INTERNATIONAL STANDARD

ISO/IEC 16512-2

First edition
2008-05-15

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

Technologies de l'information — Protocole de multidiffusion relayé: Spécifications pour applications de groupe unidirectionnel

Reference number
ISO/IEC 16512-2:2008(E)

© ISO/IEC 2008

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

© ISO/IEC 2008 – All rights reserved

Not for Resale

Contents

Page

1 Scope 1
2 Normative references 1
3 Definitions 1
4 Abbreviations 2
5 Overview 2
5.1 RMCP-2 entities 3
5.2 RMCP-2 protocol block 4
5.3 Simplex delivery model of RMCP-2 5
5.4 Types of RMCP-2 messages 5
6 Protocol operation 6
6.1 SM's operation 6
6.2 MA's operation 8
7 RMCP-2 message format 18
7.1 Common format of RMCP-2 message 18
7.2 Control data format 20
7.3 Messages 21
8 Parameters 44
8.1 Data forwarding profile 44
8.2 Parameters used in RMCP-2 45
8.3 Encoding rules to represent values used in RMCP-2 46
Annex A – Tree configuration algorithm 49
A.1 Bootstrapping rule 49
A.2 Neighbour discovering rule 50
A.3 HMA selection rule 51
A.4 CMA acceptance rule 51
A.5 Parent decision rule 52
A.6 Tree improvement rule 53
A.7 PMA's kicking-out rule 53
Annex B – Real-time data delivery scheme 54
B.1 Overview 54
B.2 IP-IP tunnel mechanism for RMCP-2 real-time data delivery 54
Annex C – Reliable data delivery scheme 56
C.1 Overview 56
C.2 Operation 56
C.3 Data encapsulation format 58
C.4 Data profile 58
Annex D – RMCP-2 API 59
D.1 Overview 59
D.2 RMCP-2 API functions 60

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 16512-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems* in collaboration with ITU-T. The identical text is published as ITU-T Rec. X.603.1 (02/2007).

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*

— *Part 3: Specification for N-plex group applications*

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale
© ISO/IEC 2008 – All rights reserved

Introduction

Relayed MultiCast Protocol Part 2 (RMCP-2) 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 a unicast network with the help of RMCP entities defined by ITU-T Rec. X.603 | ISO/IEC 16512-1.

An RMCP-2 session consists of one SM and one or more MAs; SM initiates and terminates RMCP-2 session and manages RMCP-2 session and participated MAs; MA configures an RMCP-2 tree to deliver group data by exchanging a series of RMCP-2 control messages.

Along the relayed multicast delivery path, several types of data delivery channels can be constructed according to the requirement of application services.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

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

1 Scope

This Recommendation | International Standard describes the Relayed MultiCast Protocol (RMCP) Part 2, an application-layer protocol, which constructs multicast tree for data delivery from a sender to multiple receivers over Internet where IP multicast is not fully deployed. The specified relayed multicast protocol consists of multicast agent and session manager. This Recommendation | International Standard specifies a series of functions and procedures of multicast agent to construct one-to-many relayed data path and to relay simplex data. It also specifies the operations of session manager to manage multicast sessions. This protocol can be used for applications that require one-to-many data delivery services, such as multimedia streaming service, file dissemination service, etc.

2 Normative 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.

- ITU-T Recommendation X.601 (2000), *Multi-peer communications framework.*
- ITU-T Recommendation X.603 (2004) | ISO/IEC 16512-1:2005, *Information technology – Relayed multicast protocol: Framework.*
- ITU-T Recommendation X.605 (1998) | ISO/IEC 13252:1999, *Information technology – Enhanced communications transport service definition.*
- ITU-T Recommendation X.606 (2001) | ISO/IEC 14476-1:2002, *Information technology – Enhanced communications transport protocol: Specification of simplex multicast transport.*
- ITU-T Recommendation X.606.1 (2003) | ISO/IEC 14476-2:2003, *Information technology – Enhanced communications transport protocol: Specification of QoS management for simplex multicast transport.*

3 Definitions

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

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

3.2 **IP multicast**: A multicast scheme in an IP network supported by multiple multicast-enabled IP routers.

3.3 **relayed multicast**: A multicast data delivery scheme that can be used in unicast environments; the scheme is based on intermediate multicast agents that relay multicast data from a media server to media players over a tree hierarchy.

3.4 **relayed multicast protocol (RMCP)**: A protocol that supports and manages the relayed multicast data transport.

3.5 **RMCP-2 session**: An MA set that uses the RMCP to configure the data delivery path.

3.6 **multicast agent (MA)**: An intermediate data transport entity used to relay the multicast application data. Depending on the deployment, an MA may be installed in the same system as a receiving client.

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

3.8 **receiver multicast agent (RMA)**: The MA attached to the receiver in the same system or local network.

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3.10 session manager (SM): An RMCP entity that is responsible for the overall RMCP operations; it may be located in the same system as the media server or located separately from the media server.

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

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

4 Abbreviations

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

AUTH	Authentication
CMA	Child Multicast Agent
DMA	Dedicated Multicast Agent
HANNOUNCE	HMA announce message
HB	Heartbeat message
HLEAVE	HMA leave message
HMA	Head Multicast Agent
HSOLICIT	HMA solicit message
IP-IP	IP in IP
LEAVANS	Leave answer message
LEAVREQ	Leave request message
MA	Multicast Agent
MAID	Multicast Agent Identification
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
SDP	Session Description Protocol
SID	RMCP-2 Session Identification
SMA	Sender Multicast Agent
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
T/TCP	TCP extensions to Transactions
TCP	Transmission Control Protocol
TERMANS	Termination answer message
TERMREQ	Termination request message
UDP	User Datagram Protocol

5 Overview

The RMCP-2 is an application-level protocol that uses multicast agents (MAs) and a session manager (SM) to support and manage a relayed multicast data transport over a unicast-based Internet. With the help of the SM, the RMCP-2

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

begins by constructing a relayed multicast control tree that consists of MAs. Consequently with the preconfigured control tree, each MA connects appropriate data channels with each other.

The RMCP-2 entities for a simplex delivery model are described in clause 5.1.

5.1 RMCP-2 entities

The RMCP-2 entities are the same as those described in RMCP Part 1. As shown in Figure 1, each RMCP-2 session constructs a relayed multicast data delivery model with the following entities:

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.

An SM, which can handle one or multiple sessions simultaneously, can be implemented separately or as a part of other entities in an RMCP-2 session.

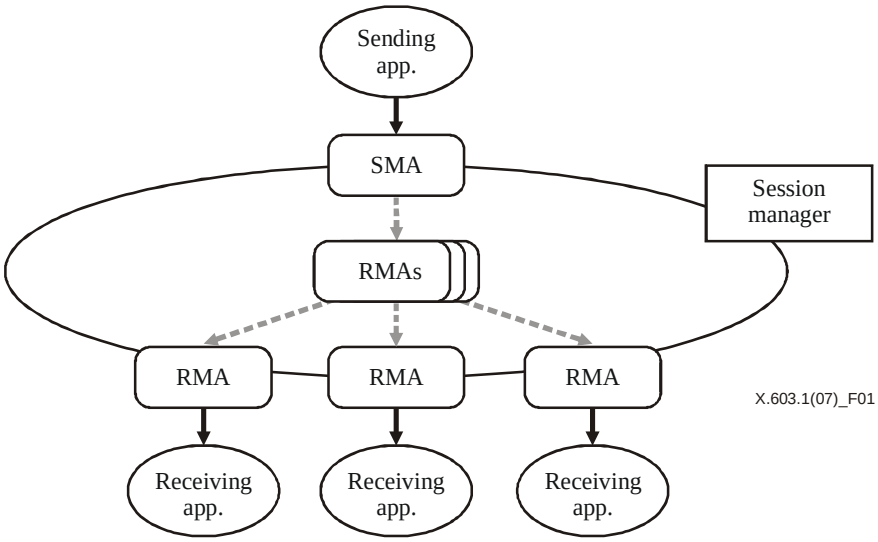

Figure 1 – RMCP-2 service topology

An SM can provide the following functionalities:

a) session initialization;

b) session release;

c) session membership management;

d) session status monitoring.

An MA, which refers to both the SMA and the RMA, constructs a relayed multicast delivery path from one sender to many receivers and then forwards data along the constructed path, can provide the following functionalities:

a) session initialization;

b) session join;

c) session leave;

d) session maintenance;

e) session status reporting;

f) application data relay.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

5.2 RMCP-2 protocol block

An SM should exchange control messages with other MAs to control and manage RMCP-2 session. The control messages used by SM should be delivered reliably; otherwise, RMCP-2 session becomes unrecoverable. Figure 2 shows a protocol stack of an SM.

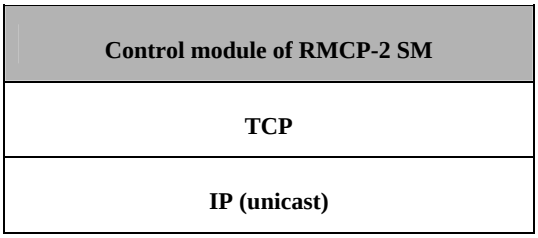

Figure 2 – Protocol stack of SM

An MA, which refers to both the SMA and the RMA, constructs a relayed multicast delivery path from one sender to many receivers and then forwards data along the constructed path. An MA consists of an *RMCP-2 control module* and a *data transport module*. The control module establishes the relayed data delivery path. The data transport module sets up a data channel along the path constructed by the control module and then relays data through the channel.

The MA's control module configures the control tree from the SMA to every leaf MAs by exchanging control messages with other MAs. Also the control module is used for session control and management by SM. Figure 3 shows the protocol stack of an MA's control module.

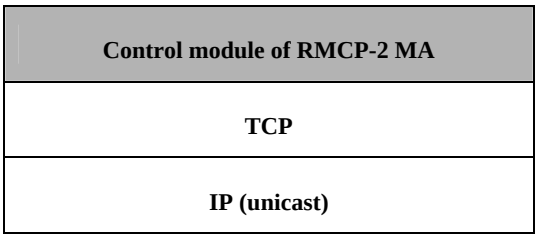

Figure 3 – Protocol stack of MA's control module

The MA's data module relays application data along the tree configured by the control module. Figure 4 shows the protocol stack of RMCP-2 data module. Any kind of transport mechanism can be inserted, if needed, because RMCP-2 imposes no restrictions on the type of application data to be delivered.

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 described later.

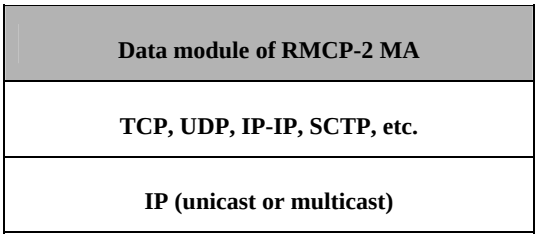

Figure 4 – Protocol stack of RMCP-2 data module

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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 B and C present two feasible real-time and reliable data delivery schemes.

5.3 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 those 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 module.

The data delivery path that 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 5 shows one of the possible relayed multicast trees configured by RMCP-2 for *simplex real-time or reliable applications.*

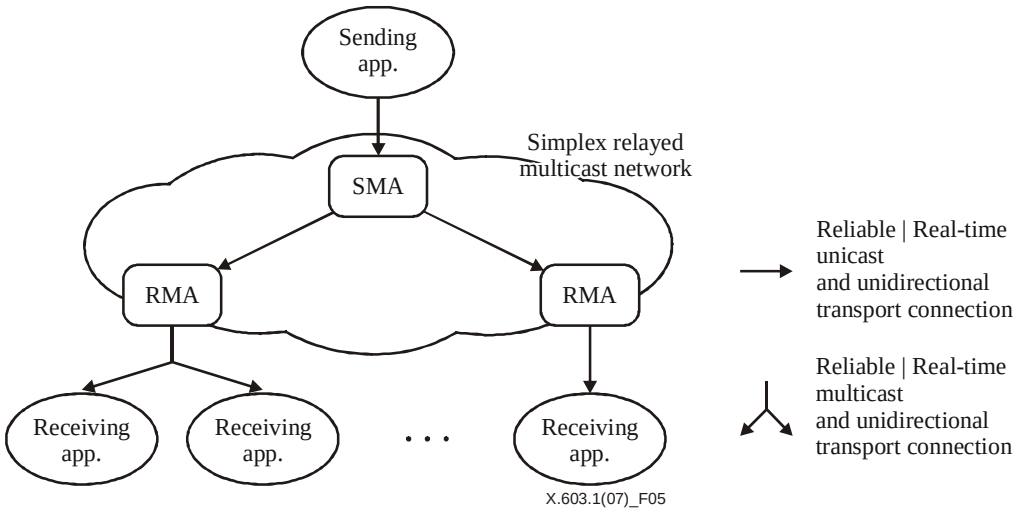

Figure 5 – Relayed multicast tree configured by RMCP-2

5.4 Types of RMCP-2 messages

To construct and maintain a relayed multicast tree, several control messages are exchanged between RMCP-2 peers in a *request-and-answer* manner. Table 1 lists the RMCP-2 control messages according to the appropriate functions.

Table 1 – RMCP-2 messages

Messages	Descriptions	RMCP operations
SUBSREQ	Subscription request	Session initialization
SUBSANS	Subscription answer	
PPROBREQ	Parent probe request	MAP discovery
PPROBANS	Parent probe answer	
HSOLICIT	HMA solicit	HMA election
HANNOUNCE	HMA announce	
HLEAVE	HMA leave	
RELREQ	Relay request	Data delivery
RELANS	Relay answer	
STREQ	Status report request	Session monitoring
STANS	Status report answer	
STCOLREQ	Status collect request	
STCOLANS	Status collect answer	

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table 1 – RMCP-2 messages

Messages	Descriptions	RMCP operations
LEAVREQ	Leave request	Session leave
LEAVANS	Leave answer	
HB	Heartbeat	Session heartbeat
TERMREQ	Termination request	Session termination
TERMANS	Termination answer	

6 Protocol operation

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

6.1 SM's operation

6.1.1 Session initiation

To make the SM create a new session, a content provider (CP) should provide a session profile, which includes details to create a session such as the session name, media characteristics, and the group address. To distinguish the sessions from each other, the SM creates a globally unique session identification (SID). After a successful session creation, the SM returns the SID to the CP. The CPs may announce the session creation by using a web server or email. But the way of session announcement is out of scope this Specification.

After the successful session creation, the SM waits for a subscription request from the MAs. When the SM receives a subscription request from an MA, the SM decides whether to accept the subscription request.

6.1.2 Admission control

On receiving MA's subscription request, firstly the SM checks the SID in the request message, and then determines whether the request is acceptable according to the session policy. RMCP-2 session can be operated privately as well as publicly with some extra information such as system information and authentication information.

When the SID in the MA's SUBSREQ is valid, then the SM checks proposed MAID and proposed data profile. If the MAID proposed by MA has null or duplicated value, then the SM proposes a unique one; otherwise, the proposed MAID will be used during the session. If the proposed data profile cannot be supported, the SM should reject the request with a reason. Otherwise, the SM can negotiate for the most effective data profile and sends back with the negotiated one.

When the MA's SUBSREQ is granted, then the SM responds with a confirmed MAID, NL and session dependent information.

To kick out a specific MA, the SM starts the discard procedure by sending a leave request (LEAVREQ) with a reason code Kicked-Out (KO) and then updates its session member list. Upon receiving SM's LEAVREQ message, MA leaves the session promptly. Figure 6 illustrates the procedure, where the SM sends a LEAVREQ message with the reason code KO and then the MA B leaves the session with notifying its PMA and CMAs of the expulsion.

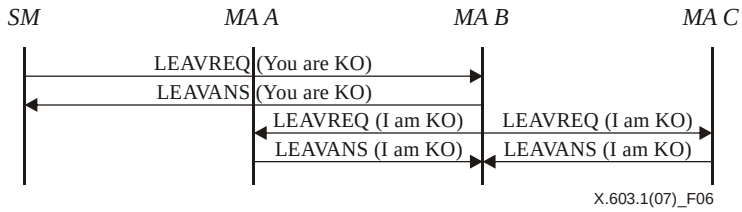

Figure 6 – When MA is kicked out by SM

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.1.3 Session monitoring

The SM can fetch status information of a specific MA by exchanging a status request and answer messages with any specific MA. Upon receiving the status request message, the MA responds with a status answer message that contains the requested information. Figure 7 shows how the SM monitors a specific MA.

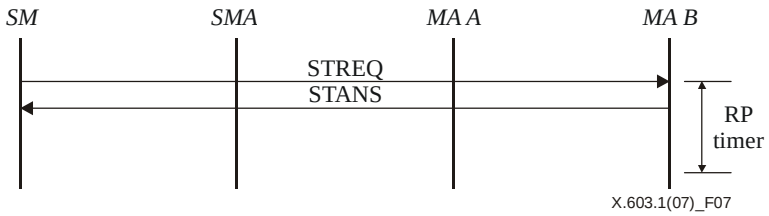

Figure 7 – Tree monitoring – Status report

SM can also collect status information of an entire or a part of a session. In this case, the SM sends a status collect request message to the top MA of the part. Upon receiving the status collect request message, the MA should send a status answer 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 overloading the network and system resources. To limit the scope of the monitoring, the status collect message should contain an option for the depth.

6.1.4 Session termination

The SM's ongoing session may terminate due to one of the following two reasons:

1) administrative request; and
2) SMA's leave.

Figure 8 shows the SM's session termination procedure.

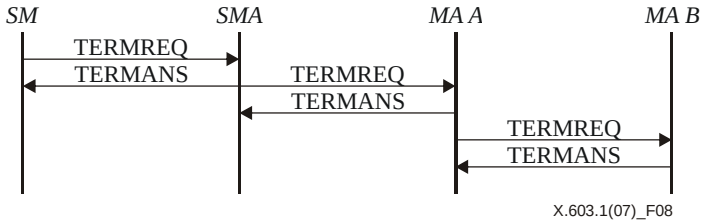

Figure 8 – Session termination issued by SM

Because a RMCP-2 session can continue only when the SMA is alive, the SMA must notify the SM when it leaves. Having been notified SMA's leave, the SM should terminate the session promptly. The session termination caused by SMA's leave is described in 6.2.4.4.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.2 MA's operation

6.2.1 Session subscription

Subscription is the first stage for an MA to be enrolled in a RMCP-2 session. Each MA must subscribe to the session by sending a subscription request (SUBSREQ) to the SM. Note that the SMA must have finished its subscription before the other MAs and it should act as a root node in the tree hierarchy. At this stage, each MA needs to know details of the session profile, such as the address of the SM and the policy.

Figure 9 shows the procedure of RMCP-2 session subscription procedure. After SMA's successful subscription, RMCP-2 session can be initiated.

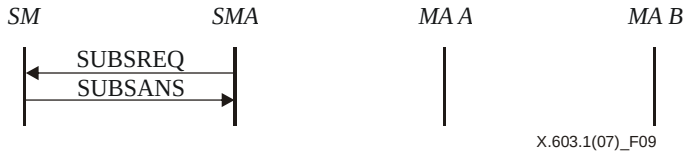

Figure 9 – SMA's subscription

Figure 10 shows the procedure of an MA subscription (for MA A and MA B). To subscribe an RMCP-2 session, each MA sends a SUBSREQ to the SM. Upon receiving SUBSREQ from the MA, the SM decides whether to accept the subscription request. If the request is accepted, the SM responds with a SUBSANS and bootstrapping information such as an NL. Otherwise, it responds with a SUBSANS with appropriate error reason code.

After receiving a successful SUBSANS from SM, the MAs (MA A and MA B) can complete the subscription phase.

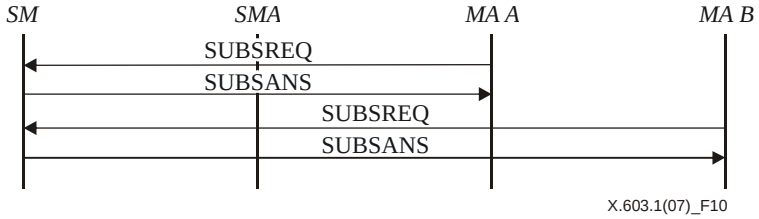

Figure 10 – MA's subscription

6.2.2 Map discovery

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

6.2.2.1 Inside multicast-enabled area

It is desirable to assign the nearest node to its PMA. The network distance in RMCP-2 depends on the delay jitter, the hop count and the bandwidth.

Normally, an MA in the same network is closer than other MAs. Each MA looks for a candidate PMA in its local network by multicasting a head multicast agent solicit (HSOLICIT) to a specific pre-assigned address (aka, broadcast) at the beginning. If there is no answer, the MA becomes the HMA, which is a representative of the MA in the multicast-enabled network.

Once an MA becomes a HMA, the HMA announces its existence to the multicast-enabled network by sending periodic HANNOUNCE messages. The HMA sends a HANNOUNCE promptly on receiving HSOLICIT from the multicast-enabled area.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Upon receiving the HANNOUNCE from the HMA, each MA considers that a HMA already exists in the same network and then assumes the HMA as its primary PMA candidate. Figure 11 shows the HMA selection procedure.

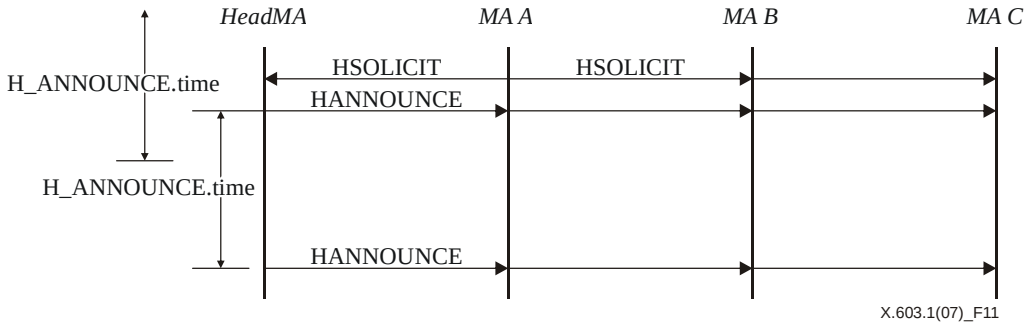

Figure 11 – HMA Solicit and its announcement

Figure 12 shows how an MA becomes a HMA. If there is no HANNOUNCE for a certain time (H_SOLICIT.time × N_SOLICIT), an MA becomes a new HMA and broadcasts a periodic HANNOUNCE every H_ANNOUNCE.time to the multicast-enabled area.

