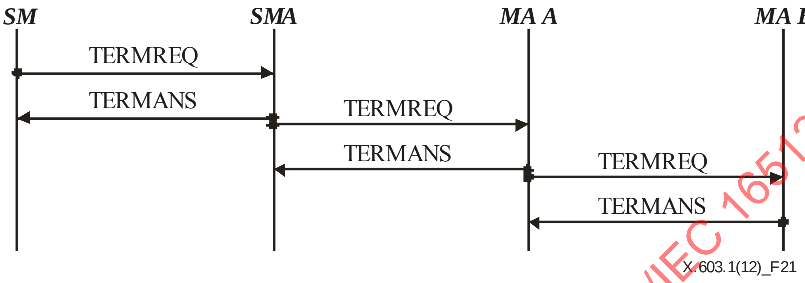


Figure 21 – Session termination issued by an SM

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 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.

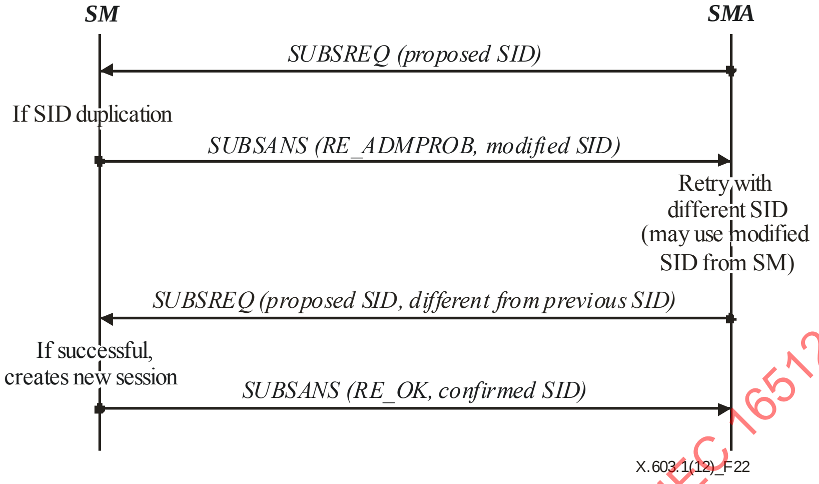

SM
SMA
SUBSREQ (proposed SID)
If SID duplication
SUBSANS (RE_ADMPROB, modified SID)
Retry with different SID (may use modified SID from SM)
SUBSREQ (proposed SID, different from previous SID)
If successful, creates new session
SUBSANS (RE_OK, confirmed SID)
X.603.1(12)_F22

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.

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.

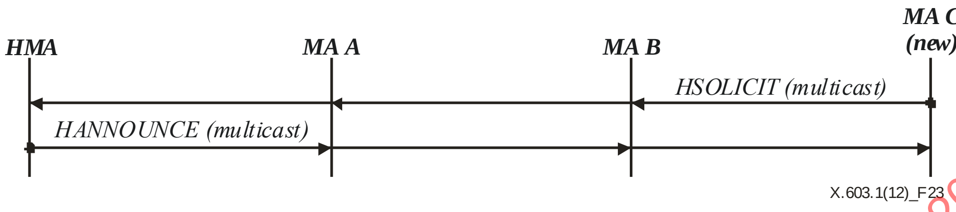


Figure 23 – HMA solicitation and announcement

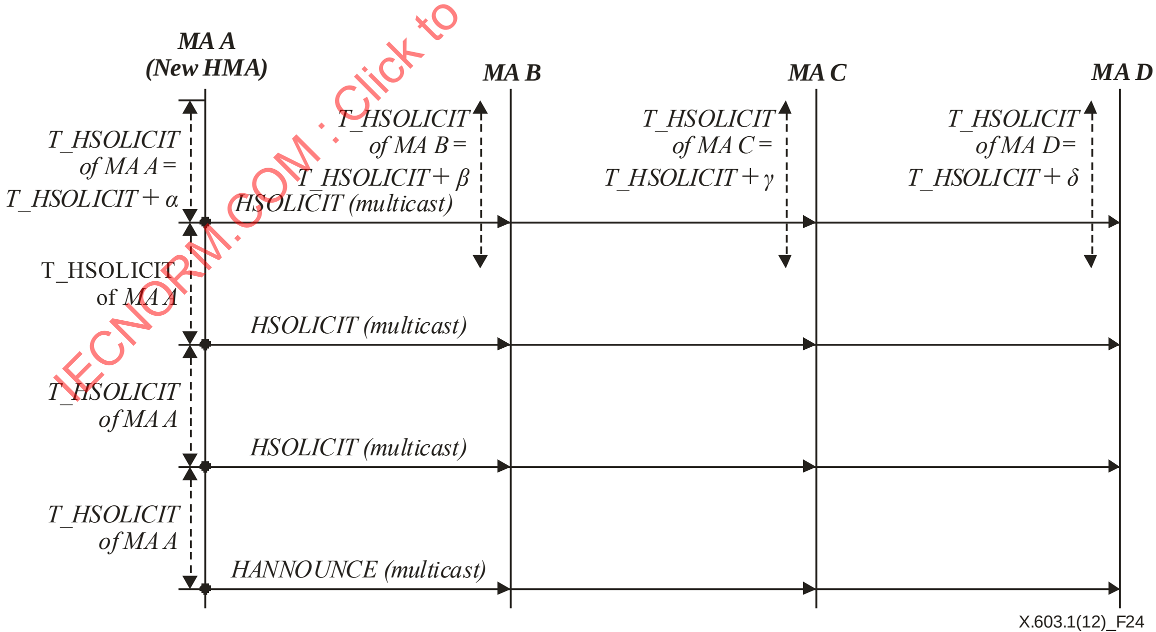
7.2.2.1.3 New HMA election

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.



$\alpha, \beta, \gamma, \delta$: Criteria factor

Figure 24 – HMA election

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.

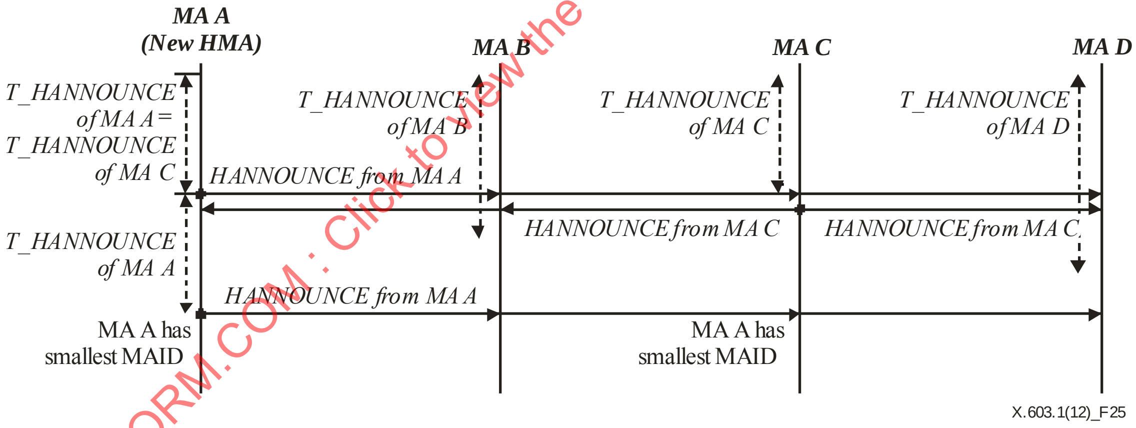


Figure 25 – HANNOUNCE message contention

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.

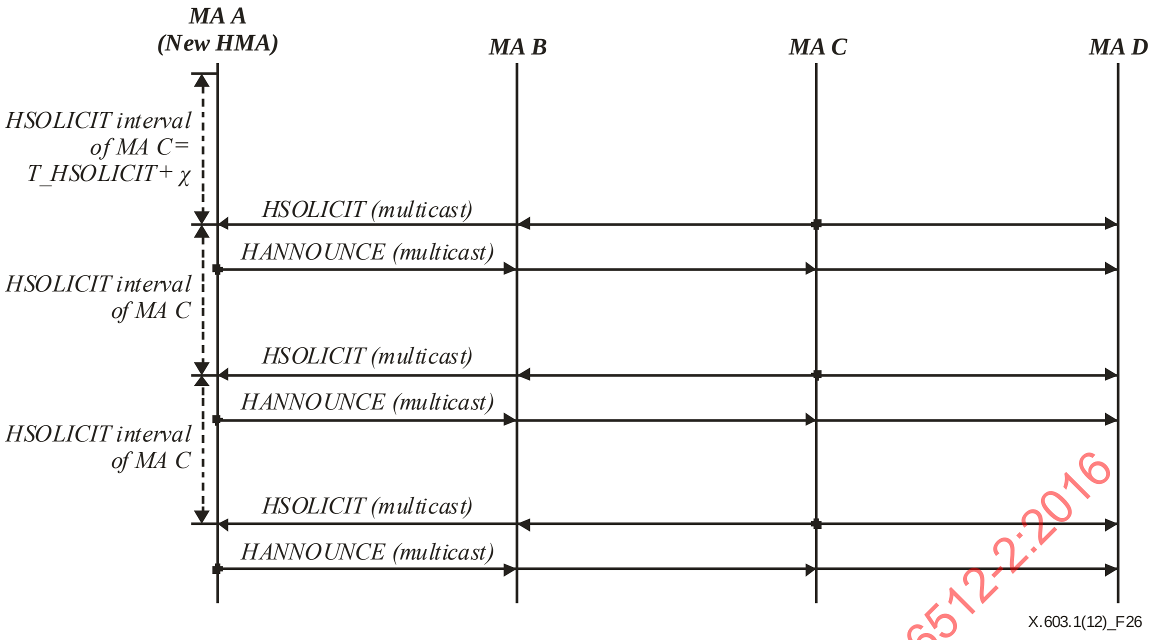


Figure 26 – Periodic HMA announcement

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.

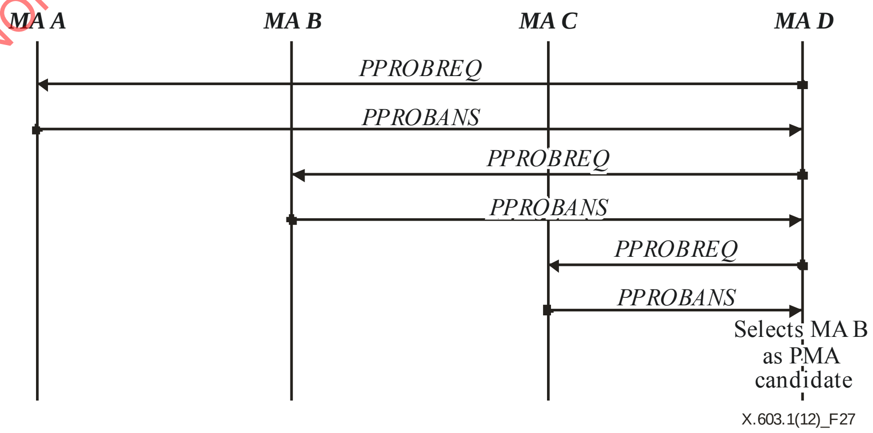


Figure 27 – Neighbour discovery in a unicast network

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.

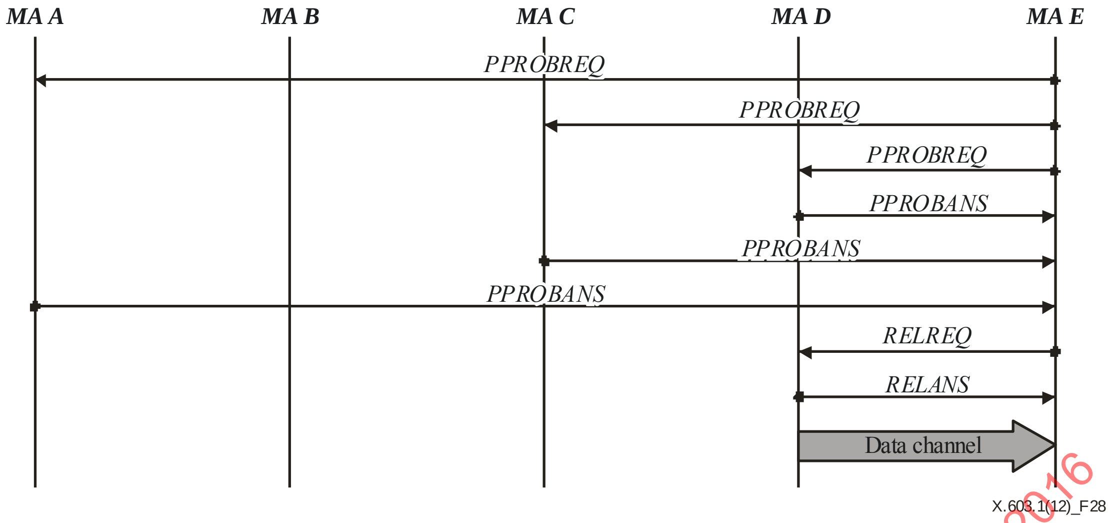


Figure 28 – Successful session join

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.

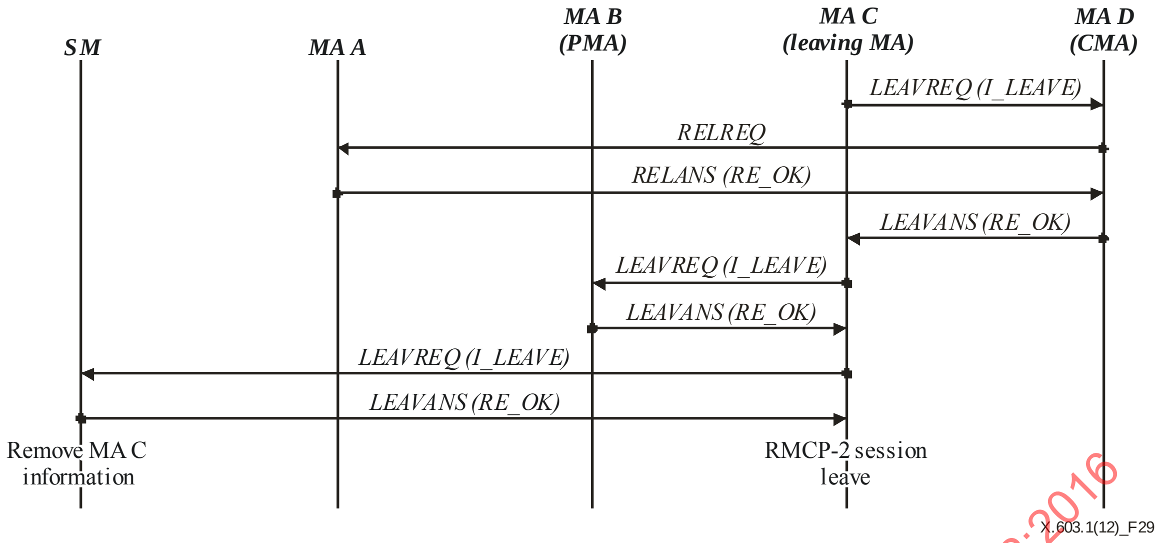


Figure 29 – MA leave in a unicast network

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.

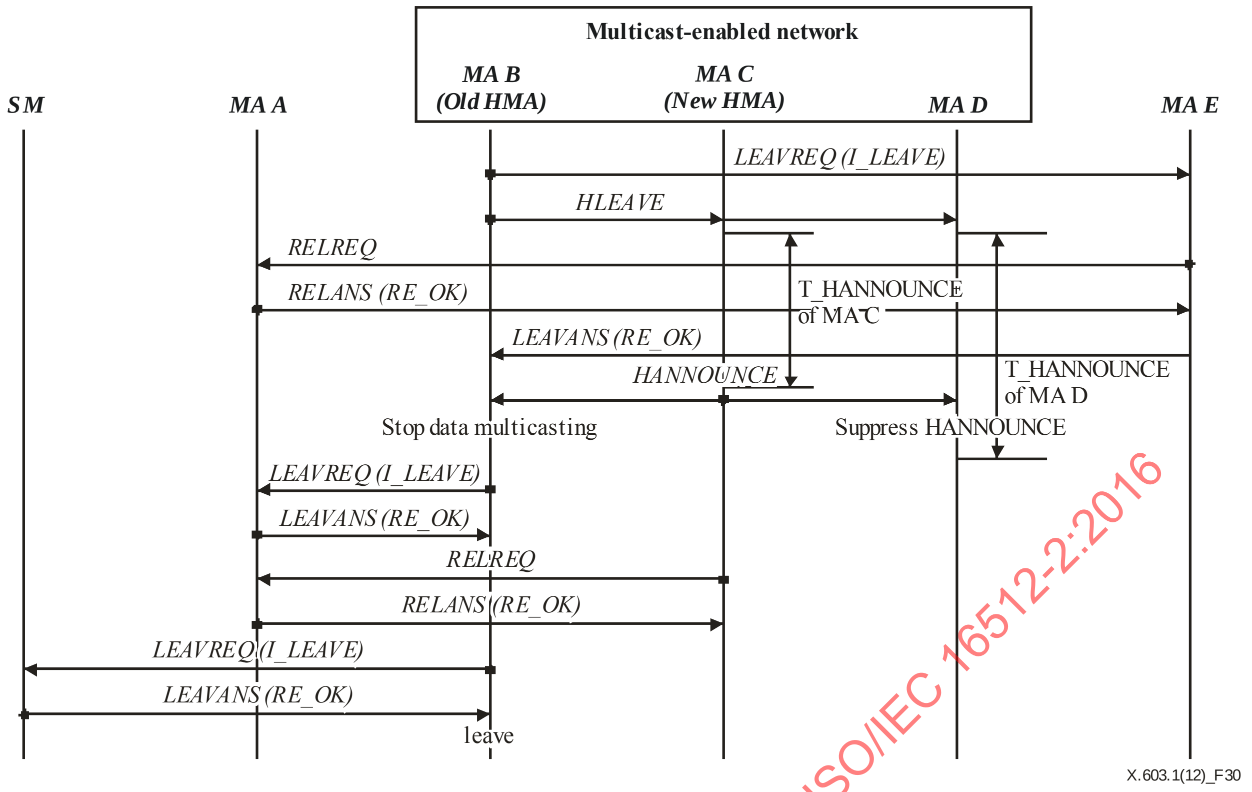


Figure 30 – HMA leave in a multicast network

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.

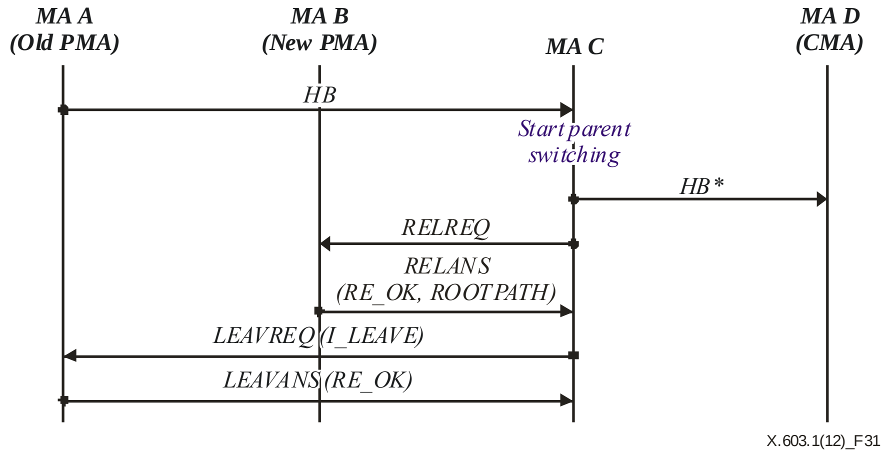


Figure 31 – Parent switching

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.

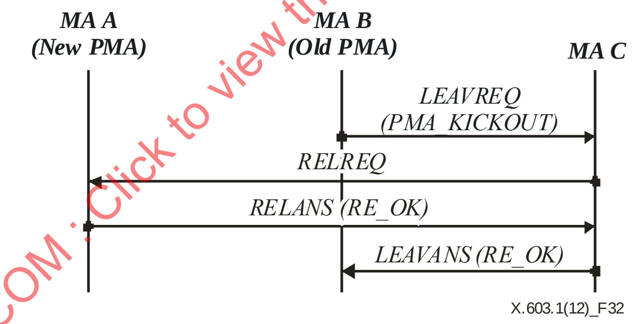


Figure 32 – Expulsion by PMA

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.

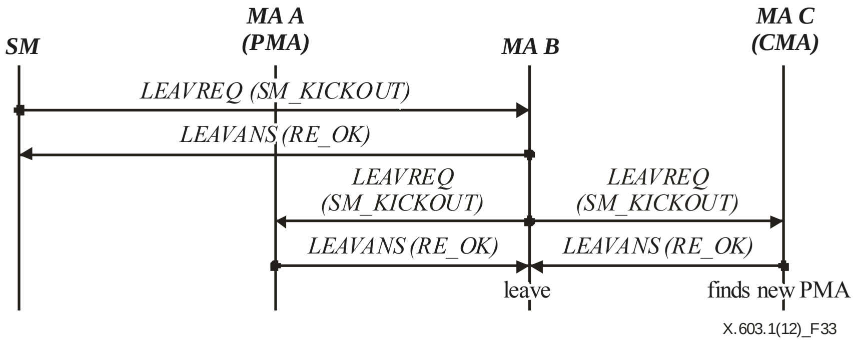


Figure 33 – Expulsion by the SM

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.

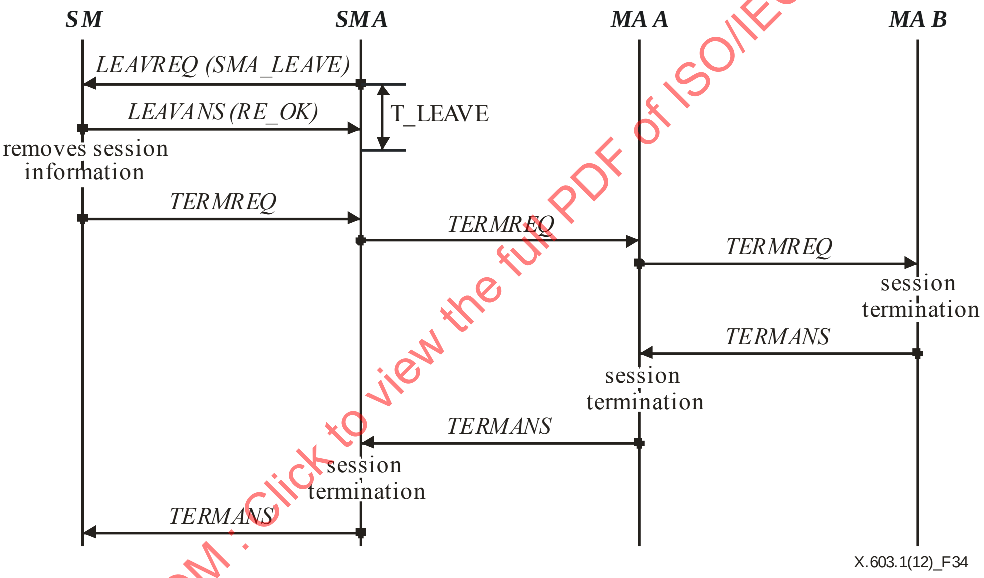


Figure 34 – SMA leave

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

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.

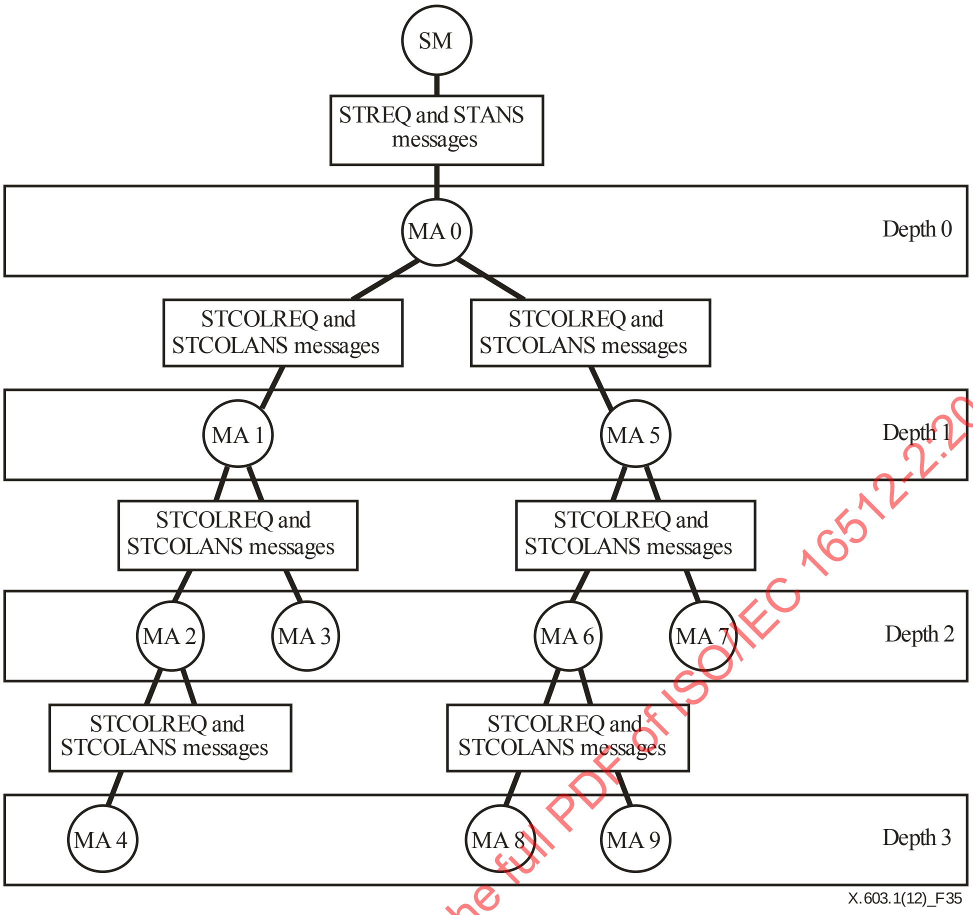

SM
STREQ and STANS messages
MA 0
Depth 0
STCOLREQ and STCOLANS messages
STCOLREQ and STCOLANS messages
MA 1
MA 5
Depth 1
STCOLREQ and STCOLANS messages
STCOLREQ and STCOLANS messages
MA 2
MA 3
MA 6
MA 7
Depth 2
STCOLREQ and STCOLANS messages
STCOLREQ and STCOLANS messages
MA 4
MA 8
MA 9
Depth 3
X.603.1(12)_F35

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.

