International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.603

(03/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

OSI networking and system aspects – Networking

Information technology – Relayed multicast protocol: Framework

Recommendation ITU-T X.603

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

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.379
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.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	X.1000–X.1099
SECURE APPLICATIONS AND SERVICES	X.1100–X.1199
CYBERSPACE SECURITY	X.1200–X.1299
SECURE APPLICATIONS AND SERVICES	X.1300–X.1399
CYBERSECURITY INFORMATION EXCHANGE	X.1500–X.1599
CLOUD COMPUTING SECURITY	X.1600–X.1699

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

INTERNATIONAL STANDARD ISO/IEC 16512-1
RECOMMENDATION ITU-T X.603

Information technology – Relayed multicast protocol: Framework

Summary

The relayed multicast protocol (RMCP) is an application-layer protocol for providing end-to-end multicast services over an IP-based network environment. Recommendation ITU-T X.603 | International Standard ISO/IEC 16512-1 specifies basic concepts of a relayed multicast scheme, data delivery models, service scenarios, required protocol functions for protocol operation, and basic message structures for subsequent protocols. This Recommendation | International Standard can be used to specify detailed relayed multicast protocols for various application requirements.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.603	2004-04-29	17	11.1002/1000/7283
2.0	ITU-T X.603	2012-03-29	11	11.1002/1000/11573

Keywords

End-to-end multicast service, framework, multicast agent, relayed multicast, session manager.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). 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, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Page

1 Scope 1
2 Normative references 1
3 Definitions 1
3.1 Terms defined elsewhere 1
3.2 Terms defined in this Recommendation | International Standard 1
4 Abbreviations 2
5 Conventions 2
6 Framework of RMCP 2
6.1 Introduction 2
6.2 Basic concept of RMCP 3
6.3 RMCP data delivery model 5
6.4 Security consideration in RMCP 8
7 RMCP functions 8
7.1 Session initiation 8
7.2 Session subscription and join 9
7.3 Session leave 9
7.4 Session termination 9
7.5 Session maintenance 9
7.6 Session monitoring 9
8 Messages 10
8.1 Basic message structure 10
8.2 Control format 10
8.3 Sub-control format 10
Bibliography 12

Introduction

This Recommendation | International Standard specifies the relayed multicast protocol (RMCP) used for realizing relayed multicast. Relayed multicast, also known as an overlay multicast or an application-layer multicast, is a data-delivery scheme for group communications applications over an IP-based network environment. RMCP employs intermediate multicast agents for relaying application data from one or more senders to many receivers.

The design of RMCP has been motivated from the following observations:

In the marketplace, diverse group applications and services have been provisioned commercially all over the world. Some of the examples include Internet TV, remote education, real-time media streaming applications, live broadcasting of special events such as the Victoria's Secret Fashion Show, stock-tickers, etc.

At present, most of the group applications mentioned above use a replicated IP unicast method to realize group services. As a result, those applications have scalability problems due to the limitation in supporting a number of simultaneous users. In terms of a business model, it would mean less revenue or profit.

IP multicast has been known as an effective transport technology for providing group communication services. Nevertheless, the IP multicast has not been deployed widely over the Internet due to several reasons, including the following:

- high deployment cost along with an uncertainty of return-on-investment (ROI)
- IP multicast alone cannot support all kinds of group applications.

Network services such as group file transfer or network games, need a reliable multicast transport mechanism. However, even current reliable multicast transport mechanisms still have unresolved problems including scalability, flow control, congestion control, etc. Until an appropriate multicast transport mechanism is laid down, group communication applications requiring reliable data transfer will continue to depend on the server-based replicated unicast method.

Although IP multicast is not deployed globally, various local networks have already been equipped with IP multicast capability. For example, Ethernet-based LANs and private networks, such as corporate and campus networks, substantially provide the multicast transport capability within their local subnet or administrative domains.

Recognizing these observations, there is a crucial need to develop an alternative group delivery scheme. RMCP is one such scheme to realize group delivery over the IP-based network. RMCP utilizes existing unicast, multicast, and/or multicast tunnelling schemes. In addition, RMCP is designed in separate forms to support any kind of group service type. RMCP is expected to provide a substantial solution for group services over the IP-based network.

