INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.602

(04/2004)

SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

OSI networking and system aspects – Networking

Information technology – Group management protocol

ITU-T Recommendation X.602

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	**X.600–X.629**
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	X.1000–

For further details, please refer to the list of ITU-T Recommendations.

INTERNATIONAL STANDARD ISO/IEC 16513
ITU-T RECOMMENDATION X.602

Information technology – Group management protocol

Summary

The Group Management Protocol (GMP) is an application-layer control protocol for creating a group session and for managing the group's participating members. Generally it is assumed that there is one GMP server, one session-creating client (or Session Creator), and one or more session-participating clients (or Session Participants).

The GMP includes session management (SM), membership management (MM), and the function of exchanging information between SM and MM.

Source

ITU-T Recommendation X.602 was approved on 29 April 2004 by ITU-T Study Group 17 (2001-2004) under the ITU-T Recommendation A.8 procedure. An identical text is also published as ISO/IEC 16513.

Keywords

Group Management, Membership Management, QoS Server, Session Management.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Page

Introduction

Conventional multicast transport protocols do not include a dynamic mechanism for group management according to the join/leave of receivers and for the modification of membership information.

GMP provides a framework for multicast session management (SM) mechanism and membership management (MM), which supports the required management of multicast sessions and their members. This protocol can be key to reliable multicast communications.

GMP will operate over conventional transport protocols and/or ECTP as shown in Figure 1.

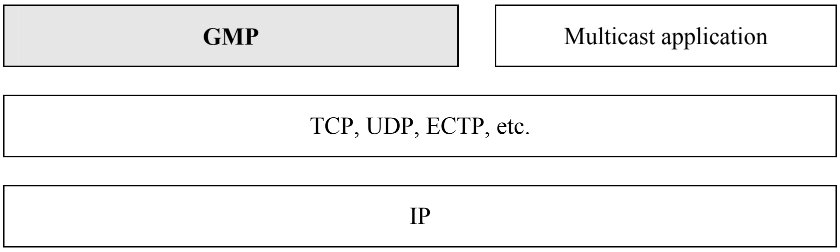

Figure 1 – GMP model (GMP protocol stack)

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Group management protocol

1 Scope

This Recommendation | International Standard provides a specification of a Group Management Protocol (GMP), which is an application-layer control protocol for creating a group session and for managing the group's participating members.

The GMP consists of session management (SM), membership management (MM), and the function of exchanging information between SM and MM. SM is responsible for session creation and deletion. MM manages the member lists based on session information retrieved from SM.

According to ITU-T Rec. X.601, "Multi-peer communications framework", the multi-peer communication service is achieved in seven distinct phases: registration, enrolment, activation, data transfer, deactivation, de-enrolment, and de-registration. Since one of these operations – data transfer – may be performed using ECTP or TCP, SM may perform the rest of operations: creation, announcement, registration, enrolment, activation, including session announcement. In addition, MM manages group members who are in enrolled or active groups.

SM may provide a convenient interface to users because it may be implemented on the Web. Operation of MM is transparent to users as in a transport protocol.

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.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

3.1 Terms defined in ITU-T Rec. X.601

This Recommendation | International Standard is based on the concepts developed in the Multi-Peer Communications Framework (ITU-T Rec. X.601) and makes use of the following terms defined in that Recommendation:

a) Multi-peer;

b) Multi-peer communication; and

c) Multicast transmission.

3.2 Terms defined in ITU-T Rec. X.605 | ISO/IEC 13252

This Recommendation | International Standard is based on the concepts developed in Enhanced Communications Transport Service Definition (ITU-T Rec. X.605 | ISO/IEC 13252) and makes use of the following terms defined in that Recommendation:

a) Enrolled Group;

b) Registered Group;

c) Active Group; and

d) TC-owner.

3.3 Terms defined in this Recommendation | International Standard

3.3.1 GMP client: An application program that sends and receives GMP. Clients store and acquire information through a server. All clients must log in to the server to acquire information from the server. Clients are largely divided between session creator and session participants.

3.3.2 GMP server: A server is an application program that is responsible for session management and membership management.

3.3.3 session creator: A client who creates and who may terminate a session. Logging on to the server through its own ID, the creator inputs information about creating a session and sends the information to the server. The server that received the request from the creator adds the information into the created session list. The Session creator may be a TC-owner defined in ECTS.

3.3.4 session client: A client who intends to be a Session Participant.

3.3.5 session participant: A Client who registers for a session intending to participate in that session. After registration, the session participant will join the session to be an active member (i.e., start session list and registered member list). A Session Participant may be a TC-participant defined in ECTS.

4 Abbreviations

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

4.1 Message types

4.1.1 SM message types

SAREQ	Session Activation Request message
SCACC	Session Creation Accept message
SCCON	Session Creation Confirm message
SCINF	Session Creation Information message
SCREJ	Session Creation Reject message
SCREQ	Session Creation Request message
SDREQ	Session Deletion Request message
SDRES	Session Deletion Response message
SJREQ	Session Join Request message
SJRES	Session Join Response message
SRACC	Session Registration Accept message
SRREJ	Session Registration Reject message
SRREQ	Session Registration Request message
SRRES	Session Registration Response message

4.1.2 MM message types

KAREQ	Keepalive Request message
KARES	Keepalive Response message
UIREQ	User Information Request message

UIRES	User Information Response message
LVREQ	Leave Request message
TRREQ	Termination Request message
TRIND	Termination Indication message
KDUPT	Key Distribution Update message

4.2 Miscellaneous

ECTP	Enhanced Communications Transport Protocol
ECTS	Enhanced Communications Transport Service
MM	Membership Management
RMT	Reliable Multicast Transport
SAP	Session Announcement Protocol
SDP	Session Description Protocol
SM	Session Management
IP	Internet Protocol
LQA	Lowest Quality Allowed
MSS	Maximum Segment Size
OT	Operating Target
QoS	Quality of Service
RSVP	Resource reSerVation Protocol

5 Conventions

In this Recommendation | International Standard, the keywords "MUST", "REQUIRED", "SHALL", "MUST NOT", "SHALL NOT", "SHOULD", "SHOULD NOT", "MAY", and "OPTIONAL" are to be interpreted as described in IETF RFC 2119, and indicate requirement levels for compliant ECTP implementations. Those keywords are case-sensitive.

6 Overview

GMP is an application-layer control protocol for creating a group session and for managing the group's participating members.

Generally it is assumed that there is one GMP server, one session creating client (or Session Creator), and one or more session participating clients (or Session Participants) as shown in Figure 2.

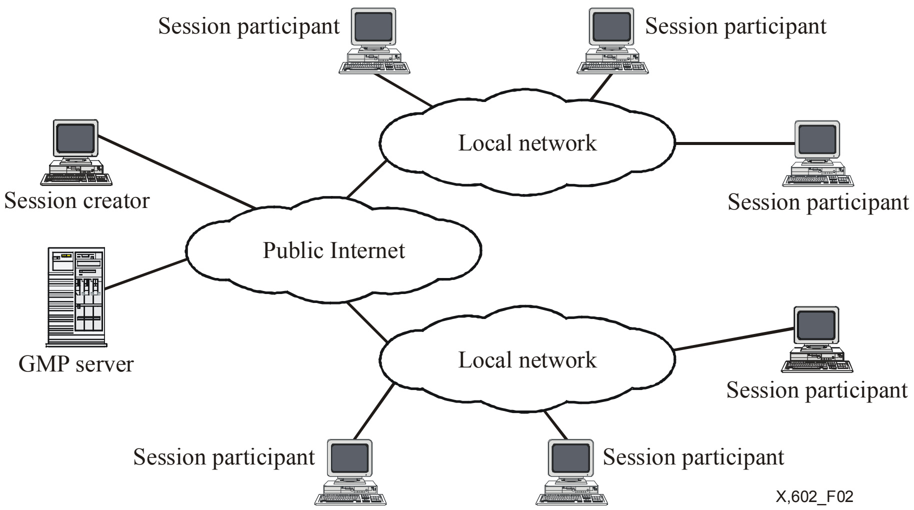

Figure 2 – Network configuration for GMP

GMP is composed of session management (SM), membership management (MM), and the function of exchanging information between SM and MM.

6.1 Session Management

SM may be achieved in eight distinct phases: creation, announcement, registration, enrolment, activation, de-registration, de-enrolment, and de-activation.

A particular client, called a session creator, creates a session. Then, SM updates the session list.

The session creator will send a Session Creation Request message to the server. If accepted, the session creator will receive the Session Creation Accept message from the server. Then the session creator will send the detailed session information to the server and receive the confirmation message. If the session cannot be created or the session creator does not have the necessary rights, then the Session Creation Reject message will be returned.

After successful session creation, the server will announce the new session to the clients. The announcement may be done by e-mail, web posting, and so on. From this point on, those clients may register in multicast groups.

A client may register for a session. Any client may register for the open-mode session, while some pre-authorized clients may register for the closed-mode session. After successful registration, the client belongs to the registered group.

When the session starts, the session's registered members will start a group application to send and receive session data. At this time, all preparations for the data transfer and group management are accomplished. The session's registered group member belongs to the enrolled group.

When the session creator sends real data or when the session's enrolled members receive real data, then those participants are said to be in active state. Membership management is then activated.

6.2 Membership Management

When a session is activated, the server immediately sends a status report request to each session's active member. The server will update the active members' list and other information based on information received from the participants. These updates will be accomplished periodically.

A session participant may leave the session by sending a leave message to the server.