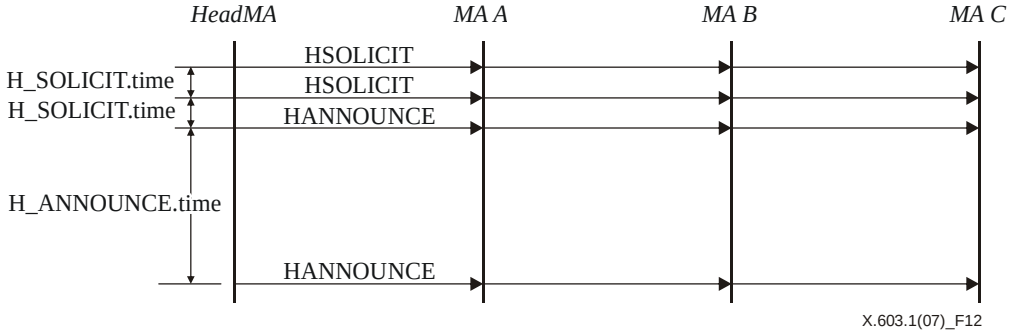

Figure 12 – An MA becomes a new HeadMA

Figure 13 shows how a HMA resumes. Once an MA becomes a HMA, it broadcasts a HANNOUNCE to the multicast-enabled network every H_ANNOUNCE.time.

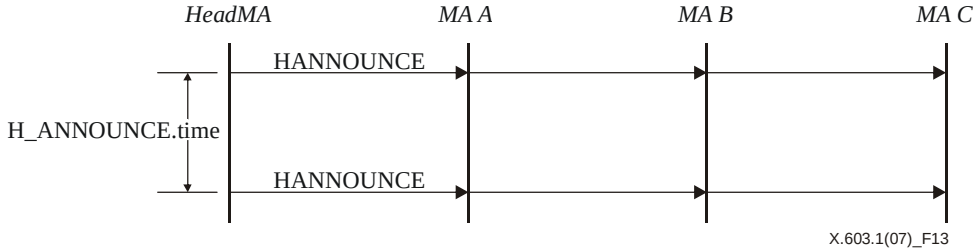

Figure 13 – Periodic head announce

Figure 14 shows how a new HMA is selected. If there is no HANNOUNCE for a certain time (H_ANNOUNCE.time × N_ANNOUNCE), the HMA waits for a HANNOUNCE for a random back-off time. If there is no HANNOUNCE, then the MA becomes the HMA of the multicast-enabled network. However, if there is a HANNOUNCE, then the MA discards the back-off time and selects the HMA as its primary PMA candidate. If there are more than two HANNOUNCE, the earliest HANNOUNCE sender becomes a HMA. If two or more HANNOUNCE have collided, then the HMA should follow the duplication suppression algorithm.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

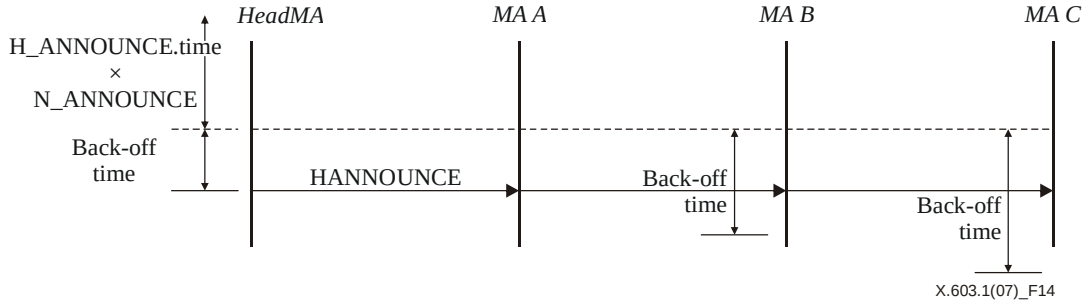

Figure 14 – New HMA selection

Because each MA in a multicast-enabled network can be elected as a HMA, each MA should also perform the map discovery mechanism for the outside network. The detailed procedure is discussed in the following subclause.

6.2.2.2 Outside multicast-enabled area

Each MA should start neighbour discovery procedure based on the initial bootstrapping information given by the SM. As shown in Figure 15, each MA can gradually learn the RMCP-2 tree topology by exchanging the tree information of each MA.

The basic map discovery mechanism is as follows: first, by using the PPROBREQ and PPROBANS, each MA can exchange a certain number of NLs at every interval (PPROBE.time). Because of the finite system resource of each MA, the maximum number of NLs to be exchanged should be bounded.

To prevent each MA suffered from PPROBREQ implosion, the maximum number of PPROBREQ messages for a certain period should be limited as N_MAX_PROBE.

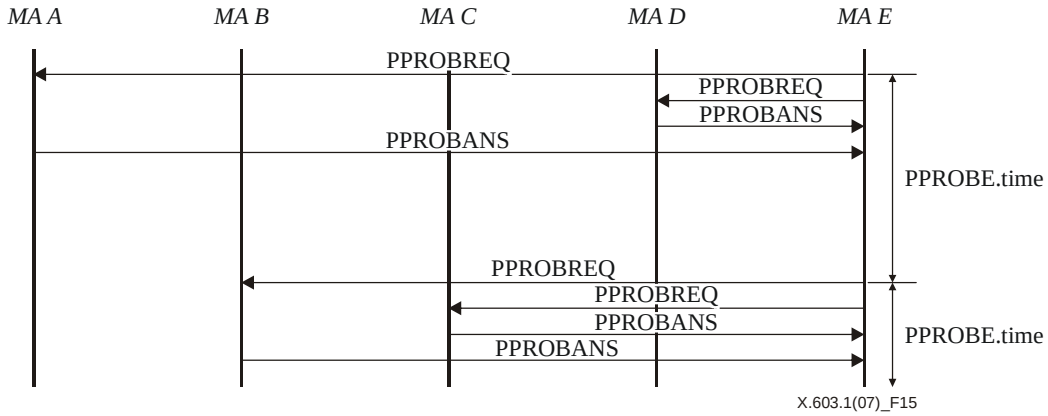

Figure 15 – Protocol sequence of map discovery

6.2.3 Tree join

Tree join procedure enables each MA to choose PMA inside a subscribed RMCP-2 session. Figure 16 shows how an MA selects its PMA based on the NL given by the SM. The joining MA (MA E) sends a PPROBREQ to one or more nodes listed in the NL (MA A, C, and D) and awaits a successful PPROBANS. Upon receiving a PPROBANS, the MA E can select the nearest MA. In Figure 16, the joining MA (node E) considers that the MA D is the best and then chooses the MA D as its PMA. After a PMA is selected, the joining MA (node E) will send to the MA D a RELREQ, which contains a proposed *data profile*.

If the RELREQ is acceptable, the MA D responds with a successful RELANS, which includes the negotiated *data profile* to be used. Otherwise, the MA D returns a reason code of the rejection.

Upon receiving a successful RELANS, data channel between the MA D and MA E is established according to the negotiated data profile. Otherwise, the MA E should try the second optimal PMA candidate.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

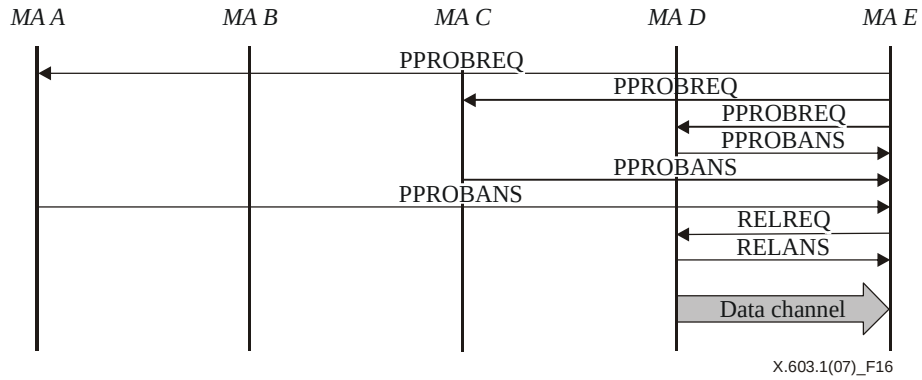

Figure 16 – Protocol sequence of successful tree join

If no MA wants to relay data to the joining MA, the joining MA can retry *tree join procedure* after a certain period. The retrial time can be set by the user, though this issue is beyond the scope of this Specification. Figure 17 shows when all the MAs listed in the NL given by the SM rejected node E's relay request. However MA E already learned about the existence of MA B during previous exchanges of PPROBREQ and PPROBANS, it can restart the joining procedure from MA B.

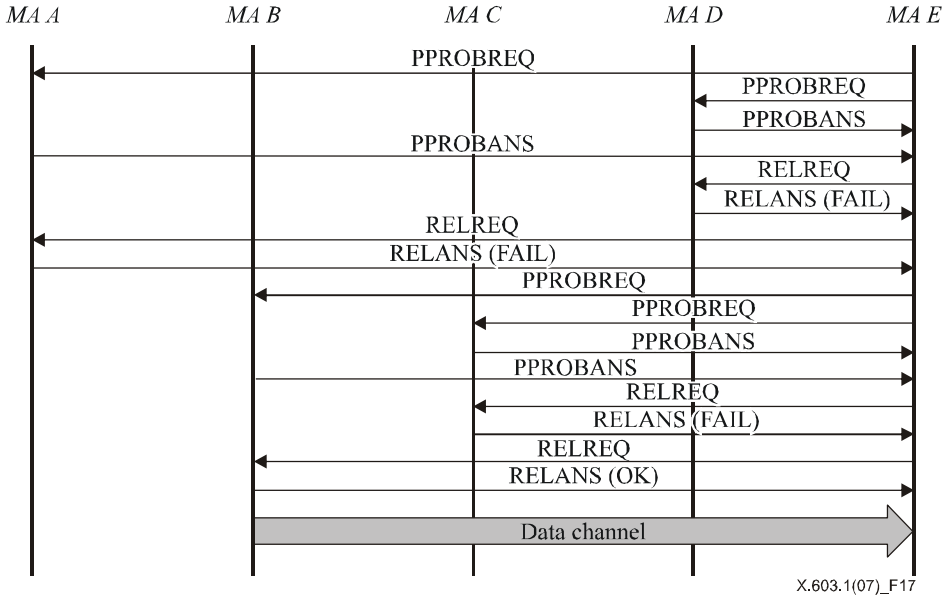

Figure 17 – Sequence of unsuccessful tree join and retrial

6.2.4 Leave

An RMCP-2 MA may leave a session during the session lifetime. To make a RMCP-2 tree robust, each MA should notify its departure to the PMA and CMAs. Upon receiving this notification, the PMA and each CMA should follow the appropriate procedure.

The RMCP-2 considers four types of departure. The first one refers to an MA that leaves the session at the request of a service user. The second one refers to an MA that leaves its PMA to switch parents. The third one refers to the expulsion of an MA from its PMA or SM. The final one refers to the departure of an SMA from a session. The detailed operations for the cases are described in the following subclauses.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.2.4.1 When MA leaves a session

MAs may leave a session at any time during the session's lifetime. Before leaving, an MA must notify the PMA and CMAs of its departure. The PMA deletes the node from its CMA list and reserves a space for a new CMA.

a) *MA's leaving with multicast-disabled data delivery scheme*

To leave a session, an MA sends a LEAVREQ to its CMAs. Each CMA who receives the LEAVREQ should promptly start to connect to an alternative PMA by sending a RELREQ to the PMA candidate. If successful, each CMA sends its old PMA a LEAVANS.

Figure 18 shows how the MA C acts when the HMA leaves a session during which the multicast data delivery scheme is not used. MA C tries to leave the session by sending a LEAVREQ to MA D and MA E, which are the CMAs of MA C. On receiving the LEAVREQ, MA D and MA E each sends a RELREQ to their own PMA candidate.

After each MA has successfully attached to a new PMA (MA A and MA B), each MA (MA D and MA E) sends a LEAVANS to the current PMA (MA C). Upon receiving the LEAVANS from its CMAs, the MA C sends a LEAVREQ to its PMA (MA B). The PMA subsequently frees the MA from its CMA list. Any departing MA without CMA simply sends a LEAVREQ to its PMA.

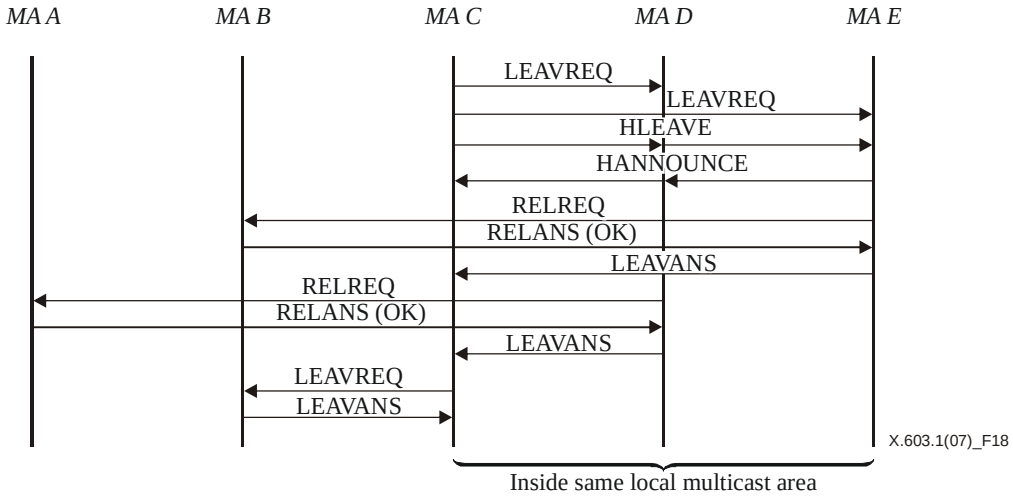

Figure 18 – HMA's leaving with multicast-disabled data delivery scheme

Figure 19 shows how a MA, which is not a HMA, leaves a session when a multicast-disabled data delivery scheme is used. In this scenario, the procedures of leaving for a non-HMA and the HMA are the same, except the HMA follows the HLEAVE exchanging sequence.

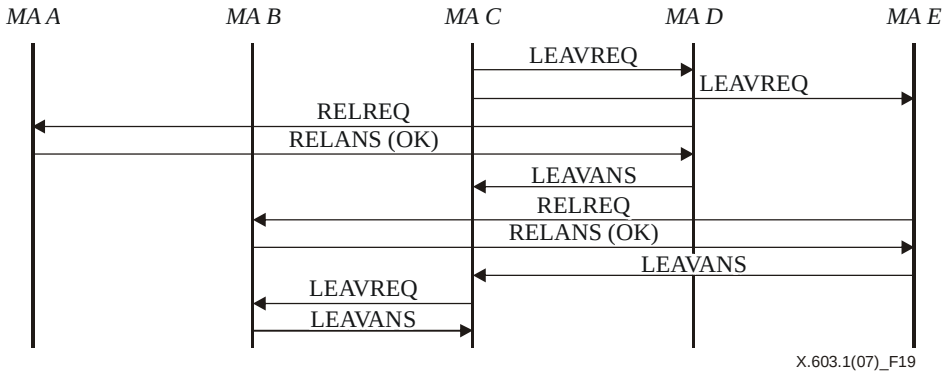

Figure 19 – Normal MA's leaving with multicast-disabled data delivery scheme

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

b) *MA's leaving with multicast-enabled data delivery scheme*

There are two cases of MA's leaving within a multicast-enabled area. The first case is of HMA's leaving and the other is of MA's leaving. Whenever the HMA of a multicast-enabled area wants to leave a session, it should notify its departure to the CMAs inside the local network as well as to the CMAs and the PMA outside the network.

Figure 20 shows how the MA C, which acts as HMA, leaves a session where the multicast data delivery scheme is used. The HMA (MA C) sends a LEAVREQ to its direct CMA (MA F) outside the local network. Upon receiving the LEAVREQ, MA F starts to switch parents and responds to MA C with a LEAVANS as well as multicasts a HLEAVE with an empty HMA candidate list to the local network. The HLEAVE message is used to announce the departure of the HMA.

Upon receiving the HLEAVE from HMA, both MA D and MA E from Figure 20 wait for a certain back-off time before multicasting the HANNOUNCE. The MA D sends the HANNOUNCE for the first time and becomes a new HMA. This step occurs because the MA D has a shorter back-off time than any other MA. Because the leaving MA C is a point which is connected to outside multicast-enabled network, the MA D should undertake the role of the MA C by connecting to the PMA outside of the network. Figure 20 shows how the MA D selects for its parent the MA B, which is the PMA of the MA C.

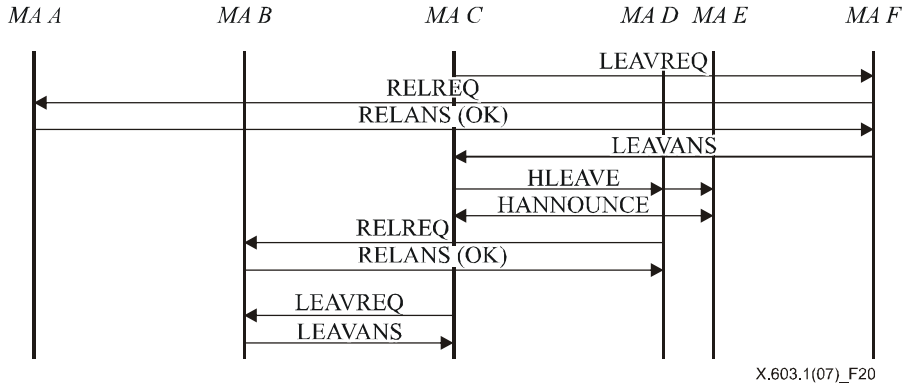

Figure 20 – MA's leaving with multicast-enabled data delivery scheme

Whenever any non-HMA of a multicast-enabled area wants to leave a session, it silently leaves the session. The MA D or MA E from Figure 20 does not need to notify other MAs of its departure.

6.2.4.2 When MA leaves from its PMA – for parent switching

An MA that wants to switch its PMA may leave its current PMA. In this case, the MA does not need to send a LEAVREQ to its CMAs. The CMAs do not need to know about the departure as long as they successfully receive data. To switch PMA, the MA sends a RELREQ to the other PMA candidate. An old PMA that receives a LEAVREQ with the reason code set to PS (parent switching) deletes the leaving MA from its CMA list but keeps the information of the departing MA in its NL because the leaving MA is still alive in the session.

Figure 21 shows how an MA switches its parents. Note that an MA can switch parents only when it receives a HB to keep tree unchanged. The HB mechanism is described in 6.2.5.1.

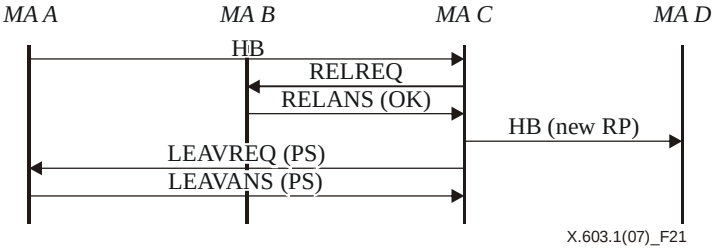

Figure 21 – MA's leaving for parent switching

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.2.4.3 When MA is kicked out

RMCP-2 has a mechanism for discarding certain MAs. For example, when a network manager wants the SM to discard a specific MA; and when an MA expels a CMA after it was aware that it cannot support more CMAs.

a) *Expulsion of an MA by its PMA*

A PMA can expel one of its CMAs when the PMA suffers from depleted system resources and can no longer feed its CMA, or when the PMA finds that one of its CMAs has depleted the system resources. An MA should find another PMA candidate, which would allow for a new CMA.

Figure 22 shows an example of a message flow. First, a PMA, namely the MA C, sends a LEAVREQ with a reason KO to expel MA D. The MA D searches other PMAs and sends a relay request. After switching parents, MA D transmits a LEAVANS to its old PMA.

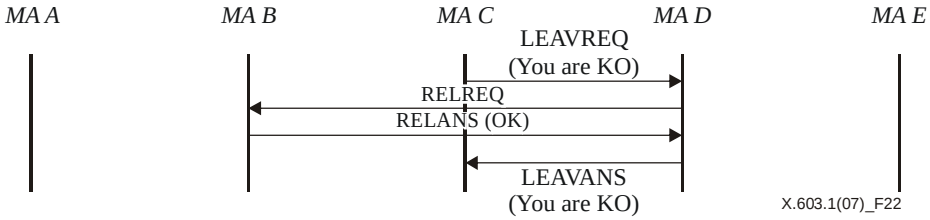

Figure 22 – When MA is kicked out by its PMA

b) *Expulsion of an MA by the SM*

The SM can discard any MA by sending a LEAVREQ with a reason kicked-out (KO). Upon receiving LEAVREQ from SM, an MA must leave the session promptly. After the expulsion, the SM should update its session member list.

In the message flow shown in Figure 23, the SM tells MA B to leave by sending a LEAVREQ with a reason KO. MA B must leave the session but, before leaving, MA B must notify its PMA and CMAs of its expulsion.

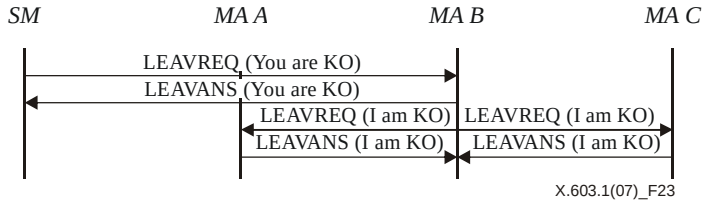

Figure 23 – When MA is kicked out by SM

6.2.4.4 When SMA leaves the session

Because an RMCP-2 session cannot exist without an SMA, an SMA never leaves a session before the session is terminated. In this case, when the SMA leaves the session, the session should be terminated.

Figure 24 shows the departure procedure of an SMA from a session. The SMA sends a LEAVREQ to the SM. Upon receiving the LEAVREQ from the SMA, the SM removes the session information and then replies with LEAVANS. Upon receiving the LEAVANS from the SM, the SMA sends a LEAVREQ with reason *SMA leave* to its direct CMAs. The LEAVREQ with reason *SMA leave* should be relayed downward promptly to make RMCP-2 session terminated.

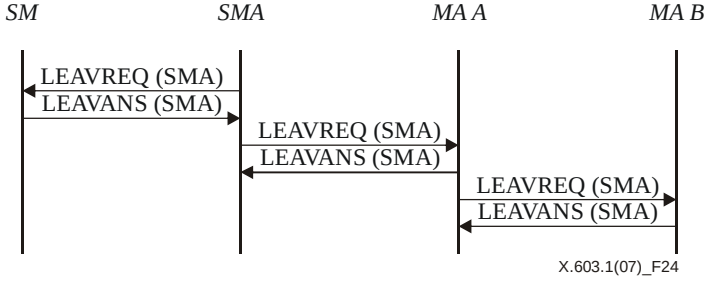

Figure 24 – SMA's leaving

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.2.5 Maintenance

6.2.5.1 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 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.