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Relayed multicast protocol: Framework

1 Scope

Relayed multicast protocol (RMCP) is a protocol which is used to realize a relayed multicast data transport scheme. Different from the conventional IP multicast, RMCP can configure a relayed multicast path that multicast traffic flows by using intermediate end-hosts. RMCP can be applied to the current unicast based IP network where IP multicast is not fully deployed.

This Recommendation | International Standard addresses the basic concepts needed to specify RMCP for relayed multicast. It defines the related terminology and proposes a framework for the future development of subsequent protocols. The framework covers network topology including network entities and the relationship among them, service scenarios, basic operations, and message format.

2 Normative references

None.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation | International Standard

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

3.2.1 child multicast agent (CMA): A next downstream multicast agent (MA) in the relayed multicast protocol (RMCP) data delivery path.

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

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

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

3.2.5 N-plex: Wherein anyone can send something, and, if someone does so, all others may receive it.

3.2.6 parent multicast agent (PMA): A next upstream multicast agent (MA) in the relayed multicast protocol (RMCP) data delivery path.

3.2.7 relayed multicast: A multicast data delivery scheme that can be used in unicast environments.

3.2.8 receiver multicast agent (RMA): A multicast agent (MA) other than sender multicast agent (SMA).

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

3.2.10 relayed multicast protocol (RMCP) session: A set of multicast agents (MAs) which configures the data delivery path using RMCP.

3.2.11 session identification (SID): Corresponds to group name and identifies relayed multicast protocol (RMCP) session uniquely.

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

3.2.13 sender multicast agent (SMA): A multicast agent (MA) attached to a sender in the same system or local network.

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

4 Abbreviations

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

CMA Child Multicast Agent

IPC Inter-Process Communication

IPIP IP in IP encapsulation

MA Multicast Agent

PMA Parent Multicast Agent

RMA Receiver Multicast Agent

RMCP Relayed Multicast Protocol

RMT Reliable Multicast Transport

SID Session ID

SM Session Manager

SMA Sender Multicast Agent

T/TCP TCP extensions to Transactions

TCP Transmission Control Protocol

TP Transport Protocol

UDP User Datagram Protocol

5 Conventions

None.

6 Framework of RMCP

6.1 Introduction

Relayed multicast protocol (RMCP) is an application-level multicast protocol. It constructs and manages a relayed multicast network to support the group communication services over the current unicast-based IP network. After a series of RMCP control connections are established, a multicast data delivery path is constructed by using multiple multicast agents (MAs). Along the delivery path, real-time or reliable data transport channels are inter-connected between upstream and downstream MAs. Only after the data delivery path and data channel are established, group communication applications can work as in the native IP multicast network.

RMCP aims to support various kinds of group-based applications and services. Table 1 categorizes the group communication services with types of communications and characteristics of data delivery.

Table 1 – Considerable group communication services

Characteristics / **Type of communications**	**Real-time data**	**Reliable data**
Simplex	Internet live TV, Internet live banner	Stock-ticker, file dissemination, software live update
N-plex	Videoconference, inter-domain multicast proxy	Distributed virtual environment, network game, data mirroring and caching

6.2 Basic concept of RMCP

Each RMCP session configures relayed multicast data delivery model with the following entities as shown in Figure 1:

a) One session manager (SM);

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

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

d) Group communication applications sending or receiving group data.