To terminate an ongoing session, the session creator sends a session termination message to the server, which then will notify the session termination to every participant, and terminate the session.

Figure 3 shows an example of GMP operations and their relation between session status and multicast group phases defined in ITU-T Rec. X.601.

After a session is created and announced, three session clients, A, B, and C try to register for the session. However, one client C is rejected because this client is not authorized to do so, or has improper rights. When the session creator and clients send the session join request to the server, they enter the enrolled state. At this time, they are ready to communicate with each other. And they enter the active state by sending a specific active request message to the server. By that message, the MM will classify members, who are either in the active state, or in the enrolled state. The server will update the active member list based on the periodic update request and reply. Session Participant A leaves the session, sending the leave message to the server. From that moment, the server will update the active list by sending the update request only to two active participants. When the session creator wants to terminate the session, the session termination request will be sent to the server, which will then send the session termination notice to the session participants.

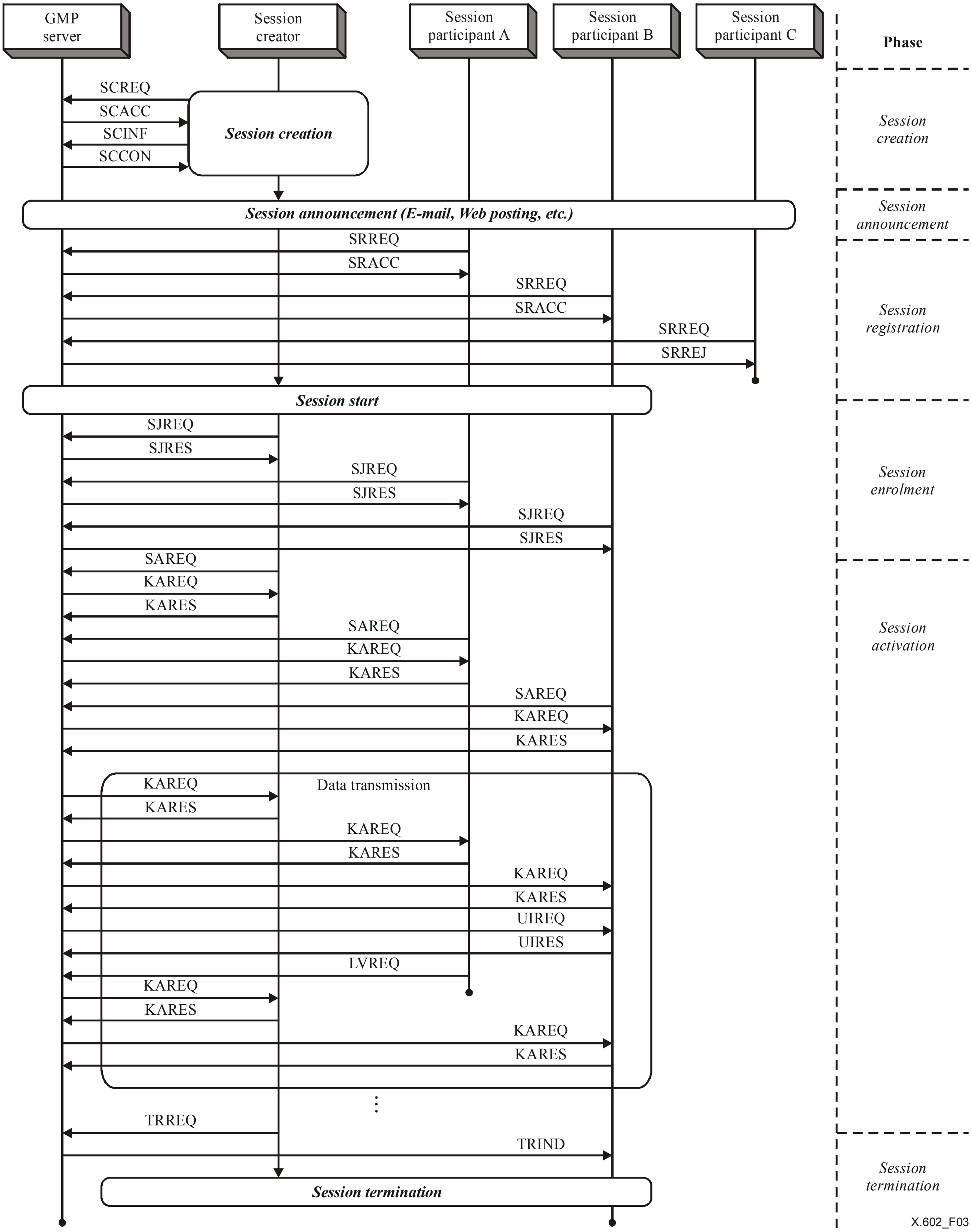

Figure 3 – An example of the GMP control

7 Protocol operations

7.1 Session Management

SM may be achieved in eight distinct phases: creation, announcement, registration, enrolment, activation, de-registration, de-enrolment, and de-activation.

SM is responsible for the following:

a) Session Creation: A session creator creates the session.

b) Session Announcement: An SM server typically announces information about the session to session clients.

c) Session Registration: Clients register for a session to the SM server.

d) Session Enrolment: After registration, an enrolment operation accomplishes the whole "set-up" that is necessary for multicast group communication.

e) Session Activation: After activation, a session participant in the session receives the data from the session creator. The session participants belong to the active group.

The mode of the session will be one of the following:

a) Closed mode;

b) Open mode.

In the closed mode, the session participation may be restricted by a session creator, who may distribute the access control message to the target participants. A participant will register for the session only after the authorization process. In the open mode, any client may register for the session.

7.1.1 Session Creation

Session creation is effected by a session creator, who will define and characterize the session with media type, application type, additional information, and so on.

A session creator may define core members, who should be registered or enrolled. If a requirement for a core member is not satisfied, the session may not start.

Figure 4 shows the successful session creation procedure. A Session Creator defines and characterizes a session and sends a Session Creation Request message, SCREQ, to the session server. SCREQ is a mere request asking whether a new creation is possible or not. Considering the multicast environment and its application, the server may allow a new session creation by replying with a Session Creation Accept message, SCACC. Then, the Session Creator will send detailed session information in Session Creation Information message, SCINF, which may include media type, application type, etc. The server will acknowledge successful session creation with a Session Creation Confirm message, SCCON, and then update its session list.

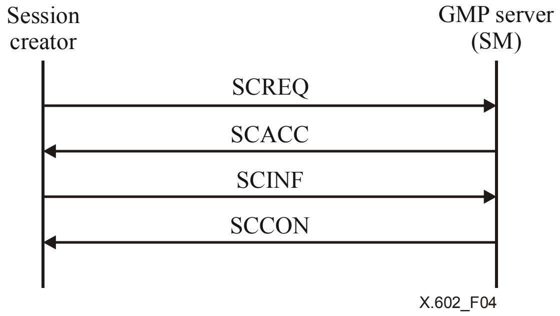

Figure 4 – Successful session creation procedure

Figure 5 shows an unsuccessful session creation procedure. When a Session Creator requests a new session creation from the server, if the server does not have enough sources, or if the requestor does not have the proper authorization, the request will be rejected by the server, and the server sends a Session Creation Reject message, SCREJ.

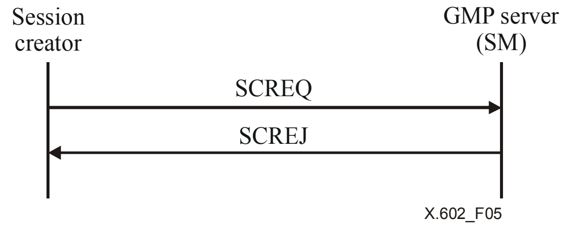

Figure 5 – Unsuccessful session creation procedure

7.1.2 Session Announcement

Session creation will be announced through e-mail, web posting or other off-line ways. Through this announcement, session clients will know the existence and the characteristics of all created sessions. Session participants may know whether the session is in the open mode or in the closed mode. In the closed mode, the access control message should be distributed to the selected clients by the session creator, with which the clients can access to the session information and register for the closed mode session later.

7.1.3 Session Registration

Session registration is to select a session and to let the server and creator know the intention of the participation.

In the open mode session, the session client will select a session and send the Session Registration Request message, SRREQ, to the server. The server will add the requesting client to the Registered Group Membership list, and reply to the requestor with Session Request Accept message, SRACC, as shown in Figure 6.

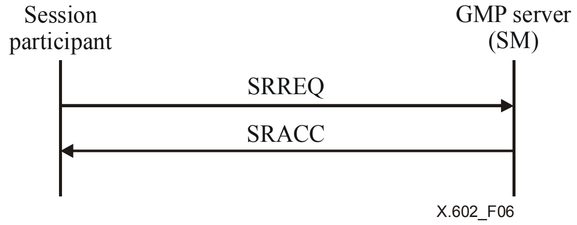

Figure 6 – Successful session registration procedure (Open mode)

In the closed mode session, the session client will select a session and send the Session Registration Request message, SRREQ to the server. Then the server will immediately reply with a Session Registration Response message, SRRES to indicate that the valid authorization process is initiated. If the registration is valid, then the server will send Session Registration Accept message, SRACC as shown in Figure 7.