Figure 25 shows the RMCP-2 heartbeat procedure. In this procedure, the SMA sends the HB, along the ROOTPATH, to its descendants; each descendant then appends the hop information, which may include MAID, per-hop network distance and system information such as in-and-out bandwidth, affordable number of CMA, etc. to the HB and forwards the modified HB to its descendants. Finally, the ROOTPATH contains all the MAs visited along the tree.

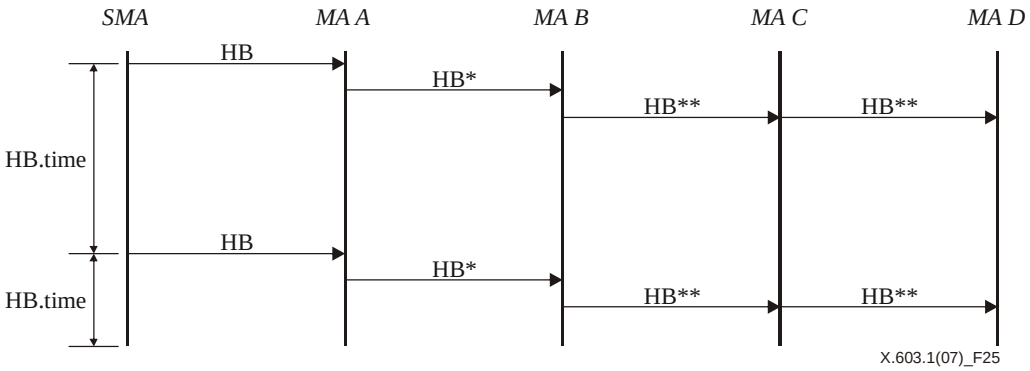

Figure 25 – Heartbeat

6.2.5.2 Monitoring

RMCP-2 has two types of monitoring mechanisms. The first one, which is shown in Figure 26, monitors a specific MA. The other one, which is shown in Figure 27, monitors a part of the tree through a specific MA.

Figure 26 shows how an SM monitors a specific MA. In this procedure, the SM sends an STREQ to MA B and requests one or more specific types of status information from MA B. In response, MA B sends the SM a STANS with the requested information.

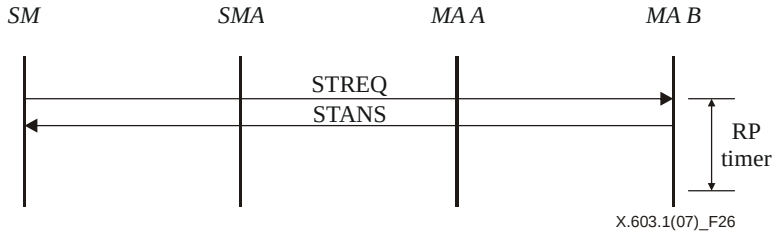

Figure 26 – Tree monitoring by status report

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Figure 27 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 to a specific MA (SMA and MA A each) to collect status information for the scoped area.

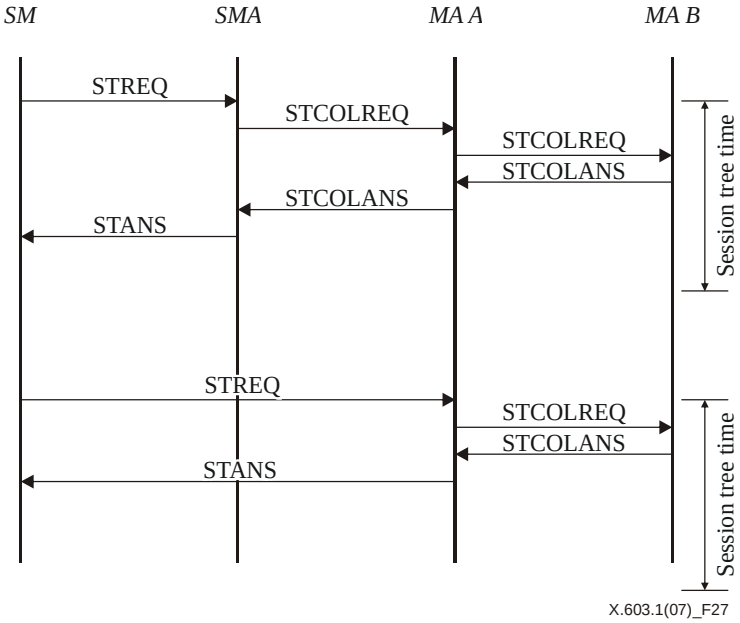

Figure 27 – Tree monitoring by collecting status report

6.2.5.3 Fault detection and recovery

This procedure is performed by each MA when each MA detects network faults and recovers from the problems to make the RMCP-2 tree robust. Network faults such as looping or partitioning are often caused by MA's frequent and careless movements. To detect and recover such network faults, RMCP-2 provides the following fault detection and recovery mechanisms.

a) *Loop detection and recovery*

A loop can be detected by checking the ROOTPATH contained in HB. Because the ROOTPATH gives the path track from the SMA to itself, the duplicated hop in the ROOTPATH means that a loop has formed. Whenever a loop occurs, each MA performs the following loop recovery mechanism: for the scenario described in Figure 28, MA Y examines the HB; MA Y then confirms the existence of a loop whenever it receives HB_{n+3} because MA Z, which is a CMA of MA Y, is already listed in the ROOTPATH twice. To recover from the loop, MA Y sends MA Z a LEAVREQ message to disconnect.

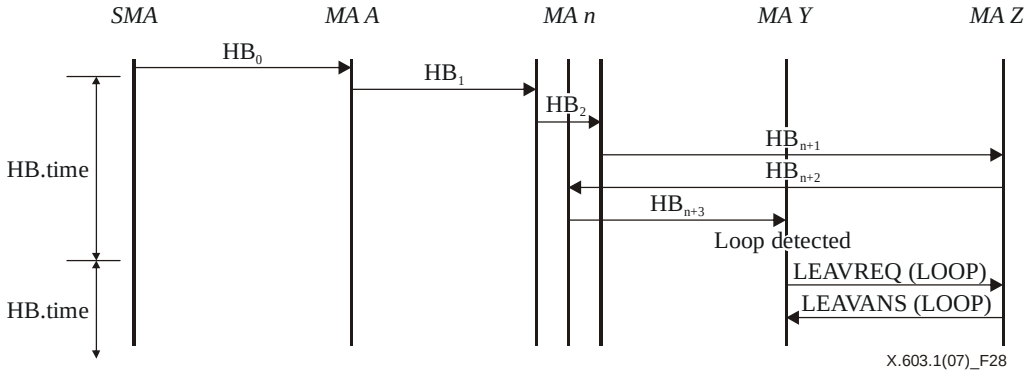

Figure 28 – Loop detection and recovery

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

b) *Network partitioning detection and recovery*

Whenever an MA fails to receive the HB message for a certain time, the MA assumes that it is partitioned from the tree. The time should be set for sufficient time to allow for a network delay. RMCP-2 defines the time as HB_TIME × MAX_PARTITION_CNT.

A partition can occur whenever one of the partition's associates fails. The MA detects the source of the partitioning by contacting its associates; the MA then solves the problem.

Figure 29 shows how MA Z detects tree partitioning: that is, a tree partition is detected whenever MA Z fails to receive the HB message for a certain period (HB_TIME × MAX_PARTITION_CNT). The failure to receive the HB message triggers the transmission of a number of PPROBREQ messages towards its associates. In Figure 29, MA Z receives a PPROBANS message from MA A and MA B but no response from MA C, the current PMA of MA Z. MA Z detects that the partitioning occurs as a result of the failure of the direct PMA of MA Z; MA Z then tries to switch parents in order to recover from the partitioning.

During an MA's repairing the partition, the MA's descendants may also consider that the network has partitioned and they may start to repair the partition. As a result, an MA's failure in just one point can cause an entire tree to collapse. To prevent this problem, an MA, which is repairing a network fault, generates a pseudo HB message to its descendants to notify that the session is temporarily partitioned and being recovered.

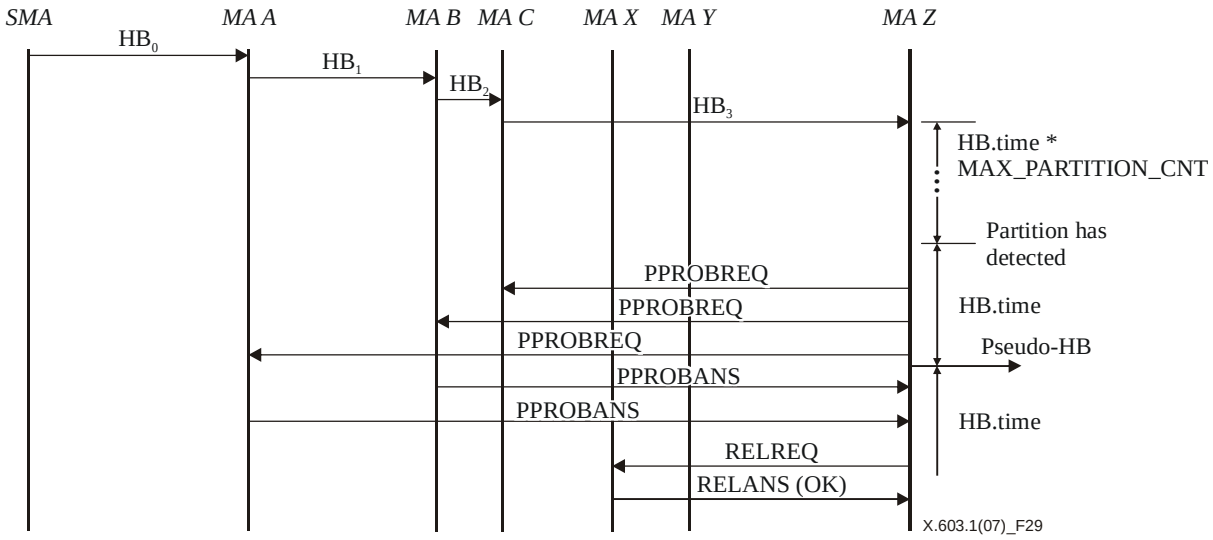

Figure 29 – Network partitioning detection and recovery

6.2.5.4 Tree improvement

Tree improvement procedure occurs when an MA finds one or more efficient PMA candidates and tries switching to the found one. By continuing the tree improvement procedure during the session, RMCP-2 tree can be improved gradually.

The procedure for finding better nodes follows the map discovery mechanism described in 6.2.2. At every turn of the map discovery, each MA compares the QoS parameters of its current PMA with those of the newly discovered node. When an MA finds a better MA than its current PMA, then the MA can switch its current PMA to a newly discovered MA according to the parent switching procedure described in 6.2.4.2.

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

To keep a tree from these hazards, RMCP-2 guarantees the atomic condition, in which each MA can switch a parent only after receiving a HB message with an unchanged ROOTPATH.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.2.6 Termination

To terminate a session, the SM sends a TERMREQ to SMA as shown in Figure 30. 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 then forwards the TERMREQ message to its CMAs until it reaches the end nodes of the tree. Finally, the session is closed.

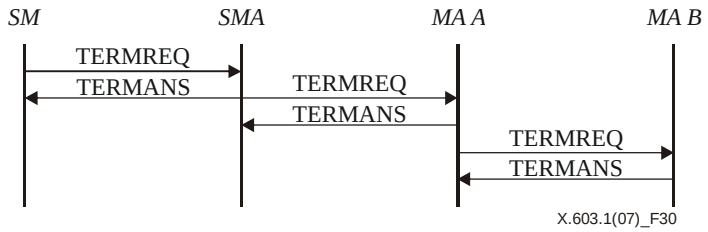

Figure 30 – Session termination issued by SM

7 RMCP-2 message format

This clause describes the formats and required information of the RMCP-2 messages. The corresponding value information of each message will be explained in clause 8.

7.1 Common format of RMCP-2 message

Figure 31 shows common RMCP-2 message format.

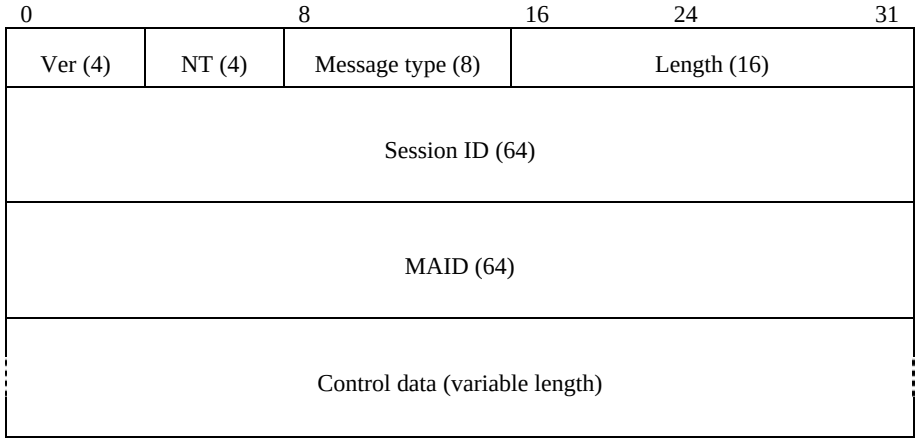

Figure 31 – Common RMCP-2 message format

The description of each field is as follows:

a) *Version* – It represents the current RMCP version. The default value for RMCP-2 is set to 0x2.

b) *NT (Node Type)* – It represents the type of node. It must be set to identify itself such as SM, SMA and MA.

c) *Message type* – It represents the type of the message.

d) *Length* – It represents the total length of the message in bytes including control data.

e) *Session ID* – It is a 64-bit integer that identifies a session.

f) *MAID* – It is a 64-bit unique value used to identify the MA for a certain session.

g) *Control data* – It contains control data used by each message as needed.

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

7.1.1 Session ID

Session ID (SID) is a combination of the local IP address of the Session Manager (SM) and the group address of the session. The group address for a new session can be allocated by SM when the SM is requested to create a session. By doing this, the SID can be guaranteed as globally unique. Figure 32 illustrates the RMCP-2 SID format.

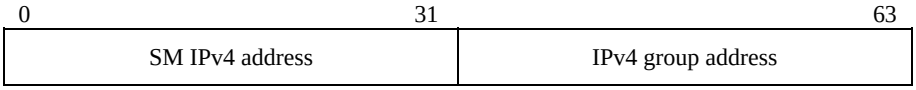

Figure 32 – RMCP-2 SID format

7.1.2 MAID

MAID consists of the local IP address, port number, and serial number as shown in Figure 33. The local IP address is the IP address of the MA. An MA in a RMCP-2 session may have to open several ports for the session. The port number used for generation of its MAID is a listening port number opened when the MA starts to run RMCP-2 in order to receive control messages from SM or other MAs.

Each MA can be identified by its port number in a multi-user system. It is, however, not possible to identify each MA inside of a Network Address Translation (NAT) based network, where it may show the same IP address for multiple MAs to the communication peer outside of the network. To handle this case, SM generates a unique MAID as it fills in a unique value in the serial number field when it receives a NAT address from an MA, and returns the ID to the MA.

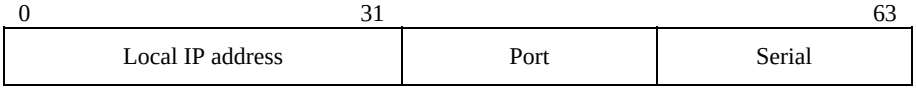

Figure 33 – RMCP-2 MAID format

Figure 34 shows the algorithm that the current version of RMCP-2 uses to generate a unique MAID.

```
If the IP address in the received MAID is a NAT address
        Search for its NAT_address_list;
        if there already exists the same address
                serial_number++;
          else
                add the list into NAT_address_list
                serial_number++;
        MAID = IP_address + port_number + serial_number;
return MAID;
```

Figure 34 – A simple algorithm to generate a unique MAID

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.2 Control data format

Figure 35 shows the RMCP-2 control data format.

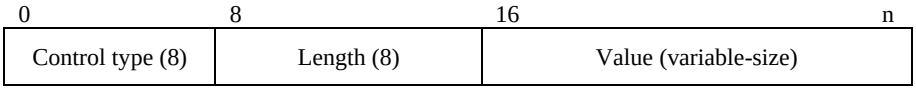

Figure 35 – RMCP-2 control format

a) *Control type* – It represents the type of control data.

b) *Length* – It represents the length in byte of control data value as well as type and length field except sub-control data field.

c) *Value* – It contains the value of control data.

Whenever RMCP-2 control data wants to specify its control in detail, it can apply sub-option data. The format of sub-option data takes that of RMCP-2 control data as shown in Figure 36.

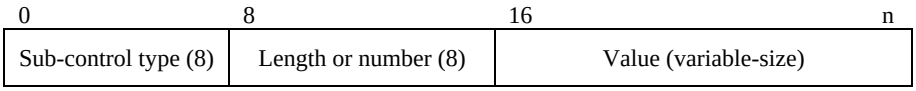

Figure 36 – RMCP-2 sub-control format

a) *Sub-control type* – It describes the type of sub-control data.

b) *Length or number* – It represents the length in byte or the number of sub-control data value depending on the sub-control data value.

c) *Value* – It represents the value of sub-control data.

A control data can be represented by using only one control data alone as shown in Figure 37.

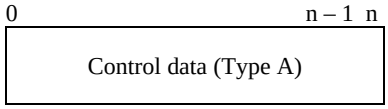

Figure 37 – Usage of control data alone

Whenever sub-control data is used, an appropriate control data must precede. Figure 38 shows an appropriate control data must precede the sub-control data to be used.

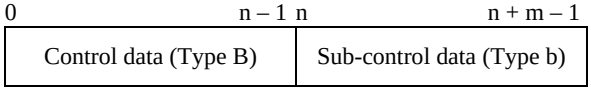

Figure 38 – Usage of control data with sub-control data

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

One or more control data can be located in RMCP-2 control data field at once. When a RMCP-2 packet wants to include multiple control data, it should align multiple control data as shown in Figure 39.

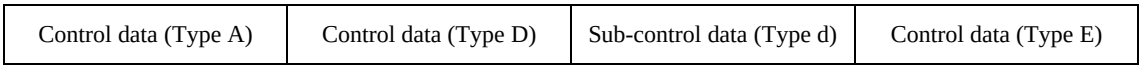

Figure 39 – Usage of multiple control data

7.3 Messages

This subclause defines each message used in RMCP-2. RMCP-2 defines seven sets of *request and reply* manner (sometimes called as *request and confirm* manner) of messages and one heartbeat message. The message types and corresponding values for the messages are listed in Table 2.

7.3.1 SUBSREQ

The SUBSREQ message is used to subscribe to a RMCP-2 session. Issuing SUBSREQ message each MA can obtain bootstrapping information from the SM when it is acceptable. The message format is shown in Figure 40.

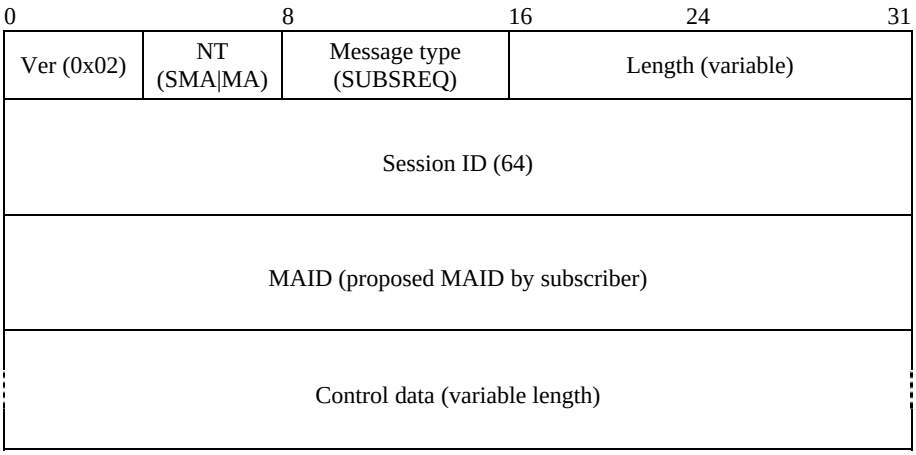

Figure 40 – SUBSREQ message

The description of each field is as follows:

a) *Ver* – It represents the version of RMCP (0x02).

b) *NT* – It is the message issuer's node type (SMA|MA).

c) *Message type* – It represents the type of the message. The value is set to SUBSREQ for the message.

d) *Length* – It shows the total length of SUBSREQ message in bytes.

e) *Session ID* – It is a 64-bit value of RMCP Session ID.

f) *Proposed MAID* – It is the unique value for identifying the entity.

g) *Control data* – It contains a set of information required to subscribe to the RMCP-2 session. It may include the following information:

- SYSINFO

This control message tells the system power of MA, such as in/out bandwidth, controllable number of CMA.

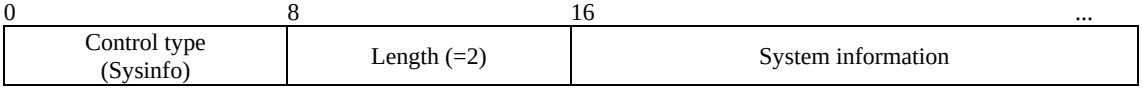

Figure 41 – SYSINFO control

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The following sub-control data shown in Figures 42 and 43 are sub-control data which may follow the SYSINFO control data shown in Figure 41.

Figure 42 shows a sub-control data followed by SYSINFO control data. The description of each field is as follows:

a) *Sub-control type* – Available_CMA (one of SYS_INFO subtypes).

b) *Length* – It represents the length of control data value.

c) *Reserved* – It is reserved for further use.

d) *Value* – It contains the appropriate system information.

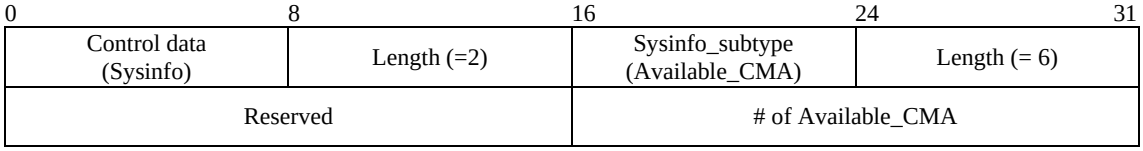

Figure 42 – AVAILABLE_CMA sub-control

Figure 43 shows a sub-control data followed by SYSINFO control data. The description of each field is as follows:

a) *Sub-control type* – Possible bandwidth (one of SYS_INFO subtypes).

b) *Length* – It represents the length of control data value.

c) *Value* – It represents the possible forwarding bandwidth which MA can afford.