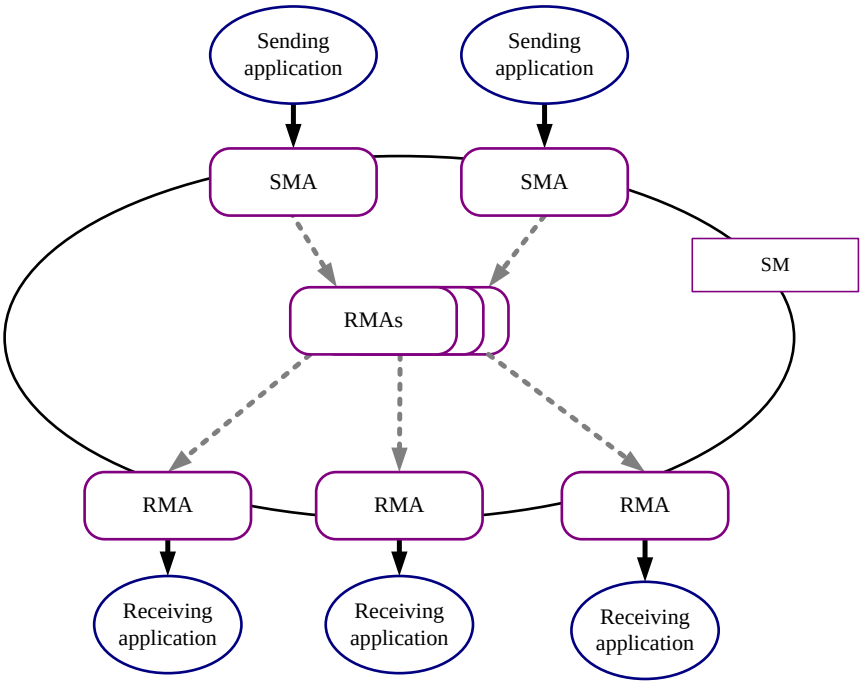


Figure 1 – RMCP entities

The SM is involved in session configuration and maintenance. A single SM can handle one or multiple sessions, simultaneously. Since the SM does not participate in data delivery, it has RMCP control module only. Figure 2 shows the protocol stack of SM.

RMCP control module
Transport protocol for message delivery
IP (unicast)

Figure 2 – Protocol stack of SM

A session manager (SM) can provide the following functionalities:

a) Session initiation;

b) Session termination;

c) Session membership management;

d) Session status monitoring and management.

The MA, which covers both SMA and RMA, constructs a relayed multicast data delivery path and forwards data along the constructed path from SMA to RMA(s). An MA consists of an RMCP control module and a data module. The main function of the control module is to establish a relayed data delivery path, and the data module is to deliver data along the constructed delivery path. Figure 3 shows the protocol stacks of the MA.

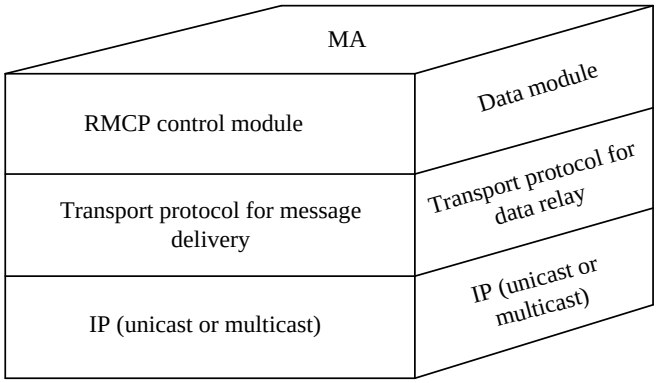


Figure 3 – Protocol stack of the MA

The RMCP control module exchanges RMCP messages with RMCP control modules in other RMCP entities. It performs the following functions:

a) Session join;

b) Session leave;

c) Session maintenance;

d) Session status report.

The message flows among RMCP control modules are shown in Figure 4. As shown in the figure, an MA can be implemented in the same system with the application or in the same local network such as Ethernet-LAN. To deliver the RMCP messages, any type of reliable transport protocols can be used such as TCP. The RMCP control module can also use multicast transport protocols for delivering RMCP messages in the multicast network. In this case, the User Datagram Protocol (UDP) can be used as a transport protocol.