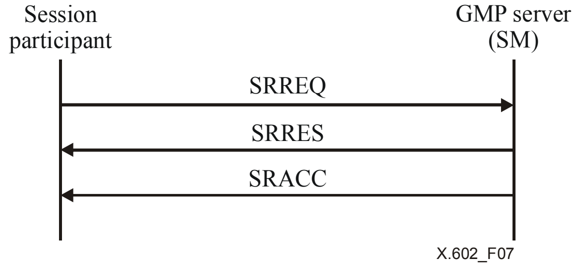

Figure 7 – Successful session registration procedure (Closed mode)

If the session registration request is not authorized in the closed mode session, the server will send the Session Registration Reject message, SRREJ, as shown in Figure 8.

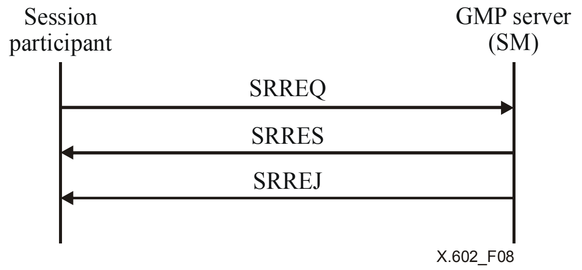

Figure 8 – Unsuccessful session registration procedure (Closed mode)

7.1.4 Session Enrolment

Session enrolment is the state where communication is possible among the session participants and the session creator. Session participants, including the session creator, should send the Session Join Request message, SJREQ. The server will add the participants to the Enrolled Group Membership list, and reply to the requestor with the Session Join Response message, SJRES, as shown in Figure 9.

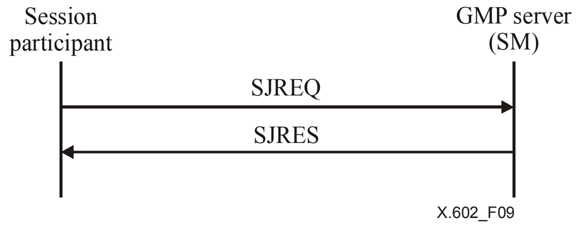

Figure 9 – Successful session enrolment

MM manages a Registered Group Membership list separate from an Enrolled Group Membership list.

7.1.5 Session Activation

Session activation is the state where the session participants and the session creator are in the data transfer phase. Session participants, including the session creator, should send the Session Activation Request message, SAREQ. The server will reply with the Keepalive Request message, KAREQ. If the server receives the Keepalive Response message, KARES, from the session participants, then it updates the Active Group Membership list, as shown in Figure 10.

The server will maintain the Active Group Membership list based on the periodic KAREQ and KARES exchanges.

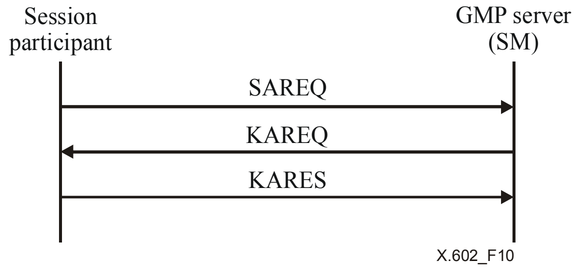

Figure 10 – Successful session activation

In the late join case, a session participant who is in the enrolled state will send the SAREQ to join the ongoing session.

If a session participant sends the KARES after receiving KAREQ, then the server will add that participant to the Active Group Membership list.

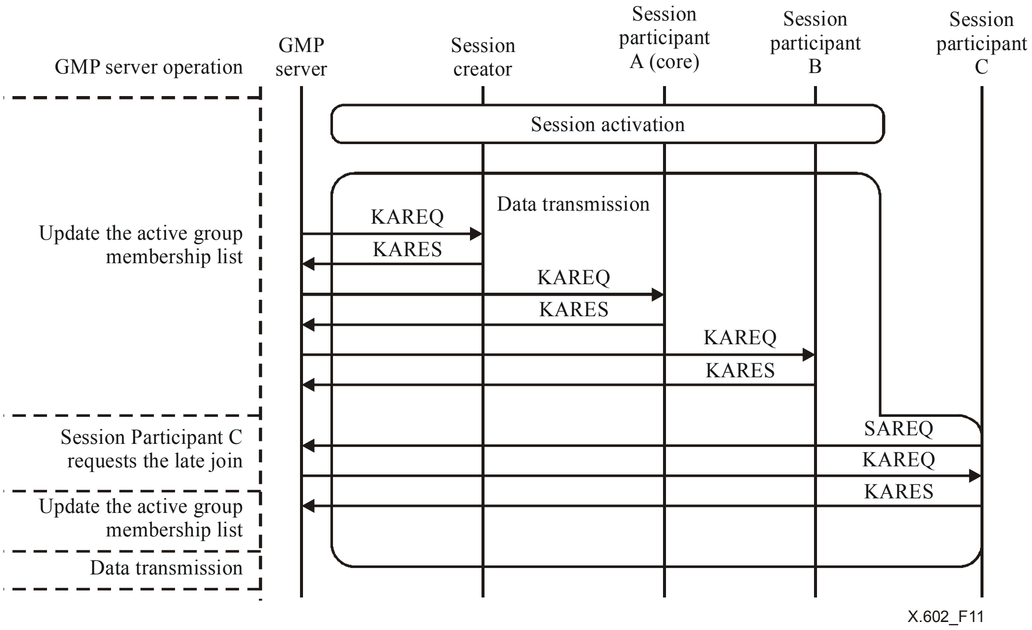

Figure 11 – Late join procedure

7.2 Membership Management

MM maintains and manages active group members.

Figure 12 shows the membership management updating the lists at the GMP server. Upon receiving KARES from the Session Participants, GMP membership management server will check whether the client belongs to the registered group list. If yes, GMP server will check whether the client belongs to the enrolled group. If the client does not belong to the enrolled group, the client will be added to the enrolled group. And if the client belongs to the enrolled group, then the GMP server will check whether the client belongs to the active group. If the client does not belong to the active group, the client will be added to the active group and reset the KeepAlive (KA) timer. If the client belongs to the active group, GMP server will reset the KA timer and waits for the next KARES.

If the GMP server does not receive KARES from a Session Participant and the KA timer to the Session Participant expires, the GMP membership management server will check which group the Session Participant belongs to. If the Session Participant belongs to the active group, that participant will be moved to the enrolled group. If the participant belongs to the enrolled group, that participant will be moved to the registered group. Then, the GMP server resets the KA timer.

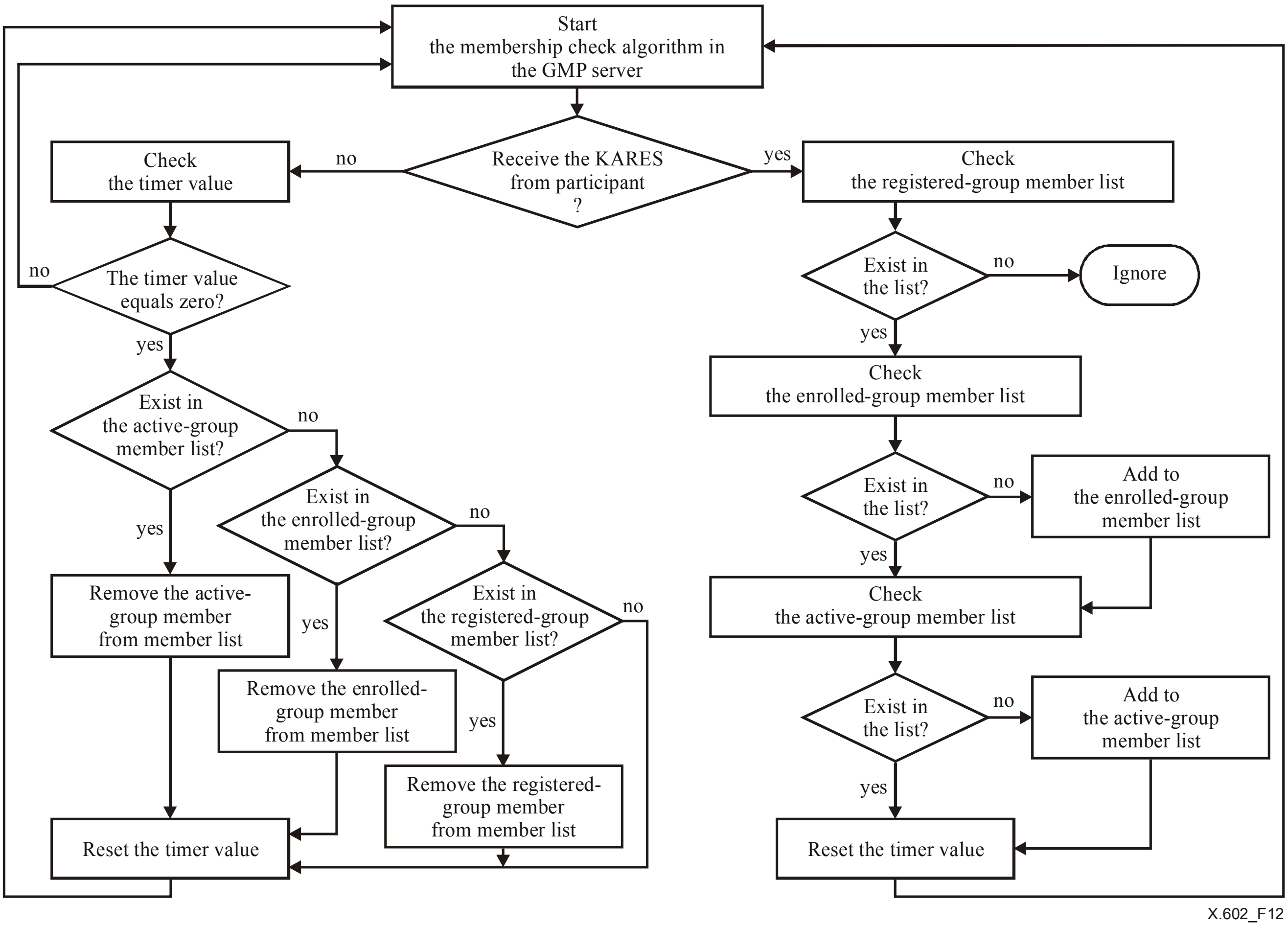

Figure 12 – Membership check algorithm in the server

Figure 13 shows the membership management message-receiving process at the GMP server.