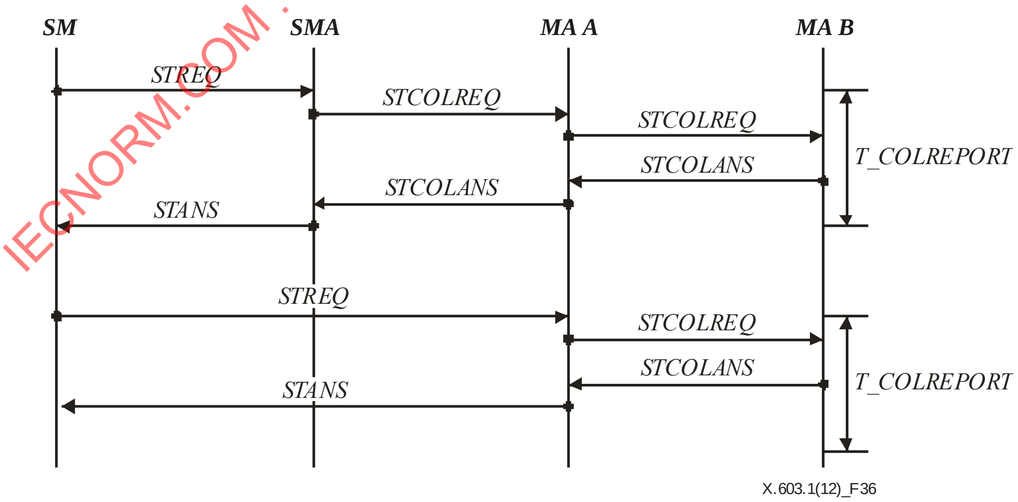


Figure 36 – Tree monitoring by collecting a status report

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.

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).

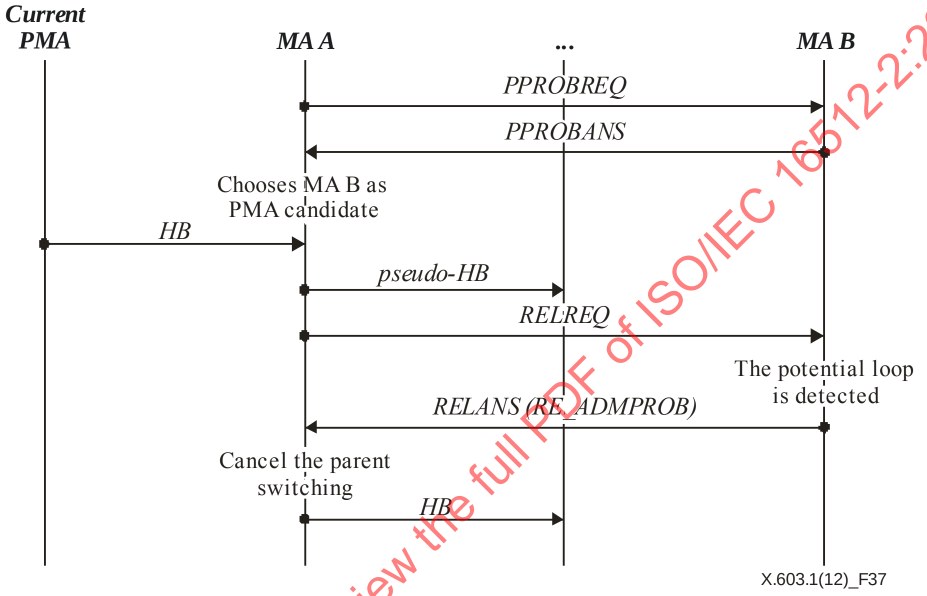


Figure 37 – Loop detection and prevention

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.

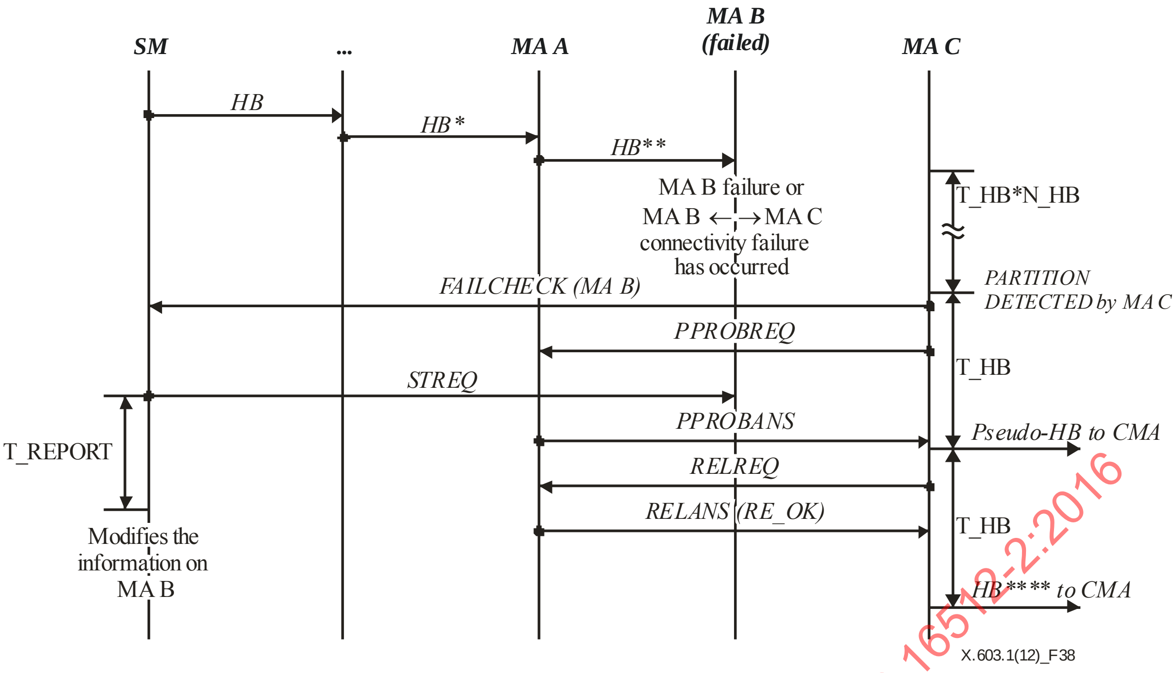


Figure 38 – Network partitioning detection and recovery

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.

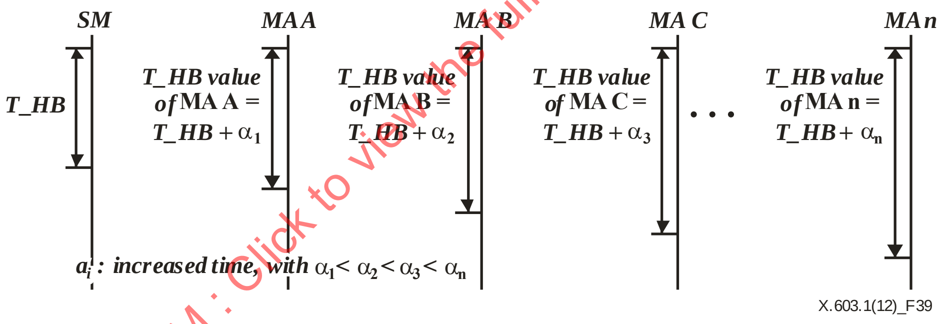

SM
MA A
MA B
MA C
MA n
T_HB
T_HB value of MA A = T_HB + α1
T_HB value of MA B = T_HB + α2
T_HB value of MA C = T_HB + α3
. . .
T_HB value of MA n = T_HB + αn
αi : increased time, with α1 < α2 < α3 < αn
X.603.1(12)_F39

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.

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.

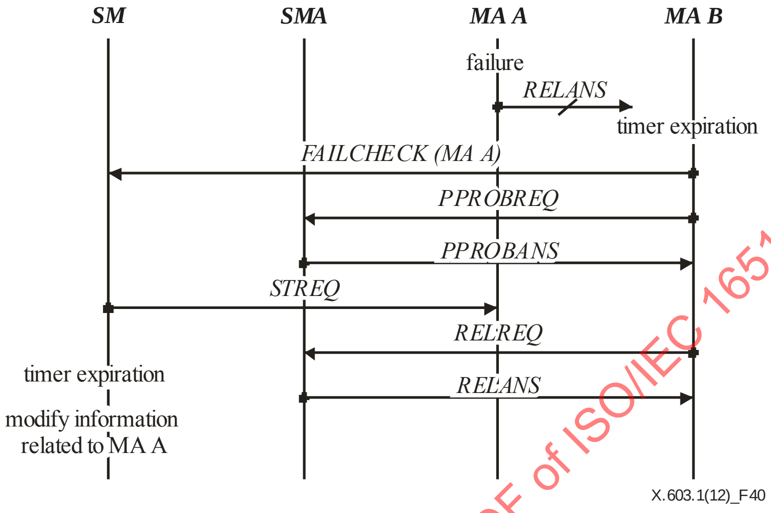


Figure 40 – PMA failure detection and recovery

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.

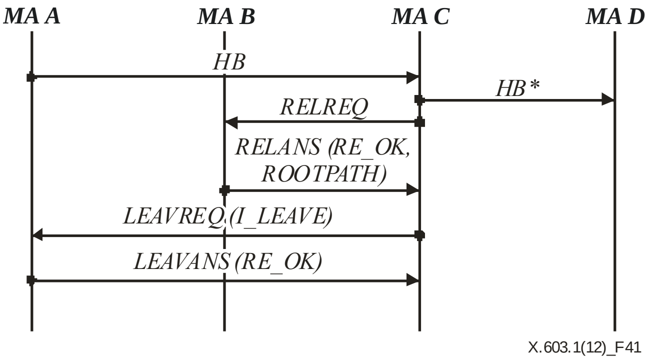


Figure 41 – Parent switching

When an MA starts parent switching, it sends a pseudo-HB message to its CMA(s) to prevent its CMA(s) from conducting partition recovery. Although an MA can change its PMA only when it receives an HB message, an MA does not change its PMA when it receives a pseudo-HB message. Since simultaneous parent switching among multiple MAs can cause network partition or loops, the MA should not conduct parent switching when its PMA is in the middle of parent switching.

7.2.6 Termination

To terminate an ongoing session, the SM sends a TERMREQ message to the SMA as shown in Figure 21. An SMA (or MA) that receives a TERMREQ message from the SM (or PMA) sends the TERMANS message back to the SM (or PMA) and forwards the TERMREQ message to its CMA(s) until it reaches the end nodes of the tree. Upon receiving a TERMANS message, the SM and MA remove the information related to the closed session.

8 Protocol operation for secure RMCP-2

8.1 Session manager's operation

The SM supports the establishment of security policies applied to each secure RMCP-2 session, and is responsible for user and MA security management such as user and MA authentication. It manages the session key for each RMCP-2 session through the creation, updating and distribution of key information. The SM also has message encryption and decryption abilities through the use of TLS and owned cryptography suites.

8.1.1 Admission control

8.1.1.1 TLS authentication

TLS authentication is performed in advance of the subscription requests of MAs (SMA, DMAs or RMAs). An MA establishes a TLS session with the SM according to IETF RFC 6066. The SM, as part of the IETF RFC 6066 procedure, decides which TLS mode, TLS_CERT or TLS_PSK, is applied for the verification of the parties concerned. The SM responds to the MA and if mutual authentication is successful, it shares a secret key K_{TLS} with the MA.

The SM also delivers the session key Ks, encrypted using K_{TLS}, to the SMA and the DMAs, but not to the RMAs.

The TLS session with the SMA and DMAs is closed after the session key is delivered, since the SM, SMA and DMAs exchange messages that have been encrypted with the session key. The TLS session with RMAs is retained and not closed until membership authentication with their parent DMA in the secure tree join procedure (see clause 8.2.4) and the individual key K_{MAS} has been established.

8.1.1.2 Admission of the SMA

A secure RMCP-2 session is initiated through the subscription of the SMA. The SMA first obtains authorization for providing the contents from the SM. The SMA is authenticated by the SM through the TLS session (see clause 8.1.1.1) and then joins the session by exchanging SUBSREQ and SUBSANS messages with the SM. As a result of this, the SMA receives the session key Ks and is enabled to act as an administrative node of the secure RMCP-2 tree.

8.1.1.3 Admission of DMAs

The DMAs, as prospective trust parties, are invited by the SM to join the session and to establish the DMA network before the subscription of RMAs. The means of this invitation are outside the scope of this Recommendation | International Standard.

The DMAs are authenticated by the SM through the TLS session and they join the session through the exchange of SUBSREQ and SUBSANS messages with the SM. They receive the session key Ks from the SM and join the RMCP-2 tree through the secure tree join procedure (see clause 8.2.4).

The SM consults with the DMAs joining the session before the announcement of the opening of the secure RMCP-2 session, giving a date and time when the subscription of RMAs begins. The means of this announcement are outside the scope of this Recommendation | International Standard.

8.1.1.4 Admission of RMAs to open groups

A potential RMA will know from the announcement of the session whether or not the session supports open groups. The RMAs are authenticated by the SM through the TLS session and join the session through the exchange of SUBSREQ and SUBSANS messages with the SM. They do not receive the session key Ks. They join the RMCP-2 tree through the secure tree join procedure (see clause 8.2.4).

8.1.1.5 Admission of RMAs to closed groups

A potential RMA will know from the announcement of the session whether or not the session supports closed groups. Access to membership of closed groups is controlled by the content provider (CP). A potential RMA requests a service user identifier from the CP. The CP provides a service user identifier to the potential RMA and also sends the service user identifier, without revealing the identity of the potential RMA, to the SM. The CP is responsible for the format of this identifier and this is not defined in this Recommendation | International Standard.

When the session is opened to RMAs, the RMAs are authenticated by the SM through the TLS session and they join the session through the exchange of SUBSREQ and SUBSANS messages with the SM. The SUBSREQ message shall contain the service user identifier. The SM shall send a rejection in the RESULT control of the SUBSANS message if the SM does not hold an identical service user identifier.

The RMAs do not receive the session key Ks. They join the RMCP-2 tree through the secure tree join procedure (see clause 8.2.4).

8.1.2 Key management for which the SM is responsible

8.1.2.1 Session key

The session key (K_s) is shared between the SM, the SMA and DMAs and is used to encrypt/decrypt messages in the RM region. It is initially created by the SM in the bootstrapping of the RMCP-2 session. K_s is encrypted by the individual key K_{TLS} (see clause 8.1.2.2) for delivery to the SMA and to each DMA through the data protection procedure of the TLS following successful TLS authentication.

K_S is updated at regular intervals through the hash function. When a DMA is truncated or an abnormal situation occurs, the SM does not use the hash function, but instead creates a totally new session key K_S, without hashing. The new key is delivered to the SMA and all DMAs in the RMCP-2 session (see Figure 42).

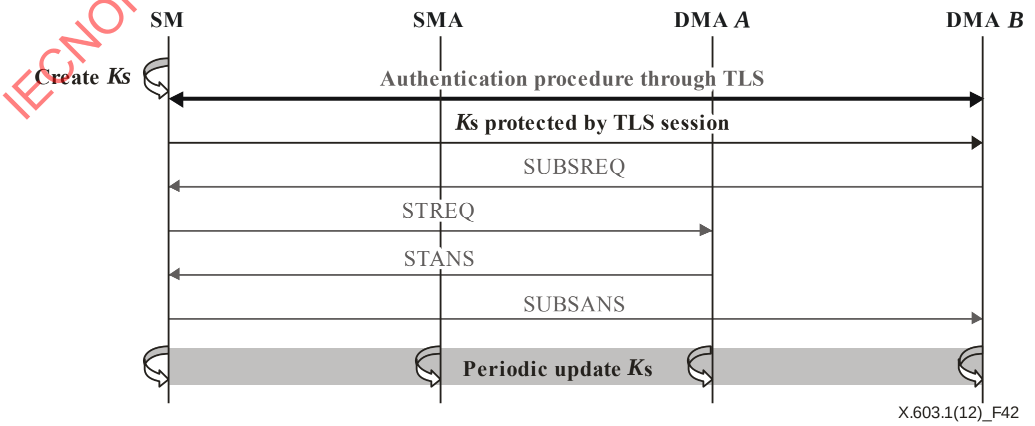


Figure 42 – Session key management

8.1.2.2 TLS key

The TLS key K_{TLS} is a private key generated through successful TLS authentication during admission control. Each MA (SMA, DMA and RMA) shares a different K_{TLS} with the SM, which is not shared with the other MAs. K_{TLS} is not updated during the lifetime of the RMCP-2 session.

8.1.3 Establishment of security policy

When a new RMCP-2 session is created, the SM, together with the SMA and the DMAs, establish the security policy for the session. The policy is established through the exchange of SECAGREQ, SECLIST and SECAGANS messages that enable the selection of the parameters in Table 2 to define the level of security that is to be provided, as well as the choice of algorithms to be used. The security policy is the set of selected attributes of policy items after the agreement on security mechanisms.

Table 2 – Multicast security policy

Item	Attributes	Definition	Further details
CON_EN_DEC_ID	– AES CBC Mode 128-bit key – AES CTR Mode 128-bit key – PKCS #1 – SEED	Notifies which encryption/decryption algorithm is used for content data	See Table 39
GK_EN_DEC_ID	– AES CBC Mode 128-bit key – AES CTR Mode 128-bit key – PKCS #1 – SEED	Notifies which encryption/decryption algorithm is used for content data for group keys	See Table 39
AUTH_ID	– HMAC-SHA – HMAC-MD5 – MD5	Notifies which hash/MAC algorithm is applied	See Table 40
GP_ATTRIBUTE	– closed – open (default)	Notifies the nature of the group	See Table 41
GK_MECHA	– static – periodic – backward – forward – periodic+backward – periodic+forward – periodic+backward +forward	Notifies updating properties of the group key	See Table 42
GK_NAME	– KDC – GKMP – MIKEY – GSAKMP – LKH	Notifies which group key mechanism is used	See Table 43
AUTH_ATTRIBUTE	– membership	Notifies the type of authentication used	See Table 44
AUTH_NAME	– MEM_AUTH	Notifies the authentication mechanism used	See Table 45

8.1.4 Agreement of security mechanisms

8.1.4.1 Agreement between SMA and DMAs

The security procedure is initiated after the admission control. The messages are protected by the session key between the SM, SMAs and DMAs, and by the K_{TLS} between the SM and the RMAs. The SMA and the DMAs perform the procedure prior to RMA subscription because the server-oriented systems (SMA and DMAs) need to set up the security policy in order to provide a stable service. The SMA and DMAs (see Figure 43) each request a security agreement (SECAGREQ) containing their own security mechanisms and algorithms. After a Security Agree.time, the SM examines the SECAGREQ messages, determines the security policy for the session and sends the security policy (SECLIST) to the SMA and DMAs. If any of these MAs do not have the algorithms of the security policy, they request copies from the SM (SECALGREQ) and the SM sends the corresponding security modules to them. The method for the delivery of these modules is outside the scope of this Recommendation | International Standard. The SMA and each DMA configures the agreed security mechanisms. After configuration, the MAs send an acknowledgement (SECAGANS) to the SM.

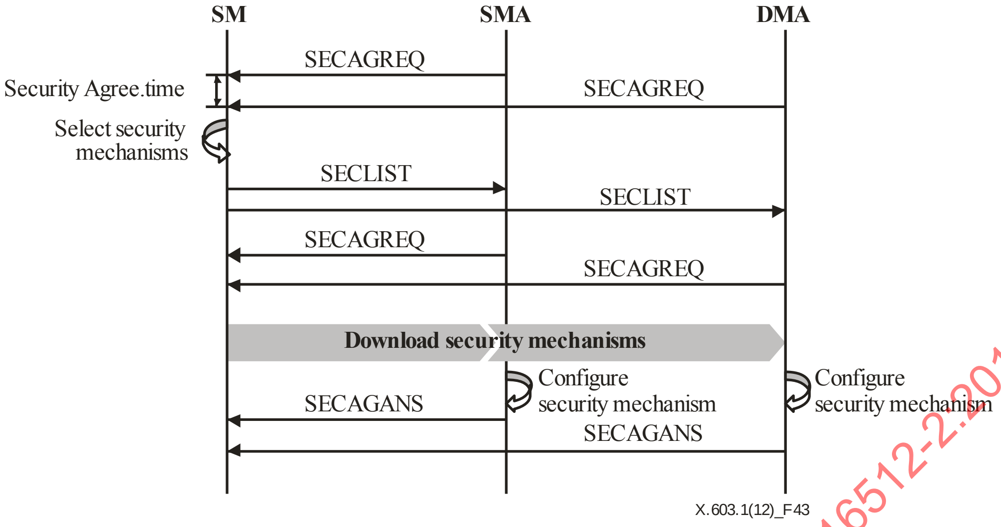

SM
SMA
DMA
SECAGREQ
SECAGREQ
Security Agree.time
Select security mechanisms
SECLIST
SECLIST
SECAGREQ
SECAGREQ
Download security mechanisms
Configure security mechanism
Configure security mechanism
SECAGANS
SECAGANS
X.603.1(12)_F43

Figure 43 – Security agreement of DMA and SMA

8.1.4.2 Agreement between RMAs

When the session is opened for RMA subscription, each RMA requests a security agreement (SECAGREQ) (see Figure 44). The SM sends the security policy (SECLIST) to the RMA. If the RMA does not have any of the algorithms of the security policy, it requests copies from the SM (SECALGREQ) and the SM sends the corresponding security modules to the RMA. The method for the delivery of these modules is outside the scope of this Recommendation | International Standard. The RMA configures the agreed security mechanisms and sends an acknowledgement (SECAGANS) to the SM.

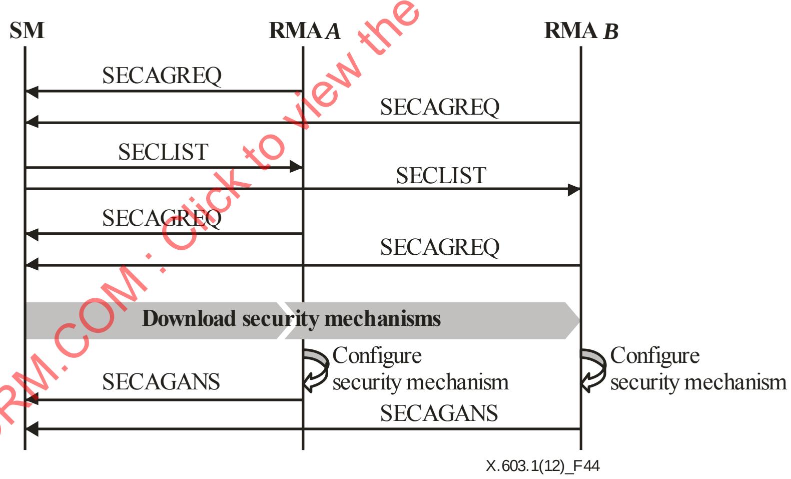


Figure 44 – Security agreement of RMAs

8.1.5 Access control for RMAs

The SM creates an access control list (ACL) containing a hashed MAID and HASHED_AUTH for each authenticated RMA in the current session. Figure 45 illustrates the ACL procedure. After the session has been opened to RMAs, a DMA may request an ACL from the SM using an HRSREQ message encrypted by Ks. The SM responds with an HRSANS message encrypted by Ks, which contains the ACL. A DMA may update its ACL information through the periodic exchange of HRSREQ and HRSANS messages with the SM.

A DMA shall reject a request from an RMA to join the group if the ACL list does not contain the information for that RMA.

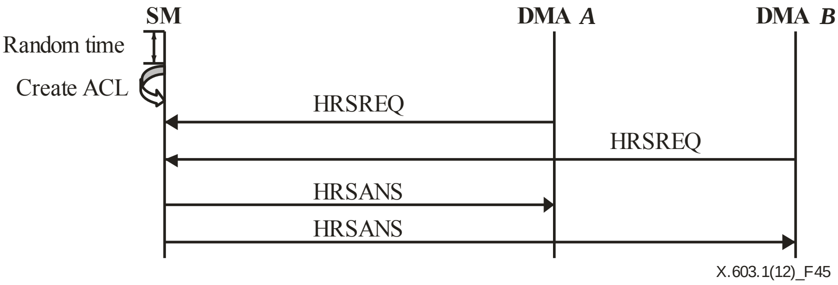


Figure 45 – ACL management

8.2 Multicast agent's operation

As main components of the secure RMCP-2, the SMA and the DMAs are responsible for secure tree configuration and key management, as well as for group and member management and message encryption/decryption.

8.2.1 Key management for which the SMA and DMAs are responsible

8.2.1.1 Group key management

A group key (Kg) is shared between a DMA and its child RMAs, and it is used in an MM-group for data delivery. The Kg is initially created by the DMA and is encrypted by K_{MAS} (see clause 8.2.1.3) for delivery to its RMAs in the RELANS message confirming successful membership authentication (see clause 9.3.9).

Kg is updated by the DMA or RMA according to the update conditions selected for the security policy (see the GK_MECHA control in Table 2). Figure 46 illustrates the group key management.

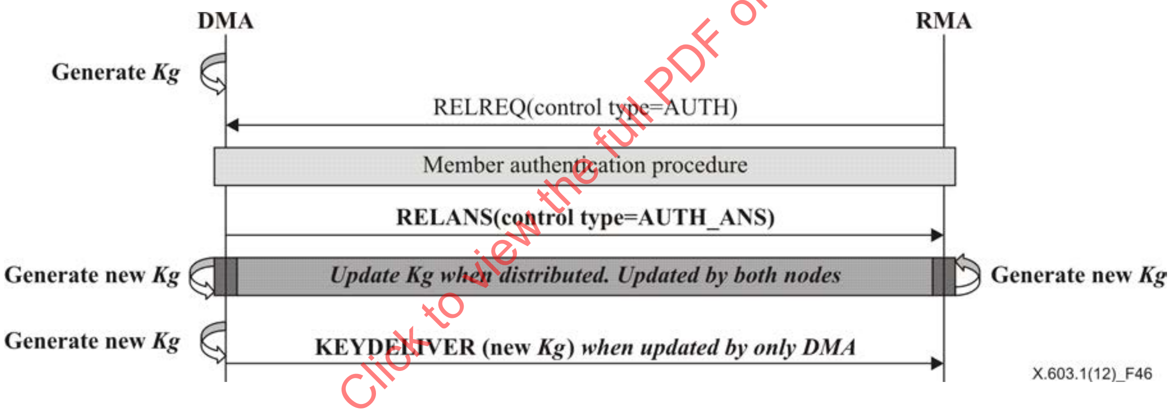

DMA
RMA
Generate Kg
RELREQ(control type=AUTH)
Member authentication procedure
RELANS(control type=AUTH_ANS)
Generate new Kg
Update Kg when distributed. Updated by both nodes
Generate new Kg
Generate new Kg
KEYDELIVER (new Kg) when updated by only DMA
X.603.1(12)_F46

Figure 46 – Group key management

8.2.1.2 Content encryption key management

The content encryption key (Kc) is shared between the SMA and RMAs in the RMCP-2 session and is used to encrypt/decrypt content data. Kc is generated by the SMA and is delivered to RMAs through the intermediate DMAs on the delivery path. Kc is encrypted by Ks for transmission between the SMA and DMAs and is encrypted by Kg for transmission between the DMAs and the RMAs. Kc key information need not be known by the SM or intermediate DMAs.

Kc is randomly updated by the SMA at periodic intervals. The delivery of Kc is synchronized with the delivery of the content data (see clause 8.2.7).

8.2.1.3 Membership authentication key

The membership authentication key K_{MAS} is a private key generated as a result of successful membership authentication between the RMAs and their parent DMA, as specified in Annex A. Each RMA shares a different K_{MAS} with the DMA and this is not shared with the other RMAs in the same group. K_{MAS} is not updated while the RMA remains a member of the relevant group.

8.2.2 Secure session subscription

The procedure for secure session subscription for the SMA, DMAs and RMAs is described in clauses 8.1.1.2, 8.1.1.3, 8.1.1.4 and 8.1.1.5. This procedure is illustrated in Figure 47.