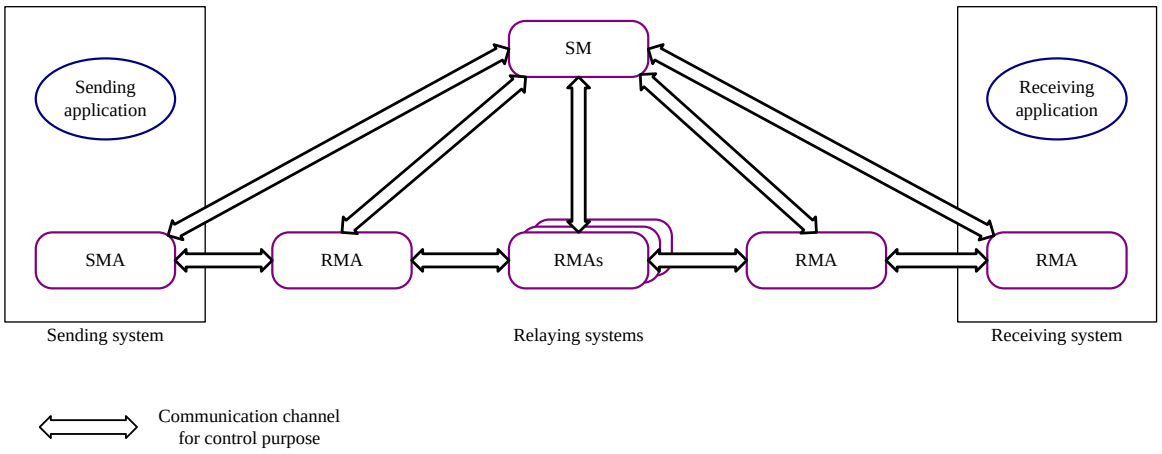


Figure 4 – RMCP control model

The data module relays data along the relayed multicast data delivery path constructed by the RMCP control module as shown in Figure 5. The relayed multicast data delivery path consists of one or more senders, a single SMA per sender, one or more RMAs and receivers. Any kind of transport protocols can be used to transport data.

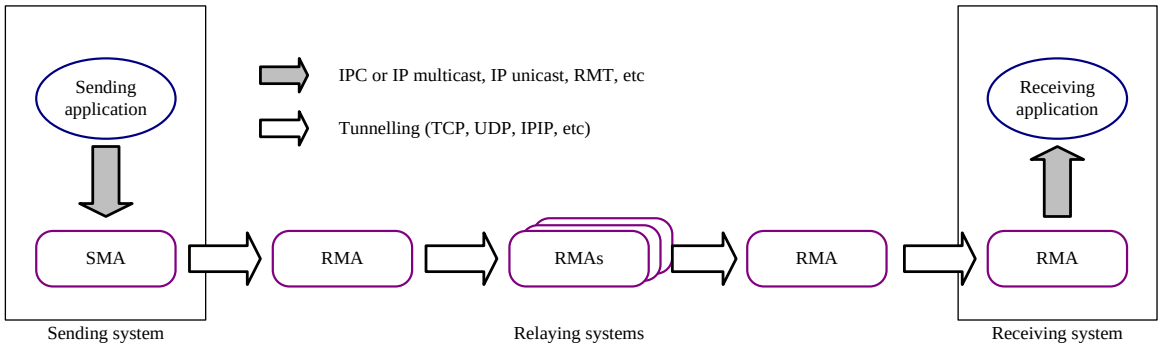


Figure 5 – RMCP data transport model

According to the direction of relaying data, an MA can act as an SMA or as an RMA. When acting as an RMA, the MA receives data from its parent multicast agent (PMA) and forwards the data to its child multicast agent(s) (CMA(s)) and data receiver(s), i.e., receiving application(s). SMA receives data from the data sender, i.e., sending application, and forwards the data to its CMA(s). The number of SMAs depends on the number of data senders.

6.3 RMCP data delivery model

RMCP can support both simplex service, where there is one sender in each session, and N-plex service, where multiple senders can be in each session.

6.3.1 Simplex delivery model for real-time services

Simplex real-time broadcasting services such as Internet live TV and software banner require a real-time data delivery path from one sender to multiple receivers. The most optimized data delivery path would be a per-source relayed multicast tree where a unidirectional real-time channel is established. Figure 6 shows one of the possible relayed multicast trees configured by the RMCP for simplex real-time applications.

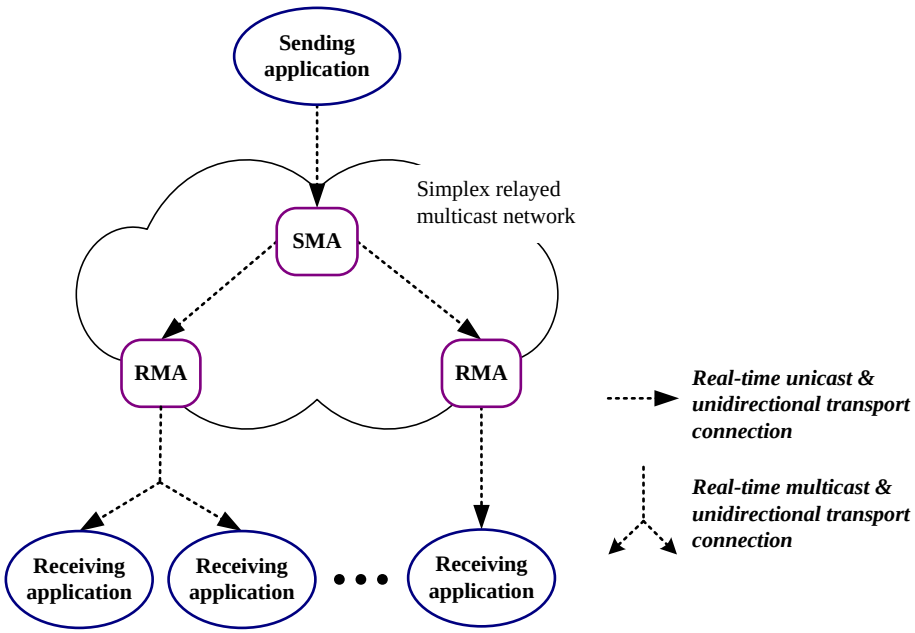


Figure 6 – Simplex real-time data delivery model

6.3.2 Simplex delivery model for reliable services

Simplex dissemination applications such as stock-ticker, file dissemination, and software updater require a reliable data delivery path from one sender to multiple receivers. The most optimized data delivery path here would also be a per-source relayed multicast tree where a unidirectional reliable channel is constructed to deliver data reliably. For reliable delivery, RMCP can use reliable transport protocol such as TCP, and can provide own reliable delivery scheme. Figure 7 shows one of the possible relayed multicast trees configured by RMCP for simplex reliable applications.

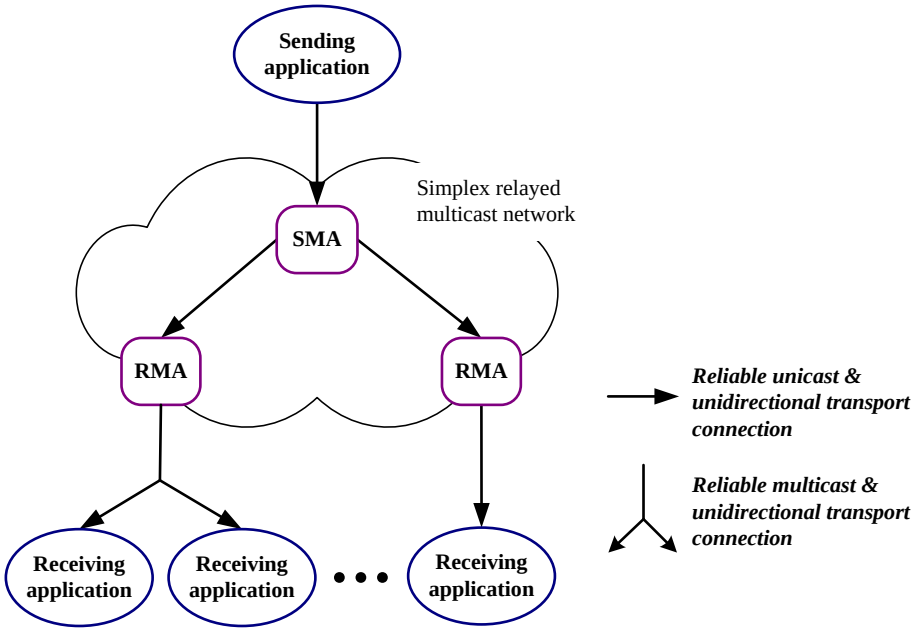


Figure 7 – Simplex reliable data delivery model

6.3.3 N-plex delivery model for real-time services

N-plex real-time interactive applications such as videoconference and inter-domain multicast proxy require a real-time data delivery path from multiple senders to multiple receivers. Figure 8 shows one of the possible relayed multicast data delivery paths configured by the RMCP for N-plex real-time group communications applications.