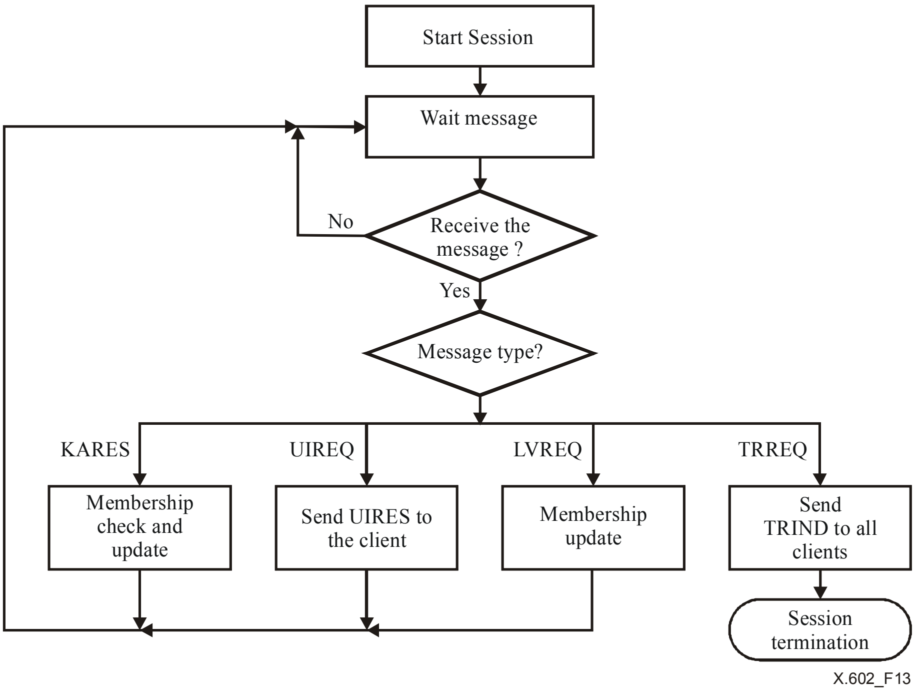

Figure 13 – GMP server (MM) operation algorithm

Figure 14 shows the membership management message sending process at the client.

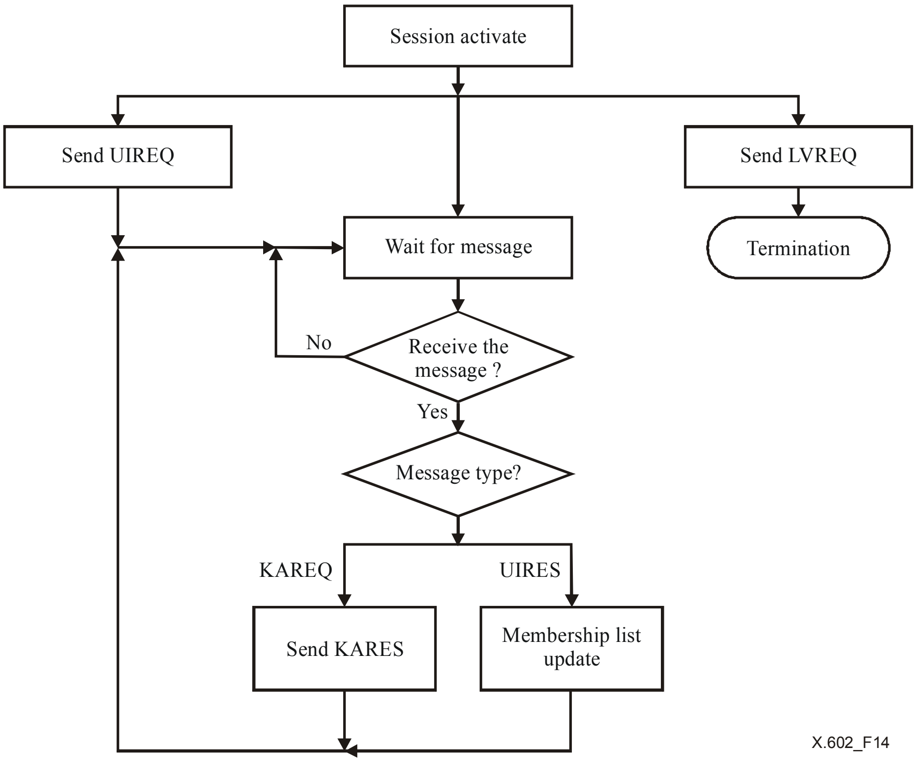

Figure 14 – MM client operation algorithm

7.2.1 Membership Update

7.2.1.1 Open mode

The server will send KAREQ periodically to all active session participants. However, the server will maintain the status information of core members and session creator from the received KARES, while the server may just count the number of other active participants from the received KARES or just ignore others, as shown in Figure 15.

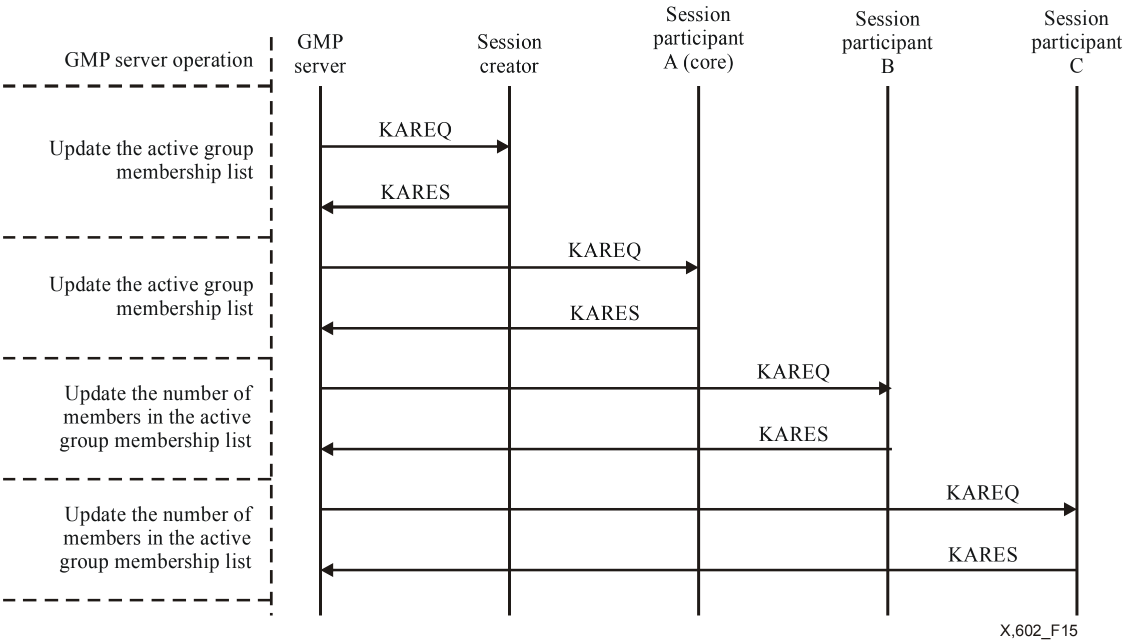
GMP server operation
GMP server
Session creator
Session participant A (core)
Session participant B
Session participant C
Update the active group membership list
KAREQ
KARES
Update the active group membership list
KAREQ
KARES
Update the number of members in the active group membership list
KAREQ
KARES
Update the number of members in the active group membership list
KAREQ
KARES
X,602_F15

Figure 15 – Status reporting procedure (Open mode)

Any session participant can ask for the active group membership list from the server.

Figure 16 shows the session termination case: If the GMP server does not receive the valid KARES from the session creator and session core members before the predefined KA timer expires, the server will send notice that the session is terminating via a Termination Indication message, TRIND, and then terminate the session.