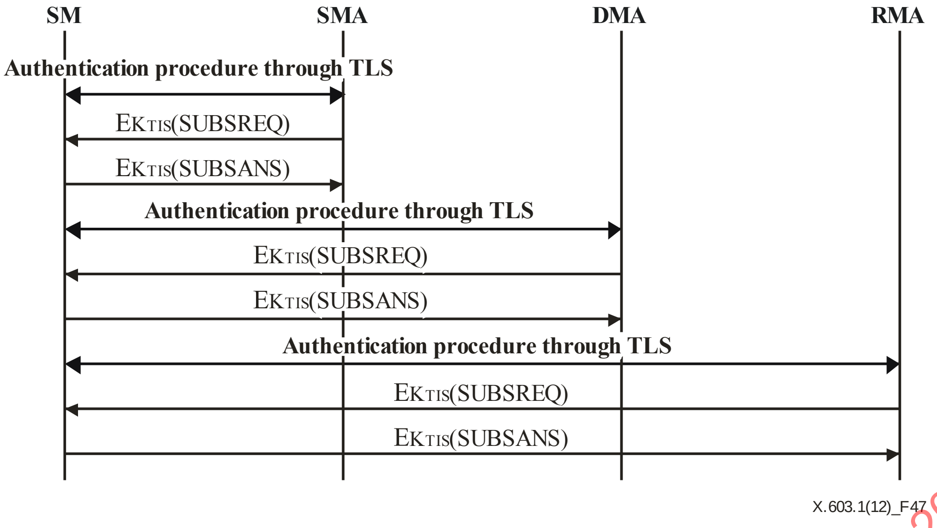


Figure 47 – Secure MA subscription

8.2.3 Membership authentication for joining the RMCP tree

Although DMAs are authenticated by the SM through TLS authentication, there is also a need for the DMAs and RMAs to verify their membership authority upon joining the RMCP tree and for the construction of the pathway from the SMA to the RMAs. This procedure is important for the integrity of the RMCP-2 tree.

The membership authentication procedure defined in Annex A is used for mutual authentication.

The procedure is illustrated in Figure 48. The RMA/DMA sends a RELREQ message confirming the use of the membership authentication mechanism defined in Annex A. The SMA/DMA responds with a RELANS message containing the authentication result in the AUTH_ANS control. If the recipient is an RMA, the message to the RMA shall include the KEY_MATERIAL sub-control.

On receipt of confirmation by the RMA, the TLS session between the SM and the RMA need not be maintained.

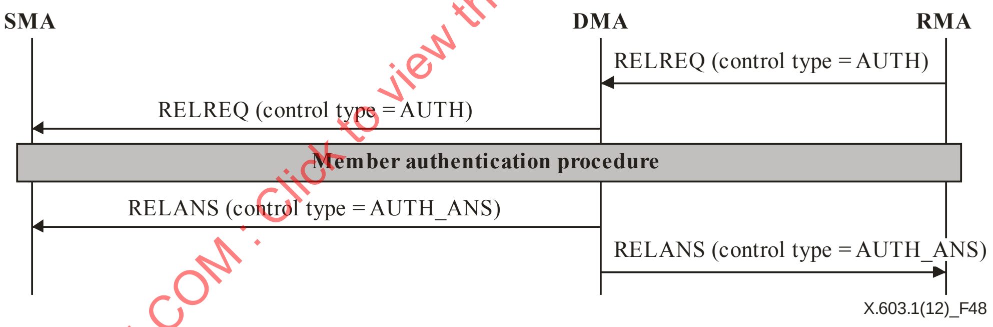

SMA
DMA
RMA
RELREQ (control type = AUTH)
RELREQ (control type = AUTH)
Member authentication procedure
RELANS (control type = AUTH_ANS)
RELANS (control type = AUTH_ANS)
X.603.1(12)_F48

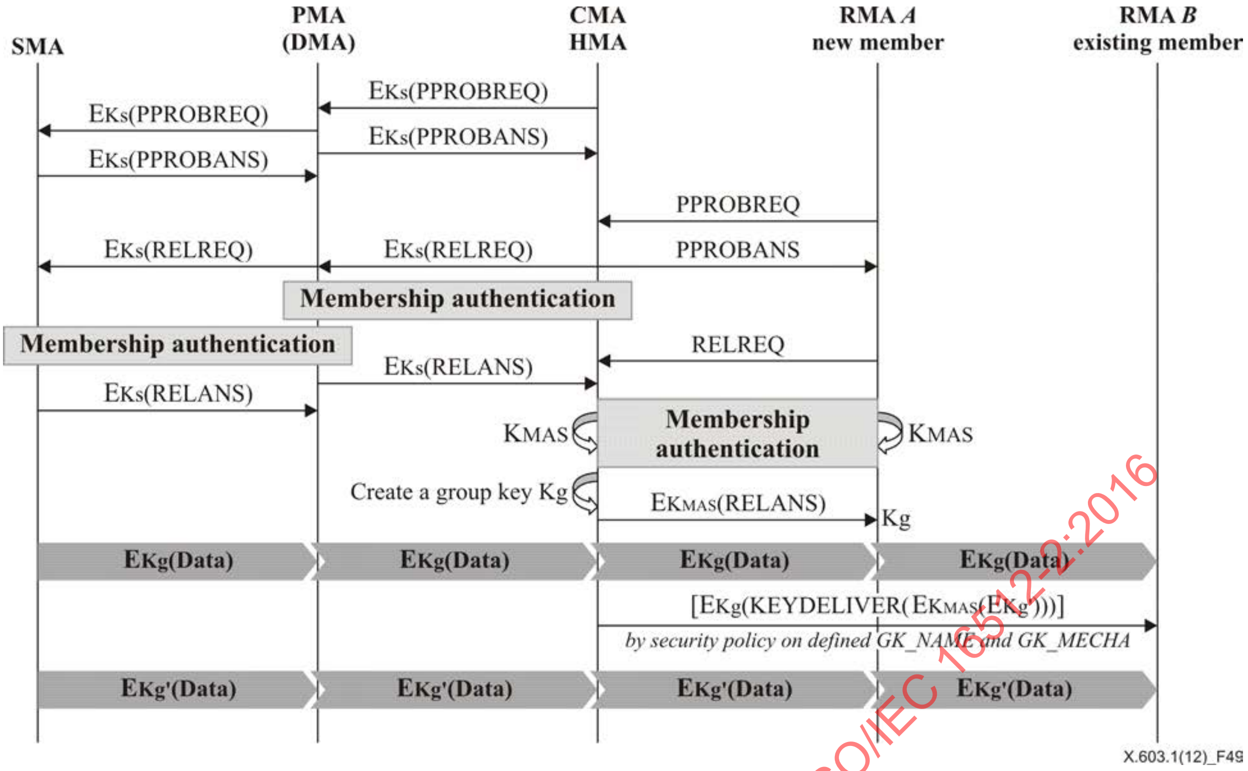
Figure 48 – Authentication between MAs

8.2.4 Secure tree join

Neighbour discovery (see clause 7.2.2) occurs before the tree join procedure. Neighbour discovery messages (PPROBREQ and PPROBANS) between DMAs are securely transmitted using Ks. Neighbour discovery messages between RMAs and DMAs are delivered with hashed AUTH in plain text.

The tree join procedure is illustrated in Figure 49. Membership authentication (see clause 8.2.3) and group key distribution are processed. When the group key update is required (as indicated by the defined GK_MECHA code in the SECLIST, see Table 42), the parent DMA (see Note) of the RMA joining the tree re-creates and distributes the group key to its RMAs using the GK_NAME mechanism selected for the security policy (see Table 43). When this procedure is completed, the TLS session between the SM and the RMA is closed.

NOTE – In the case of the group in a multicast network, the parent DMA will be the HMA.



NOTE – The PPROBREQ, PPROBANS and RELREQ messages between RMA A and the HMA are not encrypted, as RMA A has not yet received the KMAS or Kg keys.

Figure 49 – Secure tree join

8.2.5 Secure tree leave

Whenever an HMA, DMA or RMA leaves the group, the group key or the session key may be updated on the defined GK_MECHA code of multicast security policy (see Table 42).

8.2.5.1 Leave of RMA from a multicast network and unicast network

When an RMA leaves, it notifies its parent DMA (its HMA in the case of a multicast network) and it is truncated from the tree. The DMA acknowledges the result, and updates and distributes the updated group key to the remaining members (see Figure 50). No further notification is required.

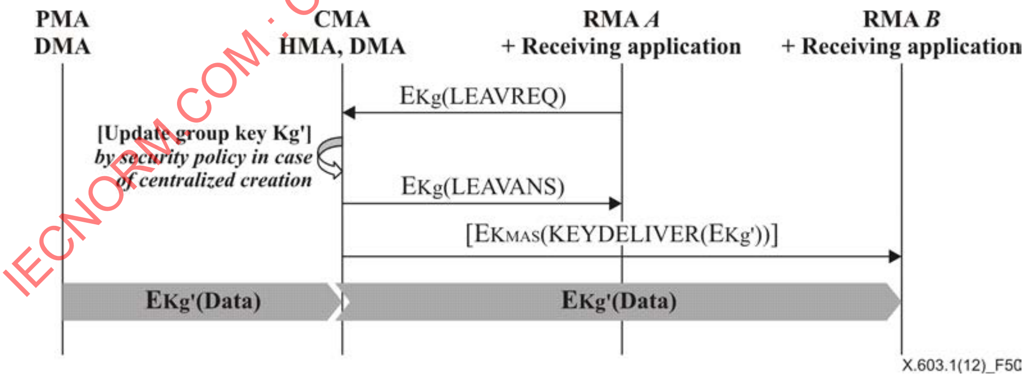

PMA DMA
CMA HMA, DMA
RMA A + Receiving application
RMA B + Receiving application
EKg(LEAVREQ)
[Update group key Kg'] by security policy in case of centralized creation
EKg(LEAVANS)
[EKMAS(KEYDELIVER(EKg'))]
EKg'(Data)
EKg'(Data)
X.603.1(12)_F50

Figure 50 – Secure leave of RMA

8.2.5.2 Leave of HMA from a multicast network

Figure 51 illustrates the HMA leave procedure. The HMA issues a leave request to its members, and announces the leave to its candidate HMAs. The successful candidate HMA joins the RMCP-2 tree and announces its existence to the RMAs in its MM group. The RMAs request to re-join tree and perform membership authentication with the new HMA. The RMAs are then able to receive multicast data normally from the new HMA, and the old HMA leaves the RMCP-2 tree or see Figure 51.

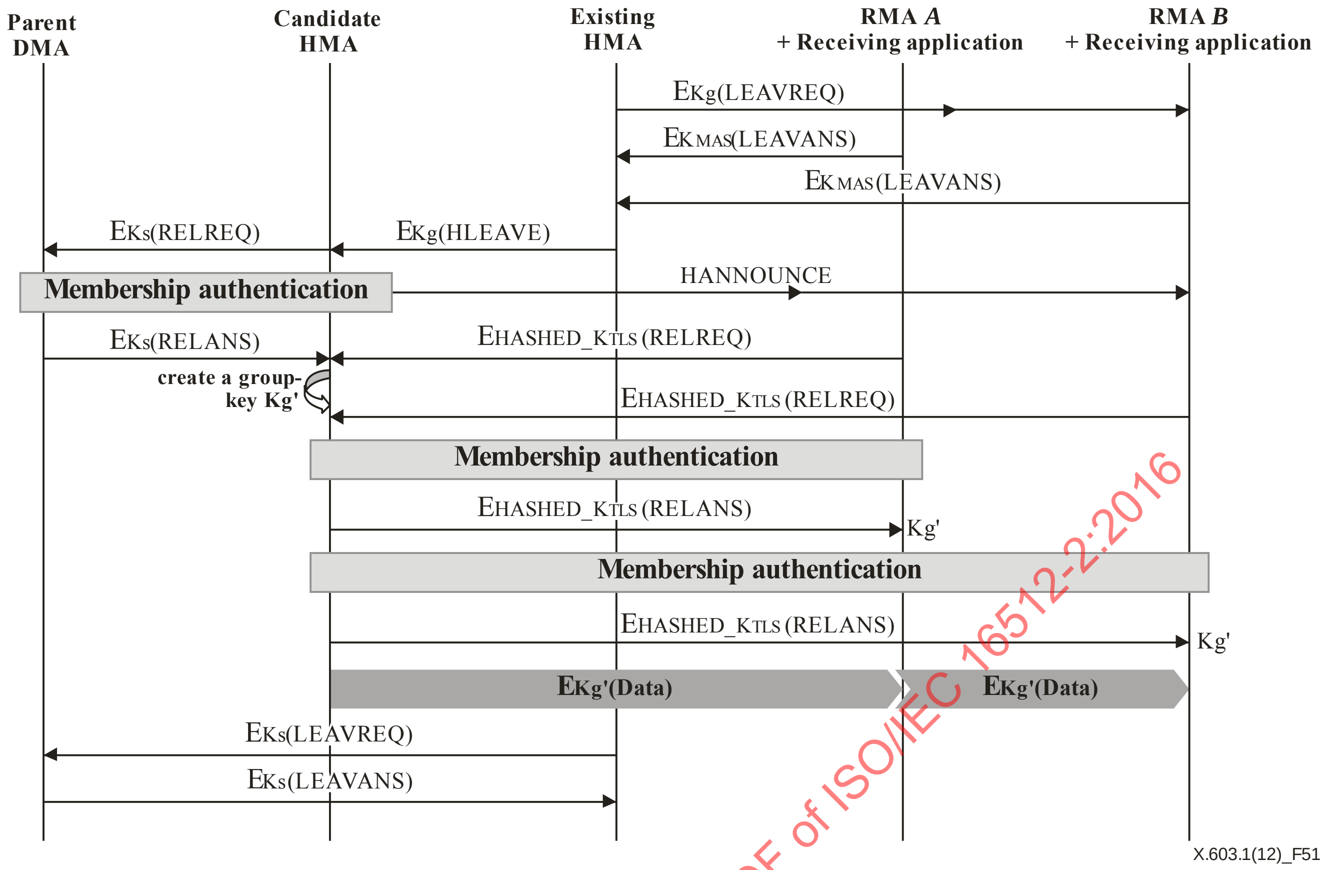


Figure 51 – HMA leave in a multicast network

8.2.5.3 Leave of DMA from a unicast network

Figure 52 illustrates the leave of a DMA from a unicast network. The DMA (PMA A of B, C) announces its departure from the RMCP tree to its CMAs (CMA B and CMA C). CMAs B and C search for their PMA candidate and perform the join procedure as shown in Figure 52. CMAs B and C request to join the RMCP tree at the node of the PMA candidate. The PMA verifies the authenticity of CMAs B and C, and if the authentication check is successful, it sends RELANS message to confirm the graft to the RMCP tree. The PMA of B, C then initiates the leaving procedure with its PMA.

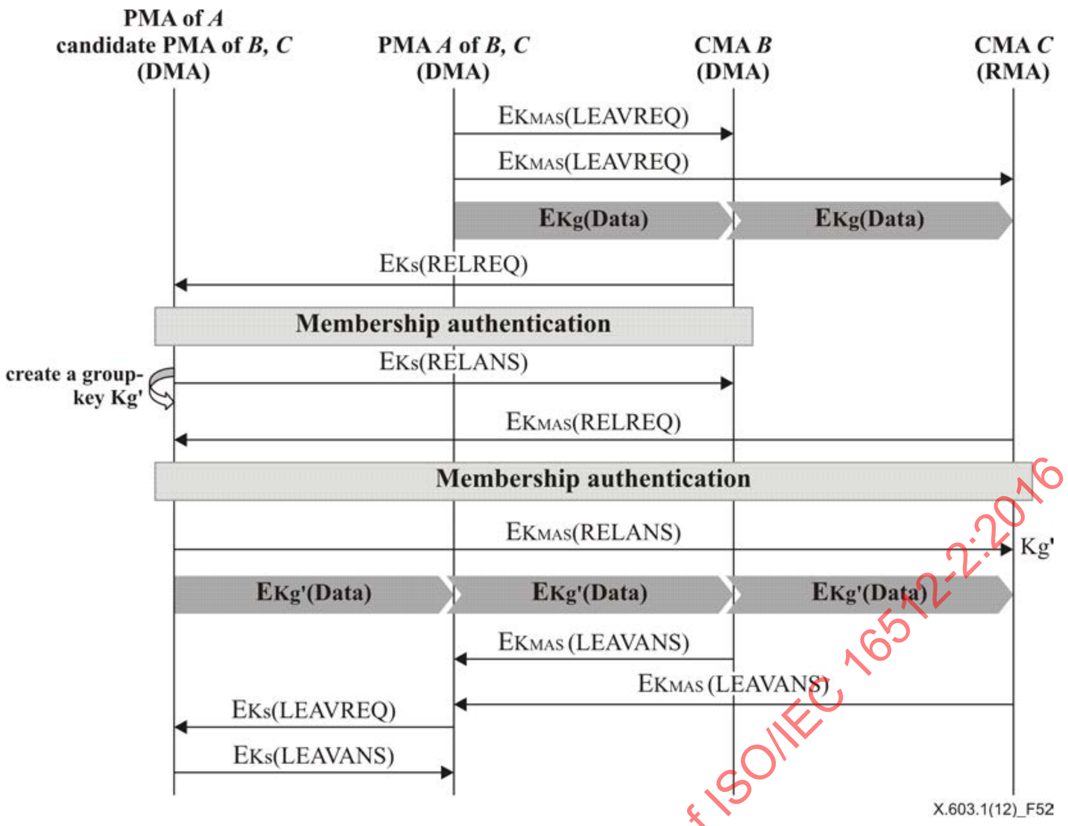


Figure 52 – DMA leave in a unicast network

Membership authentication is performed between the RELREQ and RELANS messages in cases when a CMA is expelled by the PMA. If the SM expels an MA, the LEAVREQ and LEAVANS messages are en/decrypted.

8.2.6 Message encryption/decryption

All secure RMCP-2 messages between the SM, SMA and DMAs are encrypted using agreed encryption algorithms in the SECLIST message. Messages between RMAs and their parent DMA are encrypted by K_{MAS}, as shown in Table 3.

Table 3 – Encryption of basic and secure RMCP-2 messages

Messages	Meaning	Key	
		DMA	RMA
SUBSREQ	Subscription request	Ks	K_{TLS}
SUBSANS	Subscription answer		K_{TLS}
PPROBREQ	Parent probe request		N/A
PPROBANS	Parent probe answer		N/A
HSOLICIT	HMA solicit		N/A
HANNOUNCE	HMA announce		N/A
HLEAVE	HMA leave		N/A
RELREQ	Relay request		K_{MAS}
RELANS	Relay answer		K_{MAS}
STREQ	Status report request		K_{TLS}
STANS	Status report answer		K_{TLS}
STCOLREQ	Status collect request		N/A
STCOLANS	Status collect answer		N/A
LEAVREQ	Leave request		K_{MAS}

Table 3 – Encryption of basic and secure RMCP-2 messages

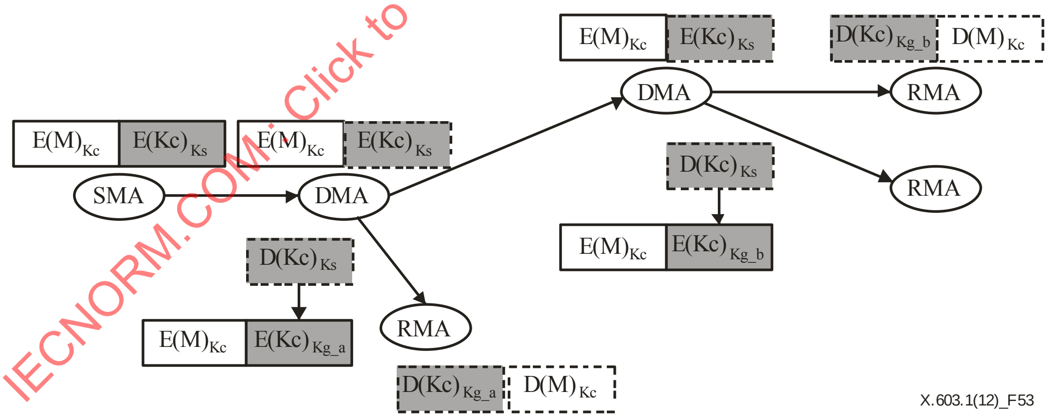
Messages	Meaning	Key	
		DMA	RMA
LEAVANS	Leave answer		K_{MAS}
HB	Heartbeat		N/A
TERMREQ	Termination request		HASHED K_{TLS}
TERMANS	Termination answer		HASHED K_{TLS}
FAILCHECK	Failure check request		N/A
SINFO	Session information		N/A
SMNOTI	SM notification		N/A
SECAGREQ	Security agreement request		K_{TLS}
SECLIST	Security list		K_{TLS}
SECALGREQ	Security algorithm request		K_{TLS}
SECAGANS	Security agreement answer		K_{TLS}
KEYDELIVER	Key delivery		K_{MAS}, K_g
HRSREQ	Head required security request		N/A
HRSANS	Head required security answer		N/A

8.2.7 Encryption/decryption and delivery of content data

The contents are securely forwarded from the SMA to the RMAs through the RMCP tree. Streaming or reliable data encrypted by *Kc* is delivered to individual RMAs without a decryption process at the intermediate nodes. In contrast, the key information is encrypted at intermediate nodes. The SMA encrypts *Kc* using *Ks* and delivers it to the DMAs. The DMAs then decrypt the key information and encrypt it using Kg for delivery to the RMAs in their own MM groups. Figure 53 illustrates how the encryption and decryption may be implemented.

The data and key information may be delivered separately. If separately transmitted, they should be synchronized.

NOTE – The encrypted data is efficiently transmitted to the RMAs without change in order to reduce the time of encryption/decryption by the intermediate nodes. Faster transmission is enabled due to the considerably reduced computation time.



NOTE – E(M) and D(M) refer to encrypted and decrypted data. E(Kc) and D(Kc) refer to encrypted and decrypted contents key information. Subscripts refer to keys used to encrypt (M) and (Kc). The suffixes $_{Kg\_a}$ and $_{Kg\_b}$ are used to distinguish different group keys used in separate MM groups.

Figure 53 – Example of data encryption/decryption

9 RMCP-2 message format

This clause describes the formats and required information of the RMCP-2 messages. This Recommendation | International Standard defines the RMCP-2 message format based on an IPv4 network.

9.1 Common format of RMCP-2 message

Figure 54 shows the common RMCP-2 message format. The values in parenthesis represent the length in bits of each field. Each field has the following meaning and value:

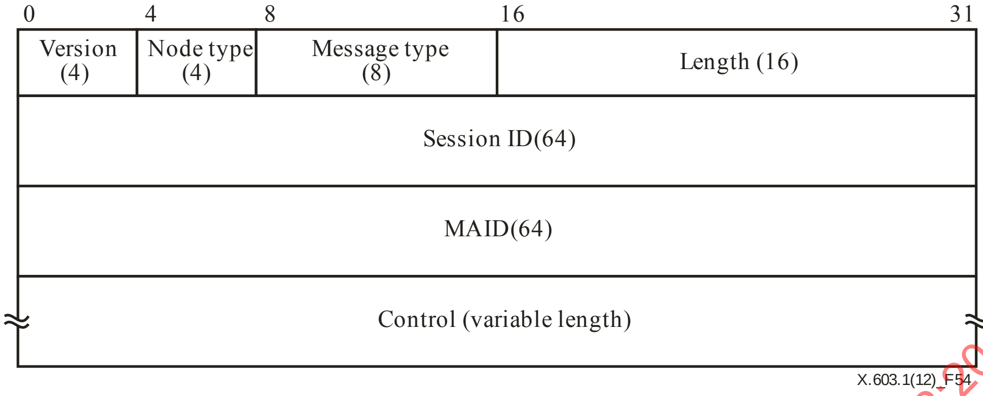


Figure 54 – Common RMCP-2 message format

a) *Version* – This field denotes the version of the protocol. Its value shall be set to 0x2 to indicate RMCP-2.

b) *Node type* – This field denotes the type of the node sending the message. Its value shall be set to one of the code values in Table 26.

c) *Message type* – This field denotes the type of the message. Its value shall be set to one of the code values in Table 27.

d) *Length* – This field denotes the total length in bytes of the message including control(s).

e) *Session ID* – This field shall be set to the 64-bit value that identifies the session. Its value shall be formatted as defined in clause 10.1.1.

f) *MAID* – This field shall be set to the MAID which is defined in each message. Its value shall be formatted as defined in clause 10.1.2.

g) *Control* – This field denotes the control used by each type of message as necessary.

9.2 Control data format

9.2.1 Common control format

The common control format used in RMCP-2 is shown in Figure 55. The meaning and value of each field is as follows:

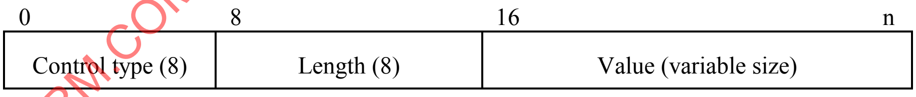


Figure 55 – RMCP-2 control format

a) *Control type* – This field denotes the type of control. Its value shall be set to one of the code values in Table 29.

b) *Length* – This field denotes the total length in bytes of the control including any sub-control(s). This field can be reserved, and it is set to zero according to the type of control.

c) *Value* – The contents of this field are defined for each control denoted in the control type field.

9.2.2 Common sub-control format

Whenever the RMCP-2 control specifies the use of sub-control(s), the sub-control(s) always follow the control type and length fields of the control. The format of the sub-control and its preceding control are shown in Figure 56. The meaning and value of each field of the sub-control is as follows:

0	8	16	24 31
Control type (8)	Length (8)	Sub-control type (8)	Length or number (8)
Value (variable length)			

Figure 56 – RMCP-2 sub-control format

a) *Sub-control type* – This field denotes the type of sub-control. Its value shall be set to one of the code values in Table 31 for sub-controls of SYSINFO control or Table 32 for sub-controls of the ROOTPATH control.

b) *Length or number* – This field denotes the length in bytes or the number of sub-control values depending on the sub-control type.

c) *Value* – The contents of this field are defined for each sub-control denoted in the sub-control type field.

9.2.3 Formatting multiple controls

One or more controls may be included in the control field of a message. Whenever multiple sub-controls for the same control are included in the control field, every sub-control shall be preceded by the control. This is illustrated in Figure 57 showing an example of the use of multiple controls (i.e., Type A, Type B, Type D) with two separate sub-controls for control type B.

Control (Type A)	Control (Type B)	Sub-control (Type b1)	Control (Type B)	Sub-control (Type b2)	Control (Type D)

Figure 57 – Example formatting of multiple controls

9.3 RMCP-2 messages

This clause defines each message used in RMCP-2. The message types and corresponding values for the messages are listed in Table 27.

9.3.1 SUBSREQ message

The SUBSREQ message is used to subscribe to an RMCP-2 session. It is also used to create a new RMCP-2 session.