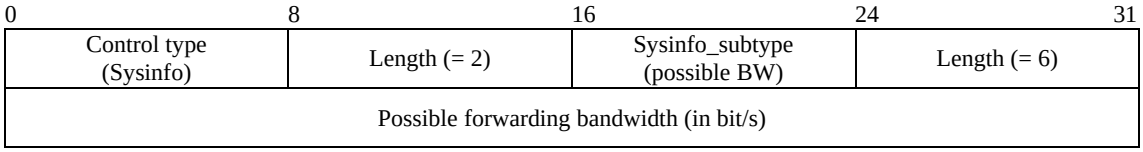

Figure 43 – POSSIBLE_BW sub-control

Note that two bytes length control frame precedes each sub-control data.

• DATAPROFILE

DATAPROFILE control delivers controllable data profile of each MA. The purpose of this DATAPROFILE control is to make SM able to keep the classified neighbour list when the SM is aware of QoS.

Whenever MA does not include this control data within SUBSREQ message, the SM is not concerned about QoS management for the MA. The description of each field is as follows:

a) *Control type* – DATA_PROFILE.

b) *Length* – It represents the length of the data profile.

c) *Possible data profile* – It represents the data profile which MA wants to use.

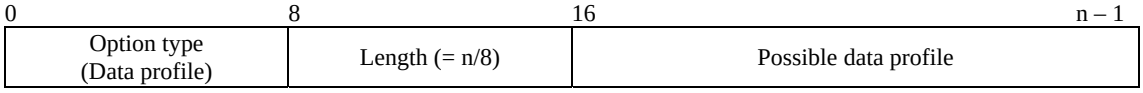

Figure 44 – DATAPROFILE control

Because DATAPROFILE control consists of text-based variable message, the size may vary. To align 4-byte length, each data profile pads zero or more 1-byte zero padding as shown in Figure 45. The description of each field is as follows:

a) *Data profile* – The data profile describes the characteristics of data channel and it follows SDL-like encoding scheme.

b) *Zero or more zero padding* – To adjust the length of data profile, zero or more zero padding follows.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale



Figure 45 – DATAPROFILE control and its padding

- AUTH

Authentication information can be delivered by using AUTH control. To support several types of authentication mechanism, extensive AUTH sub-control format is defined followed by 2-byte length AUTH control. The description of each field is as follows:

a) *Control type* – AUTH.

b) *Length* – The size of the AUTH control (should be two).

c) *Auth information* – It includes detailed AUTH information, and details are as follows:

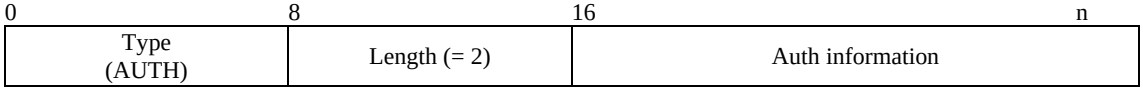

Figure 46 – AUTH control

Figure 47 shows sub-control data to deliver authentication information to be used. The description of each field is as follows:

a) *Sub-control type* – It depends on the AUTH mechanism to be used.

b) *Length* – It defines the size of the sub-control data.

c) *Value* – It represents the control data.

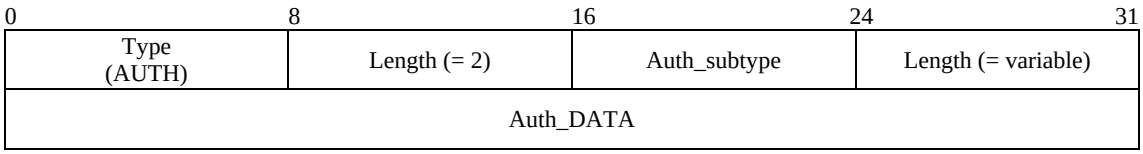

Figure 47 – AUTH sub-control

7.3.2 SUBSANS

The SUBSANS message is used by SM to give the results of subscription request and bootstrapping information for the session. The message format is shown in Figure 48.

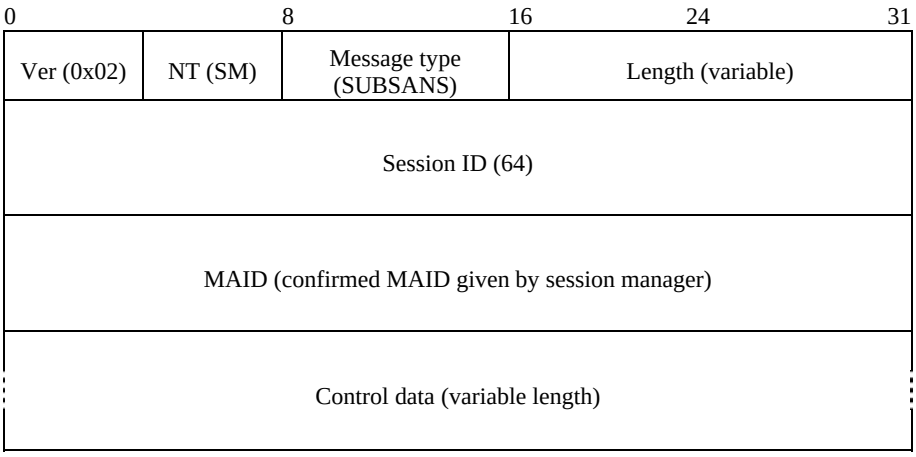

Figure 48 – SUBSANS message

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The description of each field is as follows:

a) *Ver* – It represents the version of RMCP (0x02).

b) *NT* – It is the message issuer's node type (SM).

c) *Message type* – It represents the type of the message. The value is set to SUBSANS for the message.

d) *Length* – It shows the total length of the SUBSANS message (in bytes).

e) *Session ID* – It is a 64-bit value of RMCP Session ID.

f) *Confirmed MAID* – It is the identification number of the MA. SM provides the confirmed ID as a result of the provided MAID suggested by MA in the SUBSREQ message.

g) *Control data* – It contains a set of information required to join a RMCP relayed multicast tree. It may include the following information:

- RESULT

This control message tells whether MA's subscription request is successful or not. If successful, it gives OK code within result code. If not, it gives appropriate error code such as resource exhaustion, destination unreachable. Figure 49 shows the control message format of RESULT control. The following controls are used to deliver the necessary information to join RMCP-2 tree. When subscription is disallowed, the following control cannot be included. The description of each field is as follows:

a) *Control type* – RESULT.

b) *Length* – It represents the length of the result code.

c) *Result code* – It represents the result caused by the requestor and the detailed codes are listed in Table 3.

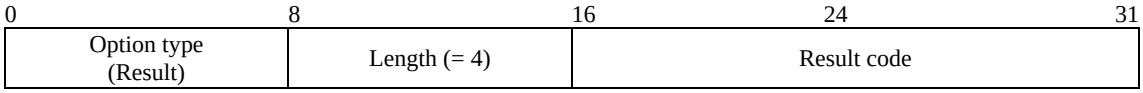

Figure 49 – RESULT control

- DATAPROFILE

DATAPROFILE control is used by SM to confirm data profile back to the subscriber. DATAPROFILE control is meaningful when SM affords extra session data information to each subscriber. The format of DATAPROFILE control is shown in Figure 44 and the content is in Figure 84.

- NEIGHBORLIST

When a subscription is successful, SM gives enough neighbour lists back to the subscriber. The meaning of NEIGHBORLIST control is that it can be used as bootstrapping information by each subscriber. Figure 50 shows the format of NEIGHBORLIST; note that it only delivers MAID. The description of each field is as follows:

a) *Control type* – NEIGHBOR_LIST.

b) *Length* – It represents the length of the control data, and the size should be two.

c) *Neighbour list information* – It includes a series of information on MAIDs, and the usage and format are as follows:

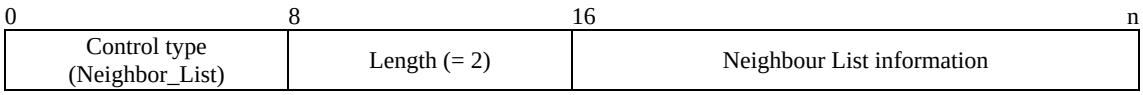

Figure 50 – NEIGHBORLIST control

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Figure 51 shows the sub-control which follows Neighbour List control. The description of each field is as follows:

a) *Sub-control type* – It defines which kind of NL will be used. In this example, the list of MAIDs is used as a NEIGHBOR_LIST.

b) *Number of NL* – It represents the number of subsequent MAIDs.

c) *MAID(s)* – It is a list of MAIDs provided by the SM. The number of MAs in the list is indicated in the "Number of NL" field.

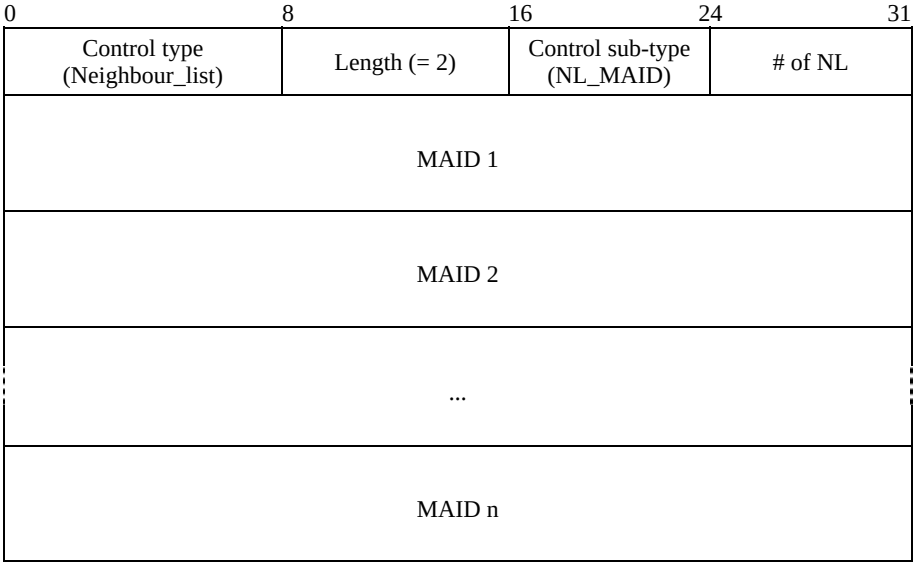

Figure 51 – NL_MAID sub-control

• AUTH

AUTH control is used to update session auth information if necessary. If updated authentication information is not necessary, it just copies the auth data sent from the subscriber. Figures 46 and 47 show the format of AUTH control.

7.3.3 PPROBREQ

It is used to perform *Map discovery* procedure to discover actual network condition and to explore network neighbouring also. It is also used to check whether its counterpart is still alive. Figure 52 illustrates the message format.

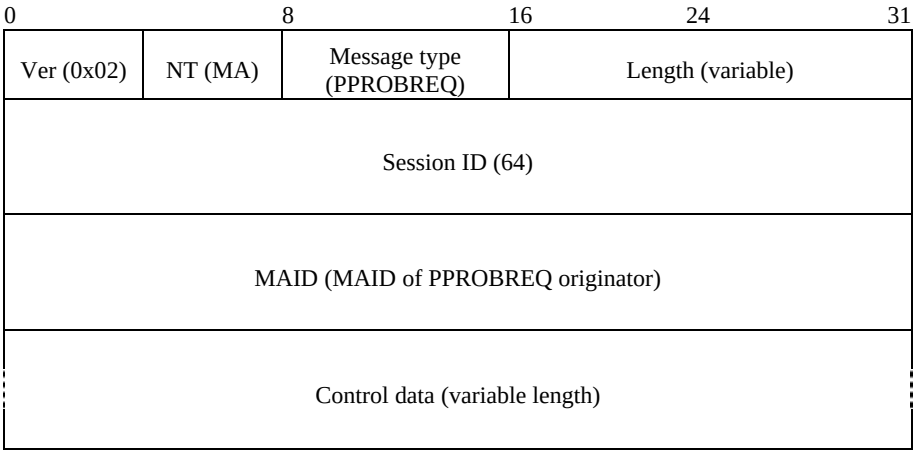

Figure 52 – PPROBREQ message

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The description of each field is as follows:

a) *Ver* – It represents the current version of RMCP (0x02).

b) *NT* – It is the message issuer's node type (MA).

c) *Message type* – It represents the type of the message. The value is set to PPROBREQ for the message.

d) *Length* – It shows the total length of the PPROBREQ message including control data (in bytes).

e) *Session ID* – It is a 64-bit value of the RMCP Session ID.

f) *MAID* – It is the MAID of the sender who sends the PPROBREQ message.

g) *Control data* – It may include the following information to inquire the map information:

- TIMESTAMP

Figure 53 shows a TIMESTAMP control which is used to examine the distance between two MAs. The description of each field is as follows:

a) *Control type* – TIMESTAMP.

b) *Length* – It represents the total length of Timestamp option, the actual size is 16 (in bytes).

c) *Reserved* – It is reserved for further use.

d) *Time 1* – It is the time when the sender of PPROBREQ sends the packet to its counterpart.

e) *Time 2* – It is the time when the PPROBREQ appears to the counterpart.

f) *Time 3* – It is the time when the receiver of PPROBREQ sends the timestamp option as a reply.

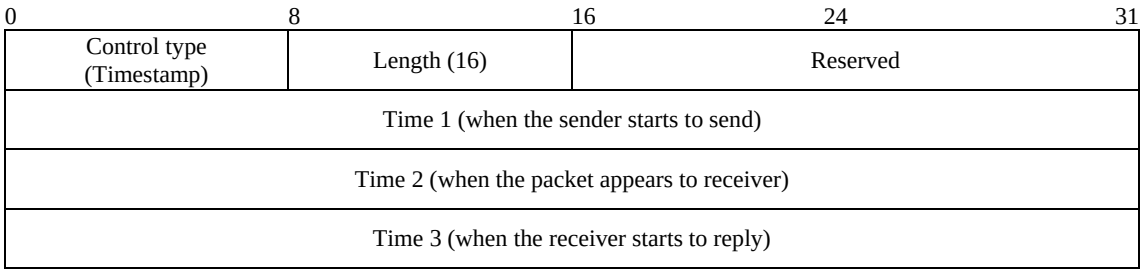

Figure 53 – TIMESTAMP control

- NEIGHBORLIST

To explore RMCP-2 participants, each MA may exchange information about their neighbour by using NEIGHBORLIST control. The control format and usage are shown in Figures 50 and 51.

- ROOTPATH

To prevent loop and solve triangular problem, probing MA may include its *from_root path* by using ROOTPATH control which is shown in Figure 54. The description of each field is as follows:

a) *Control type* – ROOTPATH.

b) *Length* – It represents the length of ROOTPATH option, the size is 2.

c) *Rootpath information* – This field includes rootpath information; the format and usage are as follows:

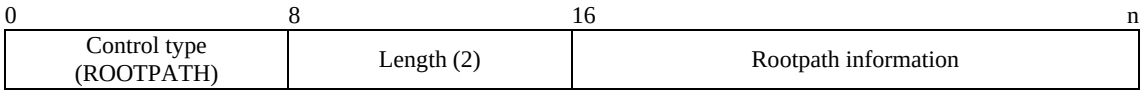

Figure 54 – ROOTPATH control

Figure 55 shows the sub-control data of ROOTPATH. The description of each field is as follows:

a) *Sub-control type* – This sub-control type field indicates which type of *from_root path* will be used. Currently seven types of path information are defined in Table 4.

b) *Number of ROOTPATH* – It represents the number of subsequent paths.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

c) *One or more ROOTPATH* – It includes the hop information by using the sub-control type. This size of each ROOTPATH is fixed and the size can be calculated by a combination of each type length. The default sizes of each ROOTPATH type are listed in Table 5.

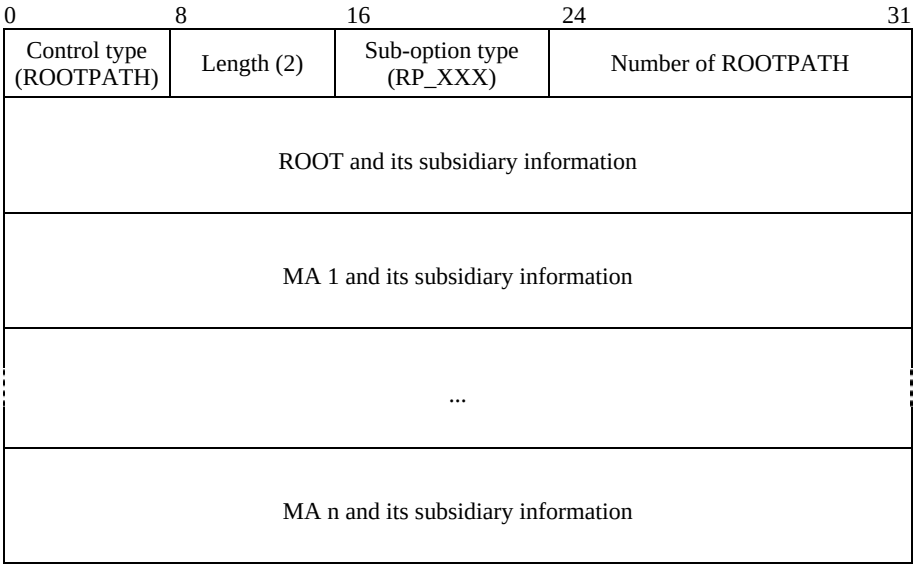

Figure 55 – RP_XXX sub-control

- SYSTEMINFO

To prevent only-leaf node or slow node may be positioned high within the tree hierarchy; it includes system information such as in-and-out bandwidth, affordable number of CMA, etc.

Figure 41 shows SYSTEMINFO control format.

- DATAPROFILE

DATAPROFILE control is used to verify whether the probed MA can afford the data delivery scheme which the probing MA wants to receive. Figure 44 shows the DATAPROFILE control format and Figure 84 shows its contents.

7.3.4 PPROBANS

It is an answer to the PPROBREQ message for performing the *map discovery* procedure and confirming if it is alive. It may contain actual network condition, and a series of its Neighbour information. Figure 56 illustrates the format of the PPROBANS message.

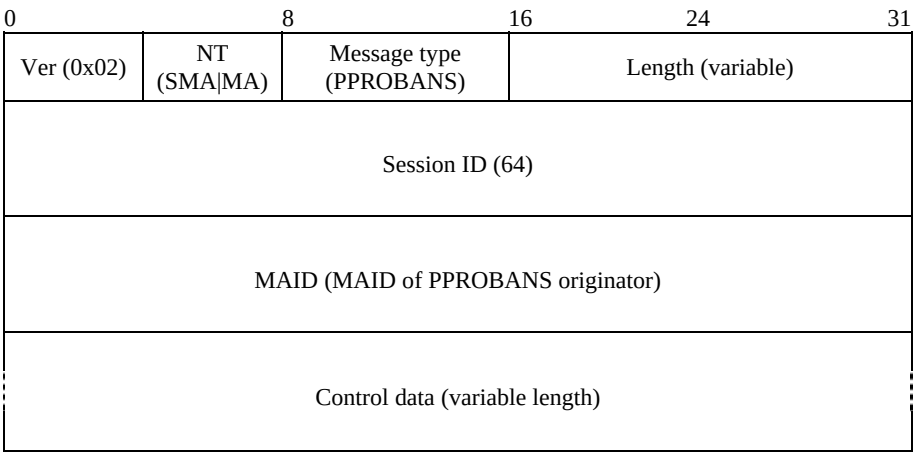

Figure 56 – PPROBANS message

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The description of each field is as follows:

a) *Ver* – It represents the current version of RMCP (0x02).

b) *NT* – It is the message issuer's node type (SMA or MA).

c) *Message type* – It represents the type of the message. The value is set to PPROBANS for the message.

d) *Length* – It shows the total length of PPROBANS message including control data (in bytes).

e) *Session ID* – It is a 64-bit value of the RMCP Session ID.

f) *MAID* – It is the MAID of the PPROBANS message sender.

g) *Control data* – It should include information appropriate to the PPROBREQ. Control data field of this message may include the following information:

- TIMESTAMP

This control is used to examine the distance between two MAs during the sequence of pprobing. Figure 53 shows the format of TIMESTAMP control data.

- NEIGHBORLIST

This NEIGHBORLIST control is designed to explore RMCP-2 participants. Each MA may gather information of its neighbour by using NEIGHBORLIST control as shown in Figures 50 and 51.

- ROOTPATH

This ROOTPATH control is used by each MA to prevent loop and solve triangular problem. The probing MA may include its information of *from_root path* by using ROOTPATH control. Figures 54 and 55 show the control format of ROOTPATH and its sub-control format.

- SYSTEMINFO

To prevent only-leaf node or slow node may be located in the high position within the tree hierarchy. PPROBANS message may include system information such as in-and-out bandwidth, affordable number of CMA, etc., by using SYSTEMINFO control. Figure 41 shows the SYSTEMINFO control format.

- DATAPROFILE

DATAPROFILE control is used to verify whether the probed MA can afford data which the probing MA wants to use during data delivery. Figure 44 shows the DATAPROFILE control format and Figure 84 shows its contents.

7.3.5 HSOLICIT

HSOLICIT is used to process self-organizing in a local network. The purpose of this is to find the HMA inside a local network. Figure 57 illustrates the message format of HSOLICIT.