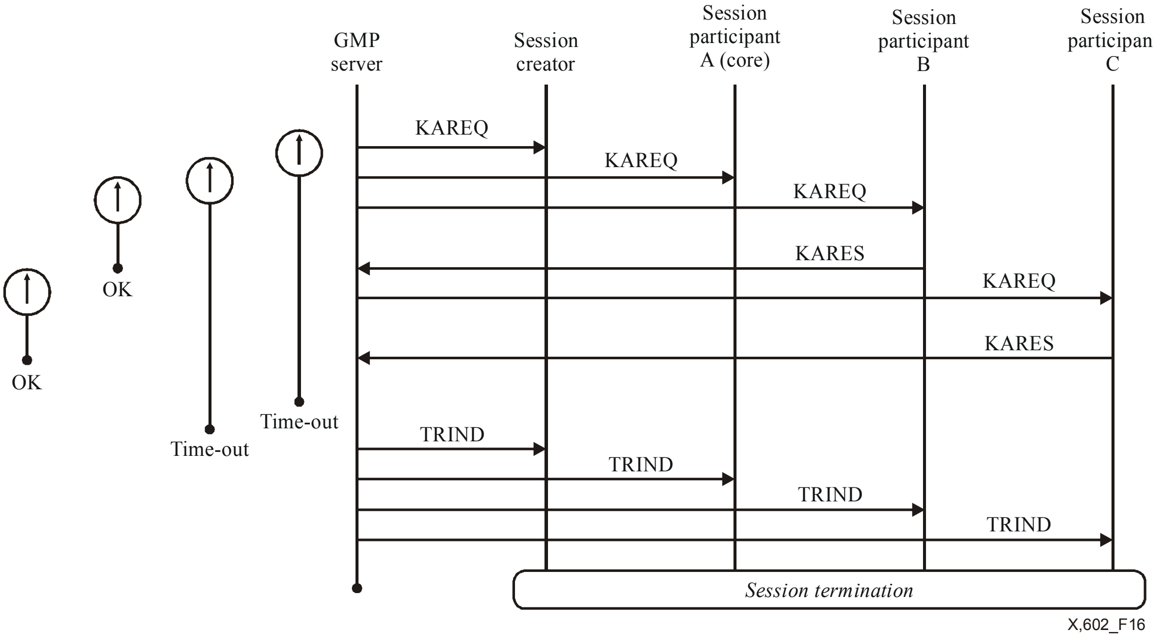

Figure 16 – Session termination (Open mode)

7.2.1.2 Closed mode

The server will send KAREQ periodically to all active session participants. The server will maintain the status information of all active members including core members and session creator from the received KARES as shown in Figure 17.

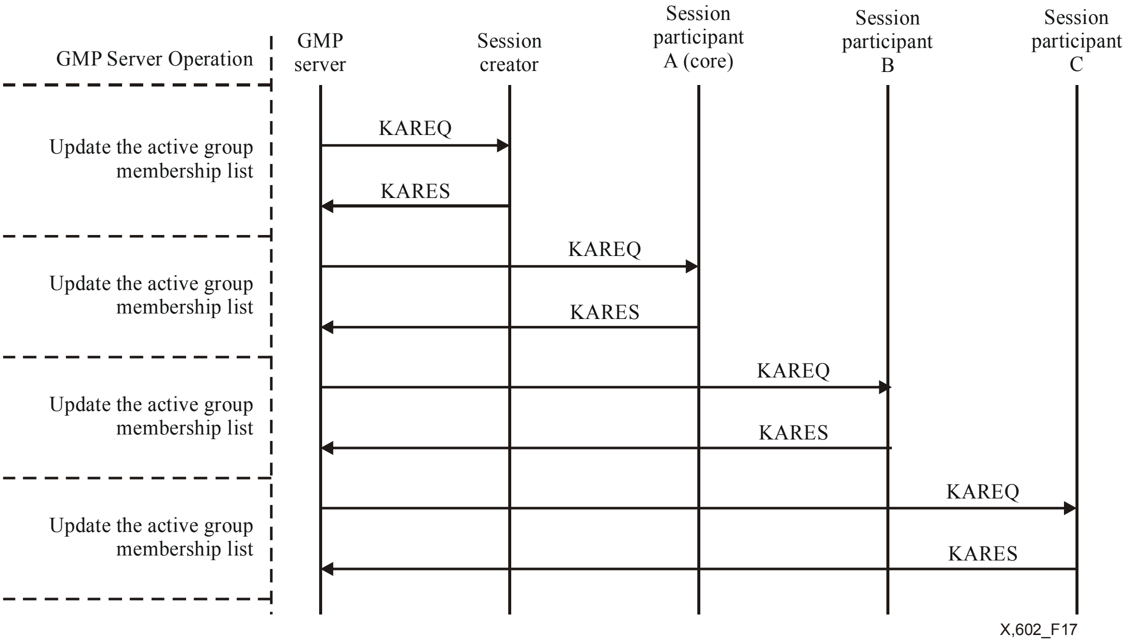
GMP Server Operation
GMP server
Session creator
Session participant A (core)
Session participant B
Session participant C
Update the active group membership list
KAREQ
KARES
Update the active group membership list
KAREQ
KARES
Update the active group membership list
KAREQ
KARES
Update the active group membership list
KAREQ
KARES
X,602_F17

Figure 17 – Status reporting procedure (Closed mode)

Any session participant can ask for the active group membership list from the server.

7.2.2 User information request and response

An active group member can request for the Active Group Member list by sending a UIREQ to the GMP server. The GMP server will reply with a UIRES including the Active Group Member list, as shown in Figure 18.

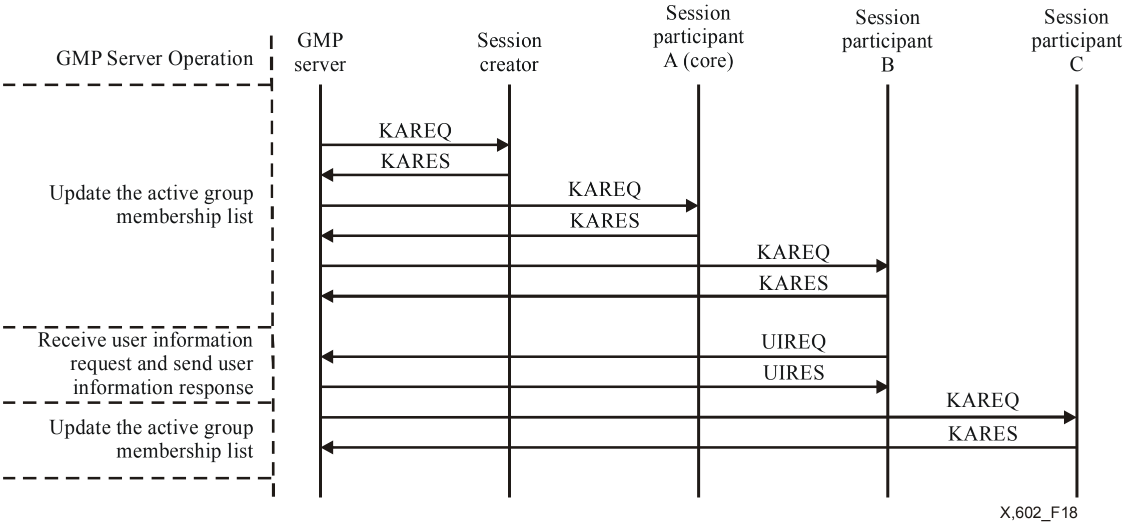
GMP Server Operation
GMP server
Session creator
Session participant A (core)
Session participant B
Session participant C
Update the active group membership list
KAREQ
KARES
KAREQ
KARES
KAREQ
KARES
Receive user information request and send user information response
UIREQ
UIRES
Update the active group membership list
KAREQ
KARES
X,602_F18

Figure 18 – UIREQ and UIRES

7.2.3 Session Leave

Usually an active Session Participant will leave the session by sending a LVREQ to the GMP server; the GMP server will then delete that client from the active group list and add that client to the enrolled group list, as shown in Figure 19.

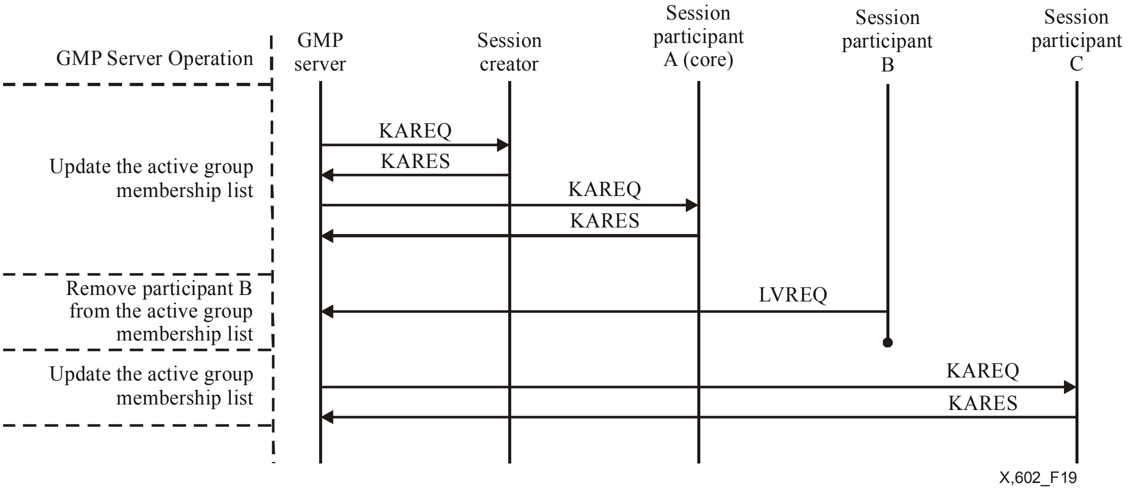
GMP Server Operation
GMP server
Session creator
Session participant A (core)
Session participant B
Session participant C
Update the active group membership list
KAREQ
KARES
KAREQ
KARES
Remove participant B from the active group membership list
LVREQ
Update the active group membership list
KAREQ
KARES
X,602_F19

Figure 19 – LVREQ

However, if an active Session Participant, who is either the Session Creator or a Session Core member, leaves the session by sending a LVREQ, the GMP server who received the LVREQ will terminate the session, sending TRIND to every active Session Participant, as shown in Figure 20.