0	4	8	16 31
Version (0x2)	Node type (SM|SMA|DMA|RMA)	Message type (SUBSREQ)	Length (variable)
Session ID			
MAID (MAID proposed by the subscriber)			
Control (variable length)			

Figure 58 – SUBSREQ message format

The format of the SUBSREQ message is shown in Figure 58. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x2. For secure RMCP-2, its value shall be set to 0x4.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to one of SM, SMA or RMA coded as in Table 26. For secure RMCP-2, its value shall be set to one of the SM, SMA, DMA or RMA coded as in clause 10.2.1.

c) *Message type* – This field denotes the SUBSREQ message. Its value shall be set to 0x01 (see Table 27).

d) *Length* – This field shall be set to the total length in bytes of the SUBSREQ message including the control data.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field denotes the MAID proposed by the subscriber. Its value shall be formatted as defined in clause 10.1.2.

g) *Control* – The control types that may be used in the SUBSREQ message and their status, are shown in Table 4.

Table 4 – Control types for the SUBSREQ message

Control type	Meaning	Status	Reference
SYSINFO	A description of the system information of an MA.	Optional	See clause 9.4.8
SERV_USER_IDENT	A description of service user identification	Optional	See clause 9.4.15

The sub-control types of the SYSINFO control that may be used in the SUBSREQ message are listed in Table 5.

Table 5 – SYSINFO sub-control types for the SUBSREQ message

Sub-control type	Meaning	Status	Reference
SI_ROOM_CMA	The number of CMA places that an MA has allocated and the total number that it is able to support.	Optional	See clause 9.4.8.3
SI_POSS_BW	The possible forwarding bandwidth that the MA can afford.	Optional	See clause 9.4.8.5

NOTE – The additional SYSINFO controls defined for other RMCP-2 messages are not relevant for a session subscription as they relate to the position once the MA has joined the RMCP-2 tree.

9.3.2 SUBSANS message

The SUBSANS message is used by the SM to provide the results of a session subscription request and bootstrapping information for the session. It is also used to provide the results on the creation of the RMCP-2 session.

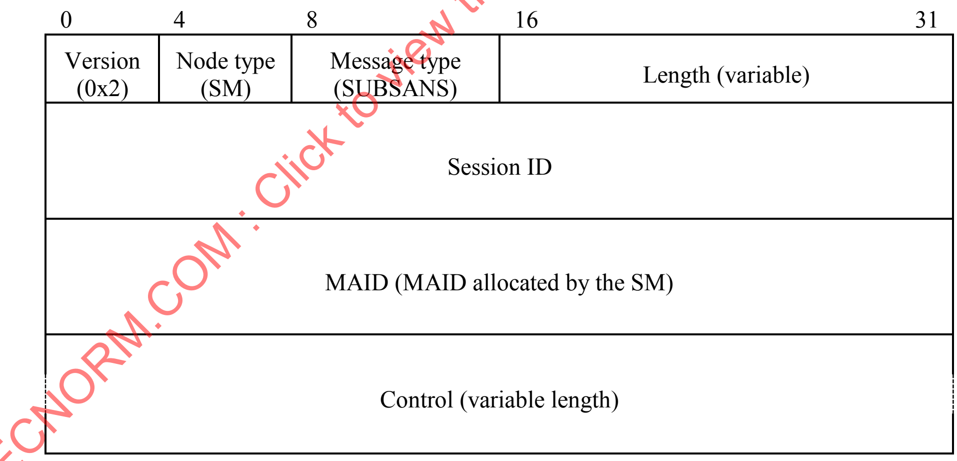


Figure 59 – SUBSANS message format

The format of the SUBSANS message is shown in Figure 59. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x2.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to the code value for the SM in Table 26.

c) *Message type* – This field denotes the SUBSANS message. Its value shall be set to 0x02 (see Table 27).

d) *Length* – This field shall be set to the total length in bytes of the SUBSANS message including control data.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field shall be set to the MAID of the subscriber as allocated by the SM. Its value shall be formatted as defined in clause 10.1.2.

NOTE – This may not be identical to the MAID proposed by the subscriber (see clause 7.1.2).

g) *Control* – The control types that may be used in the SUBSANS message and their status, are shown in Table 6.

Table 6 – Control types for the SUBSANS message

Control type	Meaning	Status	Reference
RESULT	The result of the subscription request.	Mandatory	See clause 9.4.6
PARAMETER	A list of session-related parameters.	Mandatory	See clause 9.4.14
NEIGHBORLIST	A list of MAIDs for performing neighbour discovery.	See condition 1	See clause 9.4.4
Condition 1: If the RESULT is successful, the NEIGHBORLIST is mandatory; if not, the NEIGHBORLIST shall not be included.			

9.3.3 PPROBREQ message

The PPROBREQ message is used in the neighbour discovery procedure to explore network conditions and to identify a potential near neighbour. It is also used to check whether the neighbouring MA is still active.

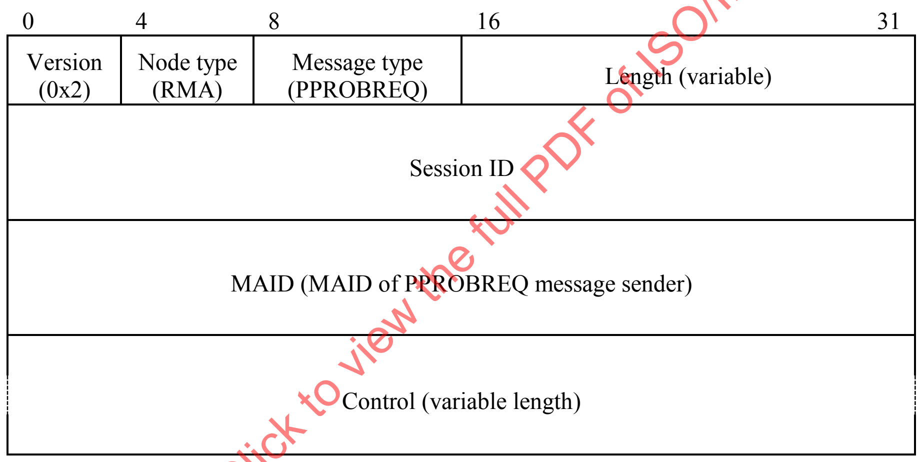


Figure 60 – PPROBREQ message format

The format of the PPROBREQ message is shown in Figure 60. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x2.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to the code value for the RMA in Table 26.

c) *Message type* – This field denotes the PPROBREQ message. Its value shall be set to 0x03 (see Table 27).

d) *Length* – This field shall be set to the total length in bytes of the PPROBREQ message including control data.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field shall be set to the MAID of the PPROBREQ message sender. Its value shall be formatted as defined in clause 10.1.2.

g) *Control* – The control types that may be used in the PPROBREQ message and their status, are shown in Table 7.

Table 7 – Control types for the PPROBREQ message

Control type	Meaning	Status	Reference
NEIGHBORLIST	A list of MAIDs for performing neighbour discovery.	Optional	See clause 9.4.4

9.3.4 PPROBANS message

The PPROBANS message provides a response to the PPROBREQ message in the neighbour discovery procedure and confirms that the probed MA is still active. It contains information about the network's condition, and a list of neighbour information.

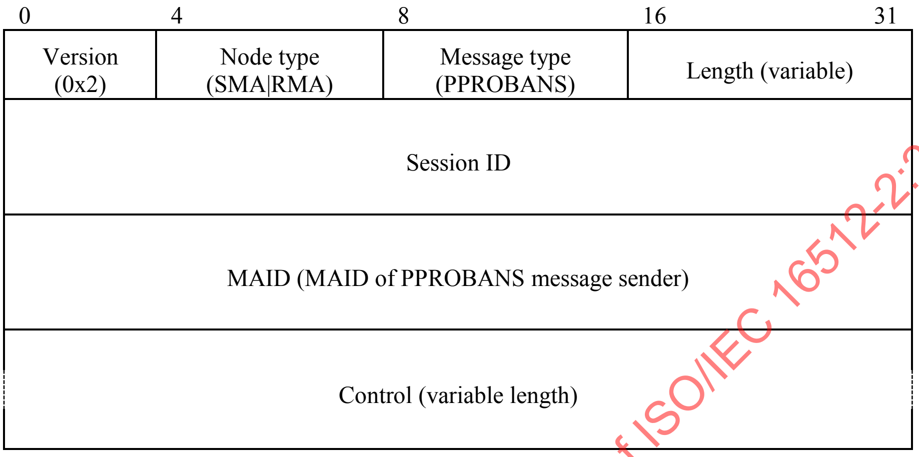


Figure 61 – PPROBANS message format

The format of the PPROBANS message is shown in Figure 61. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x2.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to one of the SMAs or RMAs coded as in Table 26.

c) *Message type* – This field denotes the PPROBANS message. Its value shall be set to 0x04 (see Table 27).

d) *Length* – This field shall be set to the total length in bytes of the PPROBANS message including control data.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field shall be set to the MAID of the PPROBANS message sender. Its value shall be formatted as defined in clause 10.1.2.

g) *Control* – The control types that may be used in the PPROBANS message, and their status, are shown in Table 8.

Table 8 – Control types for the PPROBANS message

Control type	Meaning	Status	Reference
NEIGHBORLIST	A list of MAs for performing neighbour discovery.	Mandatory	See clause 9.4.4
ROOTPATH	A description of the path from the SMA.	Mandatory	See clause 9.4.7
SYSINFO	A description of the system information of the MA.	Mandatory	See clause 9.4.8
TIMESTAMP	A measure of the transmission time between sending and receiving MAs.	Mandatory	See clause 9.4.9

9.3.5 HSOLICIT message

The HSOLICIT message is used to find the HMA inside its local multicast network.

0	4	8	16 31
Version (0x2)	Node type (RMA)	Message type (HSOLICIT)	Length (0x0014)
Session ID			
MAID (MAID of HSOLICIT message sender)			

Figure 62 – HSOLICIT message format

The format of the HSOLICIT message is shown in Figure 62. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x2.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to the code value for the RMA in Table 26.

c) *Message type* – This field denotes the HSOLICIT message. Its value shall be set to 0x05 (see Table 27).

d) *Length* – This field shall be set to the total length (20 bytes) of the HSOLICIT message. Its value shall be set to 0x0014.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field shall be set to the MAID of the HSOLICIT message sender. Its value shall be formatted as defined in clause 10.1.2.

NOTE – There is no control data associated with the HSOLICIT message.

9.3.6 HANNOUNCE message

The HANNOUNCE message is sent by the HMA as a reply to an HSOLICIT message, in order to announce the HMA's existence in a local network.

0	4	8	16 31
Version (0x2)	Node type (SMA|RMA)	Message type (HANNOUNCE)	Length (variable)
Session ID			
MAID (MAID of HANNOUNCE message sender)			
Control (variable length)			

Figure 63 – HANNOUNCE message format

The format of the HANNOUNCE message is shown in Figure 63. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x2.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to the code value for the SMA or RMA in Table 26.

c) *Message type* – This field denotes the HANNOUNCE message. Its value shall be set to 0x06 (see Table 27).

d) *Length* – This field shall be set to the total length in bytes of the HANNOUNCE message including control data.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field shall be set to the MAID of the HANNOUNCE message sender. Its value shall be formatted as defined in clause 10.1.2.

g) *Control* – The control types that may be used in the HANNOUNCE message and their status, are shown in Table 9.

Table 9 – Control types for the HANNOUNCE message

Control type	Meaning	Status	Reference
SYSINFO	A description of the system information of the MA.	Optional	See clause 9.4.8

9.3.7 HLEAVE message

The HLEAVE message is sent by the HMA to announce it is leaving from the RMCP-2 session to its local multicast network.

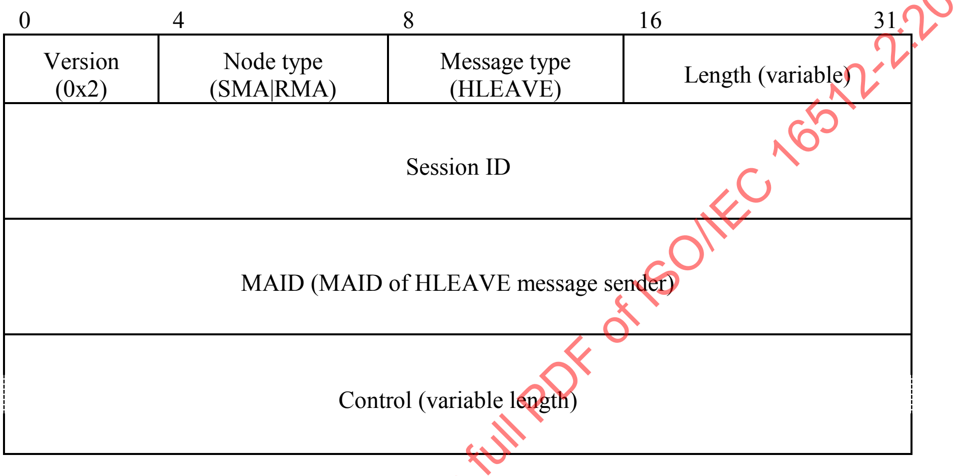


Figure 64 – HLEAVE message format

The format of the HLEAVE message is shown in Figure 64. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x2.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to the code value for the SMA or RMA in Table 26.

c) *Message type* – This field denotes the HLEAVE message. Its value shall be set to 0x07 (see Table 27).

d) *Length* – This field shall be set to the total length in bytes of the HLEAVE message including control data.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field shall be set to the MAID of the HLEAVE message sender. Its value shall be formatted as defined in clause 10.1.2.

g) *Control* – The control types that may be used in the HLEAVE message and their status, are shown in Table 10.

Table 10 – Control types for the HLEAVE message

Control type	Meaning	Status	Reference
CANDIDATEHMA	A set of candidate HMAs provided by the leaving HMA.	See conditions 1 and 2	See clause 9.4.10
NEIGHBORLIST	A list of MAs for performing neighbour discovery.	Optional	See clause 9.4.4
ROOTPATH	A description of the path from the SMA.	Mandatory	See clause 9.4.7
REASON	The reason for leaving the RMCP-2 session.	Mandatory	See clause 9.4.5
Condition 1: If the CANDIDATEHMA control is present, the competition to become the replacement HMA shall be restricted to the MAs in the list of MAIDs (see clause 9.4.10). Condition 2: If the CANDIDATEHMA control is absent, the competition to become the replacement HMA shall be open to all of the MAs in the same multicast network.			

9.3.8 RELREQ message

The RELREQ message is used by a CMA to request its PMA to forward data. It usually includes a data profile which may be negotiated through the message exchanges of RELREQ and RELANS messages. It is also used to periodically notify the PMA of its presence.

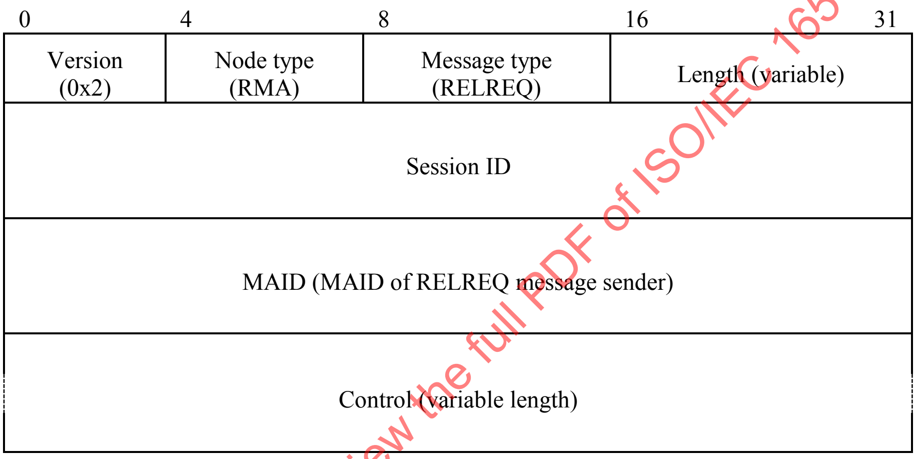


Figure 65 – RELREQ message format

The format of the RELREQ message is shown in Figure 65. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x2. For secure RMCP-2, its values shall be set to 0x4.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to the code value for the RMA in Table 26. For secure RMCP-2, its value shall be set to one of the DMA or RMA in clause 10.2.1.

c) *Message type* – This field denotes the RELREQ message. Its value shall be set to 0x08 (see Table 27).

d) *Length* – This field shall be set to the total length in bytes of the RELREQ message including control data.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field shall be set to the MAID of the RELREQ message sender. Its value shall be formatted as defined in clause 10.1.2.

g) *Control* – The control types that may be used in the RELREQ message and their status, are shown in Table 11.

Table 11 – Control types for the RELREQ message

Control type	Meaning	Status	Reference
RP_COMMAND	A request for root path information.	See condition 1	See clause 9.4.1
DATAPROFILE	A description of the requirements for forwarding data.	Optional	See clause 9.4.3
AUTH	A description for initiating membership authentication.	See condition 2	See clause 9.4.16
Condition 1: If this message is used in parent switching, the RP_COMMAND control is mandatory. If not, the RP_COMMAND shall not be included. Condition 2: If this message is used for secure RMCP-2, the AUTH control is mandatory. If not, the AUTH control shall not be included.			

9.3.9 RELANS message

The RELANS message is issued by a PMA to notify whether a relay request in a RELREQ message from its CMA has been allowed. It may also contain additional information which is necessary to negotiate the data channel between the CMA and itself. It is also used to confirm that the answering MA is still active.

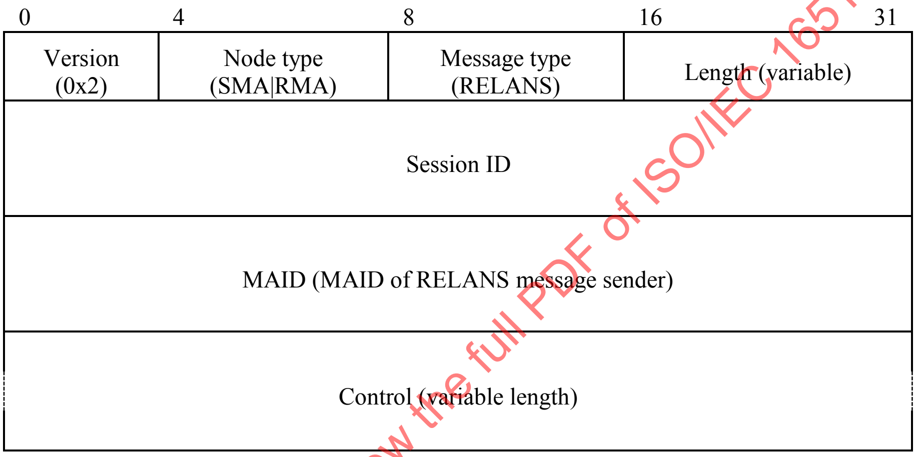


Figure 66 – RELANS message format

The format of the RELANS message is shown in Figure 66. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x2. For secure RMCP-2, its value shall be set to 0x4.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to one of the SMA or RMA coded as in Table 26. For secure RMCP-2, its value shall be set to one of the SMA or DMA in clause 10.2.1.

c) *Message type* – This field denotes the RELANS message. Its value shall be set to 0x09 (see Table 27).

d) *Length* – This field shall be set to the total length in bytes of the RELANS message including control data.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field shall be set to the MAID of the RELANS message sender. Its value shall be formatted as defined in clause 10.1.2.

g) *Control data* – The control types that may be used in the RELANS message and their status, are shown in Table 12.

Table 12 – Control types for the RELANS message

Control type	Meaning	Status	Reference
RESULT	A result of the relay request.	Mandatory	See clause 9.4.6
DATAPROFILE	A description of the requirements for forwarding data.	Optional	See clause 9.4.3
TIMESTAMP	A measure of the transmission time for sending and receiving MAs.	Mandatory	See clause 9.4.9
ROOTPATH	A description of the path from the SMA.	See condition 1	See clause 9.4.7
SYSINFO	A description of the system information of the MA. The sub-controls that may be used in the RELANS message are listed in Table 27.	Optional	See clause 9.4.8
AUTH_ANS	A result of membership authentication.	See condition 2	See clause 9.4.17
Condition 1: The ROOTPATH control shall be included, if requested, in a RELREQ message. Condition 2: If this message is used for secure RMCP-2, the AUTH_ANS control is mandatory. If not, the AUTH_ANS control shall not be included.			

9.3.10 STREQ message

The STREQ message is used by the SM to request system information from a single MA.

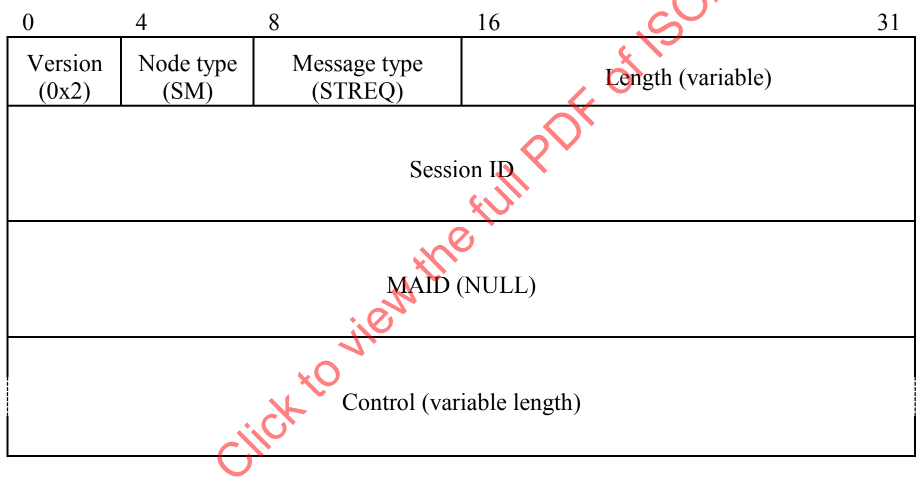


Figure 67 – STREQ message format

The format of the STREQ message is shown in Figure 67. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x2.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to the code value for the SM in Table 26.

c) *Message type* – This field denotes the STREQ message. Its value shall be set to 0x0A (see Table 27).

d) *Length* – This field shall be set to the total length in bytes of the STREQ message including control data.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field shall be set to zero because the SM does not have a MAID.

g) *Control data* – The control types that may be used in the STREQ message and their status, are shown in Table 13.

Table 13 – Control types for the STREQ message

Control type	Meaning	Status	Reference
SI_COMMAND	A request for specific information from an MA.	Mandatory	See clause 9.4.2
TREEEXPLOR	Specification limiting the scope of the tree.	See conditions 1 and 2	See clause 9.4.11
Condition 1: If the TREEEXPLOR control is absent, the STREQ message requests system information related only to the recipient of the STREQ message. Condition 2: If the TREEEXPLOR control is present, the STREQ message requests system information related to the set of MAs specified in 9.4.11 d).			

9.3.11 STANS message

The STANS message provides a response to the STREQ message.

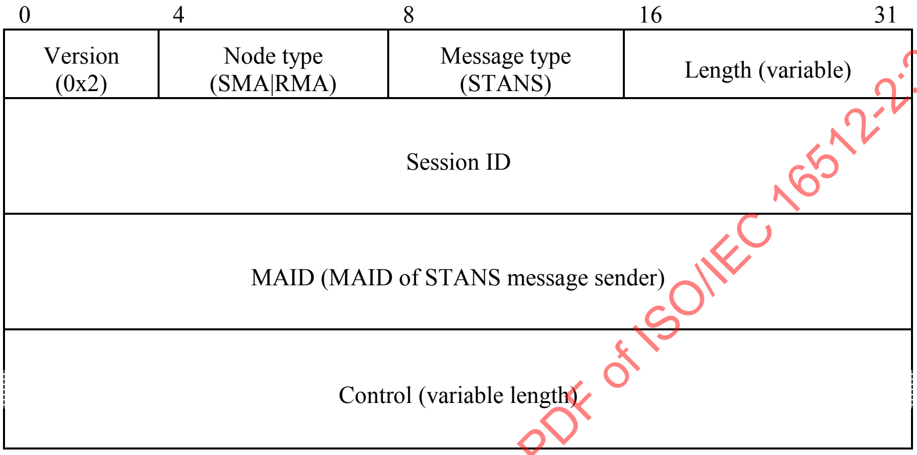


Figure 68 – STANS message format

The format of the STANS message is shown in Figure 68. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x2.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to one of the SMA or RMA coded as in Table 26.

c) *Message type* – This field denotes the STANS message. Its value shall be set to 0x0B (see Table 27).

d) *Length* – This field shall be set to the total length in bytes of the STANS message including control data.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field shall be set to the MAID of the STANS message sender. Its value shall be formatted as defined in clause 10.1.2.

g) *Control* – The control types that may be used in the STANS message and their status, are shown in Table 14.

Table 14 – Control types for the STANS message

Control type	Meaning	Status	Reference
COLLECT	A header that identifies and delimits information related to individual MAs.	See condition 1	See clause 9.4.12
SYSINFO	A description of the system information of an MA, or a set of MAs. The sub-controls that may be used in the RELANS message are listed in Table 27.	Mandatory	See clause 9.4.8
Condition 1: The COLLECT control shall be included in the STANS message that forwards data collected in the STCOLANS message (see clause 9.3.13).			

9.3.12 STCOLREQ message

STCOLREQ and STCOLANS messages are used to collect system information from a set of MAs as requested in a STREQ message. The STREQ message is issued by the SM and is sent to a selected MA (or the SMA). If the STREQ message contains a TREEEXPLOR control, it defines the set of MAs as the selected MA (or the SMA) that receives the STREQ message, all of its CMAs and all of its descendants on the RMCP-2 tree within *n* hops of the selected MA. This information is collected from members of the set through STCOLREQ and STCOLANS messages via the RMCP-2 tree.

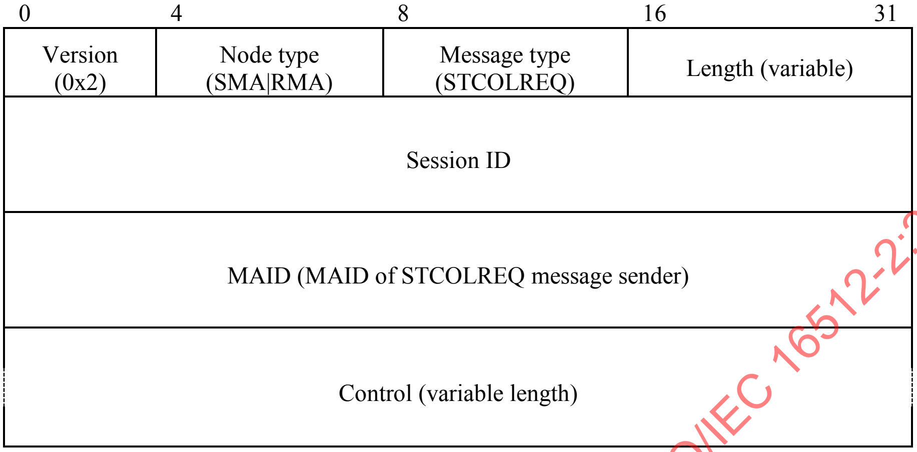


Figure 69 – STCOLREQ message format

The format of the STCOLREQ message is shown in Figure 69. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x2.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to one of the SMA or RMA coded as in Table 26.

c) *Message type* – This field denotes the STCOLREQ message. Its value shall be set to 0x1A (see Table 27).

d) *Length* – This field shall be set to the total length in bytes of the STCOLREQ message including control data.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field shall be set to the MAID of the STCOLREQ message sender. Its value shall be formatted as defined in clause 10.1.2.

g) *Control data* – The control types that may be used in the STCOLREQ message and their status, are shown in Table 15.