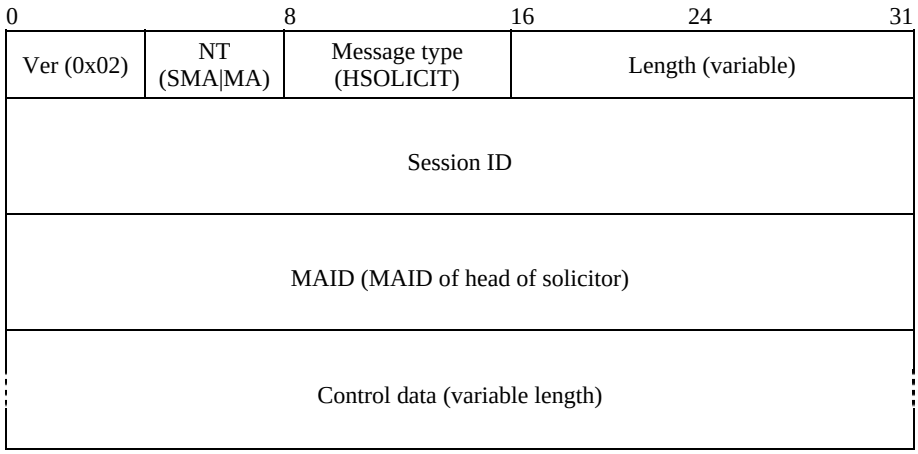

Figure 57 – HSOLICIT message

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The description of each field is as follows:

a) *Ver* – It represents the current version of RMCP (0x02).

b) *NT* – It is the message issuer's node type (SMA or MA).

c) *Message type* – It represents the type of the message. The value is set to HSOLICIT for the message.

d) *Length* – It shows the total length of HSOLICIT message including control data (in bytes).

e) *Session ID* – It is a 64-bit value of the RMCP Session ID.

f) *MAID* – It is the MAID of the node who sends this HSOLICIT to the local network.

g) *Control data* – It may include information of its neighbour list. Control data field of this message may include the following information:

- AUTH

AUTH control is used to verify the solicitor is in the same RMCP-2 session. Figures 46 and 47 show AUTH control and its sub-control.

7.3.6 HANNOUNCE

As a reply of HSOLICIT, it is used to announce the HMA's existence in a local network. Figure 58 shows the format of this message.

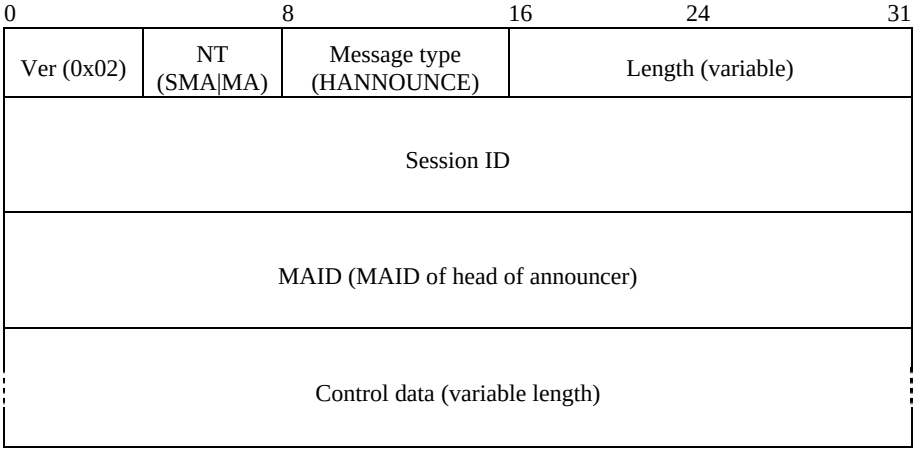

Figure 58 – HANNOUNCE message

The description of each field is as follows:

a) *Ver* – It represents the current version of RMCP (0x02).

b) *NT* – It is the message issuer's node type (SMA or MA).

c) *Message type* – It represents the type of the message. The value is set to HANNOUNCE for the message.

d) *Length* – It shows the total length of HANNOUNCE message including control data (in bytes).

e) *Session ID* – It is a 64-bit value of the RMCP Session ID.

f) *MAID* – It is the MAID of the HMA in the local network.

g) *Control data* – It may include the following information:

- AUTH

AUTH control is used to verify the HANNOUNCE sender is in the same RMCP-2 session. Figures 46 and 47 show AUTH control and its sub-control.

- SYSTEMINFO

To inform the non-HMAs in the same multicast area with the system power of HMA, HMA may include system power of MA, such as in-and-out bandwidth, controllable number of CMA. Also HMA may include additional information such as Local IP and HMA lifetime to recover from HANNOUNCE collision.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Figure 59 shows a sub-control message for Local-IP which follows SYSTEMINFO control. The description of each sub-control field is as follows:

a) *Sub-control type* – It describes the sub-control data that contains local IP address.

b) *Length* – It defines the size of the sub-control data and the value will be six.

c) *Local IP* – It represents the IP address of local host.

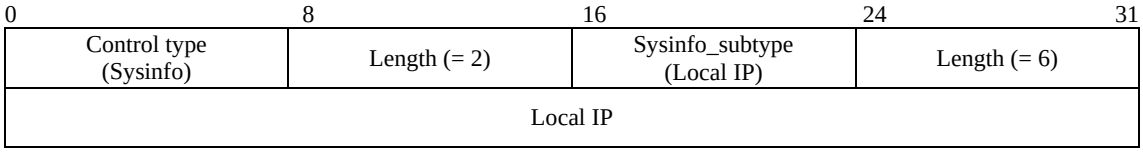

Figure 59 – Local IP sub-control

The HMA lifetime control data is shown in Figure 60.

a) *Sub-control type* – It describes the type of sub-control data.

b) *Length* – It defines the size of the sub-control data and the value will be 6.

c) *Uptime* – It represents the time after the node's joining RMCP-2 session in seconds.

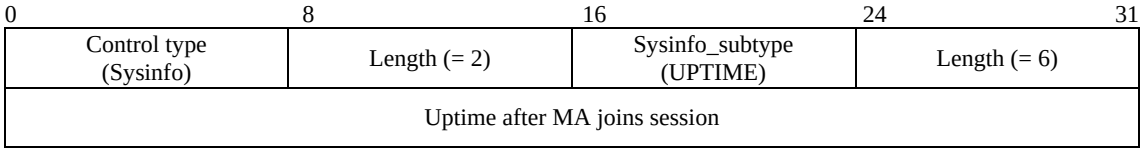

Figure 60 – UPTIME sub-control

• NEIGHBORLIST

To share explored information by HMA with non-HMA in the same multicast-enabled area, HMA may include neighbour list as shown in Figures 50 and 51.

7.3.7 HLEAVE

It is used to announce the HMA's leaving from RMCP-2 session to its local network. Figure 61 illustrates the format of this message.

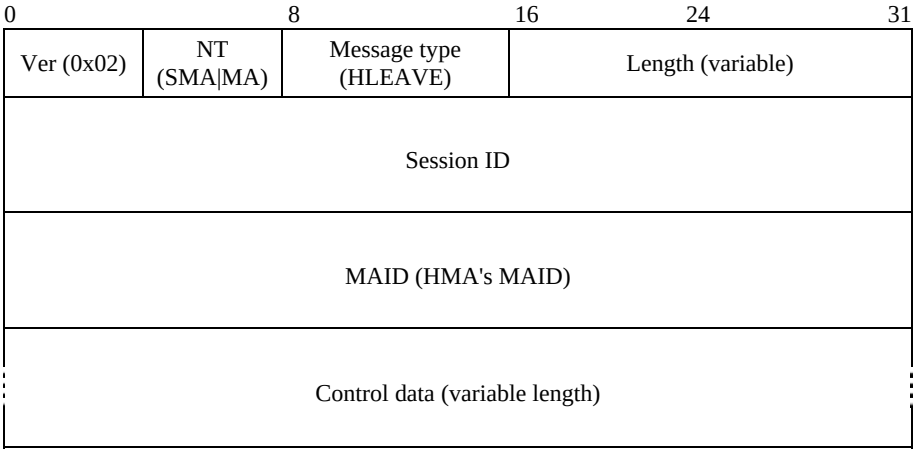

Figure 61 – HLEAVE message

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The description of each field is as follows:

a) *Ver* – It represents the current version of RMCP (0x02).

b) *NT* – It is the message issuer's node type (SMA or MA).

c) *Message type* – It represents the type of the message. The value is set to HLEAVE for the message.

d) *Length* – It shows the total length of the HLEAVE message including control data (in bytes).

e) *Session ID* – It is a 64-bit value of the RMCP Session ID.

f) *MAID* – It is the HMA's MAID in the local network.

g) *Control data* – It may include the following information:

- CANDIDATEHMA

When an HMA leaves a session, every non-HMA in the multicast-enabled area may compete to become an HMA. This may drive the multicast-enabled area be filled with HANNOUNCE message. To prevent HMA selection collision, HMA may use CANDIDATEHMA control which is shown in Figure 62. The description of each field is as follows:

a) *Control type* – It defines the type to be used.

b) *Length* – It represents the size of the control data, and it will be two.

c) *Candidate HMA information* – It is a list of candidate HMA, and the detailed format of the information is as follows:

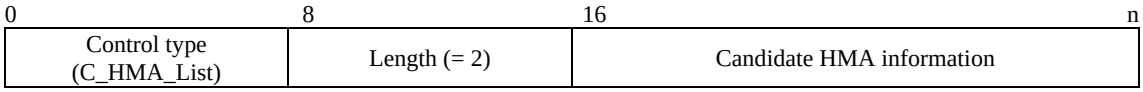

Figure 62 – CANDIDATE HMA LIST control

Figure 63 shows the sub-control for the CANDIDATE HMA LIST control. The description of each field is as follows:

a) *Sub-control type* – It defines which kind of HMA list will be used. In this example, the list of MAID is used as a candidate HMA list.

b) *Number of NL* – It represents the number of subsequent MAIDs in the list.

c) *MAID(s)* – It is a list of MAIDs of candidate HMA and which is provided by leaving HMA.

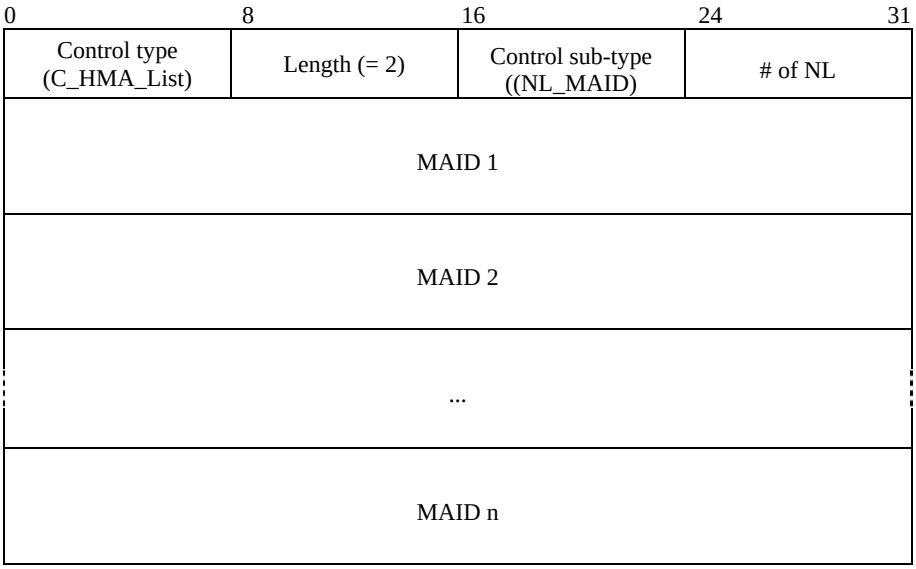

Figure 63 – CANDIDATE HMA LIST sub-control

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

- NEIGHBORLIST

To share explored information by HMA with non-HMA in the same multicast-enabled area, HMA may include NEIGHBORLIST control as shown in Figures 50 and 51.

- ROOTPATH

The leaving HMA may include its *from_root path* by using ROOTPATH control so that newly selected HMA can follow the same root path. The control data type is shown in Figures 54 and 55.

- AUTH

AUTH control is used to verify the solicitor is in the same RMCP-2 session. Figures 46 and 47 show AUTH control and its sub-control.

- REASON

The reason for HMA's leaving may vary according to the situation. For example, HMA may leave the session either of its own will or because the session has terminated. In the latter case, every non-HMA in the multicast-enabled area should leave the session promptly.

To give the reason why HMA leaves a session, HLEAVE message must include REASON control as shown in Figure 64. The description of each field is as follows:

a) *Control type* – This field represents the type of control.

b) *Length* – It represents the length of the control data and the size is 4.

c) *Reason code* – This 2-byte length field contains an integer value to indicate the specific reason for the leaving. The codes and their meaning are listed in Table 7.

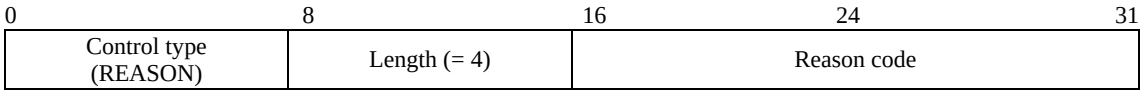

Figure 64 – REASON control

7.3.8 RELREQ

This message is used by the CMA to request to the PMA of data forwarding. It usually includes a data profile which can be negotiated through the message exchanges of RELREQ and RELANS. Figure 65 depicts the format of this message.

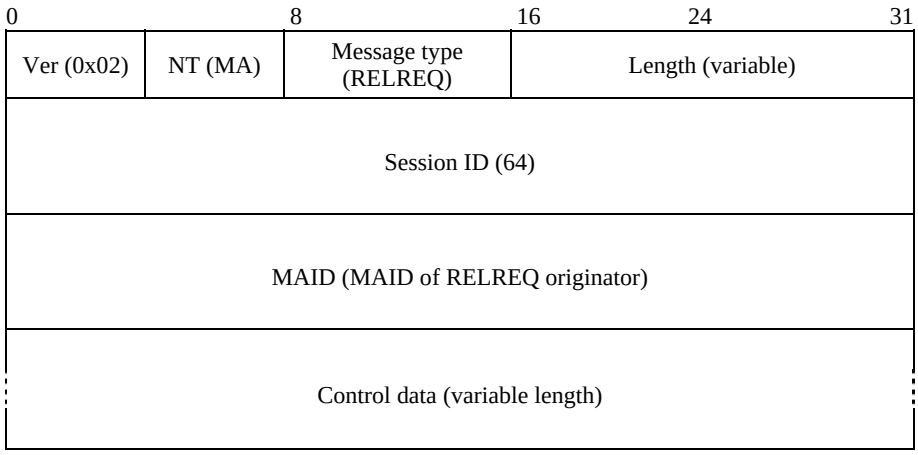

Figure 65 – RELREQ message

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The description of each field is as follows:

a) *Ver* – It represents the current version of RMCP (0x02).

b) *NT* – It is the message issuer's node type (MA).

c) *Message type* – It represents the type of the message. The value is set to RELREQ for the message.

d) *Length* – It shows the total length of the RELREQ message including control data (in bytes).

e) *Session ID* – It is a 64-bit value of the RMCP Session ID.

f) *MAID* – It is the MAID of the node who sends the RELREQ message.

g) *Control data* – It may include one or more requests related to the relay request. The controls used with this message are:

- COMMAND

When CMA needs some information from PMA, it can ask PMA by using COMMAND control within RELREQ message.

For example, whenever a MA connects to PMA during joining or parent switching procedure, the MA needs information *from_root path* of its new PMA for network diagnosis and loop detection. In this case, the MA uses then COMMAND control for ROOTPATH of newly attached PMA.

Figure 66 shows COMMAND control format. The description of each field is as follows:

a) *Control type* – This field represents the type of control.

b) *Length* – It represents the length of the control data and the size is 4.

c) *Command code* – This 2-byte length field contains an integer value to indicate the specific reason for the leaving. The encoded value and their meaning are indicated in 8.3.

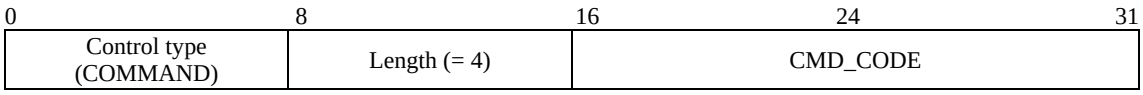

Figure 66 – COMMAND control

- DATAPROFILE

Whenever CMA connects to PMA, both MAs should agree on a data delivery scheme. To make it feasible, each CMA uses DATAPROFILE control to negotiate with its PMA. Figures 44 and 45 show DATAPROFILE control format and Figure 84 shows its contents.

- TIMESTAMP

Each CMA should measure hop-by-hop delay between PMA and itself. For this purpose, CMA includes TIMESTAMP control as shown in Figure 53 within RELREQ message.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.3.9 RELANS

As a reply of RELREQ, RELANS is issued by the PMA to the CMA. The purpose of this message is to notify whether the relay request is allowed. It may also contain additional information which is necessary to negotiate the data channel between the PMA and itself. The message format of RELANS is shown in Figure 67.

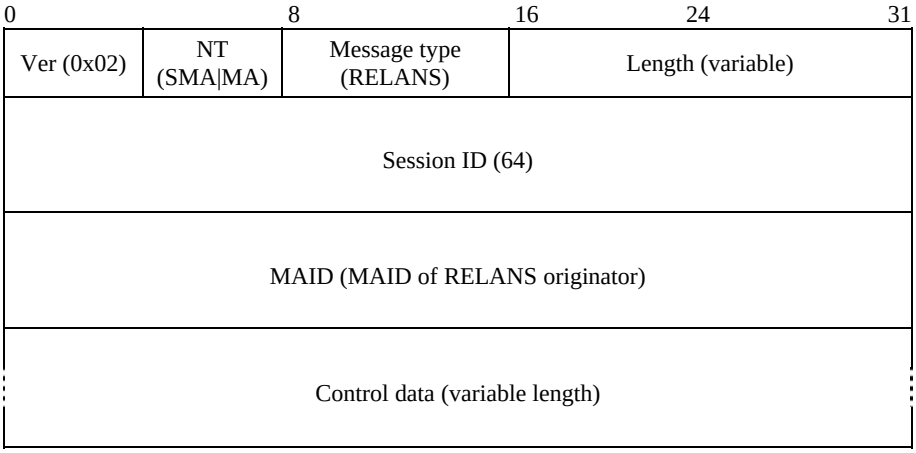

Figure 67 – RELANS message

The description of each field is as follows:

a) *Ver* – It represents the current version of RMCP (0x02).

b) *NT* – It is the message issuer's node type, because this message can be issued by the SMA and the MA, the node type for the message can be the SMA or the MA.

c) *Message type* – It represents the type of the message. The value is set to RELANS for the message.

d) *Length* – It shows the total length of the RELANS message including control data (in bytes).

e) *Session ID* – It is a 64-bit value of the RMCP Session ID.

f) *MAID* – It is the MAID of the node who sends RELANS message.

g) *Control data* – It may include one or more of the following controls:

- RESULT

To tell whether CMA's RELREQ is successful, PMA uses RESULT control inside every RELANS message. If the relay request is successful, it gives OK as a result code of RESULT control. If not, it gives an appropriate error code, such as relay denial because of policy or resource exhaustion. Figure 49 shows the RESULT control format.

- DATAPROFILE

Whenever CMA connects to PMA, it sends RELREQ message with DATAPROFILE control to negotiate data delivery scheme. Figures 44 and 45 show DATAPROFILE control format and Figure 84 shows its contents.

- TIMESTAMP

Figure 53 shows a TIMESTAMP control. TIMESTAMP control is used to examine the distance between two MAs.

- ROOTPATH

Whenever CMA asks *from_root path* with COMMAND control, PMA answer its CMA with its ROOTPATH information. Figures 54 and 55 show ROOTPATH control.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

7.3.10 STREQ

STREQ is used for monitoring the status of MAs in the session. Figure 68 shows the format of this message.

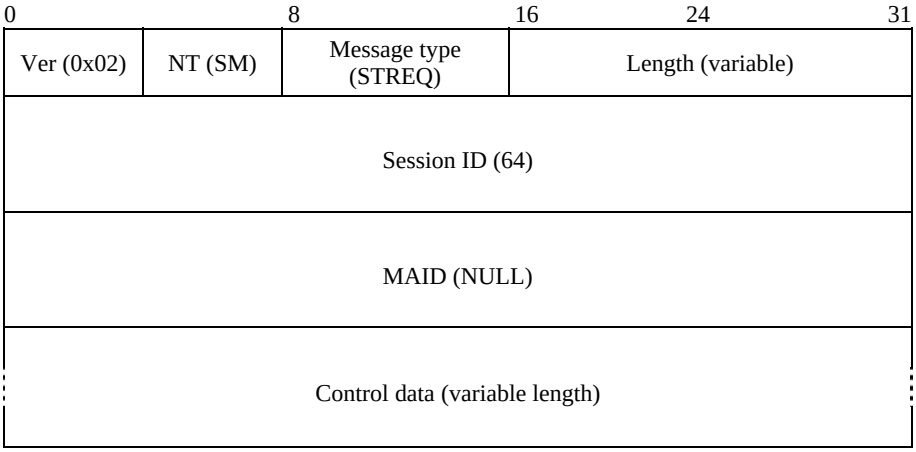

Figure 68 – STREQ message

The description of each field is as follows:

a) *Ver* – It represents the current version of RMCP (0x02).

b) *NT* – It is the message issuer's node type. Because this message can be issued only by the SM, the node type for the message is only the SM.

c) *Message type* – It represents the type of the message. It is set to STREQ for the message.

d) *Length* – It shows the total length of STREQ message including control data (in bytes).

e) *Session ID* – It is a 64-bit value of the RMCP Session ID.

f) *MAID* – Because SM does not have a MAID, this field should be set to zero.

g) *Control data* – It may include one or more requests on the status report. The controls to be considered are:

- COMMAND

STREQ message should include the COMMAND control shown in Figure 66 to express what status report it requires. To get MA's status, SM uses COMMAND control within STREQ message. Table 6 summarizes considerable commands for status monitoring and its expected reports. Figure 66 shows the format of COMMAND control.

- TREEEXPLOR

Inspecting whole tree status can cause hazards because of report implosion. So it is very important to limit the scope of tree to be inspected. Figure 69 shows TREEEXPLOR control which is used to limit the scope of tree. The fields of TREEEXPLOR control are as follows:

a) *Control type* – This field represents the control type which is TreeExplor.

b) *Length* – It represents the length of the TreeExplor option; the size should be 4.

c) *Reserved* – This field is reserved for further use.

d) *TREE_DEPTH* – It is an 8-bit integer value to specify the scope.

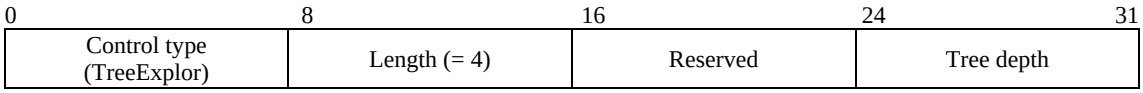

Figure 69 – TREEEXPLOR control

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.3.11 STANS

This message is used for monitoring the status of MAs in the session. Figure 70 shows the format of STANS message.