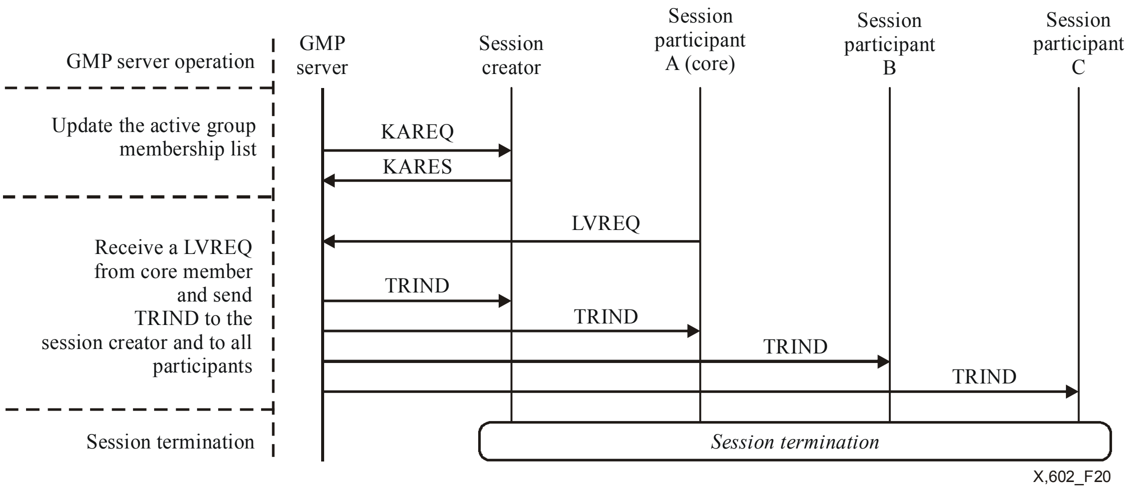

Figure 20 – LVREQ messages from core active member

7.2.4 Session Termination

To terminate a session, the Session Creator will send the TRREQ to the GMP server. The GMP server who received the TRREQ will terminate the session, sending TRIND to every active Session Participant, as shown in Figure 21.

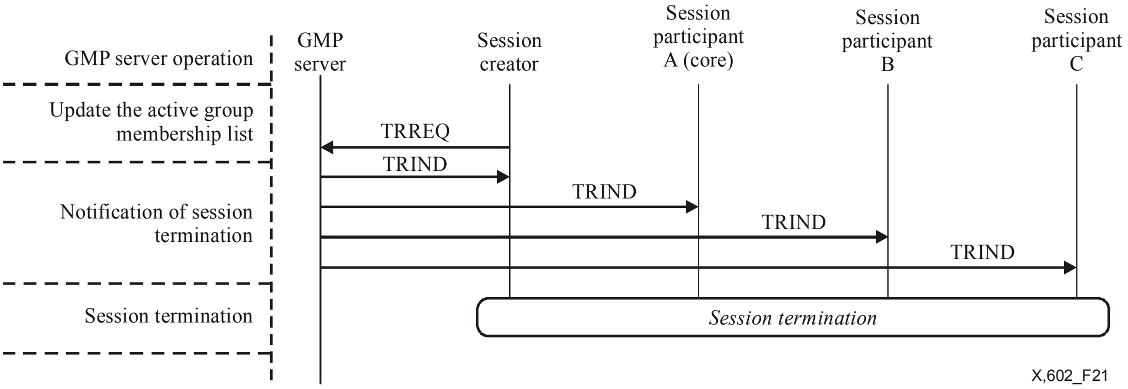

Figure 21 – Session termination

After the GMP server sends KAREQ, it activates the KeepAlive timer; if one or more responding KARESs from core active members have not arrived before the KeepAlive timer expires, the GMP server will terminate the session, sending TRIND to every active Session Participant, as shown in Figure 22.

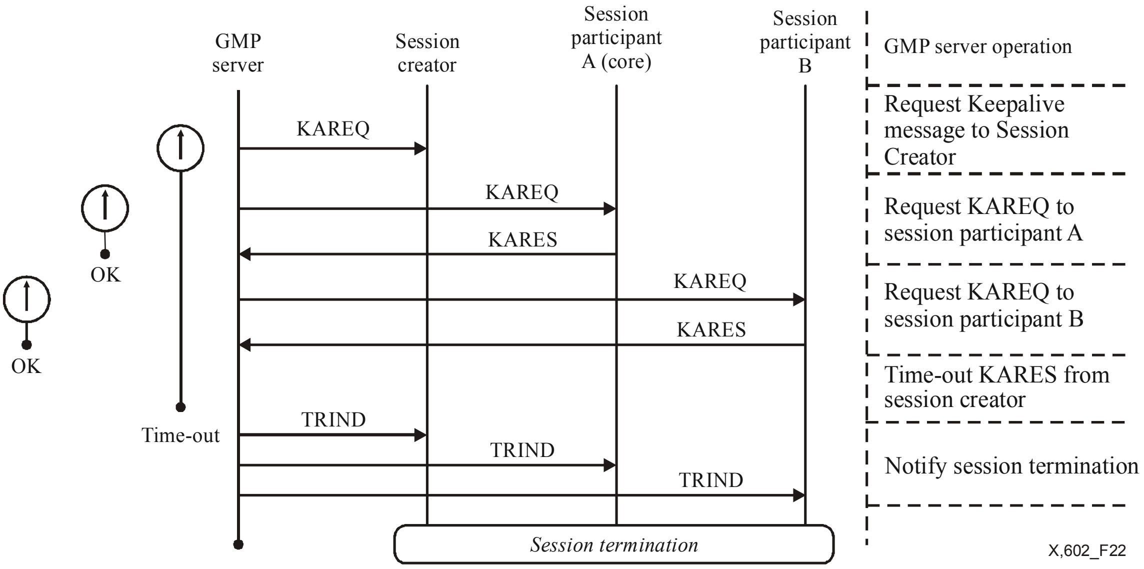
GMP server
Session creator
Session participant A (core)
Session participant B
GMP server operation
KAREQ
KAREQ
KARES
KAREQ
KARES
TRIND
TRIND
TRIND
OK
OK
Time-out
Session termination
Request Keepalive message to Session Creator
Request KAREQ to session participant A
Request KAREQ to session participant B
Time-out KARES from session creator
Notify session termination
X,602_F22

Figure 22 – Session termination

7.3 Security

GMP uses the key distribution to ensure the security of the group management protocol. Figure 23 shows the example of GMP control for the security of GMP.

If the Session Creator wants to create a session applied with security, the Session Creator sends to the GMP server a SCREQ with the 'S' bit set to ONE. However, although Session Creator requests to create a session applied with security, if the GMP server does not support the secure mode for a session, the GMP server sends to the Session Creator a SCREJ with 'S' bit set to ONE.

If the GMP server supports the secure mode for a session, the Session Participant receives SJRES with the 'S' bit set to ONE, including a Key in the enrolment phase.

If any Session Participant enrols or joins the ongoing session late, the GMP server will send SJRES with the 'S' bit set to ONE, including the Key which is currently used in the session.

Whenever any Session Participant de-enrols, the GMP server discards the Key, generates a new Key, and sends a KDUPT, including the new Key, to all enrolled group members.