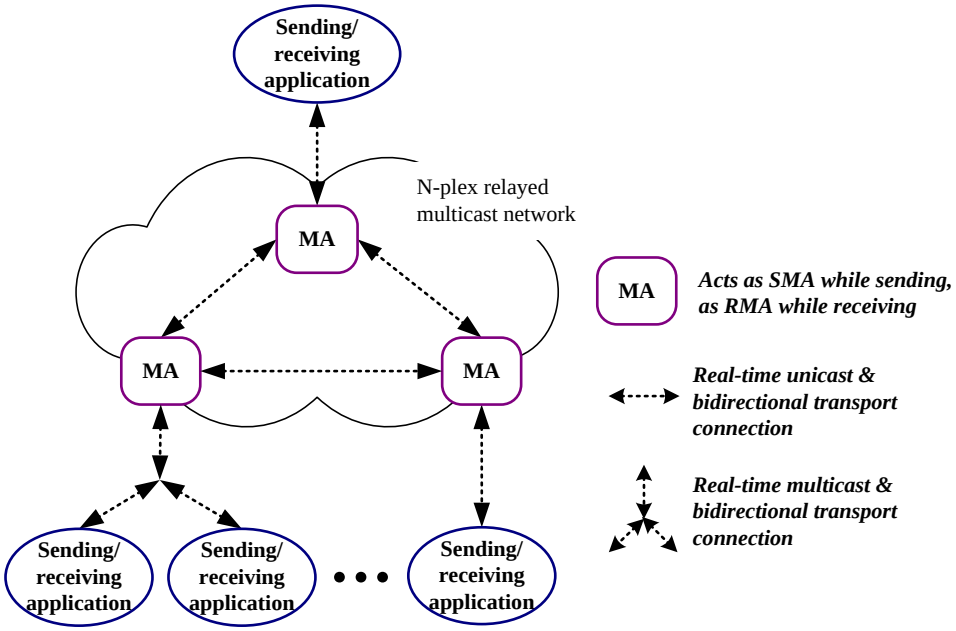


Figure 8 – N-plex real-time data delivery model

6.3.4 N-plex delivery model for reliable services

N-plex distributed applications such as distributed virtual environment, network games, data mirroring, and caching requires reliable data delivery path from multiple senders to multiple receivers. Figure 9 shows a possible relayed multicast data delivery path configured by RMCP for N-plex reliable group communication applications.