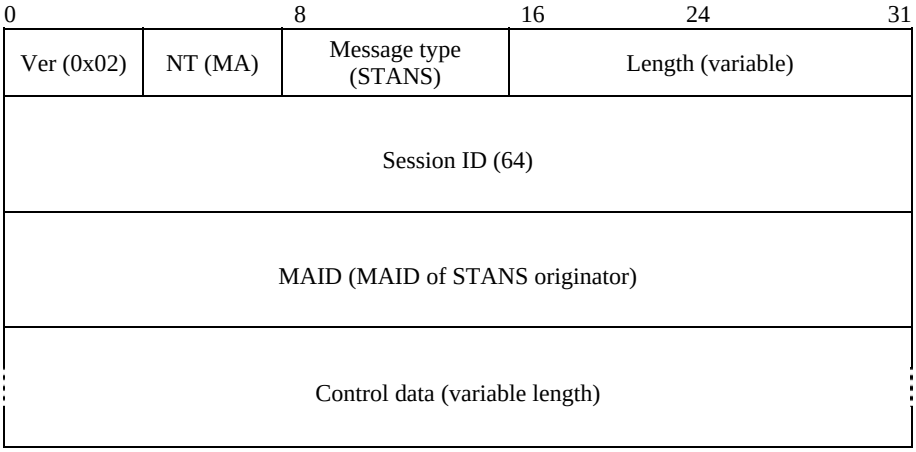

Figure 70 – STANS message

The description of each field is as follows:

a) *Ver* – It represents the current version of RMCP (0x02)

b) *NT* – It is the message issuer's node type, because this message can be issued only by the MA, the node type for the message is set to the MA.

c) *Message type* – It represents the type of the message. It is set to STANS for the message.

d) *Length* – It shows the total length of STANS message including control data (in bytes).

e) *Session ID* – It is a 64-bit value of the RMCP Session ID.

f) *MAID* – It is the MAID of the STANS issuer.

g) *Control data* – It should include one or more answers for the status report request. Control data field of STANS message may include the following information:

- REPORT

According to SM's request, the MA should answer with an appropriate report. The message format of each report has {control type, control subtype} form.

According to SM's request, listed in Table 6, each MA sends the appropriate report back to SM. Figures 71 to 76 show the corresponding reports.

Figure 71 shows the report on the room for CMAs. The description of each field is as follows:

a) *Sub-control type* – It defines which kind of HMA list will be used. In this example, the list of MAID is used as a candidate HMA list.

b) *Length* – It represents the number of list.

c) *Number of CMA allocated* – It tells the room for the CMAs.

d) *Number of CMA reserved* – It tells the room reserved by CMA. So the available number of CMA will be the difference between the number of CMA allocated and the number of CMA reserved.

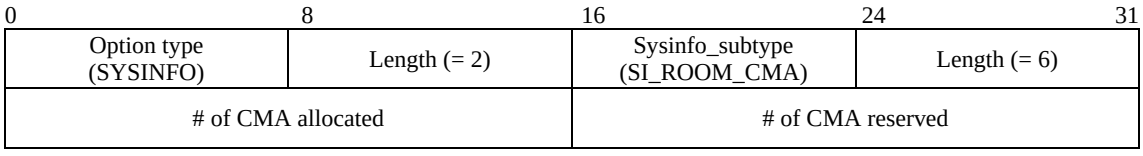

Figure 71 – SYSINFO_ROOM_CMA control

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Figure 72 shows the report on the QoS value which can be provided by a system. The description of each field is as follows:

a) *Sub-control type* – It defines the type of sub-control to be used.

b) *Length* – It represents the size of the sub-control.

c) *Incoming BW of NIC* – It represents the maximum incoming bandwidth of network interface card (in Mbit/s).

d) *Outgoing BW of NIC* – It represents the maximum outgoing bandwidth of network interface card (in Mbit/s).

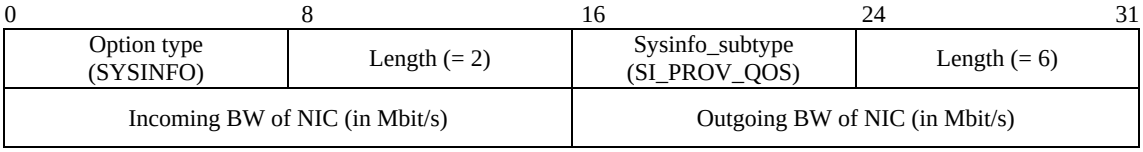

Figure 72 – SYSINFO_PROVIDABLE_QOS control

Figure 73 shows the report on the system uptime after the MA joins the session. The description of each field is as follows:

a) *Sub-control type* – It defines the type of sub-control to be used.

b) *Length* – It represents the size of the sub-control.

c) *Uptime after MA joins session* – It indicates the time elapsed since the MA has joined the session in seconds.

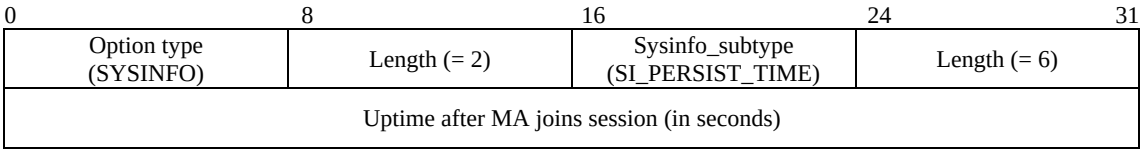

Figure 73 – SYSINFO_PERSIST_TIME control

Figure 74 shows the report on the QoS perceived by each MA. The description of each field is as follows:

a) *Sub-control type* – It defines the type of sub-control to be used.

b) *Length* – It represents the size of the sub-control and the size should be 22.

c) *Number of PMA* – It is the number of PMA attached directly.

d) *Number of CMA* – It is the number of CMAs attached directly.

e) *Total incoming bytes* – It is the total bytes of incoming data.

f) *Number of incoming packet* – It is the total number of incoming packets.

g) *Total outgoing bytes* – It is the total bytes of outgoing data.

h) *Number of outgoing packet* – It is the total number of outgoing packets.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

0	8	16	24	31
Option type (SYSINFO)	Length (= 2)	Sysinfo_subtype (ST_PERCV_QOS)	Length (= 22)	
# of PMA		# of CMA		
Total incoming bytes (bytes)				
Number of incoming packet				
Total outgoing bytes (bytes)				
Number of outgoing packet				

Figure 74 – STATE_PERCEIVED_QOS control

Figure 75 shows the report on the status of TREE. The description of each field is as follows:

a) *Sub-control type* – It defines the type of sub-control to be used.

b) *Number of MAIDs* – It is a list of MAIDs of candidate HMA and which is provided by the leaving HMA.

c) *MAID of PMA* – It is a MAID of PMA attached directly.

d) *MAID of CMA* – It is a MAID list of CMAs attached directly.

0	8	16	24	31
Option type (TREE)	Length (= 2)	Sysinfo_subtype (TREE_CONN)	# of MAIDs (= n + 1)	
MAID of PMA				
MAID of CMA 1				
MAID of CMA n				

Figure 75 – TREE_CONNECTION control

Figure 76 shows the report on the members of the TREE. The description of each field is as follows:

a) *Sub-control type* – It defines the type of sub-control to be used.

b) *Number of MAIDs* – It is a list of MAIDs listed in the control.

c) *MAIDs* – It is a MAID list for a specific branch; for example, the top node of the specific branch will be presented in the field MAID 1, the bottom node will be presented in the field MAID n.

0	8	16	24	31
Option type (TREE)	Length (= 2)	Sysinfo_subtype (TREE_MEMBER)	# of MAIDs (= n)	
MAID 1				
MAID 2				
MAID n				

Figure 76 – TREE_MEMBERSHIP control

NOTE – Every report is preceded by a 2-byte long appropriate control.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

7.3.12 STCOLREQ

STCOLREQ is used for monitoring a RMCP-2 session similarly to STREQ. But the difference is that firstly the scope of STREQ is restricted to only one MA but that of STCOLREQ can be expanded to a part or all the session. Secondly, STREQ can be issued by SM only but STCOLREQ is issued by PMA.

When a MA receives STCOLREQ from the PMA, it starts the *status collection procedure* and forwards this message to its CMAs of limited area which is confined by the TreeExplor option. Figure 77 shows the format of the STCOLREQ message.

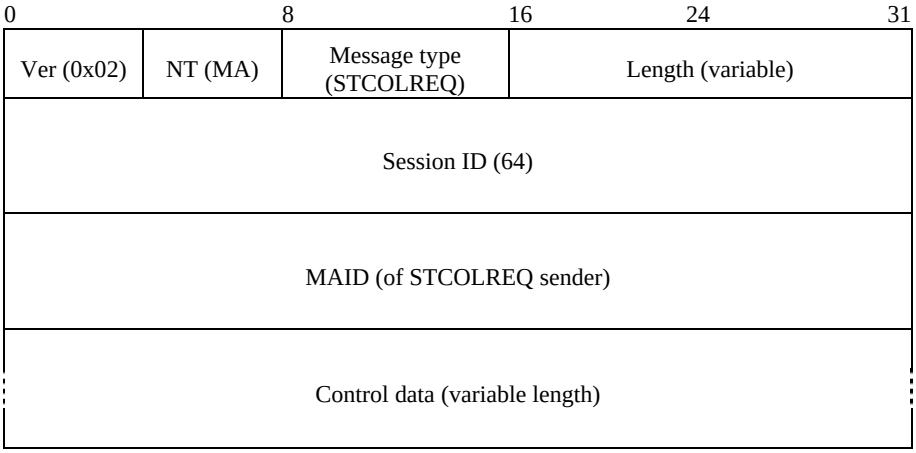

Figure 77 – STCOLREQ message

The description of each field is as follows:

a) *Ver* – It represents the current version of RMCP (0x02).

b) *NT* – It is the message issuer's node type. Because this message can be issued by the PMA, the node type for the message is set to the MA.

c) *Message type* – It represents the type of the message. It is set to STCOLREQ for the message.

d) *Length* – It shows the total length of STCOLREQ message including control data (in bytes).

e) *Session ID* – It is a 64-bit value of the RMCP Session ID.

f) *MAID* – It is the MAID of the STCOLREQ issuer; it appears normally to the CMA as the MAID of the PMA.

g) *Control data* – It may include one or more requests on the status report. Control data field of this message may include the following information:

- COMMAND

When PMA asks its CMAs of its status, it includes COMMAND control in its STCOLREQ message. Table 6 summarizes considerable commands for status monitoring.

- TREEEXPLOR

Inspecting whole tree status can cause hazards because of report implosion. So it is very important to limit the scope of tree to be inspected.

Figure 69 shows TREEEXPLOR control which is used to limit the scope of tree.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.3.13 STCOLANS

Figure 78 illustrates the format of the STCOLANS message which is used to respond to the STCOLREQ message. It informs the collected status of its downstream to its upstream. STCOLANS follows the tree hierarchy back to reach the final destination which sends STCOLREQ.

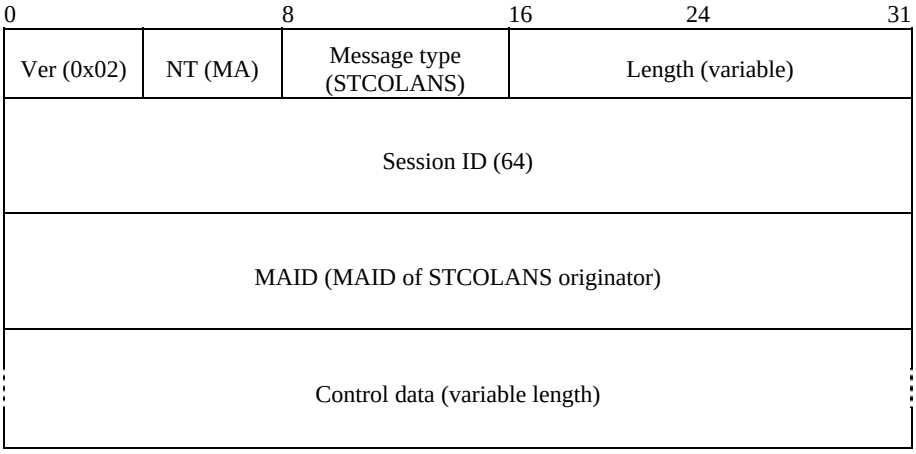

Figure 78 – STCOLANS message

The description of each field is as follows:

a) *Ver* – It represents the current version of RMCP (0x02).

b) *NT* – It is the message issuer's node type. Because this message can be issued by the CMA, the node type for the message is set to the MA.

c) *Message type* – It represents the type of the message. It is set to STCOLANS for the message.

d) *Length* – It shows the total length of STCOLANS message including control data (in bytes).

e) *Session ID* – It is a 64-bit value of the RMCP Session ID.

f) *MAID* – It is the MAID of the STCOLANS issuer. Normally it appears to the PMA as the MAID of the CMA.

g) *Control data* – It may include one or more requests on the status report. Control data field of this message may include the following information:

- REPORT

According to PMA's request, CMA should answer with an appropriate report. The message format of each report has {control type, control subtype} form.

According to the request listed in Table 6, each CMA sends appropriate reports to its PMA. Figures 71 to 76 show the corresponding reports.

7.3.14 LEAVREQ

This message is used for three different purposes. The first is for leaving. When an MA leaves from the RMCP-2 session or when an MA leaves from its PMA for parent switching, it sends LEAVEQ to the corresponding MAs by the leaving procedure.

A SM and PMA may use this message but their targets are different. The target of the SM is any MA in the session, but that of PMA is only its own CMA.

The last purpose is for terminating a session. When the SMA leaves the session, this message should be forwarded to the end-most MA in the tree hierarchy. Figure 79 illustrates the format of LEAVREQ message.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

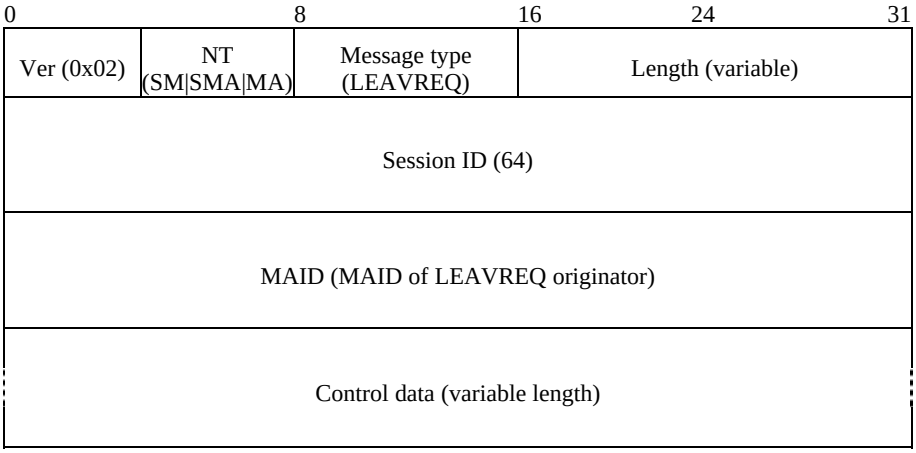

Figure 79 – LEAVREQ message

The description of each field is as follows:

a) *Ver* – It represents the current version of RMCP (0x02).

b) *NT* – It is the message issuer's node type. Because this message can be issued by all the RMCP-2 entities, the node type for the message may be set to either SM, SMA or MA.

c) *Message type* – It represents the type of the message. It is set to LEAVREQ.

d) *Length* – It shows the total length of the LEAVREQ message including control data (in bytes).

e) *Session ID* – It is a 64-bit value of the RMCP Session ID.

f) *MAID* – It is the MAID of the LEAVREQ originator. When this message is generated by SM, this field must be set to zero.

g) *Control data* – Control data field of this message may include the following information:

- REASON

To give the reason why MA tries to leave a session, LEAVREQ message must include REASON control. Figure 64 shows REASON control format.

7.3.15 LEAVANS

As a confirmation of the LEAVREQ message, the MA, which receives LEAVREQ, sends a LEAVANS back. Figure 80 illustrates the format of LEAVANS message.

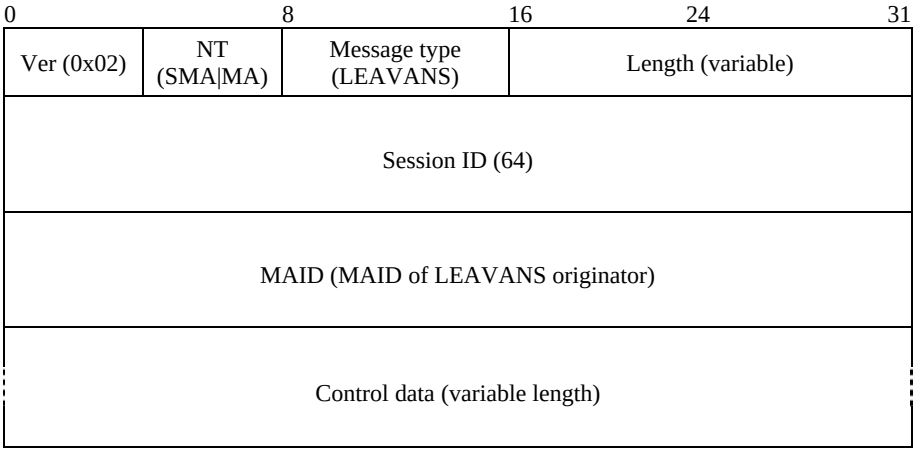

Figure 80 – LEAVANS message

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The description of each field is as follows:

a) *Ver* – It represents the current version of RMCP (0x02).

b) *NT* – It is the message issuer's node type. The node type for the message may be set to either SMA or MA.

c) *Message type* – It represents the type of the message. It is set to LEAVANS.

d) *Length* – It shows the total length of LEAVANS message including control data (in bytes).

e) *Session ID* – It is a 64-bit value of the RMCP Session ID.

f) *MAID* – It is the MAID of the LEAVANS originator.

g) *Control data* – Control data field of this message may include the following information:

- RESULT

LEAVANS message is used to indicate whether leaving MA's LEAVREQ message has successfully arrived. So the result code in RESULT control should always have the meaning of OK.

7.3.16 HB

The HB message is issued periodically by the SMA to give clock information through the RMCP-2 session. With the HB, each MA can diagnose network condition. Figure 81 illustrates the format of HB message.

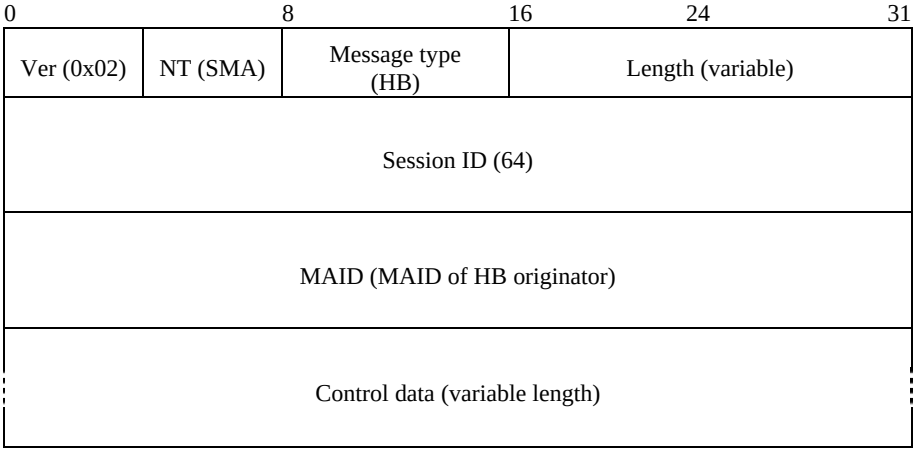

Figure 81 – HB message

The description of each field is as follows:

a) *Ver* – It represents the current version of RMCP (0x02).

b) *NT* – It is the message issuer's node type. The node type for the message may be set to SMA.

c) *Message type* – It represents the type of the message. It is set to HB.

d) *Length* – It shows the total length of the HB message including control data (in bytes).

e) *Session ID* – It is a 64-bit value of the RMCP Session ID.

f) *MAID* – It is the MAID of the HB originator. Although HB is forwarded by the PMA to the CMA, this field is not changed by the intermediate node.

g) *Control data* – It should include the ROOTPATH option which is shown in Figure 54. Control data field of this message may include the following information:

- ROOTPATH

ROOTPATH control is updated by each MA. Beginning from the root, each MA who relays HB appends its MAID as well as subsidiary information such as hop-by-hop delay, hop-by-hop bandwidth, according to its preceding session configuration. Figures 54 and 55 show ROOTPATH control and its sub-control data.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

- AUTH

To refresh authentication information during session, new authentication information can be delivered by using AUTH control. Figures 46 and 47 show AUTH control and its sub-control.

- COMMAND

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

So it is necessary to generate a pseudo-HB message to delay its descendants' fault recovery procedure and means of notifying its pseudo-HB message to its descendants.

RP_PSEUDO command in Table 4 is used to indicate that the ROOTPATH in HB message with this COMMAND is a pseudo ROOTPATH.

7.3.17 TERMREQ

TERMREQ is used to terminate an existing RMCP-2 session. It is issued by the SM and then it is forwarded by the SMA to the end-most MAs along the tree hierarchy. Figure 82 shows the format of TERMREQ message.

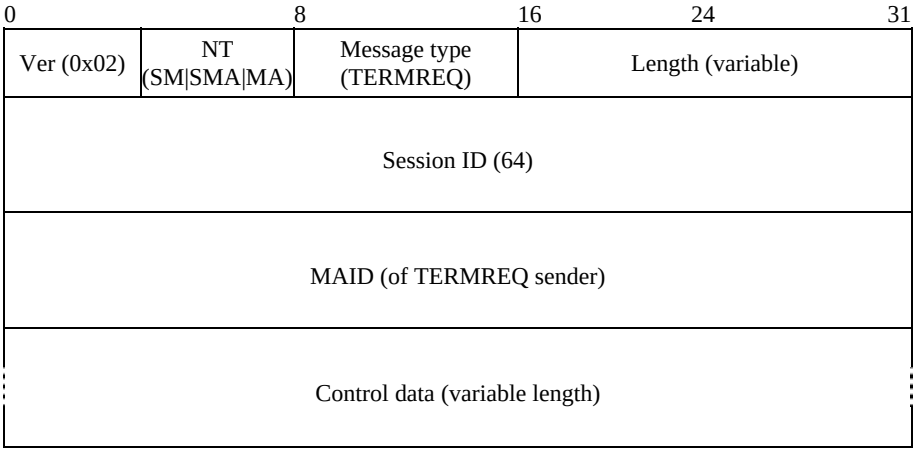

Figure 82 – TERMREQ message

The description of each field is as follows:

a) *Ver* – It represents the current version of RMCP (0x02).

b) *NT* – It is the message issuer's node type. Because this message can be issued by the SM and must be forwarded to the end-most MA along the RMCP-2 tree, the node type for the message may be set to either SM, SMA or MA.

c) *Message type* – It represents the type of the message. It is set to TERMREQ.

d) *Length* – It shows the total length of the TERMREQ message including control data (in bytes).

e) *Session ID* – It is a 64-bit value of the RMCP Session ID.

f) *MAID* – It is the MAID of the TERMREQ message sender. When this message is sent by the SM, this field must be set to zero. Normally the MAID of TERMREQ message appears to a MA as its PMA.

g) *Control data* – It may include the following reason code to explain session termination.