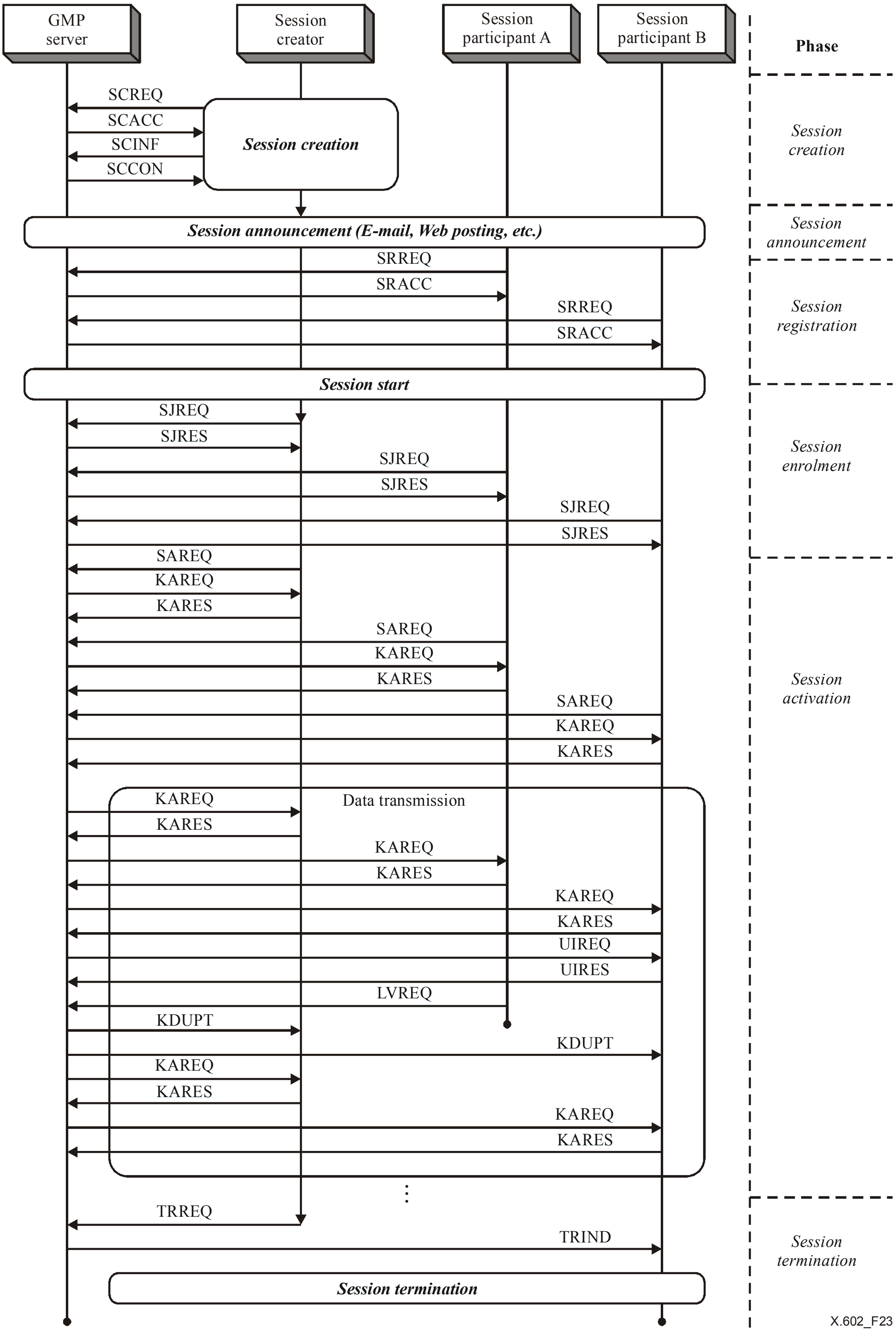

Figure 23 – An example of GMP control (secure mode)

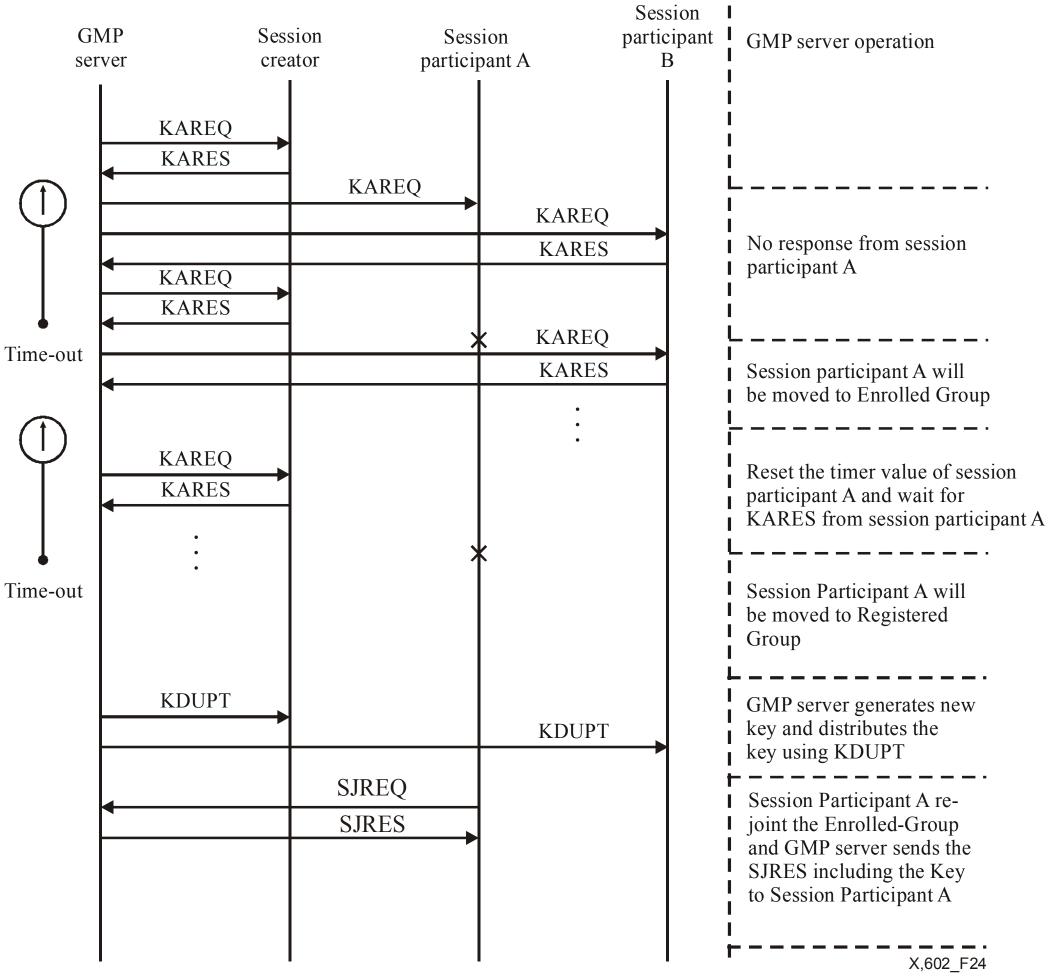
GMP server
Session creator
Session participant A
Session participant B
GMP server operation
KAREQ
KARES
KAREQ
KAREQ
KARES
No response from session participant A
KAREQ
KARES
Time-out
KAREQ
KARES
Session participant A will be moved to Enrolled Group
KAREQ
KARES
Reset the timer value of session participant A and wait for KARES from session participant A
Time-out
Session Participant A will be moved to Registered Group
KDUPT
KDUPT
GMP server generates new key and distributes the key using KDUPT
SJREQ
SJRES
Session Participant A re-joint the Enrolled-Group and GMP server sends the SJRES including the Key to Session Participant A
X,602_F24

Figure 24 – Key distribution using the KDUPT

8 GMP messages

GMP messages are classified into Session Management and Membership Management messages.

8.1 Session Management message types

Table 1 summarizes the messages and their descriptions used in GMP session management.

Table 1 – Session Management message types

Message type	Generated by	Description
SCREQ	Session Creator	Session Creation Request message
SCACC	GMP Server (SM)	Session Creation Accept message
SCREJ	GMP Server (SM)	Session Creation Reject message
SDREQ	Session Creator	Session Deletion Request message
SDRES	GMP Server (SM)	Session Deletion Response message
SCINF	Session Creator	Session Creation Information message
SCCON	GMP Server (SM)	Session Creation Confirm message
SRREQ	Session Creator, Session Participant	Session Registration Request message
SRACC	GMP Server (SM)	Session Registration Accept message

Table 1 – Session Management message types

Message type	Generated by	Description
SRREJ	GMP Server (SM)	Session Registration Reject message
SRRES	GMP Server (SM)	Session Registration Response message
SJREQ	Session Creator, Session Participant	Session Join Request message
SJRES	GMP Server (SM)	Session Join Response message
SAREQ	Session Creator, Session Participant	Session Activation Request message

a) SCREQ: Session Creator generates this message and sends it to the GMP server to get the permission to create a new session.

b) SCACC: GMP server generates this message and sends it to the Session Creator to indicate the permission of session creation.

c) SCREJ: GMP server generates this message and sends it to the Session Creator to indicate that the requested session creation is not allowed for the following reasons:

- The GMP server does not have enough resource;
- Session Creator does not have proper authorization to create a session;
- Although Session Creator requests GMP server to create a session applied with security, the GMP server does not support the secure mode for a session.

d) SDREQ: Session Creator generates this message to request to delete an existing session from the session list in GMP server.

e) SDRES: GMP server generates this message and replies to the SDREQ.

f) SCINF: Session Creator generates this message to inform the detailed session characteristics and its criteria such as media type, application, core member list, session mode, etc., to the GMP server.

g) SCCON: GMP server generates this message to reply to SCINF that the session information is successfully loaded to the session list.

h) SRREQ: Session Clients generate this message to send it to GMP server to register for a session.

i) SRACC: GMP server generates this message and sends it to indicate the successful registration of a requested Session Client.

j) SRREJ: GMP server generates this message and sends it to the registration requested Session Client. The registration may be rejected if the Session Client does not have the proper qualification.

k) SRRES: In Closed mode, GMP server generates this message and sends it to the registration requested Session Client, indicating that the registration request is being processed based on the pre-defined authorization.

l) SJREQ: Session Creator and Session Clients who registered successfully will generate this message and send it to indicate that they are in enrolled state, ready to communicate.

m) SJRES: GMP server generates this message and replies to SJREQ to indicate that the session is going to be active. If the session supports the secure mode, GMP server generates SJRES including Key.

n) SAREQ: Session Creator and Session Clients who enrolled successfully will generate this message and send it to indicate that they are now in active state, being on line. SAREQ includes the port number of the client to start the membership management in the option field.

8.2 Session Management message formats

Figure 25 shows the structure of the Session Management messages.

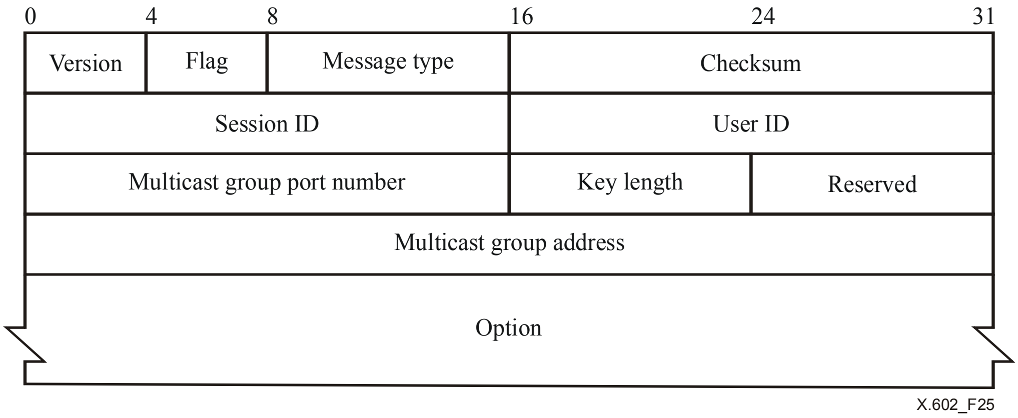

Figure 25 – Session Management message format

The SM header contains the following information:

a) Version (4 bits) – Defines the current version of the GMP protocol. It starts at '1'.

b) Flag (4 bits) – Flag bits. Depending on the message types, it has a different purpose:

– I: Indicates that the message is SCINF when 'I = 1', which has the option field.