Table 15 – Control types for the STCOLREQ message

Control type	Meaning	Status	Reference
SI_COMMAND	A request for specific information from an MA.	Mandatory	See clause 9.4.2
TREEEXPLOR	Specification limiting the scope of the tree.	Optional	See clause 9.4.11

NOTE 1 – The SI_Command code value shall be identical to that in the STREQ message from the SM that initiates the collection of the information through the STCOLREQ and STCOLANS messages.

NOTE 2 – The tree depth value set by the MA that is the recipient of the STREQ message that initiates the STCOLREQ message shall be identical to that in the STREQ message. The value of the tree depth shall be decreased by one every time that the message is relayed to a lower level.

NOTE 3 – When an MA receives an STCOLREQ message with the tree depth = 0, it will know that it is at the end of the relaying chain and that it should start to return its information in a STCOLANS message to its PMA.

9.3.13 STCOLANS message

The STCOLANS message is used to relay system information from a defined subset of the RMCP-2 tree. This information is collected in a controlled manner. Firstly, each MA in the lowest layer sends information related to their own node to their PMA. The PMA amalgamates this information and adds its own information before relaying the combined information to its parent in the next layer. The relaying continues until the head of the sub-tree has collected all the information and then forwards it in a STANS message to the SM.

0	4	8	16 31
Version (0x2)	Node type (RMA)	Message type (STCOLANS)	Length (variable)
Session ID			
MAID (MAID of STCOLANS message sender)			
Control (variable length)			

Figure 70 – STCOLANS message format

The format of the STCOLANS message is shown in Figure 70. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x2.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to the code value for the RMA as in Table 26.

c) *Message type* – This field denotes the STCOLANS message. Its value shall be set to 0x1B (see Table 27).

d) *Length* – This field shall be set to the total length in bytes of the STCOLANS message including control data.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field shall be set to the MAID of the STCOLANS message sender. Its value shall be formatted as defined in clause 10.1.2.

g) *Control data* – The control types that may be used in the STCOLANS message and their status, are shown in Table 16.

Table 16 – Control types for the STCOLANS message

Control type	Meaning	Status	Reference
COLLECT	A header that identifies and delimits information related to individual MAs.	Optional	See clause 9.4.12
SYSINFO	A description of the system information of MA.	Mandatory	See clause 9.4.8

NOTE – The SYSINFO sub-controls in an STCOLANS message shall correspond to those indicated by the SI_COMMAND in the STCOLREQ message that triggered the message.

A STCOLANS message contains system information for a set of MAs at a given level in the RMCP-2 tree. The set is defined as a PMA and its CMAs and descendants to a depth defined by the TREEEXPLOR control of the original STREQ message from the SM requesting this information.

Figure 71 shows the sequence of controls in a STCOLANS message. Each COLLECT control identifies a particular MA and the subsequent SYSINFO sub-controls contain the type of system information defined by the SI_COMMAND control of the original STREQ message from the SM requesting this information.

COLLECT control identifying MA1
SYSINFO control and sub-control A containing information relating to MA 1
SYSINFO control and sub-control B containing information relating to MA 1
SYSINFO control and sub-control C containing information relating to MA 1
COLLECT control identifying MA2
SYSINFO control and sub-control A containing information relating to MA 2
SYSINFO control and sub-control B containing information relating to MA 2
SYSINFO control and sub-control C containing information relating to MA 2
. . Fields relating to other MAs . .

Figure 71 – Sequence of COLLECT controls and SYSINFO controls in a STCOLANS message

9.3.14 LEAVREQ message

The LEAVREQ message is used:

a) by an MA to inform its PMA and CMAs of its leave;

b) by the SM or a PMA to expel an MA from the session; or

c) by an MA when it changes its PMA;

d) it is used by the SM then the SM needs to forward the receive LEAVREQ message to another SM in RMCP-2 with multiple SMs.

0	4	8	16 31
Version (0x2)	Node type (SM|SMA|RMA)	Message type (LEAVREQ)	Length (variable)
Session ID			
MAID (MAID of LEAVREQ message sender)			
Control (variable length)			

Figure 72 – LEAVREQ message format

The format of the LEAVREQ message is shown in Figure 72. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x2.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to one of the SM, SMA or RMA coded as in Table 26.

c) *Message type* – This field denotes the LEAVREQ message. Its value shall be set to 0x0C (see Table 27).

d) *Length* – This field shall be set to the total length in bytes of the LEAVREQ message including control data.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field shall be set to the MAID of the LEAVREQ message sender and its value shall be formatted as defined in clause 10.1.2. If the message is sent by the SM, this field shall be set to zero.

g) *Control* – The control type that shall be used in the LEAVREQ message and its status, is shown in Table 17.

Table 17 – Control type for the LEAVREQ message

Control type	Meaning	Status	Reference
REASON	The reason for leaving the MA.	Mandatory	See clause 9.4.5

9.3.15 LEAVANS message

The LEAVANS message is used to acknowledge the receipt of a LEAVREQ message.

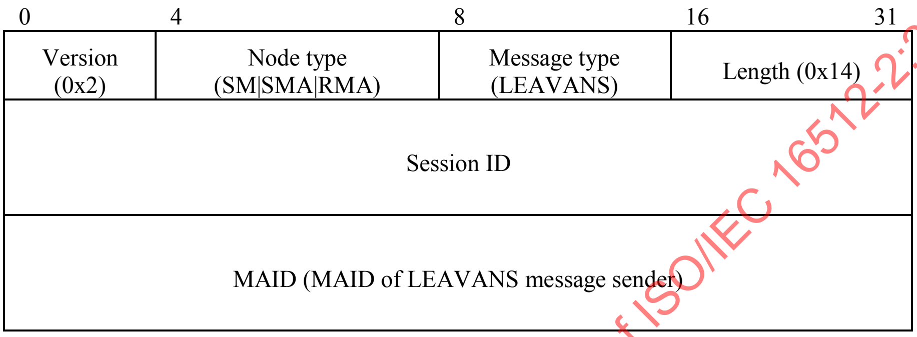


Figure 73 – LEAVANS message format

The format of the LEAVANS message is shown in Figure 73. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x2.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to one of the SM, SMA, or RMA coded as in Table 26.

c) *Message type* – This field denotes the LEAVANS message. Its value shall be set to 0x0D (see Table 27).

d) *Length* – This field shall be set to the total length (20 bytes) of the LEAVANS message. Its value shall be set to 0x14.

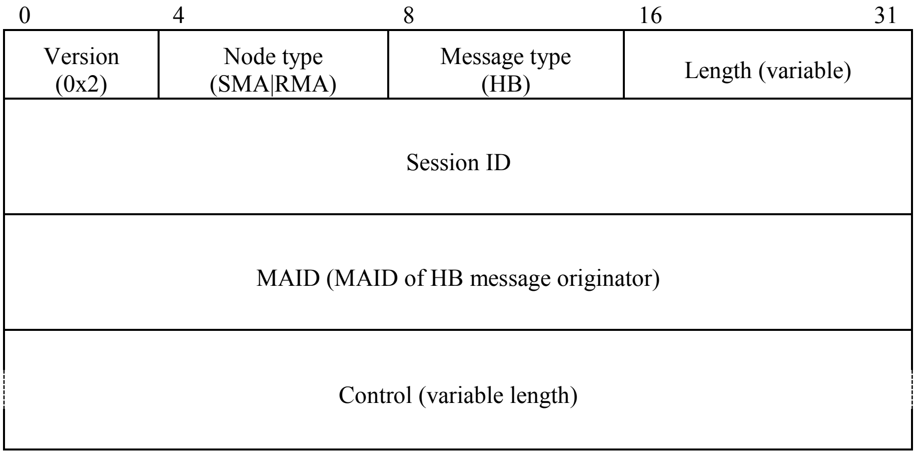
e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field shall be set to the MAID of the LEAVANS message sender. Its value shall be formatted as defined in clause 10.1.2.

NOTE – There is no control data associated with the LEAVANS message.

9.3.16 HB message

The HB message is issued periodically by the SMA to examine the condition of the RMCP-2 tree and to create the root path information for receiving MAs. This information enables each MA to diagnose the network condition.



0	4	8	16 31
Version (0x2)	Node type (SMA|RMA)	Message type (HB)	Length (variable)
Session ID			
MAID (MAID of HB message originator)			
Control (variable length)			

Figure 74 – HB message format

The format of the HB message is shown in Figure 74. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x2.

b) *Node type* – This field denotes the message originator's node type. For a regular HB message, its value shall be set to the SMA coded as in Table 26. For a pseudo-HB message, its value shall be set to that of the RMA coded as in Table 26. This field shall not be changed as the HB message is relayed down the RMCP-2 tree.

c) *Message type* – This field denotes the HB message. Its value shall be set to 0x10 (see Table 27).

d) *Length* – This field shall be set to the total length in bytes of the HB message including control data.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field shall be set to the MAID of the HB message originator. Its value shall be formatted as defined in clause 10.1.2. This field shall not be changed as the HB message is relayed down the RMCP-2 tree.

g) *Control data* – The control types that may be used in the HB message and their status, are shown in Table 18.

Table 18 – Control types for the HB message

Control type	Meaning	Status	Reference
ROOTPATH	A description of the path from the SMA.	See condition 1	See clause 9.4.7
PSEUDO_HB	An indication that the message is a pseudo-HB message for network partitioning detection and recovery.	See condition 2	See clause 9.4.13
Condition 1: The ROOTPATH control shall always be included in a regular HB message. Condition 2: The PSEUDO_HB control shall always be included in a pseudo-HB message.			

9.3.17 FAILCHECK message

The FAILCHECK message is used to request the SM to check whether the specified MA is still active.

0	4	8	16 31
Version (0x2)	Node type (SM|SMA|RMA)	Message type (FAILCHECK)	Length (0x0014)
Session ID			
MAID (MAID of node to be checked)			

Figure 75 – FAILCHECK message format

The format of the FAILCHECK message is shown in Figure 75. The description of each field is as follows:

a) *Version* – This field denotes the version of the protocol. Its value shall be set to 0x2 to indicate RMCP-2.

b) *Node type* – This field denotes the type of the node to be checked by the SM. Its value shall be set to one of the SM, SMA or RMA coded as in Table 26.

c) *Message type* – This field denotes the FAILCHECK message. Its value shall be set to 0x1C (see Table 27).

d) *Length* – This field shall be set to the total length (20 bytes) of the FAILCHECK message. The value shall be set to 0x0014.

e) *Session ID* – This field shall be set to the 64-bit value that identifies the session. Its value shall be formatted as defined in clause 10.1.1.

f) *MAID* – This field shall be set to the MAID of the node to be checked by the SM. Its value shall be formatted as defined in clause 10.1.2.

NOTE – There is no control associated with the FAILCHECK message.

9.3.18 TERMREQ message

TERMREQ message is used to terminate the existing RMCP-2 session. The SM sends the TERMREQ message to the SMA and the SMA relays the message to members of the RMCP-2 tree.

0	4	8	16 31
Version (0x2)	Node type (SM|SMA|RMA)	Message type (TERMREQ)	Length (variable)
Session ID			
MAID (MAID of TERMREQ message sender)			

Figure 76 – TERMREQ message format

The format of the TERMREQ message is shown in Figure 76. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x2.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to one of the SM, SMA, or RMA coded as in Table 26.

c) *Message type* – This field denotes the TERMREQ message. Its value shall be set to 0x0E (see Table 27).

d) *Length* – This field shall be set to the total length in bytes of TERMREQ message including control data.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field shall be set to the MAID of the TERMREQ message sender and its value shall be formatted as defined in clause 10.1.2. If the message is sent by the SM, this field shall be set to zero.

NOTE – There is no control associated with the TERMREQ message.

9.3.19 TERMANS message

The TERMANS message is used to acknowledge the receipt of a TERMREQ message.

0	4	8	16 31
Version (0x2)	Node type (SMA|RMA)	Message type (TERMANS)	Length (0x14)
Session ID			
MAID (MAID of TERMANS message sender)			

Figure 77 – TERMANS message format

The format of the TERMANS message is shown in Figure 77. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x2.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to one of the SMA or RMA coded as in Table 26.

c) *Message type* – This field denotes the TERMANS message. Its value shall be set to 0x0F (see Table 27).

d) *Length* – This field shall be set to the total length (20 bytes) of the TERMANS message. Its value shall be set to 0x14.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field shall be set to the MAID of the TERMANS message sender. Its value shall be formatted as defined in clause 10.1.2.

NOTE – There is no control data associated with the TERMANS message.

9.3.20 SECAGREQ message

The SECAGREQ message is used only in secure RMCP-2.

0	4	8	16	24 31
Version (0x4)	Node type (SMA|DMA|RMA)	Message type (SECAGREQ)	Length (variable)	
Session ID (64)				
MAID (MAID of the SECAGREQ message sender)				
Control (variable length)				

Figure 78 – SECAGREQ message format

The format of the SECAGREQ message is shown in Figure 78. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x4.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to one of the SMA, DMA or RMA coded as in clause 10.2.1.

c) *Message type* – This field denotes the type of SECAGREQ message. Its value shall be set to 0x21 (see Table 28).

d) *Length* – This field shall be set to the total length in bytes of the SECAGREQ message including the control.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field denotes the proposed MAID of the SECAGREQ sender. Its value shall be as defined in clause 10.1.2.

g) *Control* – The control types that may be used in the SECAGREQ message and their status, are shown in Table 19.

Table 19 – Control types for the SECAGREQ message

Control type	Meaning	Status	Reference
SMA_PROPOSE	A description of a value for secure RMCP-2.	See condition 1	See clause 9.4.18
GK_MECH_CAPAB	A description of capabilities in terms of the group key.	See condition 2	See clause 9.4.19
EN_DEC_CAPAB	A description of capabilities in terms of the encryption algorithm.	See condition 2	See clause 9.4.20
AUTH_ALG_CAPAB	A description of capabilities in terms of the authentication mechanism.	See condition 2	See clause 9.4.21
Condition 1: The SMA_PROPOSE control shall always be included in a SECAGREQ message if the node type is the SMA. Condition 2: These controls shall not be included in a SECAGREQ message sent by an RMA or by a DMA that joins the session after the security policy has been established.			

9.3.21 SECLIST message

The SECLIST message is used only in secure RMCP-2.

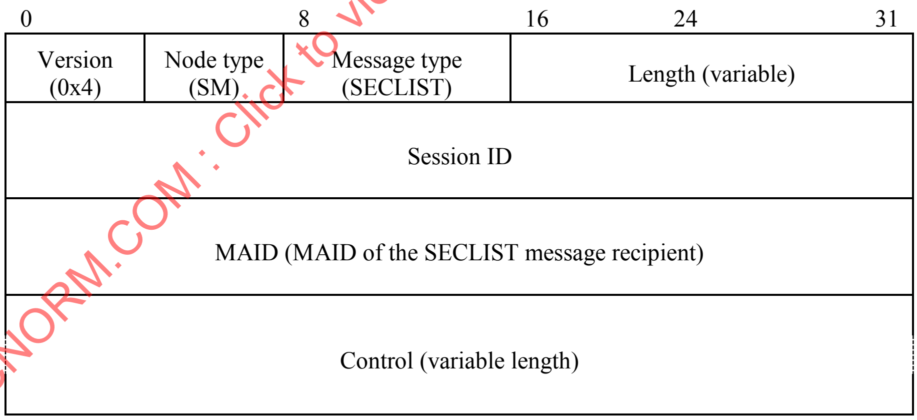


Figure 79 – SECLIST message format

The format of the SECLIST message is shown in Figure 79. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x4.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to the code value for the SM in clause 10.2.1.

c) *Message type* – This field denotes the SECLIST message. Its value shall be set to 0x22 (see Table 28).

d) *Length* – This field shall be set to the total length in bytes of the SECLIST message including the control.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field denotes the MAID of the SECLIST message recipient. Its value shall be as defined in clause 10.1.2.

g) *Control* – The control types that may be used in the SECAGREQ message and their status, are shown in Table 20.

Table 20 – Control types for the SECLIST message

Control type	Meaning	Status	Reference
GK_MECH	A description of the group key mechanism for the security policy.	Mandatory	See clause 9.4.22
AUTH_MECH	A description of the authentication type for the security policy	Mandatory	See clause 9.4.23
CON_EN_DEC_ALG	A description of the content encryption algorithm for the security policy.	Mandatory	See clause 9.4.24
GK_EN_DEC_ALG	A description of the group key encryption algorithm for the security policy.	Mandatory	See clause 9.4.25
AUTH_ALG	A description of the hash/MAC algorithm for the security policy.	Mandatory	See clause 9.4.26

9.3.22 SECALGREQ message

The SECALGREQ message is used to request the security algorithm.

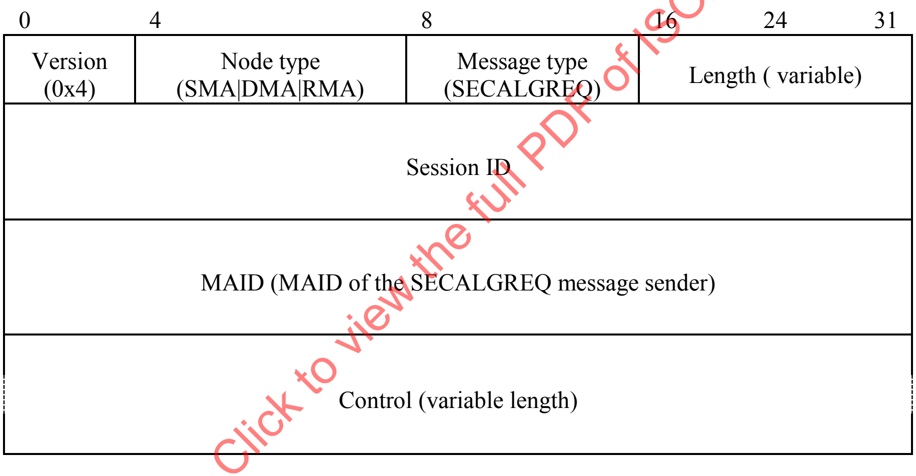


Figure 80 – SECALGREQ message format

The format of the SECALGREQ message is shown in Figure 80. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x4.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to one of the SMA, DMA or RMA coded as in clause 10.2.1.

c) *Message type* – This field denotes the SECALGREQ message. Its value shall be set to 0x23 (see Table 28).

d) *Length* – This field shall be set to the total length in bytes of the SECALGREQ message including the control.

e) *Session ID* – This field shall be set to the 64-bit value of the Session ID as defined in clause 10.1.1.

f) *MAID* – This field denotes the MAID of the SECALGREQ message sender. Its value shall be formatted as defined in clause 10.1.2.

g) *Control* – The control types that may be used in the SECALGREQ message and their status, are shown in Table 21.

Table 21 – Control types for the SECALGREQ message

Control type	Meaning	Status	Reference
GK_MECH_DELIVER	A description of the group key mechanism for the security policy.	See condition 1	See clause 9.4.27
AUTH_MECH_DELIVER	A description of the authentication type for the security policy	See condition 2	See clause 9.4.28
CON_EN_DEC_DELIVER	A description of the content encryption algorithm for the security policy.	See condition 3	See clause 9.4.29
GK_EN_DEC_DELIVER	A description of the group key encryption algorithm for the security policy.	See condition 4	See clause 9.4.30
AUTH_ALG_DELIVER	A description of the hash/MAC algorithm for the security policy.	See condition 5	See clause 9.4.31
Condition 1: The GK_MECH_DELIVER control shall only be used by the MA sending the SECALGREQ message when it does not hold the GK_NAME security algorithm, or when the configuration of this algorithm has failed. Condition 2: This AUTH_MECH_DELIVER control shall only be used by the MA sending the SECALGREQ message when it does not hold the AUTH_NAME security algorithm, or when the configuration of this algorithm has failed. Condition 3: This CON_EN_DEC_DELIVER control shall only be used by the MA sending the SECALGREQ message when it does not hold the CON_EN_DEC_ALG security algorithm, or when the configuration of this algorithm has failed. Condition 4: This GK_EN_DEC_DELIVER control shall only be used by the MA sending the SECALGREQ message when it does not hold the GK_EN_DEC_ALG security algorithm, or when the configuration of this algorithm has failed. Condition 5: This AUTH_ALG_DELIVER control shall only be used by the MA sending the SECALGREQ message when it does not hold the AUTH_ALG security algorithm, or when the configuration of this algorithm has failed.			

9.3.23 SECAGANS message

The SECAGANS message is used to indicate the result of the security algorithm request.

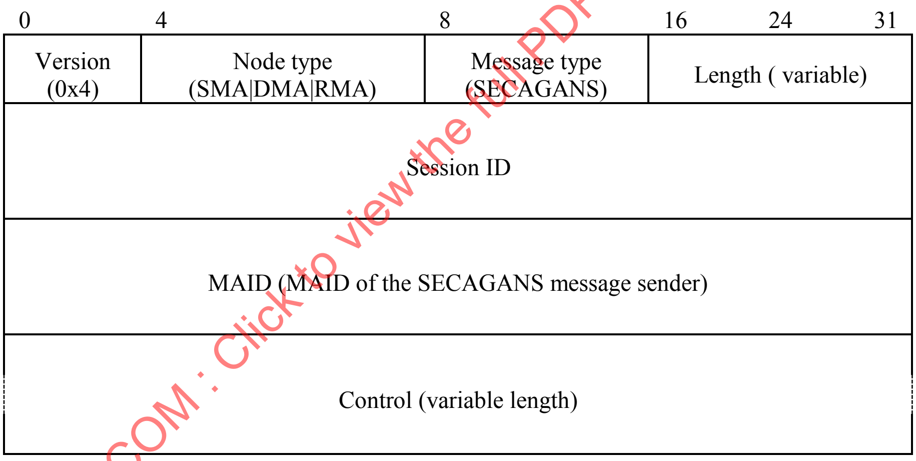


Figure 81 – SECAGANS message format

The format of the SECAGANS message is shown in Figure 81. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x4.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to one of the SMA, DMA or RMA coded, as in clause 10.2.1.

c) *Message type* – This field denotes the SECAGANS message. Its value shall be set to 0x24 (see Table 28).

d) *Length* – This field shall be set to the total length in bytes of the SECAGANS message including the control data.

e) *Session ID* – This field shall be set to the 64-bit value of the Session ID as defined in clause 10.1.1.

f) *MAID* – This field denotes the MAID of the SECAGANS message sender. Its value shall be formatted as defined in clause 10.1.2.

g) *Control* – The control types that may be used in the SECALGREQ message and their status, are shown in Table 22.

Table 22 – Control types for the SECAGANS message

Control type	Meaning	Status	Reference
SEC_RETURN	A description of the result of the security algorithm request.	Mandatory	See clause 9.4.32

9.3.24 KEYDELIVER message

The KEYDELIVER message is used to propose the key information.

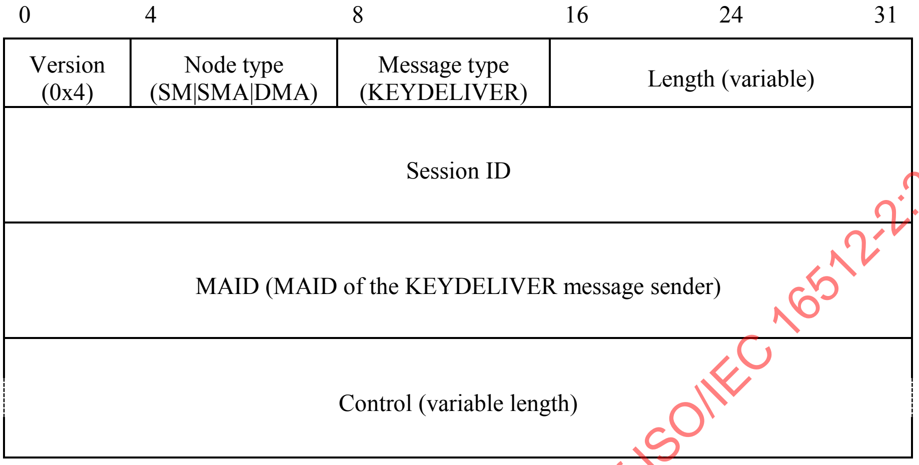

0
4
8
16
24
31
Version (0x4)
Node type (SM|SMA|DMA)
Message type (KEYDELIVER)
Length (variable)
Session ID
MAID (MAID of the KEYDELIVER message sender)
Control (variable length)

Figure 82 – KEYDELIVER message format

The format of the KEYDELIVER message is shown in Figure 82. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x4.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to:

- 0x01, the coded value for the SM in clause 10.2.1, for the delivery of the Ks key information; or
- 0x04, the coded value for the DMA in clause 10.2.1, for the delivery of the Kg key information; or
- 0x02, the coded value for the SMA in clause 10.2.1, for the delivery of the Kc key information.

c) *Message type* – This field denotes the KEYDELIVER message. The value shall be set to 0x25 (see Table 28).

d) *Length* – This field shall be set to the total length in bytes of the KEYDELIVER message including the control data.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field denotes the MAID of the KEYDELIVER message recipient. Its value shall be as defined in clause 10.1.2.

g) *Control* – The control types that may be used in the SECALGREQ message and their status, are shown in Table 23.

Table 23 – Control type for the KEYDELIVER message

Control type	Meaning	Status	Reference
KEY_INFO	The description of the proposed key information.	Mandatory	See clause 9.4.33

9.3.25 HRSREQ message

HRSREQ message is used to request the head required security.

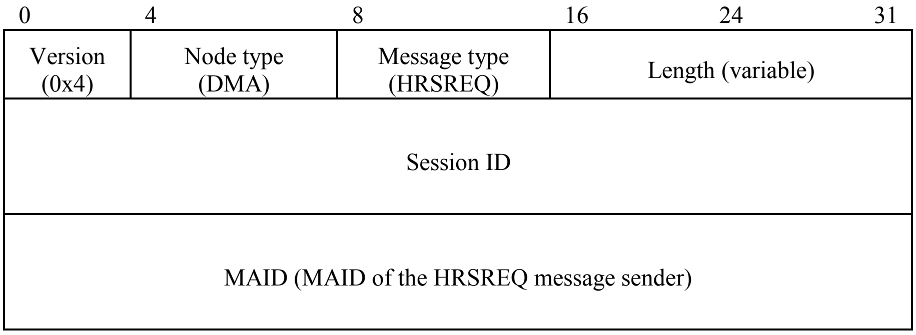


Figure 83 – HRSREQ message format

The format of the HRSREQ message is shown in Figure 83. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. The value shall be set to 0x4.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to the coded value for the DMA in clause 10.2.1.

c) *Message type* – This field denotes the HRSREQ message. The value shall be set to 0x26 (see Table 28).

d) *Length* – This field denotes the length in bytes of the HRSREQ message. Its value shall be set to 0x14.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field denotes the proposed MAID of the HRSREQ message sender. Its value shall be formatted as defined in clause 10.1.2.

NOTE – There is no control associated with the HRSREQ message.

9.3.26 HRSANS message

The HRSANS message is used to respond to the head required security.

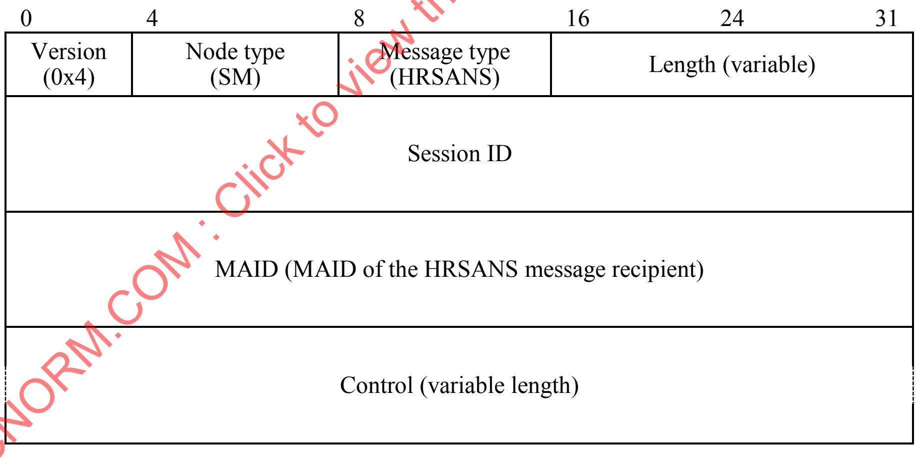


Figure 84 – HRSANS message format

The format of the HRSANS message is shown in Figure 84. The description of each field is as follows:

a) *Version* – This field denotes the current version of the RMCP. Its value shall be set to 0x4.

b) *Node type* – This field denotes the message issuer's node type. Its value shall be set to 0x01, the code value for the SM in clause 10.2.1.

c) *Message type* – This field denotes the HRSANS message. Its value shall be set to 0x27 (see Table 28).

d) *Length* – This field shall be set to the total length in bytes of the HRSANS message including the control data.

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in clause 10.1.1.

f) *MAID* – This field denotes the MAID of the HRSANS message recipient. Its value shall be as defined in clause 10.1.2.

g) *Control* – The control types that may be used in the HRSANS message and their status, are shown in Table 24.

Table 24 – Control type for the HRSANS message

Control type	Meaning	Status	Reference
ACL_LIST	The description of the hashed MAID and hashed K_{TLS} for each authenticated RMA in the current session.	Mandatory	See clause 9.4.34

9.4 RMCP-2 controls

9.4.1 RP_COMMAND control

The RP_COMMAND control in the RELREQ message is used by a CMA to request root path information from its PMA. For example, whenever an MA connects to a PMA during joining or parent switching procedures, it requires the root path information including MAID of its new PMA for network diagnosis and loop detection.

0	8	16 31
Control type (RP_COMMAND)	Length (0x04)	RP_Command code

Figure 85 – RP_COMMAND control format

The format of the RP_COMMAND control is shown in Figure 85. The description of each field is as follows:

a) *Control type* – This field denotes the RP_COMMAND control. Its value shall be set to 0x01 (see Table 29).

b) *Length* – This field denotes the length (4 bytes) of the RP_COMMAND control. Its value shall be set to 0x04.

c) *RP_Command code* – This field denotes the components to be returned in the ROOTPATH control of the RELANS message. Its value shall be set to one of the code values in Table 31.

9.4.2 SI_COMMAND control

The SI_COMMAND control in a STREQ message is used by the SM to specify the specific information that is required from the recipient MA.

0	8	16 31
Control type (SI_COMMAND)	Length (0x04)	SI_Command code

Figure 86 – SI_COMMAND control format

The format of the SI_COMMAND control is shown in Figure 86. The description of each field is as follows:

a) *Control type* – This field denotes the SI_COMMAND control. Its value shall be set to 0x02 (see Table 29).

b) *Length* – This field denotes the length (4 bytes) of the SI_COMMAND control. Its value shall be set to 0x04.

c) *SI_Command code* –This field shall be set to the arithmetic total of the command codes in Table 33 corresponding to the combination of SYSINFO sub-controls for which an answer is required (see clause 10.3.2).

9.4.3 DATAPROFILE control

The DATAPROFILE control is used to describe the proposed data profile of the subscribing MA.

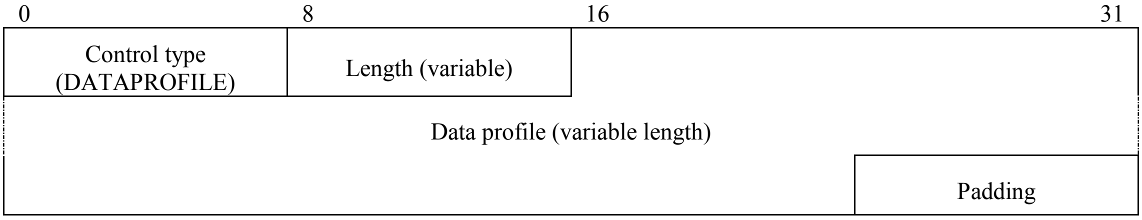


Figure 87 – DATAPROFILE control format

The format of the DATAPROFILE control is shown in Figure 87. The description of each field is as follows:

a) *Control type* – This field denotes the DATAPROFILE control. Its value shall be set to 0x03 (see Table 29).

b) *Length* – This field denotes the length in bytes of the DATAPROFILE control. Its value shall be a multiple of four bytes (see item d) in this list) and it shall not exceed 0xFC.

c) *Data profile* – This field shall contain the data profile for the MA formatted in text mode. It follows an SDL-like encoding scheme. An example is shown in Figure 135.

d) *Padding* – If the total length of the control type, length and data profile fields is not a multiple of 4 bytes, the padding field shall be filled with zeros to ensure that the length of the DATAPROFILE control is a multiple of 4 bytes.

9.4.4 NEIGHBORLIST control

The NEIGHBORLIST control in a SUBSANS message to a successful subscriber is used to convey a list of active MAs that may be used for bootstrapping purposes.

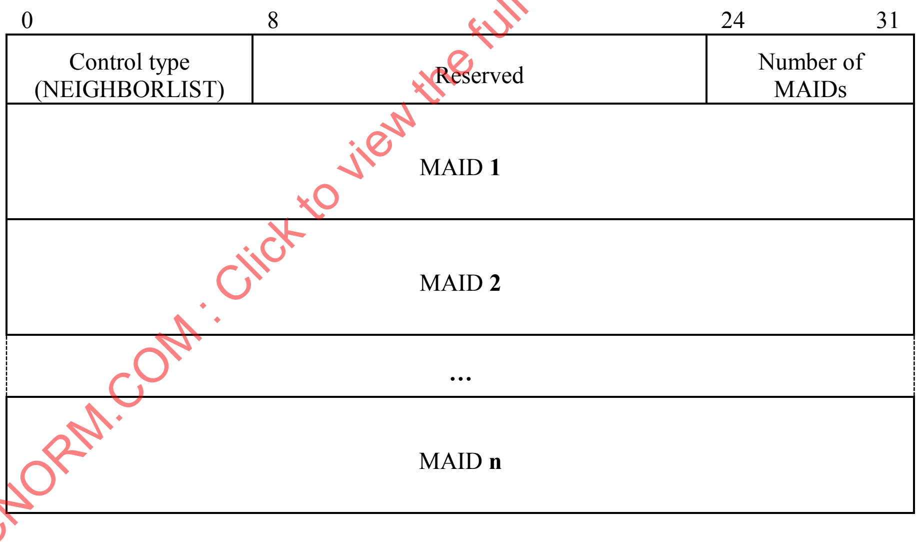


Figure 88 – NEIGHBORLIST control format

The format of the NEIGHBORLIST control is shown in Figure 88. The description of each field is as follows:

a) *Control type* – This field denotes the NEIGHBORLIST control. Its value shall be set to 0x04 (see Table 29).

b) *Reserved* – This field is reserved for future use. Its value shall be set to zero. It is ignored by the receiver.

c) *Number of MAIDs* – This field shall be set to the number of MAIDs listed in the NEIGHBORLIST control.

d) *MAID(s)* – These fields MAID *1* to MAID *n* shall contain a list of MAIDs up to 255 active neighbours.

9.4.5 REASON control

The REASON control in an HLEAVE message is used to convey the HMA's reason for leaving the session.

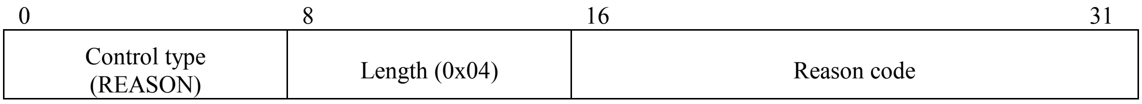


Figure 89 – REASON control format

The format of the REASON control is shown in Figure 89. The description of each field is as follows:

a) *Control type* – This field denotes the REASON control. Its value shall be set to 0x05 (see Table 29).

b) *Length* – This field denotes the length (4 bytes) of the REASON control. Its value shall be set to 0x04.

c) *Reason code* – This field denotes the reason for leaving. Its value shall be set to 0x10 00, leave initiated by the MA (see Table 35).

9.4.6 RESULT control

The RESULT control in a SUBSANS message is used to convey whether or not the MA's subscription request is successful. If successful, it returns an RE_OK result code. If not, it returns an appropriate error code.

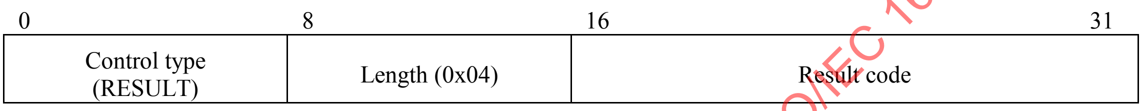


Figure 90 – RESULT control format

The format of the RESULT control is shown in Figure 90. The description of each field is as follows:

a) *Control type* – This field denotes the RESULT control. Its value shall be set to 0x06 (see Table 29).

b) *Length* – This field denotes the length (4 bytes) of the RESULT control. Its value shall be set to 0x04.

c) *Result code* – This field denotes the result of the request. It shall be set to one of the result codes listed in Table 36.

9.4.7 ROOTPATH control

The ROOTPATH control is used to convey the root path from the SMA to the message sender. It may be used for network diagnosis and loop detection.

NOTE – This control cannot be used before an MA has joined the RMCP-2 tree as it will not yet have a root path.

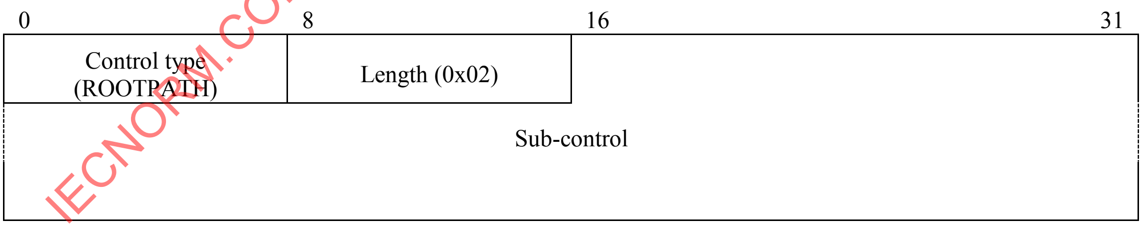


Figure 91 – ROOTPATH control format

The format of the ROOTPATH control is shown in Figure 91. The description of each field is as follows:

a) *Control type* – This field denotes the ROOTPATH control. Its value shall be set to 0x07 (see Table 29).

b) *Length* – This field denotes the length (2 bytes) of the ROOTPATH control. Its value shall be set to 0x02.

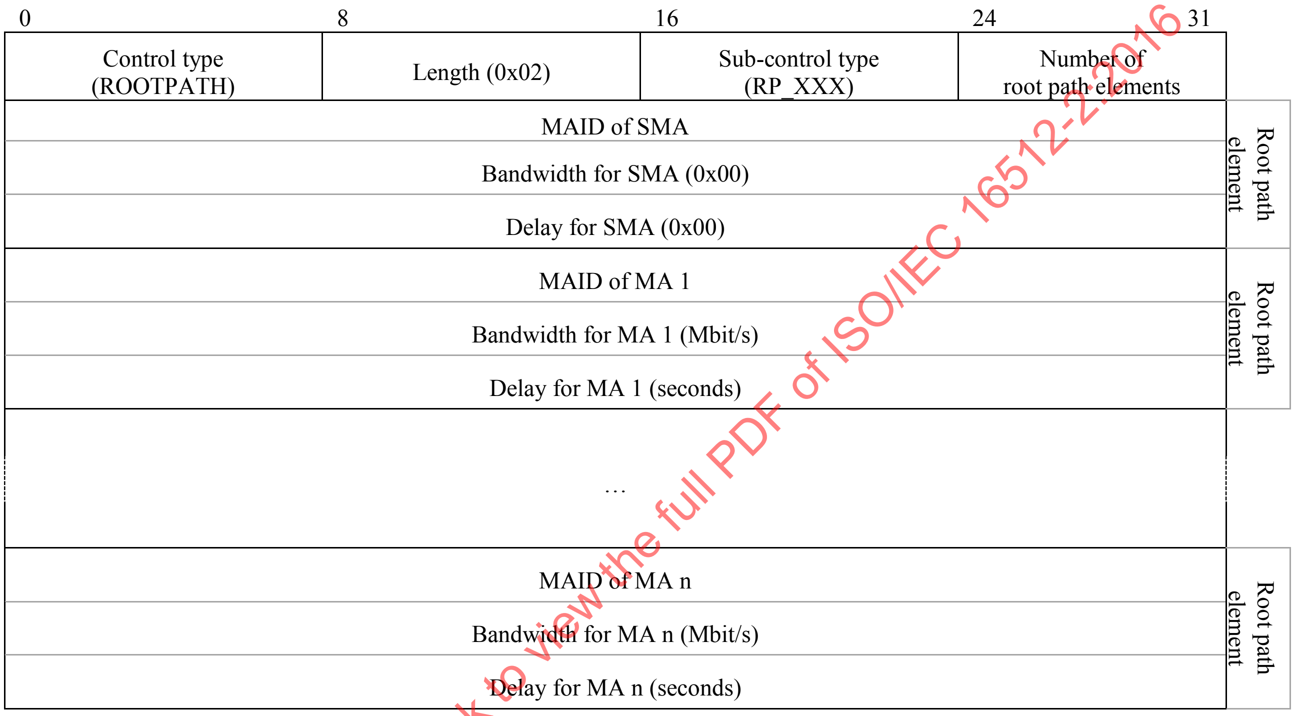
c) *Sub-control* – The RP_XXX sub-control that shall be used in the ROOTPATH control is shown in Table 25.

Table 25 – RP_XXX sub-control type for the ROOTPATH control

Sub-control type	Meaning	Status	Reference
RP_XXX	Specification of root path elements to be used.	Mandatory	See clause 9.4.7.1

9.4.7.1 RP_XXX sub-control

RP_XXX stands for one of the sub-control types listed in Table 31 (see the Note in the table). This RP_XXX sub-control represents different combinations of fields for MAIDs, bandwidth and delay. If the RP_XXX sub-control indicates that any of the MAIDs, bandwidth or delay fields are not needed, these fields shall not be present in the RP_XXX sub-control. The length of the root path element, in bytes, for each of the RP_XXX sub-control is indicated in Table 31.



0	8	16	24 31	
Control type (ROOTPATH)	Length (0x02)	Sub-control type (RP_XXX)	Number of root path elements	
MAID of SMA				Root path element
Bandwidth for SMA (0x00)				
Delay for SMA (0x00)				
MAID of MA 1				Root path element
Bandwidth for MA 1 (Mbit/s)				
Delay for MA 1 (seconds)				
…				
MAID of MA n				Root path element
Bandwidth for MA n (Mbit/s)				
Delay for MA n (seconds)				

Figure 92 – General format for RP_XXX sub-control format

The format of an RP_XXX sub-control preceded by a ROOTPATH control is shown in Figure 92. The description of each field of the RP_XXX sub-control is as follows:

a) *Sub-control type* – This field denotes the RP_XXX sub-control. Its value shall be set to one of the code values in Table 31.

b) *Number of root path elements* – This field shall be set to the number of root path elements in the RP_XXX sub-control.

c) *MAID* – This field shall be set to that of the MAID corresponding to that element, if present. This field is for each element in the root path, listed in order from the SMA.

d) *Bandwidth* – This field shall be set to the bandwidth, in Mbit/s, between the MA and its parent, as perceived by the MA for each element in the root path, listed in order from the SMA, if present. In the case of the SMA element, the value for the bandwidth shall be set to zero.

e) *Delay* – This field shall be set to the delay in seconds from the SMA as perceived by the MA for each element in the root path, listed in order from the SMA, if present. In the case of the SMA element, the value for the bandwidth shall be set to zero.

NOTE – The values for the perceived bandwidth and delay for the SMA elements are set to zero as the root path is assumed to start at the SMA.

9.4.8 SYSINFO control

The SYSINFO control in the SUBSREQ message is used to convey system information about the subscribing MA in its SYSINFO sub-controls.

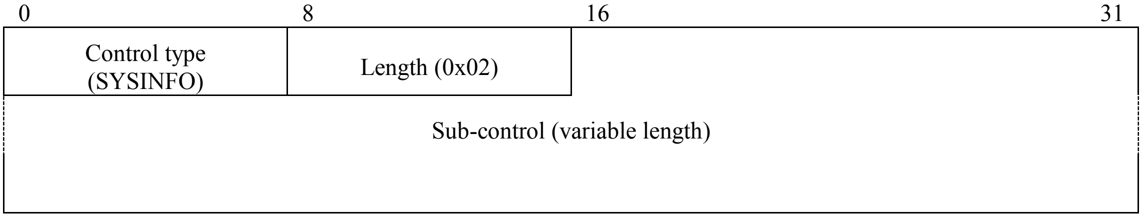


Figure 93 – SYSINFO control format

The format of the SYSINFO control is shown in Figure 93. The description of each field is as follows:

a) *Control type* – This field denotes the SYSINFO control. Its value shall be set to 0x08 (see Table 29).

b) *Length* – This field denotes the length (2 bytes) of the SYSINFO control. Its value shall be set to 0x02.

c) *Sub-control* – The sub-control types that can be used in the SYSINFO control are listed in Table 32. If more than one sub-control is required, each sub-control shall be preceded by a two-byte SYSINFO control.

9.4.8.1 SI_UPTIME sub-control

The format of the SI_UPTIME sub-control preceded by a SYSINFO control is shown in Figure 94. The description of each field of the SI_UPTIME sub-control is as follows:

a) *Sub-control type* – This field denotes the SI_UPTIME sub-control. Its value shall be set to 0x11 (see Table 32).

b) *Length* – This field denotes the length (6 bytes) of the SI_UPTIME sub-control. Its value shall be set to 0x06.

c) *Uptime* – This field shall be set to the elapsed time in seconds since the MA joined the RMCP-2 session.

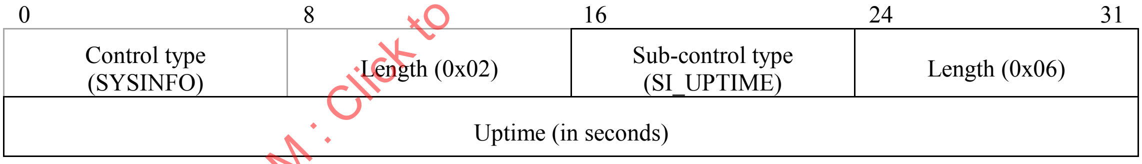


Figure 94 – SI_UPTIME sub-control format

9.4.8.2 SI_DELAY sub-control

The format of the SI_DELAY sub-control preceded by a SYSINFO control is shown in Figure 95. The description of each field of the SI_DELAY sub-control is as follows:

a) *Sub-control type* – This field denotes the SI_DELAY sub-control. Its value shall be set to 0x12 (see Table 32).

b) *Length* – This field denotes the length (6 bytes) of the SI_DELAY sub-control. Its value shall be set to 0x06.

c) *Delay* – This field shall be set to the delay in seconds from the SMA, as perceived by the MA.

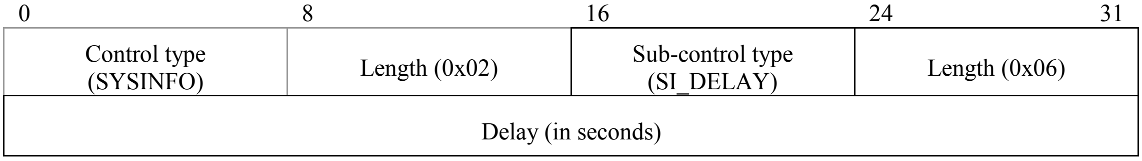


Figure 95 – SI_DELAY sub-control format

9.4.8.3 SI_ROOM_CMA sub-control

The format of the SI_ROOM_CMA sub-control preceded by a SYSINFO control is shown in Figure 96. The description of each field of the SI_ROOM_CMA sub-control is as follows:

a) *Sub-control type* – This field denotes the SI_ROOM_CMA sub-control. Its value shall be set to 0x13 (see Table 32).

b) *Length* – This field denotes the length (6 bytes) of the SI_ROOM_CMA sub-control. Its value shall be set to 0x06.

c) *Number of CMAs allocated* – This field shall be set to the number of CMA places that have been allocated by the MA. When the SI_ROOM_CMA sub-control is used in a SUBSREQ message this field shall be set to 0x0000.

d) *Total CMA capacity* – This field shall be set to the total number of CMA capacity that the MA is able to support.

NOTE – The available number of CMAs will be the difference between the total number of CMA capacity and the number of CMAs allocated.

0	8	16	24 31
Control type (SYSINFO)	Length (0x02)	Sub-control type (SI_ROOM_CMA)	Length (0x06)
Number of CMAs allocated		Total CMA capacity	

Figure 96 – SI_ROOM_CMA sub-control format

9.4.8.4 SI_PROV_BW sub-control

The format of the SI_PROV_BW sub-control preceded by a SYSINFO control is shown in Figure 97. The description of each field of the SI_PROV_BW is as follows:

a) *Sub-control type* – This field denotes the SI_PROV_BW sub-control. Its value shall be set to 0x15 (see Table 32).

b) *Length* – This field denotes the length of the SI_PROV_BW sub-control. Its value shall be set to 0x06.

c) *Incoming BW of NIC* – This field shall be set to the maximum incoming bandwidth in Mbit/s of the network interface card.

d) *Outgoing BW of NIC* – This field shall be set to the maximum outgoing bandwidth in Mbit/s of the network interface card.

0	8	16	24 31
Control type (SYSINFO)	Length (0x02)	Sub-control type (SI_PROV_BW)	Length (0x06)
Incoming BW of NIC (in Mbit/s)		Outgoing BW of NIC (in Mbit/s)	

Figure 97 – SI_PROV_BW sub-control format

9.4.8.5 SI_POSS_BW sub-control

The format of the SI_POSS_BW sub-control preceded by a SYSINFO control is shown in Figure 98. The description of each field of the SI_POSS_BW sub-control is as follows:

a) *Sub-control type* – This field denotes the SI_POSS_BW sub-control. Its value shall be set to 0x25 (see Table 32).

b) *Length* – This field denotes the length (6 bytes) of the SI_POSS_BW sub-control. Its value shall be set to 0x06.

c) *Forwarding bandwidth* – This field shall be set to the possible forwarding bandwidth in Mbit/s that the MA can support.

0	8	16	24 31
Control type (SYSINFO)	Length (0x02)	Sub-control type (SI_POSS_BW)	Length (0x06)
Forwarding bandwidth (in Mbit/s)			

Figure 98 – SI_POSS_BW sub-control format

9.4.8.6 SI_SND_BW sub-control

The format of the SI_SND_BW sub-control preceded by a SYSINFO control is shown in Figure 99. The description of each field of the SI_SND_BW sub-control is as follows:

a) *Sub-control type* – This field denotes the SI_SND_BW sub-control. Its value shall be set to 0x35 (see Table 32).

b) *Length* – This field denotes the length (6 bytes) of the SI_SND_BW sub-control. Its value shall be set to 0x06.

c) *Bandwidth* – This field shall be set to the total bandwidth in Mbit/s consumed by the MA to serve its CMAs.

0	8	16	24 31
Control type (SYSINFO)	Length (0x02)	Sub-control type (SI_SND_BW)	Length (0x06)
Bandwidth (in Mbit/s)			

Figure 99 – SI_SND_BW sub-control format

9.4.8.7 SI_SND_PACKET sub-control

The format of the SI_SND_PACKET sub-control preceded by a SYSINFO control is shown in Figure 100. The description of each field of the SI_SND_PACKET sub-control is as follows:

a) *Sub-control type* – This field denotes the SI_SND_PACKET sub-control. Its value shall be set to 0x36 (see Table 32).

b) *Length* – This field denotes the length (6 bytes) of the SI_SND_PACKET sub-control. Its value shall be set to 0x06.

c) *Number of packets* – This field shall be set to the total number of packets sent by the MA from start-up.

0	8	16	24 31
Control type (SYSINFO)	Length (0x02)	Sub-control type (SI_SND_PACKET)	Length (0x06)
Number of packets			

Figure 100 – SI_SND_PACKET sub-control format

9.4.8.8 SI_SND_BYTES sub-control

The format of the SI_SND_BYTES sub-control preceded by a SYSINFO control is shown in Figure 101. The description of each field of the SI_SND_BYTES sub-control is as follows:

a) *Sub-control type* – This field denotes the SI_SND_BYTES sub-control. Its value shall be set to 0x37 (see Table 32).

b) *Length* – This field denotes the length (6 bytes) of the SI_SND_BYTES sub-control. Its value shall be set to 0x06.

c) *Number of bytes* – This field shall be set to the total number of bytes sent by the MA from start-up.

0	8	16	24 31
Control type (SYSINFO)	Length (0x02)	Sub-control type (SI_SND_BYTES)	Length (0x06)
Number of bytes			

Figure 101 – SI_SND_BYTES sub-control format

9.4.8.9 SI_RCV_BW sub-control

The format of the SI_RCV_BW sub-control preceded by a SYSINFO control is shown in Figure 102. The description of each field of the SI_RCV_BW sub-control is as follows:

a) *Sub-control type* – This field denotes the SI_RCV_BW sub-control. Its value shall be set to 0x45 (see Table 32).

b) *Length* – This field denotes the length (6 bytes) of the SI_RCV_BW sub-control. Its value shall be set to 0x06.

c) *Bandwidth* – This field shall be set to the bandwidth in Mbit/s perceived by the MA between itself and its PMA.

0	8	16	24 31
Control type (SYSINFO)	Length (0x02)	Sub-control type (SI_RCV_BW)	Length (0x06)
Bandwidth (in Mbit/s)			

Figure 102 – SI_RCV_BW sub-control format

9.4.8.10 SI_RCV_PACKET sub-control

The format of the SI_RCV_PACKET sub-control preceded by a SYSINFO control is shown in Figure 103. The description of each field of the SI_RCV_PACKET sub-control is as follows:

a) *Sub-control type* – This field denotes the SI_RCV_PACKET sub-control. Its value shall be set to 0x46 (see Table 32).

b) *Length* – This field denotes the length (6 bytes) of the SI_RCV_PACKET sub-control. Its value shall be set to 0x06.

c) *Number of packets* – This field shall be set to the number of packets received by the MA from start-up.