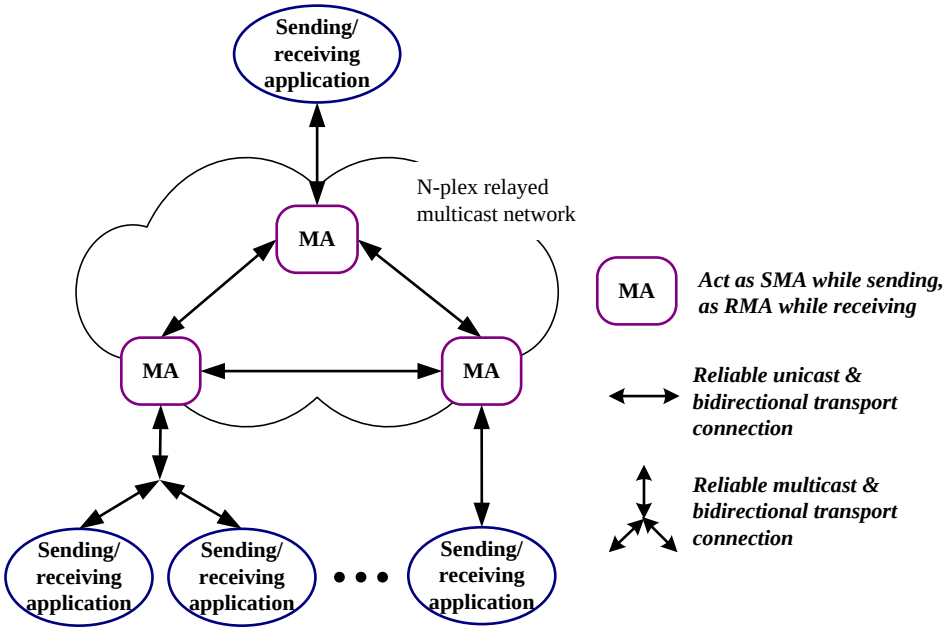


Figure 9 – N-plex reliable data delivery model

6.4 Security consideration in RMCP

For providing RMCP-based services in the Internet, the RMCP does not consider security as mandatory. If it is needed to provide secure RMCP-based services, it is recommended to add security features to the RMCP entities to interact with the pre-deployed trust server for secure communications among the RMCP entities. Figure 10 shows the relationship between secure RMCP and basic RMCP.

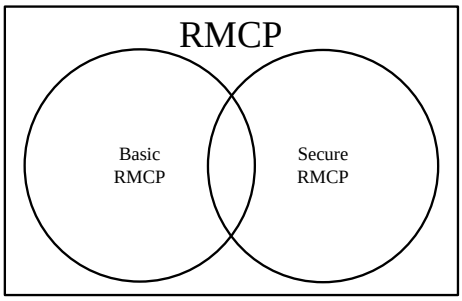


Figure 10 – Relationship between basic RMCP and secure RMCP

Figure 10 implies that subsequent protocols may have security features with own functions and also that secure RMCP can use some functions of basic RMCP.

7 RMCP functions

7.1 Session initiation

The SM initiates a new session upon receiving a session initiation request from the SMA. The SM allocates a SID for each new session. The SID corresponds to the group name that identifies the session. The SM has the information about the constructed sessions. The information may include characteristics of media, session, authentication, etc.

7.2 Session subscription and join

In order to receive service, RMA communicates with SM to subscribe to the session. After successful session subscription, RMA joins the session by interacting with other RMAs which are participating in the RMCP session. Detailed descriptions for session subscription and join are as follows.

Each MA contacts the SM by sending a subscription request. The location of the SM has been already notified to each MA. The SM is recommended to respond to the subscription request to indicate whether the requester is qualified to subscribe to the session. If the MA's subscription request is successful, SM sends a list of PMA candidates that the requesting MA can join. SM does not assign a specific MA to the requesting MA as a PMA. The MA voluntarily chooses the most adequate PMA. The criteria for selecting PMA may be different according to the requesting MA; however, MA would want to select the best PMA in terms of performance and expenses. If the SM does not respond or rejects the session subscription request, the MA cannot subscribe to the RMCP session.

The RMA with successful subscription can send a relay request to its PMA candidate. The relay request includes information such as IP address and port number of the MA for data channel and preferred data channel type. If the PMA candidate approves the relay request, it answers with a successful relay response and sets the requesting MA as its CMA. PMA establishes a data channel with the requester by invoking its data module with the requested data channel.

If the PMA candidate rejects the relay request, it replies with the reason for rejection. The RMA will need to find another PMA candidate or it will have to quit RMCP session join. After successful join with the PMA, the MA will be receiving multicast data from the PMA through the data module. This session join procedure pertains to RMA only. SMA will not need to join the RMCP session.

7.3 Session leave

When an MA wants to leave the session, it needs to notify its PMA, CMA(s), and SM of its departure.

7.4 Session termination

An RMCP session can be terminated as needed or abruptly due to an SMA failure.

7.5 Session maintenance

After a data channel has been established successfully, the relay request and response will be periodically exchanged between the two MAs. This procedure is needed for detection of MA failure and for data delivery path maintenance. If a PMA detects that one of its CMAs has failed, the PMA will stop sending multicast data to the pertaining CMA. If the CMA detects failure of its PMA, the CMA searches for another PMA to join.

The topology of the relayed multicast data delivery path changes constantly due to the join and leave of MAs, MA failure, or problem in the data channel. These changes can cause partition or loop in the data delivery path. Therefore, it is necessary for each MA to maintain the data delivery path.

If an MA finds a PMA candidate that can provide better service quality compared with its current PMA, the MA changes its PMA.

The maintenance function of relayed multicast data delivery path consists of the following:

a) Loop detection and avoidance;

b) Network partition detection and recovery;

c) Parent switching.

7.6 Session monitoring

Session monitoring is used for SM to monitor session status such as membership dynamics and QoS perceived by MAs. The status reports are exchanged between MA and SM. The SM requests a specific MA to report its status and the pertaining MA should report the result to the SM.

The RMCP session monitoring function consists of the following:

a) Reporting the status of the data channel: data throughput, etc.;

b) RMCP membership information gathering;

c) Relayed multicast data delivery path topology information gathering.

8 Messages

8.1 Basic message structure

RMCP messages are used to initialize and manage both RMCP session and the relayed multicast data delivery path. They are encapsulated in transport segments, as shown in Figure 11.

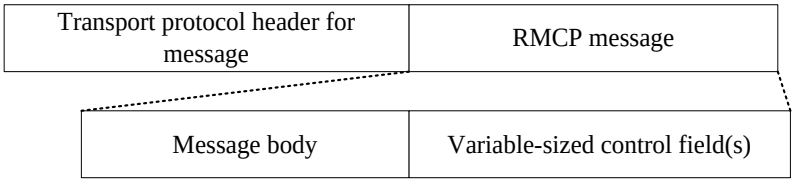


Figure 11 – Encapsulation of the RMCP message

Data from the data sender is encapsulated as shown in Figure 12. Multicast data delivered is not part of the RMCP message. The multicast data are encapsulated when delivered from/to MA, thus, original data is retained during transport.

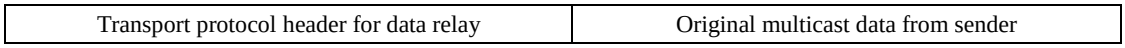
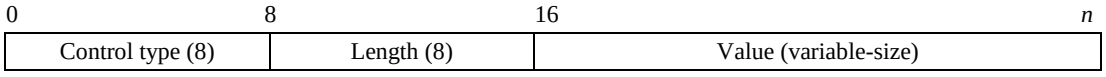


Figure 12 – Encapsulation of original data

8.2 Control format

RMCP message can include a control field(s), if needed. It is concatenated at the end of the RMCP message.

Figure 13 shows the RMCP control format. The meaning and value of each field is as follows:



NOTE – The digit in parentheses in each field indicates the length of the field in bits.

Figure 13 – RMCP control format

a) *Control type* – This field denotes the type of the control;

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

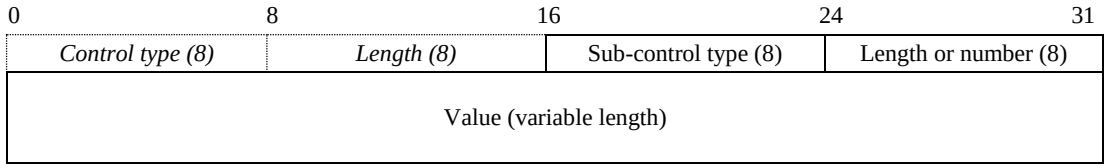
c) *Value* – The content of this field is defined for each control denoted in the Control type field.

8.2.1 Control types and values

Each RMCP message can include the predefined control(s) at its disposal.

8.3 Sub-control format

In order to specify detailed control information, the RMCP control can have one or more sub-controls in its value field. The format of sub-control and its preceding control are shown in Figure 14. The meaning and value of each field of the sub-control is as follows:



NOTE – The digit in parentheses in each field indicates the length of the field in bits.

Figure 14 – RMCP control format when sub-control is used

a) *Sub-control type* – This field denotes the type of sub-control;

b) *Length or number* – This field denotes the length in byte or the number of sub-control value depending on the sub-control type;

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

One or more controls may be included in the Control field of a message. Whenever multiple sub-controls for the same control are included in the Control field, every sub-control shall be preceded by the control. This is illustrated in Figure 15, which shows an example of the use of multiple controls (i.e., type A, type B, type D) with two separate sub-controls for control type B.

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

Figure 15 – Example formatting of multiple controls

Bibliography

– 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 1644 (1994), *T/TCP – TCP Extensions for Transactions Functional Specification*.

– IETF RFC 1853 (1995), *IP in IP Tunneling*.

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

– IETF RFC 2960 (2000), *Stream Control Transmission Protocol*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
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	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
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, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016