– M: Indicates whether the mode is open or close.

Closed mode: 'M = 1' Open mode: 'M = 0'

– S: Indicates whether the mode is secure or non-secure.

Secure mode: 'S = 1' Non-secure mode: 'S = 0'

– Q: Reserved for QoS.

3	2	1	0
Q	S	M	I

c) Message type (8 bits) – Indicates the type of SM message. Table 2 summarizes the message types and encodings.

Table 2 – Encoding table of Session Management message types

Message Type	Encoding
SCREQ	0000 0001
SCACC	0000 0010
SCREJ	0000 0011
SDREQ	0000 0100
SDRES	0000 0101
SCINF	0000 0110
SCCON	0000 0111
SRREQ	0000 1000
SRRES	0000 1001
SRACC	0000 1010
SRREJ	0000 1011
SJREQ	0000 1100
SJRES	0000 1101
SAREQ	0000 1110
Reserved	0000 0000

d) Checksum (16 bits) – Checks the segment validity of the message.

e) Session ID (16 bits) – Identifies each session.

f) User ID (16 bits) – Identifies each session participant. The ID for Session Creator and other participants will be assigned by the GMP server at creation phase and registration phase, respectively.

g) Key length (8 bits): Key length values in GMP in units of 8 bits.

h) Multicast Group Port Number: Port number for multicast group communication.

i) Multicast Group Address: Multicast group address.

j) Option (32 bits × N)

   - This field will be attached to the SCINF: Indicates the detailed information for a new session.
   - This field will be attached to the SJRES: Indicates the Key for the secure mode.
   - This field will be attached to the SAREQ: Indicates the port number of the client to start the membership management.

k) Reserved (8 bits): Reserved.

8.3 Membership Management message types

Table 3 summarizes the messages and their descriptions used in GMP membership management.

Table 3 – Membership Management message types

Message type	Generated by	Description
KAREQ	GMP Server (MM)	Keepalive Request message
KARES	Session Creator Session Participant	Keepalive Response message
UIREQ	Session Creator Session Participant	User Information Request message
UIRES	GMP Server (MM)	User Information Response message
LVREQ	Session Creator Session Participant	Leave Request message
TRREQ	Session Creator	Termination Request message
TRIND	GMP Server (MM)	Termination Indication message
KDUPT	GMP Server (MM)	Key Distribution Update message

a) KAREQ: GMP server generates this message and sends it to active Session Participants periodically to maintain the Active membership list.

b) KARES: Active Session Participant generates this message and replies to the KAREQ to notify the active state.

c) UIREQ: Active Session Client generates this message and sends it to the GMP server to ask the Active-Group Membership list.

d) UIRES: GMP server generates this message and replies to UIREQ with the Active-Group Membership list.

e) LVREQ: Active Session Participant generates this message and sends it to the GMP server to notify its leave. GMP server will update the Active-Group Membership list and the Enrolled Group Membership list.

f) TRREQ: Session Creator generates this message and sends it to GMP server to terminate the session that he created and owned.

g) TRIND: GMP server generates this message and sends it to the active Session Participants to notify that the session is to be terminated.

h) KDUPT: GMP server generates this message and sends it to the active Session Participants and the Enrolled Group members to distribute the Key.

8.4 Membership Management message formats

Figure 26 shows the structure of the Membership Management messages. The Option field is only used in the UIRES to list the active Session Participants.

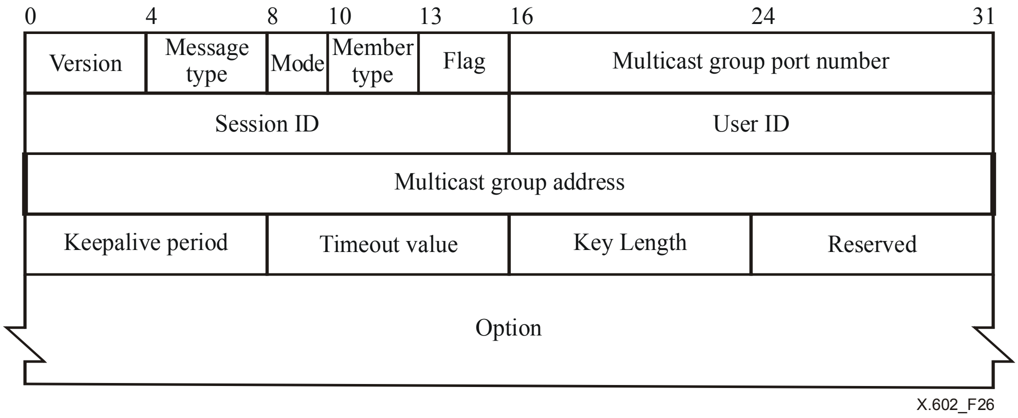

Figure 26 – Membership Management message format, including list state

MM header contains the following information:

a) Version (4 bits): Defines the current version of the GMP protocol. It starts at '1'.

b) Message Type (4 bits): Indicates the type of MM message. Table 4 summarizes the message types and encodings.

Table 4 – Encoding table of Membership Management message types

Message type	Encoding
KAREQ	0001
KARES	0010
UIREQ	0011
UIRES	0100
LVREQ	0101
TRREQ	0110
TRIND	0111
Reserved	0000

c) Mode (2 bits): Indicates the session is open or closed.

Table 5 – Encoding table of the mode

Mode	Encoding
Open Mode	01
Closed Mode	10

d) Member type (3 bits): Identifies the type of Session Participants as shown in Table 6.

Table 6 – Encoding table of the member types

Member type	Encoding
Session Creator	100
Core	010
Session Participant	001

e) Flag (3 bits): flag bits. Depending on the message types, it has a different purpose:

– User Info (UI): Indicates that the message is UIRES when 'UI = 1'.

– Session State (SS): Indicates the session state. 'SS = 1' indicates the session is terminating.

– R: Reserved.

2	1	0
R	SS	UI

f) Multicast Group Port Number (16 bits): Port number for multicast group communication.

g) Session ID (16 bits): Identifies each session, assigned by the GMP server.

h) User ID (16 bits): Identifies each session participant. The ID for Session Creator and other participants will be assigned by the GMP server at creation phase and registration phase, respectively.

i) Multicast Group Address (32 bits): Multicast group address.

j) Keepalive period (8 bits): Specifies a timer to generate a KAREQ in units of 100 ms. It will be chosen by the Session Creator.

k) Timeout value (8 bits): Specifies a timer to limit the waiting time for the KARES.

l) Key length (8 bits): Key length values in GMP in units of 8 bits.

m) Reserved (8 bits): Reserved.

9 GMP variables

9.1 Session-wide variables

GMP SM maintains and processes the following parameters as summarized in Table 7.

Table 7 – Session information parameters

Parameter	Description
Session Name and Object	Session name and object generated by the Session Creator
Session Content	Session subject, introduction, and contents
Owner Information	Creator information
Session StartTime	Session Start time
Session CloseTime	Session Termination time
Media Information	Media type and requirements
Address Information	Address for communications
Registered Member List	Registered member list

9.2 Timers

KeepAlive period, KeepAlive time, and KeepAlive timer are defined in GMP in units of 100 milliseconds.

a) KeepAlive period: GMP server sends KAREQ to active Session participants every KeepAlive period.

b) KeepAlive Time: After GMP server sends KAREQ, it activates KeepAlive timer. KA timer expires after KeepAlive time. If the responding KARES has not arrived before the KeepAlive timer expires, the GMP server updates the active Session Participants list and decides whether the session is to be terminated or not, depending on the Session Creator's criteria.

BIBLIOGRAPHY

The following IETF RFCs are useful to understand this Recommendation | International Standard:

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

– IETF RFC 791 (1981), *Internet Protocol.*

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

– IETF RFC 1112 (1989), *Host extensions for IP multicasting.*

– IETF RFC 1119 (1989), *Network Time Protocol (Version 2) Specification and Implementation.*

– IETF RFC 2119 (1997), *Key words for use in RFCs to indicate requirement levels.*

– IETF RFC 2236 (1997), *Internet Group Management Protocol, Version 2.*

– IETF RFC 2327 (1998), *SDP: Session Description Protocol.*

– IETF RFC 2362 (1998), *Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification.*

– IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Specification.*

– IETF RFC 2543 (1998), *SIP: Session Initiation Protocol.*

– IETF RFC 2887 (2000), *The Reliable Multicast Design Space for Bulk Data Transfer.*

– IETF RFC 2974 (2000), *Session Announcement Protocol.*

– IETF RFC 3048 (2001), *Reliable Multicast Transport Building Blocks for One-to-Many Bulk-Data Transfer.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks and open system communications**
Series Y	Global information infrastructure, Internet protocol aspects and Next Generation Networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2004