0	8	16	24 31
Control type (SYSINFO)	Length (0x02)	Sub-control type (SI_RCV_PACKET)	Length (0x06)
Number of packets			

Figure 103 – SI_RCV_PACKET sub-control format

9.4.8.11 SI_RCV_BYTES sub-control

The format of the SI_RCV_BYTES sub-control preceded by a SYSINFO control is shown in Figure 104. The description of each field of the SI_RCV_BYTES sub-control is as follows:

a) *Sub-control type* – This field denotes the SI_RCV_BYTES sub-control. Its value shall be set to 0x47 (see Table 32).

b) *Length* – This field denotes the length (6 bytes) of the SI_RCV_BYTES sub-control. Its value shall be set to 0x06.

c) *Number of bytes* – This field shall be set to the number of bytes received by the MA from start-up.

0	8	16	24 31
Control type (SYSINFO)	Length (0x02)	Sub-control type (SI_RCV_BYTES)	Length (0x06)
Number of bytes			

Figure 104 – SI_RCV_BYTES sub-control format

9.4.8.12 SI_TREE_CONN sub-control

The format of the SI_TREE_CONN sub-control preceded by a SYSINFO control is shown in Figure 105. The description of each field of the SI_TREE_CONN sub-control is as follows:

a) *Sub-control type* – This field denotes the SI_TREE_CONN sub-control. Its value shall be set to 0x68 (see Table 32).

b) *Number of MAIDs* – This field shall be set to the number of MAIDs in the list including that of the PMA.

c) *MAID of PMA* – This field shall be set to the MAID of the PMA of the reporting MA.

d) *MAIDs of CMAs* – These fields shall be set to the MAIDs of the CMAs of the reporting MA.

NOTE – There is no significance in the ordering of MAIDs.

0	8	16	24 31
Control type (SYSINFO)	Length (0x02)	Sub-control type (SI_TREE_CONN)	Number of MAIDs (n + 1)
MAID of PMA			
MAID of CMA 1			
…			
MAID of CMA n			

Figure 105 – SI_TREE_CONN sub-control format

9.4.8.13 SI_TREE_MEM sub-control

The format of the SI_TREE_MEM sub-control preceded by a SYSINFO control is shown in Figure 106. The description of each field of the SI_TREE_MEM sub-control is as follows:

a) *Sub-control type* – This field denotes the SI_TREE_MEM sub-control. Its value shall be set to 0x69 (see Table 32).

b) *Number of MAIDs* – This field shall be set to the number of MAIDs listed in the SI_TREE_MEM sub-control.

c) *MAIDs of member* – These fields shall be set to the MAIDs of the members of the sub-tree defined by a TREEEXPLOR control.

NOTE – There is no significance in the ordering of MAIDs.

0	8	16	24 31
Control type (SYSINFO)	Length (0x02)	Sub-control type (SI_TREE_MEM)	Number of MAIDs (n)
MAID of member 1			
…			
MAID of member n			

Figure 106 – SI_TREE_MEM sub-control format

9.4.9 TIMESTAMP control

The TIMESTAMP control is used to measure the transmission time between the sending MA and the receiving MA.

<table>
<tr><th>0</th><th>8</th><th>16</th><th>31</th></tr>
<tr><td>Control type
(TIMESTAMP)</td><td>Length (0x10)</td><td colspan="2">Reserved</td></tr>
<tr><td colspan="4">Time 1 (when the sender starts to send)</td></tr>
<tr><td colspan="4">Time 2 (when the packet appears at receiver)</td></tr>
<tr><td colspan="4">Time 3 (when the receiver starts to reply)</td></tr>
</table>

Figure 107 – TIMESTAMP control format

The format of the TIMESTAMP control is shown in Figure 107. The description of each field is as follows:

a) *Control type* – This field denotes the TIMESTAMP control. Its value shall be set to 0x09 (see Table 29).

b) *Length* – This field denotes the length (16 bytes) of the TIMESTAMP control. Its value shall be set to 0x10.

c) *Reserved* – This field is reserved for future use. Its value shall be set to zero. It is ignored by the receiver.

d) *Time 1* – This field shall be set to the time when the request message has started to be sent to its recipient.

e) *Time 2* – This field shall be set to the time when the request message appears at the recipient. When this field is included in a request message, its value shall be set to zero.

f) *Time 3* – This field shall be set to the time when the answer message has started to be sent to the requestor. When this field is included in a request message, its value shall be set to zero.

9.4.10 CANDIDATEHMA control

When an HMA leaves a session, every non-HMA in the multicast network area may compete to become an HMA. This can cause the multicast network to be flooded with the HANNOUNCE message. To prevent HMA selection collision, CANDIDATEHMA control in an HLEAVE message is used to convey a restricted list of candidate HMAs that are invited, selected by the leaving HMA, to compete to become the replacement HMA.

<table>
<tr><th>0</th><th>8</th><th>24</th><th>31</th></tr>
<tr><td>Control type
(CANDIDATEHMA)</td><td>Reserved</td><td colspan="2">Number of
MAIDs</td></tr>
<tr><td colspan="4">MAID 1</td></tr>
<tr><td colspan="4">MAID 2</td></tr>
<tr><td colspan="4">...</td></tr>
<tr><td colspan="4">MAID n</td></tr>
</table>

Figure 108 – CANDIDATEHMA control format

The format of the CANDIDATEHMA control is shown in Figure 108. The description of each field is as follows:

a) *Control type* – This field denotes the CANDIDATEHMA control. Its value shall be set to 0x0A (see Table 29).

b) *Reserved* – This field is reserved for future use. Its value shall be set to zero. It is ignored by the receiver.

c) *Number of MAIDs* – This field shall be set to the number of MAIDs listed in CANDIDATEHMA control.

d) *MAID(s)* – These fields shall be set to the MAIDs of candidate HMAs selected by the leaving HMA.

9.4.11 TREEEXPLOR control

The TREEEXPLOR control is used to limit the inspection size of a tree.

0	8	16	24 31
Control type (TREEEXPLOR)	Length (0x04)	Reserved	Tree depth

Figure 109 – TREEEXPLOR control format

The format of the TREEEXPLOR control is shown in Figure 109. The description of each field is as follows:

a) *Control type* – This field denotes the TREEEXPLOR control. Its value shall be set to 0x0B (see Table 29).

b) *Length* – This field denotes the length (4 bytes) of the TREEEXPLOR control. Its value shall be set to 0x04.

c) *Reserved* – This field is reserved for future use. Its value shall be set to zero. It is ignored by the receiver.

d) *Tree depth* – This field shall be set to a value to specify the scope of tree inspection. A tree depth of *n* defines the set of MAs consisting of the selected MA (or the SMA) that receives the STREQ message, all of its CMAs and all of its descendants on the RMCP-2 tree within *n* hops of the selected MA (or the SMA).

9.4.12 COLLECT control

0	8	16	24 31
Control type (COLLECT)	Length (0x0C)	Reserved	Number of sub-controls
MAID (MAID of MA to which the following status reports apply)			

Figure 110 – COLLECT control format

The format of the COLLECT control is shown in Figure 110. The description of each field of the COLLECT control is as follows:

a) *Control type* – This field denotes the COLLECT control. Its value shall be set to 0x0C (see Table 29).

b) *Length* – This field denotes the length (12 bytes) of the COLLECT control. Its value shall be set to 0x0C.

c) *Reserved* – This field is reserved for future use. Its value shall be set to zero. It is ignored by the receiver.

d) *Number of sub-controls* – This field shall be set to the number of sub-controls associated with the MA identified in the MAID in e).

e) *MAID* – This field shall be set to the MAID of the MA to which the status reports in the following SYSINFO sub-controls apply (see Figure 71).

9.4.13 PSEUDO_HB control

When a PMA tries to recover from network partition, its descendants may start the network fault recovery procedure due to HB message timeout. A single point of partitioning may cause a fault recovery chain effect.

To avoid this, the MA generates a PSEUDO_HB control in order to notify its descendants of a network fault and to delay its descendants' fault recovery procedure.

0	8	16	31
Control type (PSEUDO_HB)	Length (0x04)	Reserved	

Figure 111 – PSEUDO_HB control format

The format of the PSEUDO_HB control for a pseudo-HB message is shown in Figure 111. The description of each field is as follows:

a) *Control type* – This field denotes the PSEUDO_HB control. Its value shall be set to 0x0D (see Table 29).

b) *Length* – This field denotes the length (4 bytes) of the PSEUDO_HB control for the HB message. Its value shall be set to 0x04.

c) *Reserved* – This field is reserved for future use. Its value shall be set to zero. It is ignored by the receiver.

9.4.14 PARAMETER control

The operations of the MA including SMAs such as RMCP-2 tree maintenance and HMA-related operations are conducted based on some parameters, e.g., timer. The session-related parameters are provided by the SM to the MA during the session subscription process. The PARAMETER control is used to deliver the session-related parameters from the SM to the MA.

0	8	16	31
Control type (PARAMETER)	Length (0x10)	T_PPROBE	N_PPROBE
T_HB	N_HB	T_HSOLICIT	N_HSOLICIT
T_HANNOUNCE	N_HANNOUNCE	T_RELAY	N_RELAY
T_LEAVE	Reserved (0x000000)		

Figure 112 – PARAMETER control format

The format of the PARAMETER control is shown in Figure 112. The description of each field is as follows:

a) *Control type* – This field denotes the PARAMETER control. Its value shall be set to 0x0E (see Table 29).

b) *Length* – This field denotes the length (16 bytes) of the PARAMETER control for the SUBSANS message. Its value shall be set to 0x10.

c) *T_PPROBE* – Retransmission interval of the PPROBREQ message (in seconds).

d) *N_PPROBE* – Maximum number of PPROBREQ messages delivered in a single trial.

e) *T_HB* – Retransmission interval of the HB message (in seconds).

f) *N_HB* – Maximum count of T_HB timeout before recognition of the network partition.

g) *T_HSOLICIT* – Retransmission interval of the HSOLICIT message (in second).

h) *N_HSOLICIT* – Maximum counts of T_HSOLICIT timeout before recognition of the absence of other MAs in the local multicast network.

i) *T_HANNOUNCE* – Expectation timeout for the HANNOUNCE message (in seconds).

j) *N_HANNOUNCE* – Maximum counts of T_HANNOUNCE timeout before recognition of HMA absence.

k) *T_RELAY* – Retransmission interval of the RELREQ message (in seconds).

l) N*_RELAY* – Maximum count of T_RELAY timeout before recognizance of connectivity problem between PMA and CMA.

m) *T_LEAVE* – Expectation timeout for the LEAVANS message (in seconds).

n) *Reserved* – This field is reserved for future use. Its value shall be set to zero. It is ignored by the receiver.

9.4.15 SERV_USER_IDENT control

SERV_USER_IDENT control is used to confirm that the RMA issuing the SUBSREQ message has been registered by the content provider for participation in closed groups (see clause 8.1.1.5). The SERV_USER_IDENT control type shall be used only when the RMA joins a secure RMCP-2 session in which the MM groups are defined as closed. The SERV_USER_IDENT control is used only in a secure RMCP-2.

0	8	16	31
Control type (SERV_USER_IDENT)	Length (variable)		
SERV_USER_ID (variable length)			

Figure 113 – SERV_USER_IDENT control format

The format of the SERV_USER_IDENT control is shown in Figure 113. The description of each field is as follows:

a) *Control type* – This field denotes the SERV_USER_IDENT control. Its value shall be set to 0x22 (see Table 30).

b) *Length* – This field shall be set to the length in bytes of the SERV_USER_IDENT control in bytes.

c) *SERV_USER_ID* – This field denotes the service user identifier allocated to the RMA by the content provider (see clause 8.1.1.5). Its value shall be identical to that provided to the RMA by the content provider.

NOTE – The length of the SERV_USER_ID field and the SERV_USER_IDENT control will be dependent on the length of the identifier provided by the content provider.

9.4.16 AUTH control

AUTH control is used to initiate membership authentication. This control is a mandatory part of the secure RMCP-2 RELREQ message. The AUTH control is used only in a secure RMCP-2.

0	8	16	31
Control type (AUTH)	Length (0x04)	AUTH_NAME	Reserved (0x00)

Figure 114 – AUTH control format

The format of the AUTH control is shown in Figure 114. The description of each field is as follows:

a) *Control type* – This field denotes the AUTH control. Its value shall be set to 0x23 (see Table 30).

b) *Length* – This field denotes the length in bytes of the AUTH control. Its value shall be set to 0x04.

c) *AUTH_NAME* – This field denotes the authentication mechanism. Its value shall be set to 0x01 denoting MEM_AUTH (see Table 45).

d) *Reserved* – This field is reserved for future use. Its value shall be set to 0x00.

9.4.17 AUTH_ANS control

AUTH_ANS control is used to notify the result of membership authentication. This control is a mandatory part of the secure RMCP-2 RELANS message. The AUTH_ANS control is used only in a secure RMCP-2.

0	8	16	24 31
Control type (AUTH_ANS)	Length (0x04)	Auth_result	Key_Flag
Sub-control type (KEY_MATERIAL)	Length (= variable up to 0x0804)		Key_Type
Key_DATA			

Figure 115 – AUTH_ANS control, including KEY_MATERIAL sub-control format

The format of the AUTH_ANS control and its KEY_MATERIAL sub-control are shown in Figure 115. The description of each field of the AUTH_ANS control is as follows:

a) *Control type* – This field denotes the AUTH_ANS control. Its value shall be set to 0x24 (see Table 30).

b) *Length* – This field denotes the length in bytes of the AUTH_ANS control. Its value shall be set to 0x04.

c) *Auth_result* – This field denotes the result of authentication. Its value shall be set to 0x01 for successful authentication; in the case of unsuccessful authentication, the value shall be set to one of the other codes in Table 37.

d) *Key_Flag* – This field denotes the presence or absence of key information in the KEY_MATERIAL sub-control of the AUTH_ANS control. Its value shall be set to 0x01 if key information is provided in the message; its value shall be set to 0x00 if this information is not provided.

9.4.17.1 KEY_MATERIAL sub-control

The KEY_MATERIAL sub-control shall not be included in the RELANS message if the key flag is set to 0x00. The description of each field of the KEY_MATERIAL sub-control is as follows:

a) *Sub-control type* – This field denotes the KEY_MATERIAL sub-control. Its value shall be set to 0x01 (see Table 34).

b) *Length* – This field shall be set to the total length of the KEY_MATERIAL sub-control in bytes. Its value shall not exceed 0x0804.

c) *Key_Type* – This field denotes the type of the key information. Its value shall be set to one of the code values in Table 38.

d) *Key_DATA* – This field shall contain key information resulting from clause 8.2.3, and it shall be included if the receiver is an RMA.

9.4.18 SMA_PROPOSE control

The SMA_PROPOSE control is used by the SMA to propose values to the SM for GR_ATTRIBUTE, GK_MECHA and CON_EN_DEC_ID. The SMA_PROPOSE control is used only in a secure RMCP-2.

0	8	16	24 31
Control type (SMA_PROPOSE)	Length (0x08)	GP_ATTRIBUTE	GK_MECHA
CON_EN_DEC_ID	Reserved (0x00)		

Figure 116 – SMA_PROPOSE control format

The format of the SMA_PROPOSE control is shown in Figure 116. The description of each field is as follows:

a) *Control type* – This field denotes the SMA_PROPOSE control. Its value shall be set to 0x11 (see Table 30).

b) *Length* – This field denotes the length in bytes of the SMA_PROPOSE control. Its value shall be set to 0x08.

c) *GP_ATTRIBUTE* – This field denotes the group property proposed by the SMA. Its value shall be set to one of the code values in Table 41.

d) *GK_MECHA* – This field denotes the update property of the group key proposed by the SMA. Its value shall be set to one of the code values in Table 42.

e) *CON_EN_DEC_ID* – This field denotes the content encryption algorithm proposed by the SMA. Its value shall be set to one of the code values less than 1x00 in Table 39.

f) *Reserved* – This field is reserved for future use. Its value shall be set to 0x00.

9.4.19 GK_MECH_CAPAB control

The GK_MECH_CAPAB control is used to indicate the capabilities of the SMA and DMAs during the establishment of the security policy. The GK_MECH_CAPAB control is used only in a secure RMCP-2.

0	8	16	24 31
Control type (GK_MECH_CAPAB)	Length (0x04)	GK_NAME	PREFER

Figure 117 – GK_MECH_CAPAB control format

The format of the GK_MECH_CAPAB control is shown in Figure 117. This control may be repeated in order to indicate several mechanisms, each with their own order of preference. The description of each field is as follows:

a) *Control type* – This field denotes the GK_MECH_CAPAB control. Its value shall be set to 0x12 (see Table 30).

b) *Length* – This field denotes the length in bytes of the GK_MECH_CAPAB control. Its value shall be set to 0x04.

c) *GK_NAME* – This field denotes a security mechanism held by the SMA or DMA for possible use in the secure RMCP-2 session. Its value shall be set to one of the code values in Table 43.

d) *PREFER* – This field denotes the priority of the proposed security mechanism in the preceding field. Its value shall be set to an integer in the range 1 to 6. The integer '1' shall indicate the highest priority.

9.4.20 EN_DEC_CAPAB control

The EN_DEC_CAPAB control is used to indicate the capabilities of the SMA and DMAs during the establishment of the security policy. The EN_DEC_CAPAB control is used only in a secure RMCP-2.

0	8	16	24 31
Control type (EN_DEC_CAPAB)	Length (0x04)	EN_DEC_ID	PREFER

Figure 118 – EN_DEC_CAPAB control format

The format of the EN_DEC_CAPAB control is shown in Figure 118. This control may be repeated in order to indicate several mechanisms, each with their own order of preference. The description of each field is as follows:

a) *Control type* – This field denotes the EN_DEC_CAPAB control. Its value shall be set to 0x13 (see Table 30).

b) *Length* – This field denotes the length in bytes of the EN_DEC_CAPAB control. Its value shall be set to 0x04.

c) *EN_DEC_ID* – This field denotes a proposed encryption algorithm held by the SMA or DMA for possible use in the secure RMCP-2 session. Its value shall be set to one of the code values in Table 39.

d) *PREFER* – This field denotes the priority of the proposed security mechanism in the preceding field. Its value shall be set to an integer in the range 1 to 5. The integer '1' shall indicate the highest priority.

9.4.21 AUTH_ALG_CAPAB control

The AUTH_ALG_CAPAB control is used to indicate the capabilities of the SMA and DMAs during the establishment of the security policy. The AUTH_ALG_CAPAB control is used only in a secure RMCP-2.

0	8	16	24 31
Control type (AUTH_ALG_CAPAB)	Length (0x04)	AUTH_ID	PREFER

Figure 119 – AUTH_ALG_CAPAB control format

The format of the AUTH_ALG_CAPAB control is shown in Figure 119. This control type may be repeated in order to indicate several mechanisms, each with their own order of preference. The description of each field is as follows:

a) *Control type* – This field denotes the AUTH_ALG_CAPAB control. Its value shall be set to 0x14 (see Table 30).

b) *Length* – This field denotes the length in bytes of the AUTH_ALG_CAPAB control. Its value shall be set to 0x04.

c) *AUTH_ID* – This field denotes a hash/MAC algorithm held by the SMA or DMA for possible use in the secure RMCP-2 session. Its value shall be set to one of the code values in Table 40.

d) *PREFER* – This field denotes the priority of the proposed security mechanism in the preceding field. Its value shall be set to an integer in the range 1 to 3. The integer '1' shall indicate the highest priority.

9.4.22 GK_MECH control

The GK_MECH control is used to indicate the group key mechanism for the security policy. The GK_MECH control is used only in a secure RMCP-2.

0	8	16	24 31
Control type (GK_MECH)	Length (0x08)	GP_ATTRIBUTE	GK_NAME
GK_MECHA	Reserved (0x00)		

Figure 120 – GK_MECH control format

The format of the GK_MECH control is shown in Figure 120. The description of each field is as follows:

a) *Control type* – This field denotes the GK_MECH control. Its value shall be set to 0x15 (see Table 30).

b) *Length* – This field denotes the length in bytes of GK_MECH control. Its value shall be set to 0x08.

c) *GP_ATTRIBUTE* – This field denotes the group property for the security policy. Its value shall be set to one of the code values in Table 41.

d) *GK_NAME* – This field defines the group key mechanism for the security policy. Its value shall be set to one of the code values in Table 43.

e) *GK_MECHA* – This field denotes the update property of the group key for the security policy. Its value shall be set to one of the code values in Table 42.

9.4.23 AUTH_MECH control

The AUTH_MECH control is used to indicate the authentication type for the security policy. The AUTH_MECH control is used only in a secure RMCP-2.

0	8	16	24 31
Control type (AUTH_MECH)	Length (0x04)	AUTH_ATTRIBUTE	AUTH_NAME

Figure 121 – AUTH_MECH control format

The format of the AUTH_MECH control is shown in Figure 121. The description of each field is as follows:

a) *Control type* – This field denotes the AUTH_MECH control. Its value shall be set to 0x16 (see Table 30).

b) *Length* – This field denotes the length in bytes of the AUTH_MECH control. Its value shall be set to 0x04.

c) *AUTH_ATTRIBUTE* – This field denotes the authentication type for the security policy. Its value shall be set to 0x01 denoting MEMBERSHIP (see Table 44).

d) *AUTH_NAME* – This denotes the authentication mechanism for the security policy. Its value shall be set to 0x01 denoting MEM_AUTH (see Table 45).

9.4.24 CON_EN_DEC_ALG control

The CON_EN_DEC_ALG control is used to indicate the content encryption algorithm for the security policy. The CON_EN_DEC_ALG control is used only in a secure RMCP-2.

0	8	16	24 31
Control type (CON_EN_DEC_ALG)	Length (0x04)	CON_EN_DEC_ID	Reserved (0x00)

Figure 122 – CON_EN_DEC_ALG control format

The format of the CON_EN_DEC_ALG control is shown in Figure 122. The description of each field is as follows:

a) *Control type* – This field denotes the CON_EN_DEC_ALG control. Its value shall be set to 0x17 (see Table 30).

b) *Length* – This field denotes the length in bytes of the CON_EN_DEC_ALG control. Its value shall be set to 0x04.

c) *CON_EN_DEC_ID* – This field denotes the content encryption algorithm for the security policy. Its value shall be set to one of the code values in Table 39.

d) *Reserved* – This field is reserved for future use. Its value shall be set to 0x00.

9.4.25 GK_EN_DEC_ALG control

The GK_EN_DEC_ALG control is used to indicate the group key encryption algorithm for the security policy. The GK_EN_DEC_ALG control is used only in a secure RMCP-2.

0	8	16	24 31
Control type (GK_EN_DEC_ALG)	Length (0x04)	GK_EN_DEC_ID	Reserved (0x00)

Figure 123 – GK_EN_DEC_ALG control format

The format of the GK_EN_DEC_ALG control is shown in Figure 123. The description of each field is as follows:

a) *Control type* – This field denotes the GK_EN_DEC_ALG control. Its value shall be set to 0x18 (see Table 30).

b) *Length* – This field denotes the length of the GK_EN_DEC_ALG control in bytes. Its value shall be set to 0x04.

c) *GK_EN_DEC_ID* – This field denotes the group key encryption algorithm for the security policy. Its value shall be set to one of the code values in Table 39.

d) *Reserved* – This field is reserved for future use. Its value shall be set to 0x00.

9.4.26 AUTH_ALG control

The AUTH_ALG control is used to indicate the group key encryption algorithm for the security policy. The AUTH_ALG control is used only in a secure RMCP-2.

0	8	16	24 31
Control type (AUTH_ALG)	Length (0x04)	AUTH_ID	Reserved (0x00)

Figure 124 – AUTH_ALG control format

The format of the AUTH_ALG control is shown in Figure 124. The description of each field is as follows:

a) *Control type* – This field denotes the AUTH_ALG control. Its value shall be set to 0x19 (see Table 30).

b) *Length* – This field denotes the length in bytes of the AUTH_ALG control. Its value shall be set to 0x04.

c) *AUTH_ID* – This field denotes the hash/MAC algorithm for the security policy. Its value shall be set to one of the code values in Table 40.

d) *Reserved* – This field is reserved for future use. Its value shall be set to 0x00.

9.4.27 GK_MECH_DELIVER control

The GK_MECH_DELIVER control is used to indicate the group key mechanism for the security policy when it does not hold the GK_NAME security algorithm, or when the configuration of this algorithm has failed. The GK_MECH_DELIVER control is used only in a secure RMCP-2.

0	8	16	24 31
Control type (GK_MECH_DELIVER)	Length (0x04)	GK_NAME	Reserved (0x00)

Figure 125 – GK_MECH_DELIVER control format

The format of the GK_MECH_DELIVER control is shown in Figure 125. The description of each field is as follows:

a) *Control type* – This field denotes the GK_MECH_DELIVER control. Its value shall be set to 0x1A (see Table 30).

b) *Length* – This field denotes the length in bytes of GK_MECH_DELIVER control. Its value shall be set to 0x04.

c) *GK_NAME* – This field denotes the group key mechanism for the security policy. Its value shall be identical to that in the GK_NAME field in the GK_MECH control of the SECLIST message (see clause 9.4.22 d)).

d) *Reserved* – This field is reserved for future use. Its value shall be set to 0x00.

9.4.28 AUTH_MECH_DELIVER control

The AUTH_MECH_DELIVER control is used to indicate the authentication type for the security policy when it does not hold the AUTH_NAME security algorithm, or when the configuration of this algorithm has failed. The AUTH_MECH_DELIVER control is used only in a secure RMCP-2.

0	8	16	24 31
Control type (AUTH_MECH_DELIVER)	Length (0x04)	AUTH_NAME	Reserved (0x00)

Figure 126 – AUTH_MECH_DELIVER control format

The format of the AUTH_MECH_DELIVER control is shown in Figure 126. The description of each field is as follows:

a) *Control type* – This field denotes the AUTH_MECH_DELIVER control. Its value shall be set to 0x1B (see Table 30).

b) *Length* – This field denotes the length in bytes of the AUTH_MECH_DELIVER control. Its value shall be set to 0x04.

c) *AUTH_NAME* – This field denotes the authentication mechanism for the security policy. Its value shall be set to 0x01 denoting MEM_AUTH (see Table 45).

d) *Reserved* – This field is reserved for future use. Its value shall be set to 0x00.

9.4.29 CON_EN_DEC_DELIVER control

The CON_EN_DEC_DELIVER control is used to indicate the content encryption algorithm for the security policy when it does not hold the CON_EN_DEC_ALG security algorithm, or when the configuration of this algorithm has failed. The CON_EN_DEC_DELIVER control is used only in a secure RMCP-2.

0	8	16	24 31
Control type (CON_EN_DEC_DELIVER)	Length (0x04)	CON_EN_DEC_ID	Reserved (0x00)

Figure 127 – CON_EN_DEC_DELIVER control format

The format of the CON_EN_DEC_DELIVER control is shown in Figure 127. The description of each field is as follows:

a) *Control type* – This field denotes the CON_EN_DEC_DELIVER control. Its value shall be set to 0x1C (see Table 30).

b) *Length* – This field denotes the length of the CON_EN_DEC_DELIVER control in bytes. Its value shall be set to 0x04.

c) *CON_EN_DEC_ID* – This field denotes the content encryption algorithm for the security policy. Its value shall be identical to that in the CON_EN_DEC_ID field of the CON_EN_DEC_ALG control in the SECLIST message (see clause 9.4.24 c)).

d) *Reserved* – This field is reserved for future use. Its value shall be set to 0x00.

9.4.30 GK_EN_DEC_DELIVER control

The GK_EN_DEC_DELIVER control is used to indicate the group key encryption algorithm for the security policy when it does not hold the GK_EN_DEC_ALG security algorithm, or when the configuration of this algorithm has failed. The GK_EN_DEC_DELIVER control is used only in a secure RMCP-2.

0	8	16	24 31
Control type (GK_EN_DEC_DELIVER)	Length (0x04)	GK_EN_DEC_ID	Reserved (0x00)

Figure 128 – GK_EN_DEC_DELIVER control format

The format of the GK_EN_DEC_DELIVER control is shown in Figure 128. The description of each field is as follows:

a) *Control type* – This field denotes the GK_EN_DEC_DELIVER control. Its value shall be set to 0x1D (see Table 30).

b) *Length* – This field denotes the length in bytes of the GK_EN_DEC_DELIVER control. Its value shall be set to 0x04.

c) *GK_EN_DEC_ID* – This field denotes the group key encryption algorithm for the security policy. Its value shall be identical to that in the GK_EN_DEC_ID field of the GK_EN_DEC_ALG control in the SECLIST message (see clause 9.4.25 c)).

d) *Reserved* – This field is reserved for future use. Its value shall be set to 0x00.

9.4.31 AUTH_ALG_DELIVER control

The AUTH_ALG_DELIVER control is used to indicate the hash/MAC algorithm for the security policy when it does not hold the AUTH_ALG security algorithm, or when the configuration of this algorithm has failed. The AUTH_ALG_DELIVER control is used only in a secure RMCP-2.

0	8	16	24 31
Control type (AUTH_ALG_DELIVER)	Length (0x04)	AUTH_ID	Reserved (0x00)

Figure 129 – AUTH_ALG_DELIVER control format

The format of the AUTH_ALG_DELIVER control is shown in Figure 129. The description of each field is as follows:

a) *Control type* – This field denotes the AUTH_ALG_DELIVER control. Its value shall be set to 0x1E (see Table 30).

b) *Length* – This field denotes the length in bytes of the AUTH_ALG_DELIVER control. Its value shall be set to 0x04.

c) *AUTH_ID* – This field denotes the hash/MAC algorithm for the security policy. Its value shall be identical to that in the AUTH_ID field of the AUTH_ALG control in the SECLIST message (see clause 9.4.26 c)).

d) *Reserved* – This field is reserved for future use. Its value shall be set to 0x00.

9.4.32 SEC_RETURN control

The SEC_RETURN control is used to indicate the result of SECAGREQ message. The SEC_RETURN control is used only in a secure RMCP-2.

0	8	16	24 31
Control type (SEC_RETURN)	Length (0x04)	SEC_RETURN	Reserved (0x00)

Figure 130 – SEC_RETURN control format

The format of the SEC_RETURN control is shown in Figure 130. The description of each field is as follows:

a) *Control type* – This field denotes the SEC_RETURN control. Its value shall be set to 0x1F (see Table 30).

b) *Length* – This field denotes the length in bytes of the SEC_RETURN control. Its value shall be set to 0x04.

c) *SEC_RETURN* – This field denotes the result of SECAGREQ request. Its value shall be set to 0x01 for a successful return; the value for other results shall be indicated by one of the other remaining codes in Table 38.

d) *Reserved* – This field is reserved for future use. Its value shall be set to 0x00.

9.4.33 KEY_INFO control

The KEY_INFO control is used to indicate the proposed key information. The KEY_INFO control is used only in a secure RMCP-2.

0	8	16	24 31
Control type (KEY_INFO)	Length (0x04)	Key_type	Reserved (0x00)
Sub-control type (KEY_MATERIAL)	Length (= variable up to 0x0804)		Key_type
KEY_DATA			

Figure 131 – KEY_INFO control, including KEY_MATERIAL sub-control format

The format of the KEY_INFO control and its KEY_MATERIAL sub-control is shown in Figure 131. The description of each field of the KEY_INFO control is as follows:

a) *Control type* – This field denotes the KEY_INFO control. Its value shall be set to 0x20 (see Table 30).

b) *Length* – This field denotes the length of the KEY_INFO control in bytes. Its value shall be set to 0x04.

c) *Key_type* – This field denotes the type of the proposed key information. Its value shall be set to one of the code values in Table 38.

9.4.33.1 KEY_MATERIAL sub-control

The description of each field of the KEY_MATERIAL sub-control is as follows:

a) *Sub-control type* – This field denotes the KEY_MATERIAL sub-control. Its value shall be set to 0x01 (see Table 30).

b) *Length* – This field shall be set to the total length in bytes of the KEY_MATERIAL sub-control. Its value shall not exceed 0x0804.

c) *Key_type* – This field denotes the type of the key information. Its value shall be set to one of the code values in Table 38.

d) *KEY_DATA* – This field shall contain the time information and seed value needed to generate the key identified by Key_type.

9.4.34 ACL_LIST control

The ACL_LIST control is used to contain the hashed MAID and hashed K_{TLS} for each authenticated RMA in the current session. The ACL_LIST control is used only in a secure RMCP-2.

<table>
<tr><th>0</th><th>8</th><th>16</th><th>24 31</th></tr>
<tr><td>Control type
(ACL_LIST)</td><td>Length (0x02)</td><td>Sub-control type
(ACL_DATA)</td><td>Reserved (0x00)</td></tr>
<tr><td colspan="2">Length (variable)</td><td colspan="2">N_ACL</td></tr>
<tr><td colspan="4">DATA(HASHED MAID|| HASHED K_{TLS})</td></tr>
</table>

Figure 132 – ACL_LIST control, including ACL_DATA sub-control format

The format of the ACL_LIST control and its ACL_DATA sub-control is shown in Figure 132. The description of each field of the ACL_LIST control type is as follows:

a) *Control type* – This field denotes the ACL_LIST control. Its value shall be set to 0x21 (see Table 30).

b) *Length* – This field denotes the length in bytes of the ACL_LST control. Its value shall be set to 0x02.

9.4.34.1 ACL_DATA sub-control

The description of each field of the ACL_DATA sub-control is as follows:

a) *Sub-control type* – This field denotes the ACL_DATA sub-control. Its value shall be set to 0x02 (see Table 34).

b) *Length* – This field shall be set to the length in bytes of the ACL_DATA sub-control.

c) *N_ACL* – This field shall be set to the number of the entries in the ACL_LIST control.

d) *ACL_DATA* – This field shall contain the HASHED MAID, HASHED K_{TLS} for each authenticated RMA in the current session.

10 Parameters

This clause explains the parameter values of RMCP-2 tree management. Session ID and MAID must be a unique value to identify the session and MA, respectively. RMCP-2 provides a generation rule of the ID value used for a session and MA.

10.1 Identifications used in RMCP-2

10.1.1 Session ID

SID is a 64-bit value that identifies the RMCP-2 session. SID is a combination of the local IP address of the SM and the multicast address of the session. The multicast address should be a unique value that distinguishes the RMCP-2 session.

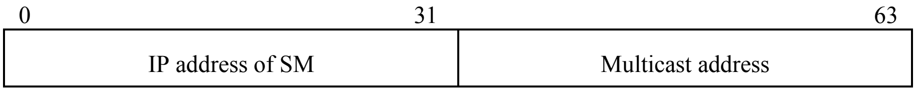


Figure 133 – RMCP-2 SID format

The format of the SID is shown in Figure 133. The description of each field is as follows.

a) *IP address of SM* – This field denotes the IPv4 address of the SM. It shall be in the format of a 32-bit IPv4 address.

b) *Multicast address* – This field denotes the IPv4 multicast address that is used in a session. It shall be in the format of the 32-bit Class D multicast address.

10.1.2 Multicast agent ID (MAID)

MAID is a 64-bit value that identifies the MA. MAID is combination of the IP address and port number.

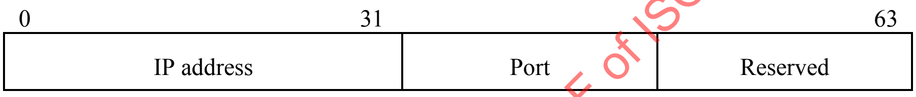


Figure 134 – RMCP-2 MAID format

The format of the MAID is shown in Figure 134. The description of each field is as follows.

a) *IP address* – This field denotes the IPv4 address of the MA. It shall be in the format of a 32-bit IPv4 address.

b) *Port* – This field denotes the port number that is used by the MA for exchanging RMCP-2 messages. It shall be in the format of a 32-bit IPv4 address.

c) *Reserved* – This field is reserved for future use. Its value shall be set to zero.

10.2 Code values used in RMCP-2

This clause defines code values for the following:

a) node types

b) message types

c) control types

d) sub-control types

10.2.1 Codes values for basic RMCP-2 node types

Table 26 lists the node types for the basic RMCP-2 and their corresponding 4-bit code values.

Table 26 – Node type code values for basic RMCP-2

Node type	Code value (4 bits)
SM	0x1
SMA	0x2
RMA	0x4
DMA (For secure RMCP-2 only)	0x5

10.2.2 Code values for RMCP-2 message types

Table 27 lists the RMCP-2 message types and their corresponding code values.

Table 27 – Code values for basic RMCP-2 message types

Message type	Code value (Hexadecimal)
SUBSREQ	0x01
SUBSANS	0x02
PPROBREQ	0x03
PPROBANS	0x04
HSOLICIT	0x05
HANNOUNCE	0x06
HLEAVE	0x07
RELREQ	0x08
RELANS	0x09
STREQ	0x0A
STANS	0x0B
STCOLREQ	0x1A
STCOLANS	0x1B
LEAVREQ	0x0C
LEAVANS	0x0D
HB	0x10
FAILCHECK	0x1C
TERMREQ	0x0E
TERMANS	0x0F
SINFO	0x11
SMNOTI	0x12

NOTE – The SINFO and SMNOTI messages are defined in Annex B which is used to provide RMCP-2 with multiple SMs.

Table 28 lists the secure RMCP-2 message types and their corresponding code values. The code values for the SUBREQ, RELREQ and RELANS messages are the same as for the code values used in basic RMCP-2.

Table 28 – Code values for secure RMCP-2 message types

Message type	Code value (Hexadecimal)
SECAGREQ	0x21
SECLIST	0x22
SECALGREQ	0x23
SECAGANS	0x24
KEYDELIVER	0x25
HRSREQ	0x26
HRSANS	0x27

10.2.3 Code values for RMCP-2 control types

Table 29 lists the RMCP-2 control types and their corresponding code values

Table 29 – Code values for RMCP-2 control types

Control type	Value (Hexadecimal)
RP_COMMAND	0x01
SI_COMMAND	0x02
DATAPROFILE	0x03
NEIGHBORLIST	0x04
REASON	0x05
RESULT	0x06
ROOTPATH	0x07
SYSINFO	0x08
TIMESTAMP	0x09
CANDIDATEHMA	0x0A
TREEEXPLOR	0x0B
COLLECT	0x0C
PSEUDO_HB	0x0D
PARAMETER	0x0E

Table 30 lists the control types and their corresponding code values used for secure RMCP-2 only.

Table 30 – Code values for secure RMCP-2 control types

Control type	Value (Hexadecimal)
SMA_PROPOSE	0x11
GK_MECH_CAPAB	0x12
EN_DEC_CAPAB	0x13
AUTH_ALG_CAPAB	0x14
GK_MECH	0x15
AUTH_MECH	0x16
CON_EN_DEC_ALG	0x17
GK_EN_DEC_ALG	0x18
AUTH_ALG	0x19
GK_MECH_DELIVER	0x1A
AUTH_MECH_DELIVER	0x1B
CON_EN_DEC_DELIVER	0x1C
GK_EN_DEC_DELIVER	0x1D
AUTH_ALG_DELIVER	0x1E
SEC_RETURN	0x1F
KEY_INFO	0x20
ACL_LIST	0x21
SERV_USER_IDENT	0x22
AUTH	0x23
AUTH_ANS	0x24

10.3 Code values for sub-control types

10.3.1 Sub-control types for the ROOTPATH control

Table 31 lists the code values for the sub-controls of the ROOTPATH control. The length in bytes of each root path element is indicated for each ROOTPATH type.

Table 31 – Sub-control type codes for the ROOTPATH control and the RP_COMMAND control

Sub-control type	Code (8 bits)	Command code (16 bits)	Meaning	Length of root path element (in bytes)
RP_ID	0x11	0x00 01	The ROOTPATH control contains only the MAID for each node.	8
RP_BW	0x12	0x00 02	The ROOTPATH control contains only the bandwidth in Mbit/s as perceived by the MA for each node.	4
RP_DL	0x14	0x00 04	The ROOTPATH control contains only the delay in seconds from the SMA as perceived by the MA for each node.	4
RP_ID_BW	0x13	0x00 03	The ROOTPATH control contains the MAID and bandwidth in Mbit/s as perceived by the MA for each node.	12
RP_ID_DL	0x15	0x00 05	The ROOTPATH control contains the MAID and the delay in seconds from the SMA as perceived by the MA for each node.	12
RP_ID_BW_DL	0x17	0x00 07	The ROOTPATH control contains the MAID, bandwidth in Mbit/s and the delay in seconds as perceived by the MA for each node.	16
NOTE – The code values for RP_ID_BW, RP_ID_DL and RP_ID_BW_DL sub-controls are calculated by 0x10 plus the arithmetic sums of the last four bits of the individual codes of the RP_ID, RP_BW and RP_DL components.				

10.3.2 Sub-control types for the SYSINFO control

Table 32 lists the sub-control types, their code values, and meanings.

Table 32 – Sub-control types for the SYSINFO control

Type	Code (8 bits)	Meaning
SI_UPTIME	0x11	The elapsed time in seconds since the node joined the RMCP-2 session.
SI_DELAY	0x12	The delay in seconds from the SMA, as perceived by the MA.
SI_ROOM_CMA	0x13	The number of CMA places that an MA has allocated and the total number that it is able to support.
SI_PROV_BW	0x15	The maximum incoming and outgoing bandwidths in Mbit/s of the network interface card.
SI_POSS_BW	0x25	The possible forwarding bandwidth that the MA can afford.
SI_SND_BW	0x35	The total bandwidth in Mbit/s consumed by the MA to serve its CMAs.
SI_SND_PACKET	0x36	The total number of packets sent by the MA from start-up.
SI_SND_BYTES	0x37	The total number of bytes sent by the MA from start-up.
SI_RCV_BW	0x45	The bandwidth in Mbit/s perceived by the MA.
SI_RCV_PACKET	0x46	The number of packets received by the MA from start-up.
SI_RCV_BYTES	0x47	The number of bytes received by the MA from start-up.
SI_TREE_CONN	0x68	A list of PMAs and CMAs directly attached to the sending MA.
SI_TREE_MEM	0x69	A set of MAs defined by the use of a TREEEXPLOR control.

Table 33 lists the command codes corresponding to the sub-controls for the SYSINFO control. Combinations of different sub-controls may be indicated by adding together the corresponding individual SI_Command codes.

NOTE – The 16-bit format column in Table 33 demonstrates how the SI_Command code values may be added together to give unique combinations. The bit positions can be considered as representing individual sub-control types and the 1 or 0 values can be interpreted as presence or absence of these sub-control types. For example, 0000 0010 0100 0010 represents the combination of SI_DELAY, SI_SND_PACKET and SI_RCV_PACKET sub-controls.

Table 33 – SI_Command codes for sub-control types for SYSINFO control

Sub-control type	Sub-control code	Command code	16-bit format
SI_UPTIME	0x11	0x00 01	0000 0000 0000 0001
SI_DELAY	0x12	0x00 02	0000 0000 0000 0010
SI_ROOM_CMA	0x13	0x00 04	0000 0000 0000 0100
SI_PROV_BW	0x15	0x00 08	0000 0000 0000 1000
SI_POSS_BW	0x25	0x00 10	0000 0000 0001 0000
SI_SND_BW	0x35	0x00 20	0000 0000 0010 0000
SI_SND_PACKET	0x36	0x00 40	0000 0000 0100 0000
SI_SND_BYTES	0x37	0x00 80	0000 000 1000 0000
SI_RCV_BW	0x45	0x01 00	0000 0001 0000 0000
SI_RCV_PACKET	0x46	0x02 00	0000 0010 0000 0000
SI_RCV_BYTES	0x47	0x04 00	0000 0100 0000 0000
SI_TREE_CONN	0x68	0x10 00	0001 0000 0000 0000
SI_TREE_MEM	0x69	0x20 00	0010 0000 0000 0000

10.3.3 Sub-control types for a secure RMCP-2

Table 34 lists the code values for the sub-control types used in a secure RMCP-2.

Table 34 – Sub-control types for a secure RMCP-2

Sub-control type	Meaning	Code value (hexadecimal)	Message types containing the control type
KEY_MATERIAL	Key material to generate the key	0x01	RELANS KEYDELIVER
ACL_DATA	ACL_list	0x02	HRSANS

10.4 Code values used in control

10.4.1 Reason code

Table 35 lists the reasons for leave of RMCP-2 nodes and their code values.

Table 35 – Reason code

Reason type	Value	Code (16 bits)	Meaning
Leave	I_LEAVE	0x01 00	Leave of the MA
	SMA_LEAVE	0x02 00	Leave of the SMA
Kick out	SM_KICKOUT	0x03 00	Expulsion by the SM
	PMA_KICKOUT	0x03 01	Expulsion by PMA

10.4.2 Result code

Table 36 lists the codes that are used in the RESULT control.

Table 36 – Result codes

Result type	Code (16 bits)	Meaning
RE_OK	0x01 00	OK
RE_SYSPROB	0x02 00	System problem
RE_ADMPROB	0x03 00	Administrative problem
RE_SERV_MISS	0x41 00	SERV_USER_ID missing
RE_SERV_NREC	0x42 00	SERV_USER_ID not recognized

NOTE – both RE_SERV_MISS and RE_SERV_NREC codes are used for the secure RMCP-2 only.

10.4.3 Return code

Table 37 lists the codes that are used in the SEC_RETURN control of the secure RMCP-2.

Table 37 – Return codes

Result type	Code (8 bits)	Meaning
RT_OK	0x01	Authentication satisfactory
RT_ERROR	0x02	Error found on authentication
RT_RETRANSMISSION_REQ	0x03	Retransmission Requested
RT_FAILEDCONFIGURATION	0x04	Applies only to SEC_RETURN in the SECAGANS message

10.4.4 Key type code

Table 38 lists the key type codes that are used in controls of the secure RMCP-2.

Table 38 – Key type codes

Result type	Code (8 bits)	Meaning
K_s	0x01	Session key
K_g	0x02	Group key
K_c	0x03	Content encryption key

10.5 Code values related to the security policy for a secure RMCP-2

Table 39 lists the EN_DEC_ID, CON_EN_DEC_ID and GK_EN_DEC_ID codes for the security policy for a secure RMCP-2.

Table 39 – EN_DEC_ID, CON_EN_DEC_ID and GK_EN_DEC_ID codes

Code	Meaning	Reference
0x01	AES CBC Mode 128-bit key	ISO/IEC 18033-3
0x02	AES CTR Mode 128-bit key	ISO/IEC 18033-4
0x03	PKCS #1	ISO/IEC 18033-2
0x04	The SEED Encryption Algorithm	ISO/IEC 18033-3
1x01	Values greater than 1x00 are reserved for other modes of AES and SEED defined by the SM	ISO/IEC 18033-3
1x02		
1x03		

NOTE – EN_DEC_ID, CON_EN_DEC_ID and GK_EN_DEC_ID are located in separate fields of the secure RMCP-2 messages. Although the values for the EN_DEC_ID, CON_EN_DEC_ID and GK_EN_DEC_ID parameters may differ, the meaning of each code, as listed above, is identical wherever it is used.

Table 40 lists the AUTH_ID codes for the security policy for a secure RMCP-2.

Table 40 – AUTH_ID codes

Code	Acronym	Meaning	Reference
0x01	HMAC-SHA1	Hash Message Authentication Code – US Secure Hash Algorithm 1	ISO/IEC 9797-2
0x02	HMAC-MD5	Hash Message Authentication Code – Message-Digest Algorithm 5	ISO/IEC 9797-2
0x03	MD5	Message-Digest Algorithm 5	ISO/IEC 9797-2

Table 41 lists the GP_ATTRIBUTE codes for the security policy for a secure RMCP-2.

Table 41 – GP_ATTRIBUTE codes

Code	Attribute	Meaning
0x01	OPEN	A service user identifier is not required by an RMA before subscribing to the secure RMCP-2 session
0x02	CLOSED	A service user identifier is required by an RMA before subscribing to the secure RMCP-2 session

Table 42 lists the GK_MECHA codes for the security policy for a secure RMCP-2.

Table 42 – GK_MECHA Codes

Code	Attribute	Meaning
0x00	STATIC	Only one group key is used per one session
0x01	PERIODIC	Group key is updated periodically
0x02	BACKWARD	Group key is updated whenever any member leaves the group
0x04	FORWARD	Group key is updated whenever any member joins the group
0x03	PERIODIC+BACKWARD	
0x05	PERIODIC+FORWARD	
0x06	BACKWARD+FORWARD	
0x07	PERIOIDC+FORWARD+BACKWARD	

Table 43 lists the GK_NAME codes for the security policy for a secure RMCP-2.

Table 43 – GK_NAME codes

Code	Acronym	Meaning	Reference
0x01	KDC	Group key management protocol (GKMP) architecture	IETF RFC 2094
0x02	GKMP	Group key management protocol (GKMP) specification	IETF RFC 2093
0x03	MIKEY	Multimedia Internet KEYing	IETF RFC 3830
0x04	GSAKMP	Group secure association key management protocol	IETF RFC 4535
0x05	LKH	Key management for multicast: Issues and architectures	IETF RFC 2627

Table 44 shows the AUTH_ATTRIBUTE code for the security policy for a secure RMCP-2.

Table 44 – AUTH_ATTRIBUTE code

Code	Value	Meaning
0x01	MEMBERSHIP	Membership of the session is authenticated using the membership authentication procedure defined in Annex A

Table 45 shows the AUTH_NAME code for the security policy for a secure RMCP-2.

Table 45 – AUTH_NAME code

Code	Acronym	Meaning	Reference
0x01	MEM_AUTH	Membership authentication	The procedure is defined in Annex A

10.6 Timer related parameters

This clause defines timers and related parameters used in RMCP-2.

10.6.1 Parameters for neighbour discovery

The following parameters in Table 46 are used to support the neighbour discovery which is described in clause 7.2.2.

Table 46 – Parameters for neighbour discovery

Parameter	Default value	Description
T_PPROBE	45 seconds	Retransmission interval of the PPROBREQ message (in seconds).
N_PPROBE	5 attempts	Maximum number of PPROBREQ messages delivered in a single trial.
PPROBANS message timeout	135 seconds	Maximum waiting time for the PPROBANS message used to recognize the problem of the probed neighbour; the estimated value is calculated as T_PPROBE * 3.

10.6.2 Parameters for heartbeat

The following parameters in Table 47 are used to support the heartbeat mechanism which is described in clause 7.1.3.

Table 47 – Parameters for heartbeat

Parameter	Default value	Description
T_HB	15 seconds	Retransmission interval of the HB message (in seconds).
N_HB	2 counts	Maximum counts of T_HB timeout before recognition of the network partition.
HB message timeout	30 seconds	Maximum waiting time for the HB message used to recognize the network partition problem; the estimated value is calculated as T_HB * N_HB.

10.6.3 Parameters for report and monitoring

The following parameters in Table 48 are used for report and monitoring.

Table 48 – Parameters for report and monitoring

Parameter	Default value	Description
T_REPORT	15 seconds	Expectation timeout for the STANS message (in seconds).
T_COLREPORT	T_REPORT * tree depth value of TREEEXPLOR control	Expectation timeout for the STANS message in case of sub-tree monitoring (in seconds).

10.6.4 Parameters for HMA-related operation

The following parameters in Table 49 are used to support HMA-related operation which is described in clause 7.2.2.1.

Table 49 – Parameters for HMA-related operation

Parameter	Default value	Description
T_HSOLICIT	10 seconds	Retransmission interval of the HSOLICIT message (in seconds).
N_HSOLICIT	3 counts	Maximum counts of T_HSOLICIT timeout before recognition of absence of other MAs in the local multicast network.
N_HANNOUNCE	3 counts	Maximum counts of T_HANNOUNCE timeout before recognition of HMA absence.
T_HANNOUNCE	1 second	Expectation timeout for the HANNOUNCE message (in seconds).
HANNOUNCE message timeout	3 seconds	Maximum waiting time for the HANNOUNCE message used to recognize the absence of the HMA; the estimated value is calculated as T_HANNOUNCE * N_HANNOUNCE.

Table 49 – Parameters for HMA-related operation

Parameter	Default value	Description
HSOLICIT message timeout	30 seconds	Maximum waiting time for the HSOLICIT message used to recognize the absence of other MAs in the local multicast network; the estimated value is calculated as T_HSOLICIT * N_HSOLICIT.

NOTE – Each MA recognizes absence of the HMA after an HANNOUNCE message timeout, which is calculated as T_HANNOUNCE * N_HANNOUNCE.

10.6.5 Parameters for maintenance of the tree

The following parameters in Table 50 are used to support the maintenance of an RMCP-2 tree, which is described in clause 7.2.5.3.2.

Table 50 – Parameters for maintenance of the tree

Parameter	Default value	Description
T_RELAY	6 seconds	Retransmission interval of the RELREQ message (in seconds).
N_RELAY	3 counts	Maximum count of T_RELAY timeout before recognition of connectivity problems between the PMA and CMA.
RELREQ message timeout	18 seconds	Maximum waiting time for the RELREQ message used to recognize the connectivity problem with the CMA; the estimated value is calculated as T_RELAY * N_RELAY.
RELANS message timeout	18 seconds	Maximum waiting time for the RELANS message used to recognize the connectivity problem with the PMA; the estimated value is calculated as T_RELAY * N_RELAY.

10.6.6 Parameters for session leave

The following parameter in Table 51 is used to support session leave of an RMCP-2 node:

Table 51 – Parameter for session leave

Parameter	Default value	Description
T_LEAVE	10 seconds	Expectation timeout for the LEAVANS message (in seconds).

10.7 Data profile used in RMCP-2

The following parameters in Table 52 are used to support the data profile.

Table 52 – Parameters for the data profile

Parameter	Value	Description	Reference
Transport protocol	TCP	Data channel will be established using the TCP.	IETF RFC 793
	UDP	Data channel will be established using the UCP.	IETF RFC 768
	SCTP	Data channel will be established using the SCTP.	IETF RFC 4960
Listening address	*IPv4 address:port number*	Listening address and port number of the MA.	–
Encapsulation scheme	IP in IP	Encapsulation scheme will be IP in IP.	IETF RFC 2003
	None	If encapsulation is not used, this parameter shall not be included in the data profile.	–

An example format of the data profile is shown in Figure 135. The data profile shall be sent in the text mode and shall contain the values, as defined in Table 31, for the transport protocol, listening address and encapsulation scheme. If the encapsulation scheme is not used, the encapsulation scheme parameter shall not be included.

Transport protocol = UDP, Listen address = a.b.c.d:9898, Encapsulation scheme = IP in IP

Figure 135 – Example of RMCP-2 data profile