- REASON

To give the reason why a session is to be terminated, TERMREQ message should include REASON control as shown in Figure 64. The reason for session termination will be either SMA's inexistence or the termination by session owner.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.3.18 TERMANS

Figure 83 illustrates the format of the TERMANS message.

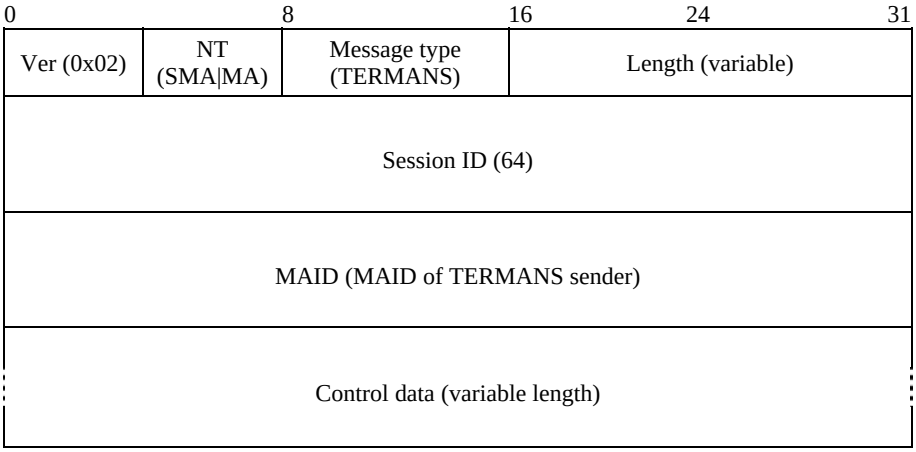

Figure 83 – TERMANS message

The description of each field is as follows:

a) *Ver* – It represents the current version of RMCP (0x02).

b) *NT* – It is the message issuer's node type because this message can be issued along the reverse direction of the RMCP-2 tree as a reply to the TERMREQ. The node type for the message may be set to either SMA or MA.

c) *Message type* – It represents the type of the message. It is set to TERMANS.

d) *Length* – It shows the total length of the TERMANS message including control data (in bytes).

e) *Session ID* – It is a 64-bit value of the RMCP Session ID.

f) *MAID* – It is the MAID of the TERMANS message sender. Normally the MAID of TERMANS message appears to the receiver as one of its CMAs.

g) *Control data* – Control data field of this message may include the following information:

- RESULT

TERMANS message is used to indicate whether TERMREQ message has successfully arrived. So the result code in Figure 49 should always be OK.

8 Parameters

This clause explains the parameter values of RMCP-2 tree management. RMCP-2 defines the data forwarding profile as a means of specifying the data channel information in terms of data types. In addition, some of the control parameters are used for efficient and optimized management of the control tree.

8.1 Data forwarding profile

RMCP-2 defines the data forwarding profile as a profile that describes the requirements for forwarding data between a PMA and the PMA's direct CMA. The data forwarding profile is used to negotiate the data channel in terms of the type of data delivered during the session. When multiple types of data are simultaneously transmitted in a session, the information of each data stream is described for the negotiation.

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

In Figure 84, a data forwarding profile is illustrated as SDP-style text format.

Stream1: Protocol = UDP, Listen address = a.b.c.d:9898, Encapsulation = IP-IP

Stream2: Protocol = UDP, Listen address = a.b.c.d:9899, Encapsulation = UDP

Stream3: Protocol = TCP, Llisten address = a.b.c.d:9899, Encapsulation = TCP, CurrentSeq=xxxx, BufferedSeq = yyyy, CurrentRcvdSeq = xxxx-1

Figure 84 – An example of the data forwarding profile

8.2 Parameters used in RMCP-2

RMCP-2 defines some parameters to manage the control tree. These parameters control the time information of the RMCP-2 session or define the number of messages or provide other information.

8.2.1 Parameters for session initialization

Each MA that wants to join an RMCP-2 session should contact the SM to fetch the bootstrapping information for the session. The SM gives an NL as the bootstrapping information. Because of resource limitations, the NL cannot keep all the MAs of the session. Hence, the following parameter is used to limit the size of the NL:

a) *N_StartNL*: It defines the number of MAs listed in the Neighbour List. It can be changed by the SM before the session starts as well as after the session started. The default value for *N_StartNL* is 100.

8.2.2 Parameters for map discovery

Every MA in the RMCP-2 performs a map discovery procedure by periodically exchanging PPROBREQ messages and PPROBANS messages with neighbouring MAs. The following parameters are related to the map discovery procedure:

a) *PPROB.time*: It defines the period of issuing PPROBREQ message. Each MA sends PPROBREQ messages at every *PPROB.time*. The default value for *PPROB.time* is 45 seconds but it can be changed arbitrarily.

b) *N_MAX_PROBE*: This parameter limits the maximum number of PPROBREQ messages that can be sent by each MA simultaneously to prevent PPROBREQ implosion. The default value for *N_MAX_PROBE* is 1, but it can be changed arbitrarily.

8.2.3 Parameters for session maintenance

This subclause includes the mechanism for the session heartbeat as well as the session maintenance.

RMCP-2 uses the HB for tree maintenance. The HB synchronizes the whole session along the data delivery path. Within the synchronized session, each MA can switch its parent to improve the RMCP-2 session. The HB also detects any network faults, such as loops and partitions. RMCP-2 defines the parameters for heartbeat as follows:

a) *HB.time*: It is the period of HB message. The SMA of a session sends a HB message at every HB.time. The default value for *HB.time* is 15 seconds.

b) *MAX_PARTITION_CNT*: It is used to examine the tree is partitioned. If a MA does not receive HB message for MAX_PARTITION_CNT * HB.time, then it can detect tree has partitioned. The default value for *MAX_PARTITION_CNT* is 3.

8.2.4 Parameters for HMA selection

RMCP-2 enables an IP multicast data transmission in a multicast-enabled area. The following parameters support this functionality:

a) *H_SOLICIT.time*: It defines the time period of HSOLICIT message. An MA in the multicast-enabled area sends H_SOLICIT message at every H_SOLICIT.time. The default value for *H_SOLICIT.time* is 2 seconds.

b) *N_SOLICIT*: It is the maximum trial number of HSOLICIT message generation as non-HMA. After N_SOLICIT times of HSOLICIT message issue, the MA tries to become new HMA in the multicast-enabled area. The default value for *N_SOLICIT* is 3.

c) *H_ANNOUNCE.time*: It defines the period of HANNOUNCE message. HMA sends an H_ANNOUNCE message at every H_ANNOUNCE.time. The default value for *H_ ANNOUNCE.time* is 6 seconds.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

d) *N_ANNOUNCE*: It is the maximum trial number of HANNOUNCE message generation as HMA. If no HSOLICIT message appears, HMA stops forwarding data into the multicast-enabled area. The default value for *N_ ANNOUNCE* is set to 3.

8.2.5 Parameters used during data delivery

To connect and continue the data relay, each CMA periodically sends a RELREQ message to its PMA. The following parameters are used to support data relay procedure:

a) *RELREQ.time*: It is the maximal period to generate the RELREQ message. Both PMA and CMA have the same size of RELREQ.time. The initial value of *RELREQ.time* is 6 seconds.

b) *N_ RELREQ*: It is used to examine whether the CMA is still alive or not. If a PMA does not receive RELREQ message for RELREQ.time * N_RELREQ, then the PMA considers that its CMA has left the session abruptly. The default value for *N_ RELREQ* is 3.

8.2.6 Parameters for session leave

RMCP-2 allows MA's early session leave. When an MA in the middle of a tree is due to leave a session, the MA should wait for a certain period for soft tree reconfiguration. The following parameters are used to support session leave procedure:

a) *LEAVE.time*: It is the duration managed by leaving PMA to make its CMA enable to find new PMAs and attach to them. The default value for *LEAVE.time* is 10 seconds.

8.3 Encoding rules to represent values used in RMCP-2

8.3.1 RMCP-2 message encoding rule

Table 2 lists the types of messages and the corresponding encoded values for each message.

Table 2 – RMCP-2 message types and its encoded values

Message type	Value (8 bits)
SUBSREQ	$00000010_{(2)}$
SUBSANS	$00000011_{(2)}$
PPROBREQ	$00000100_{(2)}$
PPROBANS	$00000101_{(2)}$
HSOLICIT	$00000110_{(2)}$
HANNOUNCE	$00000111_{(2)}$
HLEAVE	$00001000_{(2)}$
RELREQ	$00001001_{(2)}$
RELANS	$00001100_{(2)}$
STREQ	$00010010_{(2)}$
STANS	$00010011_{(2)}$
STCOLREQ	$00010100_{(2)}$
STCOLANS	$00010101_{(2)}$
LEAVREQ	$00010110_{(2)}$
LEAVANS	$00010111_{(2)}$
HB	$00011000_{(2)}$
TERMREQ	$00011001_{(2)}$
TERMANS	$00011010_{(2)}$

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

8.3.2 RMCP-2 return value

Table 3 lists the encoded values and meaning of the result codes, which are normally used as the return codes for an RMCP-2 request such as SUBSREQ and RELREQ.

Table 3 – Result codes

Result code	Meaning
0x01 00	OK
0x02 00	System Problem
0x03 00	Administrative Problem

8.3.3 Values related to RMCP-2 ROOTPATH

Table 4 lists the encoded command codes that specify the various types of ROOTPATH. The command code for the ROOTPATH can be formed into a new value.

Table 4 – Command code for ROOTPATH

Type	Code	Meaning
RP_ID	0x01 01	It makes ROOTPATH to have only MAID of each hop
RP_ BW	0x01 02	It makes ROOTPATH to have only bandwidth by each hop
RP_ DL	0x01 04	It makes ROOTPATH to have only delay perceived by each hop
RP_ID _BW	0x01 03	It makes ROOTPATH to have MAID and bandwidth of each hop
RP_ID _DL	0x01 05	It makes ROOTPATH to have MAID and its delay of each hop
RP_ID _BW_DL	0x01 07	It makes ROOTPATH to have MAID, bandwidth and delay of each hop
RP_PSEUDO	0x01 00	It makes ROOTPATH to have a pseudo-ROOTPATH for fault recovery

Table 5 lists the size of each ROOTPATH element.

Table 5 – The size of each ROOTPATH type

Type	Length (in bytes)
RP_ID	16
RP_ BW	4
RP_ DL	4

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8.3.4 Values related to the collection of RMCP-2 status

Table 6 lists the encoded values for the command codes of an STREQ and an STCOLREQ. Each code has a two-byte length. The list specifies the type of query to ensure that the requestee can reply properly. These command codes can be combined to make new codes.

Table 6 – Command code for status query

Type	Code	Meaning
SI_UPTIME	0x02 01	The time of the MA's uptime
SI_DELAY	0x04 01	The status of delay perceived by the MA from ROOT
SI_RCV_PACKET	0x08 01	The number of packets received by the MA from startup
SI_RCV_BYTES	0x08 02	The number of bytes received by the MA from startup
SI_RCV_BW	0x08 04	The bandwidth perceived by the MA between its PMA
SI_SND_PACKET	0x0F 01	The total number of packets sent by the MA from startup
SI_SND _BYTES	0x11 02	The total number of bytes sent by the MA from startup
SI_SND _BW	0x11 04	The total bandwidth consumed by the PMA to serve its CMAs
TI_DEPTH	0x12 01	The depth of the MA inside of RMCP-2 tree
TI_MA_LIST	0x14 01	A list of the MAs of RMCP-2 tree limited by TreeExplor option
TI_AV_DELAY	0x14 02	An average delay limited by TreeExplor option
TI_AV_BW	0x14 04	An average bandwidth scoped by TreeExplor option

The eight most significant bits of the encoded code specify the category of the command; the lowest eight bits specify the detailed items such as bandwidth, packets and bytes.

8.3.5 Values related to the leave

Table 7 lists the reason codes for leaving. The eight most significant bits of the encoded rules specify the main cause of leaving, and the eight least significant bits specify the detailed reasons for leaving, such as exhaustion of system resources or termination by the user's request.

Table 7 – Leave reason code

Category	LR Reason code	Meaning
Leave	0x01 00	MA's Own leave
	0x02 00	SMA leave
Kick out	0x03 00	SM kick out
	0x03 01	PMA kick out
Parent switching	0x04 00	MA's parent switching

8.3.6 Values related to the session termination

Table 8 lists the reason codes for the session termination. The eight most significant bits of the encoded rules specify the main reason of the session termination, and the eight least significant bits elaborate the reasons.

Table 8 – Termination reason code

Category	TR_code	Meaning
Normal session termination	0xF1 00	Session is terminated normally
Abnormal session termination	0xF2 00	Session is terminated abnormally without reason
	0xF2 01	Session is terminated abnormally by user request

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A

Tree configuration algorithm

(This annex does not form an integral part of this Recommendation | International Standard)

A.1 Bootstrapping rule

An MA that joins an RMCP-2 session for the first time should retrieve bootstrapping information from the SM to attach to the existing tree. Because none of the MAs has any information about the tree, each MA needs to gather information about the existing tree. To independently construct the RMCP-2 tree, the SM gives the bootstrapping information to the newly joined MAs. Hence, the bootstrapping information that is managed by the SM should be as reliable and optimized as possible. The bootstrapping information basically consists of a series of MA lists managed by the SM. Because the amount of bootstrapping information is limited, the information cannot list all members. Rather, the limited information should include only the most optimized to describe the session.

Among the MAs acquired from bootstrapping information, the most optimized MA will be a MA with high forwarding capability, short network delays and high possibility of successful attachment. However, the SM cannot tell the exact network distance between MAs, SM only gives information about MA's capabilities for pre-configured network speed and space for downstream. In an RMCP-2 session, MAs are listed in the following order of preference:

1) Dedicated MA;
2) MA having lower tree depth;
3) MA having higher bandwidth.

In addition, each MA should know how many downstream nodes are allowed.

1) Available Room for new CMA.

In view of all these considerations the bootstrapping information, which contains a list of candidate MA parents, should be managed by the SM as follows:

```
if it is dedicated MA
    give highest priority

else
    priority = available number of CMA * pw_cma                 +
               possible_forwarding_bandwidth * pw_bandwidth     +
               diff_hop_rate * pw_hop

pw_cma = policy based weight factor for cma      (%/cma)
pw_bandwidth = policy based weight factor for bandwidth      (%/bit/s)
pw_hop = policy based weight factor for hop      (%/level)
```

If all the dedicated MAs in a session have enough room for downstream MAs, or if the network administrator wants to keep every MA leaf of the MA, the SM only sends information on the DMAs. In addition, the SM should guarantee that all the MAs that appear in this information are alive.

To ensure that the list of MAs is up to date, the SM periodically checks the status of the MAs and uses the following rule to keep the status information up to date.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

if when MA_LIST_PROB timer expires

probe and update MA's status listed in MA_LIST

if when there is a successful subscription

probe and update the status of the successfully subscribed MA

If the size of an RMCP-2 session is quite small or an SM wants to tightly control a session, the SM gives a complete list of MAs to every new MA.

if RMCP-2 session is tightly controlled by SM

else if the number of MA_LIST is less than the maximum size of one SUBSANS msg

send all MA_list in SM's database

A.2 Neighbour discovering rule

Because the bootstrapping information from the SM is only a portion of the whole RMCP-2 session, the information is insufficient for each MA to find its best PMA. In addition, the MA cannot recognize its nearest neighbours. Thus, each MA, regardless of whether it has already attached itself to the session, should explore its neighbours by exchanging their NLs. This mechanism also enables the MA to measure the network distance and the status of each MA.

The NL used for neighbour discovery is constructed as follows:

include DMA to the MA_LIST_FOR_ND

if the session operates based on DMA

break;

else

include its root_path to the MA_LIST_FOR_ND

include its directly attached CMA list to the MA_LIST_FOR_ND

include its probed and non-probed MA list

until the size of PPROB message satisfies

the MA_LIST_FOR_ND is completed

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

The network condition for the two MAs that participate in the neighbour discovery can be calculated as follows:

```
delay = RTT/2
bandwidth = packet size received / (RTT/2)
```

A.3 HMA selection rule

When there are two or more MAs in a same multicast-enabled area, HMA contention problem may occur. In case of HMA contention, each MA tries to send HANNOUNCE message to become a new HMA so every MA in the same multicast-enabled area may have duplicate HANNOUNCE messages from different MAs. The following rule is used to detect HMA contention.

```
if duplicated HANNOUNCE of valid Auth and same SID arrives from different MAID
    decide HANNOUNCE is collided
```

The following rule solves the problem of any HMA contention:

```
if they have different session join time
        choose earlier session joiner as HMA
else
    choose lower MAID as HMA
```

A.4 CMA acceptance rule

Upon receiving a new RELREQ from an MA, a PMA should decide whether to accept the relay request. The decision rule is as follows:

```
new RELAY request has arrived

if it has enough room for new CMA
        if Matched QoS && policy &&Matched data profile && data condition
            accept the MA's relay request
else
            deny the MA's relay request
```


Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.5 Parent decision rule

Each MA, including the new MAs, should select from among the probed MAs the MA that has the minimum cost. The selected MA then becomes a PMA candidate. Whenever an MA joins an RMCP-2 session for the first time, the MA regards the PMA candidate as its PMA; otherwise, the candidate PMA is reserved for the parent switching. The rule for calculating the cost and for selecting the best PMA is expressed as follows:

if there is a MA in the same multicast-enabled area

if the MA is in the same local LAN

select the MA as its candidate PMA

else

find the MA having minimum cost

cost = diff_delay_rate * wt_delay +

diff_bandwidth_rate * w_bandwidth +

diff_hop_rate * w_hop

if there are two or more candidate PMAs having the same cost

select the node which has the minimum difference between the two MAIDs

*) sum(wt_delay, w_bandwidth, w_hop) = 1

w_delay = weight factor for delay

w_bandwidth = weight factor for bandwidth

w_hop = weight factor for tree depth

The cost of selecting the PMA can be calculated as follows: RMCP-2 uses a weighing factor to configure the most optimized data delivery tree, and the weighing factor should be given by a network administrator or the session creator. The following information of MA A and MA B is assumed to have been acquired by MA C:

	MA A	**MA B**
Delay	10 ms	11 ms
Bandwidth	100 Mbit/s	90 Mbit/s
tree depth	level 5	level 7

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

With information on these measurements, the MA C can distinguish which MA is closer to itself. The following examples show how the MA C calculates the cost on the basis of the weighing factor:

	Case 1	Case 2	Case 3
Comparison of MA A and MA B	cost = (10-11)/E(10,11)*0.5 + (100–90)/E(100,90)*0.4 + (5-7)/E(5,7) * 0.1 = **–0.039**	cost = (10-11)/E(10,11)* 0.4 + (100–90)/E(100,90)*0.4 + (5-7)/E(5,7) * 0.2 = **–0.063**	cost = (10-11)/E(10,11)*0.4 + (100–90)/E(100,90)*0.6 + (5-7)/E(5,7) * 0.0 = **0.025**
Decision	Choose MA A	Choose MA A	Choose MA B
Case 1) weighing factor (w_delay/w_bandwidth/w_hop) = (0.5/0.4/0.1) Case 2) weighing factor (w_delay/w_bandwidth/w_hop) = (0.4/0.4/0.2) Case 3) weighing factor (w_delay/w_bandwidth/w_hop) = (0.4/0.6/0.0)			

When the cost of two PMA candidates is equal, the MA uses the following rule to choose one of the two candidates:

if there are two or more candidate PMAs having the same cost

select the node which has the minimum difference between the two MAIDs

A.6 Tree improvement rule

Because each MA cannot know the exact information on the entire network topology, the MA's parent decision may not be most optimized. Therefore, each MA should gradually enhance the RMCP-2 session with respect to the parent switching mechanism. The following rule calculates when the parent switching is triggered:

If | (perceived QoS – new QoS) / perceived QoS | > Stability (policy)

trigger parent_switching

*) Stability factor is given by administrator when the session is created.

Stability = 0 ~ 100% (the larger stability factor, the less parent switching)

A.7 PMA's kicking-out rule

The PMA can expel one of its CMAs whenever the number of CMAs allowed by an MA decreases or whenever a CMA of the PMA makes trouble. The PMA uses the following rule when making an expulsion decision:

if(maximum # of CMA < current # of CMA)

select the worst CMA, send LEAVREQ to the CMA

else if(relaying QoS degraded by CMA)

send LEAVREQ to the CMA

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Annex B

Real-time data delivery scheme

(This annex does not form an integral part of this Recommendation | International Standard)

B.1 Overview

Whenever an MA needs to transfer real-time data to multiple users, it adopts an IP-IP tunnelling scheme for high throughput. This subclause describes how the IP tunnelling method is used for real-time data delivery. Figure B.1 shows the general architecture of IP tunnelling.

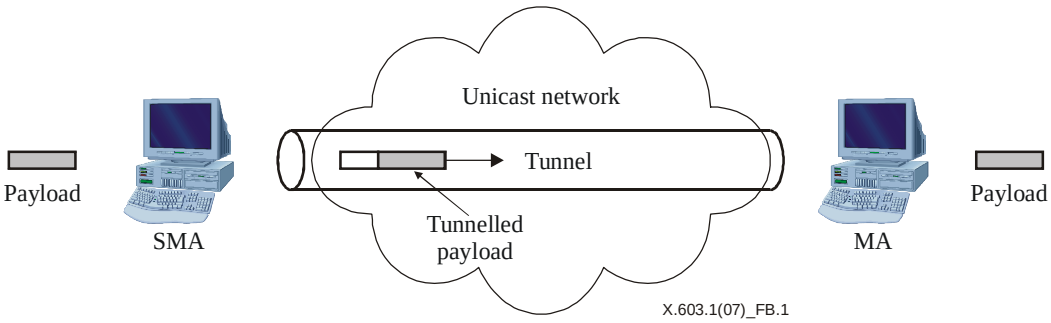

Figure B.1 – IP tunnelling scheme

B.2 IP-IP tunnel mechanism for RMCP-2 real-time data delivery

After exchanging a series of RMCP-2 control messages, a multicast data delivery path is constructed over the control path. The MA constructs the data delivery path to its subordinate MAs. The control module provides a data module with the IP address of subordinate MAs and an encapsulation scheme, and this information is contained in the data profile of the SUBSREQ message for the construction of the data delivery table. The data module of each MA stores the address of subordinate MAs in the delivery table. In this method, a real-time data delivery channel between PMA and CMA gradually constructs real-time data delivery channel from SMA to each leaf MAs. After the data delivery channel is set up, the group application operates as if it belongs to the IP multicast network, as shown in Figure B.2.

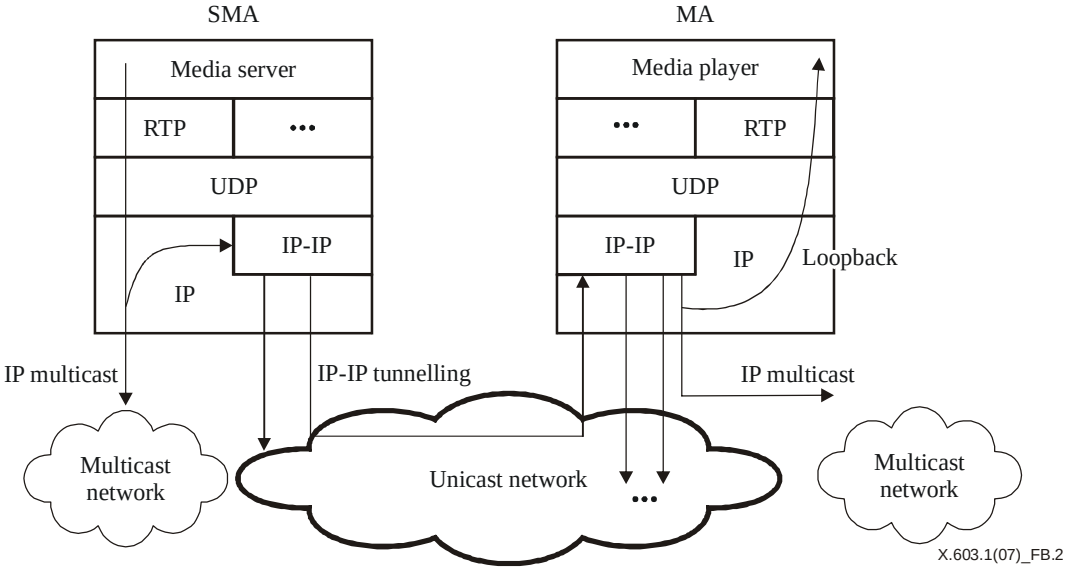

Figure B.2 – Real-time data channel with IP-IP encapsulation

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The SMA encapsulates the IP multicast data packets in the unicast data packets and transmits the encapsulated data to the downstream MAs by unicasting them over the unicast network. The SMA also multicasts the IP multicast data packets to a multicast-enabled area. Upon receiving the tunnelled data packets, each CMA de-capsulates the packets into the IP multicast data packets.

When CMAs are in the same multicast region, a PMA simply forwards the multicast data to the multicast region. If one or more CMAs are in the unicast region, a PMA should encapsulate the IP multicast data packets and then transmits the tunnelled data to its CMAs.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex C

Reliable data delivery scheme

(This annex does not form an integral part of this Recommendation | International Standard)

C.1 Overview

The scheme described here is an overlay multicast data delivery scheme that can handle reliable data. The nodes of the parent-child relationship exchange data profiles to find a set of available data. To make it feasible, each node opens the TCP connection for reliable data delivery. Once the data delivery channel is set, each node receives data from its parent and then forwards the received data to its downstream, if any. In this manner, the data from the root can reach the leaf nodes via multiple intermediate nodes.

By using data profiles, each node can search for a node with the necessary data, and, if necessary, any node that uses this scheme can change its upstream node. The following subclause describes the protocol sequence of the overlay multicast scheme for simplex reliable data delivery.

C.2 Operation

C.2.1 Channel connection

Figure C.1 shows the procedure of channel connection and follows the following four steps:

1) The CMA sends the PMA a data profile that contains the new joiner's local address and the sequence number to receive. When the new joiner has no information on the data delivery, the sequence number to receiver will be set to NEWEST.
2) After receiving the CMA's data profile, the PMA replies with data profile which contains the listening address and current sequence number.
3) Two MAs, which exchange channel information, establish TCP connections between them and then allocate a channel ID for the established connection.
4) The PMA sends encapsulated user data with the channel ID, which is allocated by the PMA itself, as well as the sequence number.

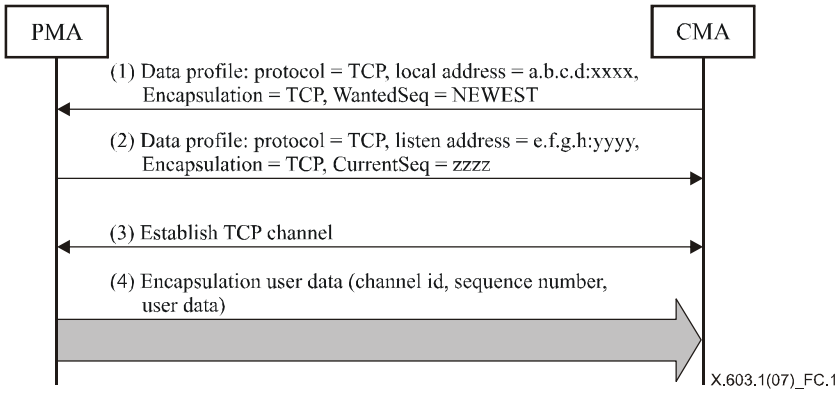

Figure C.1 – Procedure for channel connection

C.2.2 Channel disconnection

As shown in Figure C.2, the procedure for disconnecting channels has the following three steps:

1) A TCP connection is established between two MAs.
2) The PMA sends encapsulated user data with the channel ID, which is allocated by the PMA itself, along with the sequence number.
3) Either MA can eliminate the TCP channel by calling for the TCP to be closed.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

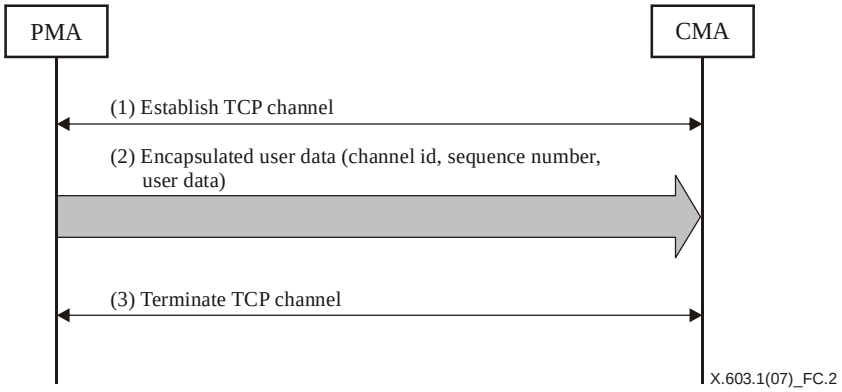

Figure C.2 – Procedure for channel disconnection

C.2.3 Channel switching

As shown in Figure C.3, the procedure for channel switching has the following seven steps:

1) A TCP connection is established between two MAs.
2) The PMA sends encapsulated data with the channel ID, which is allocated by the PMA itself, along with the sequence number and user data.
3) The CMA sends a data profile, which contains its local address and sequence number to receive, to the new PMA.
4) Upon receiving data profile from a new CMA, the new PMA replies with data profile which contains listening address, current sequence number and buffered sequence number.
5) If the wanted sequence is between the buffered sequence number and the current sequence number, the CMA disconnects the TCP channel with an old PMA.
6) The new PMA and CMA, which are connected by TCP, allocate new channel identification for the connection.
7) The new PMA sends encapsulated user data with the channel id allocated by itself and sequence number from the wanted sequence number.

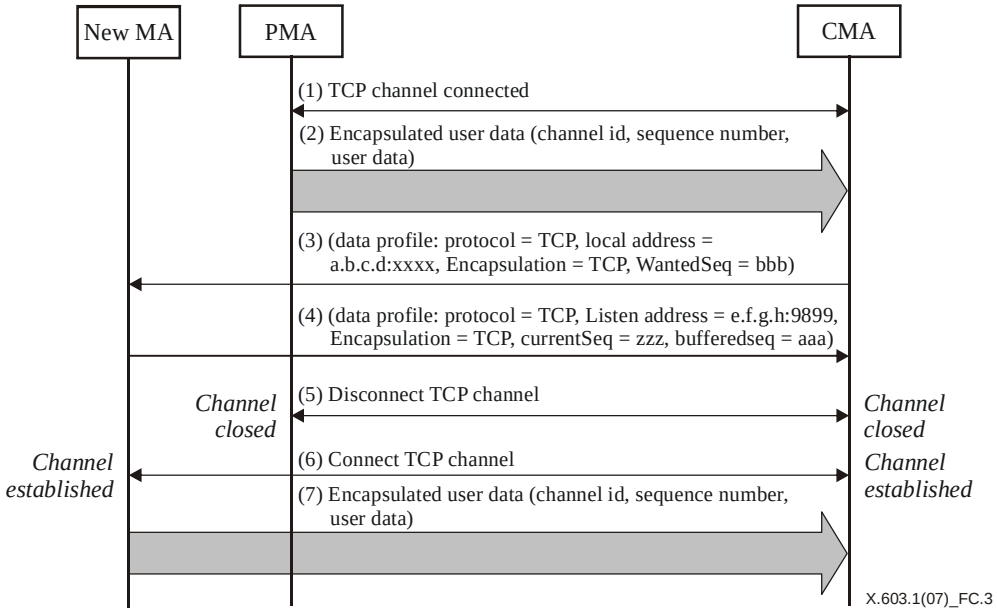

Figure C.3 – Procedure for channel switching

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

C.3 Data encapsulation format

Figure C.4 shows the user data message for reliable data delivery:

a) Reserved: Reserved for future use and set to zero now.

b) Length: Total byte length of current message.

c) Channel ID: Identification of the data channel between the data hops.

d) Sequence number: The sequence number allocated by an SMA of the current service data unit; this value can be allocated globally in a round robin manner.

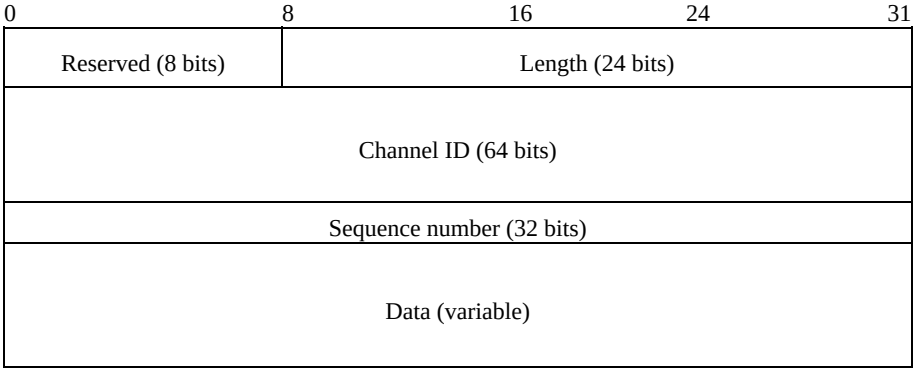

Figure C.4 – Data encapsulation format

C.4 Data profile

When the data tunnelling scheme is used in RMCP-2, the following format should be used for the data profile:

"Protocol = TCP, Listen address = a.b.c.d:9899, Encapsulation= TCP, CurrentSeq=xxxx, BufferedSeq=yyyy, WantedSeq=zzz"

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Annex D

RMCP-2 API

(This annex does not form an integral part of this Recommendation | International Standard)

This annex specifies the application programming interfaces (APIs) for RMCP-2. The APIs described in this annex can be used in applications that utilize the capabilities of RMCP-2.

The RMCP-2 APIs follow the Berkeley socket APIs. However, to differentiate the RMCP-2 APIs from existing Berkeley socket functions, the RMCP-2 APIs are prefixed with 'rmcp2_' (for example, rmcp2_socket).

D.1 Overview

D.1.1 APIs

Table D.1 summarizes the API functions in RMCP-2:

Table D.1 – Summary of RMCP-2 APIs

Category	Name	Description
MA control	*rmcp2_socket()*	Creates a new RMCP-2 socket.
	rmcp2_bind()	Associates a set of information about session, such as session id, role, local and group addresses, data profile, etc.
	rmcp2_connect()	Joins RMCP-2 session.
	rmcp2_close()	Terminates connection and releases socket.
	rmcp2_setsockopt()	Sets socket and protocol options to RMCP-2 MA control module.
	rmcp2_getsockopt()	Gets socket and protocol options from RMCP-2 MA control module.
	rmcp2_recv()	Delivers received data to application.
	rmcp2_send()	Sends application data to a RMCP-2 group.
Data delivery	*rmcp2_recv()*	Delivers received data to application.
	rmcp2_send()	Sends application data to a RMCP-2 group.
Session management	*rmcp2_session_open()*	Creates a new RMCP-2 session.
	rmcp2_session_close()	Terminates RMCP-2 session and releases resources allocated.
	rmcp2_member_out()	Kicks the trouble maker out from the session.
	rmcp2_status_report()	Examines the condition of a specific RMCP-2 session.
	rmcp2_char_change()	Sets or changes RMCP-2 session characteristics.

D.1.2 Use of RMCP-2 API

Figure D.1 illustrates the use of RMCP-2 APIs and shows API sequences in terms of the SM and two MAs.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

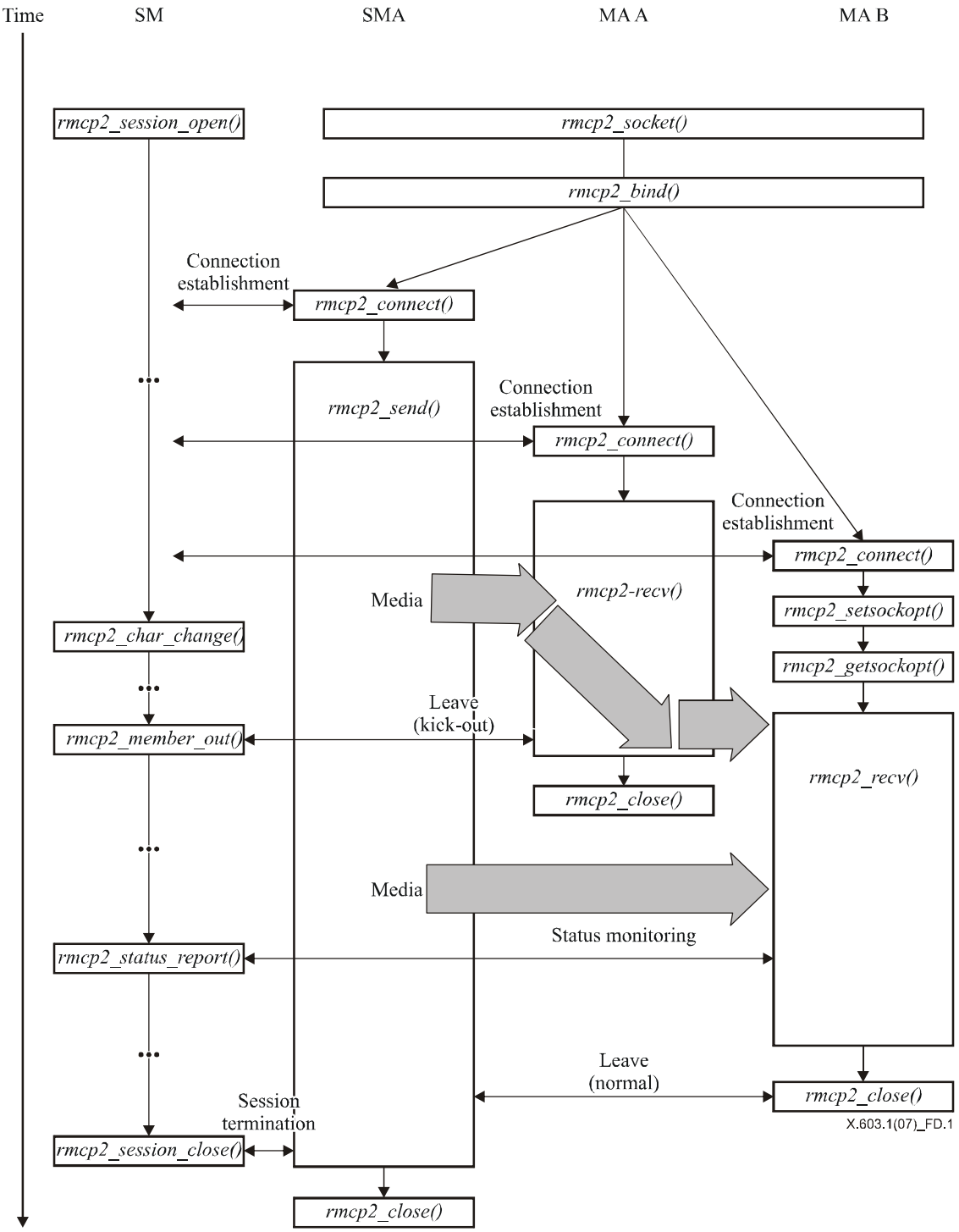

Figure D.1 – Usage of RMCP-2 APIs

D.2 RMCP-2 API functions

D.2.1 Functions related to MA control

This subclause defines a series of RMCP-2 APIs that are related to the MA. RMCP-2 applications use the functions defined here to join and leave RMCP-2 sessions. The functions to send and receive data are defined in the next subclause.

int rmcp2_socket (void)

Under the RMCP-2 protocol, an application asks an RMCP-2 MA to start an RMCP-2 session by calling the *rmcp2_socket()* function. If successful, this function returns a non-zero RMCP-2 socket identifier; otherwise, it returns a negative value with error codes.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

*int rmcp2_bind(int sd, session_profile *profile, int profile_len)*

Whenever an RMCP-2 application wants to impose some information about a session, it can call the *rmcp2_bind()* function. This function sets the MA information that is crucial for joining an RMCP-2 session. Some of the most important details of a session are as follows:

a) session ID;

b) its role inside RMCP-2 session, such as sender-side MA, leaf MA;

c) a specific MA address to be operated;

d) a group address;

e) data profile which it wants to use;

f) other vendor-specific information, etc.

After a successful bind, this function returns zero; otherwise, it returns a negative return value with the proper error code.

*int rmcp2_connect(int sd, struct sockaddr *sm_addr, int addrlen)*

Only after a bind is successful, an RMCP-2 application can start to join an RMCP-2 session. By calling the *rmcp2_connect()* function, each RMCP-2 application can invoke the MA to subscribe to and join an RMCP-2 session. The arguments associated with this function are the address of the SM and the session ID to join an RMCP-2 session. After successfully joining a session, this function returns zero; otherwise, it returns a negative value with an error code.

int rmcp2_close(int sd)

To leave a session, an RMCP-2 application calls the *rmcp2_close()* function. By calling the *rmcp2_close()* function, an application can make an RMCP-2 MA initiate a departure procedure and then free the protocol control block. After successful session leave, this function returns a zero; otherwise, it returns a negative integer with the appropriate error code.

*int rmcp2_setsockopt(int sd, int opt_type, char *opt, int optlen)*

The *rmcp2_setsockopt()* function enables an application to set or change one or more protocol parameters. If it is successful, this function returns zero; otherwise, it returns a negative integer with the appropriate error code.

*int rmcp2_getsockopt(int sd, int opt_type, char *opt, int *optlen)*

An application that wants to know one or more protocol parameters from the MA calls the *rmcp2_getsockopt()* function by offering an *opt_type* and an empty **opt* which is large enough to hold the resultant information from the MA. If it is successful, this function returns zero; otherwise, it returns a negative integer with the appropriate error code.

D.2.2 Functions related to MA's data delivery

This subclause defines a series of RMCP-2 APIs that are related to RMCP-2 data delivery. These APIs are used by applications to send or receive RMCP-2 data traffic.

*int rmcp2_recv(int sd, char *buf, int len, int flags)*

A receiving application that wants to receive data from an RMCP-2 session calls the *rmcp2_recv()* function and copies the received data of *len* from the MA data module. If it is successful, this function returns zero; otherwise, it returns a negative value with an error code.

*int rmcp2_send(int sd, char *buf, int len, int flags)*

To send data to an RMCP-2 session, an RMCP-2 application calls the *rmcp2_send()* function. However, because RMCP-2 only supports a one-to-many data delivery service, the MA of the sending application must be an SMA. This function copies the data of *len* to the MA data module. If it is successful, this function returns the number of bytes that it sends; otherwise, it returns a negative value with an error code.

D.2.3 Functions related to session management

A session manager application (SM application) can initiate, manage or terminate an RMCP-2 session by calling one of the APIs defined in this subclause. To clarify that ambiguity between *an application that uses the RMCP-2 SM* and the *RMCP-2 SM* itself, the term *SM application* is used to refer to the application that uses the RMCP-2 SM.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

*SID rmcp2_session_open(session_profile *session_profile)*

An SM application that wants the SM to start an RMCP-2 session calls the *session_open()* function with session profile. The *session_profile* argument should be packed with sufficient session information to create and manage an RMCP-2 session. Upon receiving the session profile, the SM allocates enough room for a specific RMCP-2 session. After the successful creation of a session, this function returns the created session ID; otherwise, it returns zero with an appropriate error code.

int rmcp2_session_close(SID session_id)

An SM application that wants the SM to terminate an RMCP-2 session calls the *session_close()* API. This function asks the SM to start the procedure for terminating an RMCP-2 session and then frees enough room for the RMCP-2 session. After the session has been successfully terminated, this function returns a non-negative value; otherwise, it returns a negative value with an error code.

int rmcp2_member_out(SID session_id, MAID maid)

Whenever a session member, or MA, causes critical problems or violates session policy, the SM application may expel the trouble maker from the session. If an SM application wants an SM to expel a specific member from the session, then it calls the *member_out()* API with a session ID, along with the ID of the member to be expelled.

*int rmcp2_status_report(SID session_id, int command, char *result, int *result_len)*

The *status_report()* function enables an SM application to examine the condition of a session. This function is usually called with arguments such as the session ID, the operation commands and buffer for the results. If it is successful, this function returns zero; otherwise, it returns a negative value and an error code.

*int rmcp2_char_change(SID session_id, int command, char *opt, int optlen)*

The *rmcp2_ char _change setsockopt()* function enables an SM application to set or change the characteristics of an RMCP-2 session, such as the AUTH information. If it is successful, this function returns zero; otherwise, it returns a negative integer with an appropriate error code.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

ICS 35.100.70

Price based on 62 pages

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale