International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.609.8

(12/2019)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

OSI networking and system aspects – Networking

Managed P2P communications: Management protocol for live data sources

Recommendation ITU-T X.609.8

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 (1)	X.1100–X.1199
CYBERSPACE SECURITY	X.1200–X.1299
SECURE APPLICATIONS AND SERVICES (2)	X.1300–X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500–X.1599
CLOUD COMPUTING SECURITY	X.1600–X.1699
QUANTUM COMMUNICATION	X.1700–X.1729

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

Recommendation ITU-T X.609.8

Managed P2P communications: Management protocol for live data sources

Summary

Recommendation ITU-T X.609.8 describes the management protocol for live data sources in managed peer-to-peer (MP2P) communications, which is an overlay protocol that runs in the application layer to manage a live data from multiple data sources. The examples of live data generated from a data source include a live sensor data and, a live closed-circuit television (CCTV) stream, and they can be applicable to disaster recovery, autonomous vehicles, etc. This Recommendation also specifies the identification, functions and the procedures of the data sources involved.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T X.609.8	2019-12-14	11	11.1002/1000/14147

Keywords

Data source, live data, managed P2P communications, management protocol.

[*] 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/.

Table of Contents

Recommendation ITU-T X.609.8

Managed P2P communications: Management protocol for live data sources

1 Scope

This Recommendation specifies a management protocol for data sources that generate live data continuously. The examples of live data include a live sensor data and a live CCTV stream, and they can be applicable to disaster recovery, autonomous vehicles, etc.

The protocol specified by this Recommendation includes:

– Identification for involved data sources;

– Primitive service flows;

– Message exchange and message format;

– Fault recovery;

– Security considerations.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.609] Recommendation ITU-T X.609 (2015), *Managed peer-to-peer (P2P) communications: Functional architecture*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 overlay network [b-ITU-T X.1162]: An overlay network is a virtual network that runs on top of another network. Like any other network, the overlay network comprises a set of nodes and links between them. Because the links are logical ones, they may correspond to many physical links of the underlying network.

3.1.2 peer [b-ITU-T X.1161]: Communication node on P2P network that functions simultaneously as both "client" and "server" to the other nodes on the network.

3.1.3 peer-to-peer (P2P) [b-ITU-T Y.2206]: A system is considered to be P2P if the nodes of the system share their resources in order to provide the service the system supports. The nodes in the system both provide services to other nodes and request services from other nodes.

NOTE – Peer is the node in a P2P system.

3.1.4 managed peer-to-per (MP2P) [b-ISO/IEC TR 20002]: P2P with manageability features to manage the P2P-based service and P2P network by the P2P participants such as P2P service provider, ISP, and peer.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

CCTV	Closed Circuit Television
IMT-2020	International Mobile Telecommunications-2020
LDMP	Live Data source Management Protocol
MP2P	Managed P2P
WLAN	Wireless Local Area Network

5 Conventions

In this Recommendation:

– The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

– The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

– The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 Overview

6.1 Management of data source

Live data source management protocol (LDMP) is a protocol to manage data sources that generates data to be distributed over managed P2P (MP2P) network. The data sources generate data continuously or on specific events, and the examples of the data include a live sensor data, a live CCTV stream which can be applicable to many areas such as disaster recovery, vehicle-to-vehicle communications and so on.

Figure 1 shows the relationship between data source and MP2P communication systems. As shown in Figure 1, a data source generates data and sends the data to a source peer in order to distribute the generated data. The data source and source peer can be connected through any network, including wireless local area network (WLAN), and IMT-2020. Once the data arrives at the source peer of an MP2P communication system then the data can be distributed to peers in an MP2P network.

NOTE – The reason why the LDMP needs to separate the live data source from MP2P source node is due to the number of live data source nodes that are quite large and the frequency of inclusion and exclusion of data source is too high, resulting in the increased burden of managing MP2P network . Also, the live data sources can be located in different network environments such as a private network, therefore the management of all the data source nodes simultaneously will be difficult.

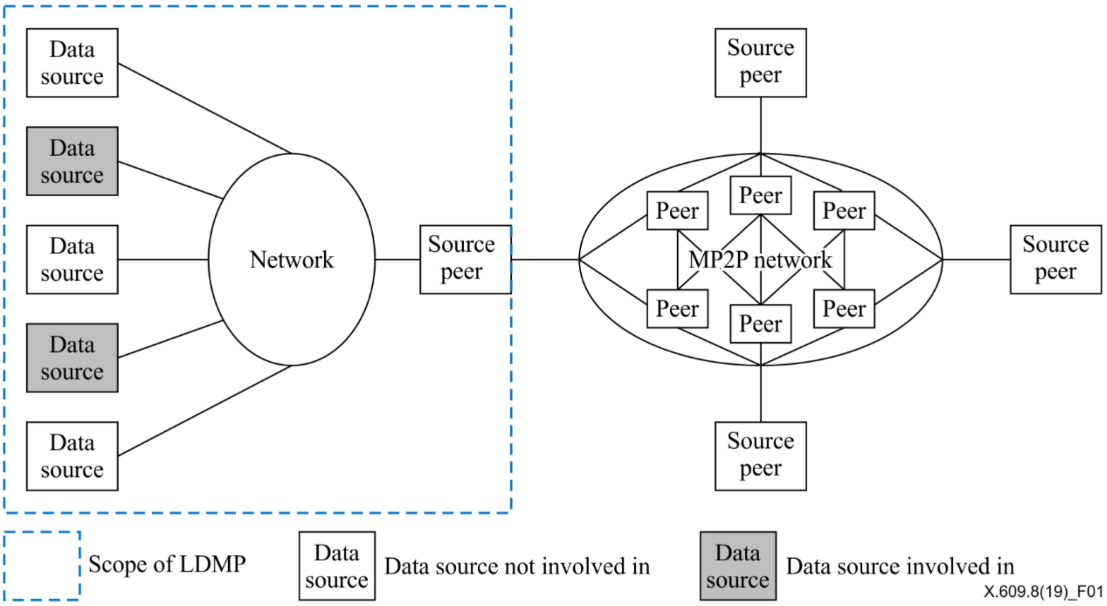

Figure 1 – Relationship between data source and MP2P communications system

The dashed box in Figure 1 represents the scope of LDMP. LDMP enables a source peer to manage multiple data sources in both data and control perspective. With the help of LDMP, each source peer can acquire data from data sources, and it can also configure data sources appropriately.

6.2 Functional requirements

To harvest data and control data sources, LDMP requires the following high-level functionality:

– Identification of data source

– Identification of data

– Identification of source peer

– Registration of data source

– Registration of source peer

– Connection management

– De-registration of data source

– De-registration of source peer

– Protocol error detection and recovery

– Initialization of data source

– One-way message delivery through notification

– Two-way message delivery through request and response

6.3 Protocol blocks and relationship among entities

As shown in Figure 2, LDMP is an application layer protocol like MP2P peer protocol. Source peer is responsible for handling data from data source in order to distribute the data to peers in MP2P network.

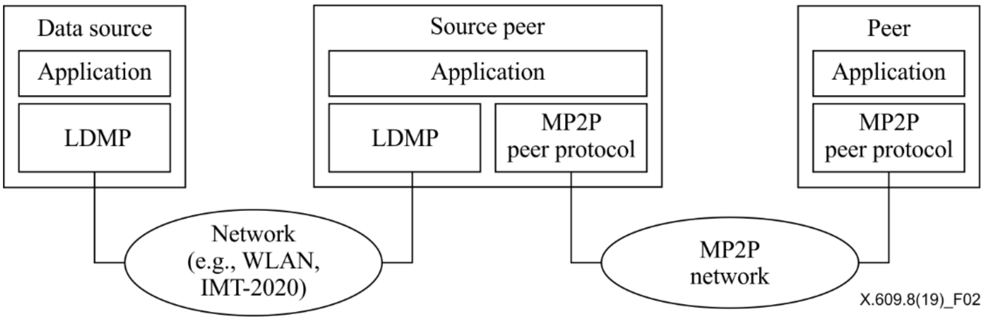

Figure 2 – Protocol blocks and relationship among entities

7 Protocol behaviour

7.1 Registration

To distribute own data, a data source is required to register itself on a source peer which will be a gateway toward managed peer-to-peer network. Figure 3 shows the procedure for the successful registration of a data source. As an initiation operation, a data source sends a request message to a source peer. The request message indicates that a response from a recipient is required. The source peer will then respond with a message indicating that registration has been successfully done, if the request from the data source was accepted. After successful registration, a source peer can control and manage the registered data source.

NOTE – A data source can connect with only one source peer, whereas a source peer can connect with multiple data sources.

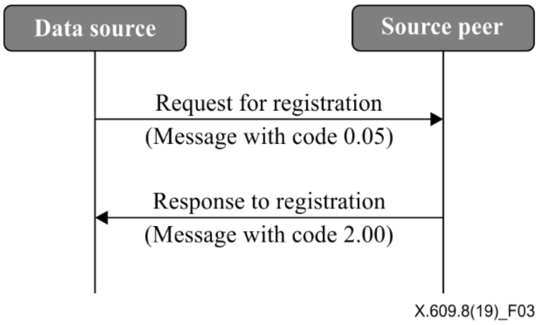

Figure 3 – Procedure for successful registration of a data source

Figure 4 shows interactions between a data source and a source peer when the registration of the data source failed. In such a case, the response from the source peer is required to indicate the reason of failure using a message with a code.

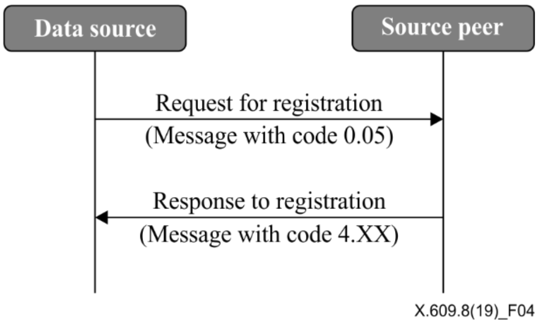

Figure 4 – Procedure for unsuccessful registration of a data source

7.2 Deregistration

A data source sends a request for deregistration to the source peer which the data source registered, when it needs to leave a data streaming session. Figure 5 shows the procedure for deregistration. The data source sends a request message to the source peer, which indicates that a response from a recipient is required. The source peer will then respond with a message indicating that deregistration has been successfully done, if the request from the data source was accepted.

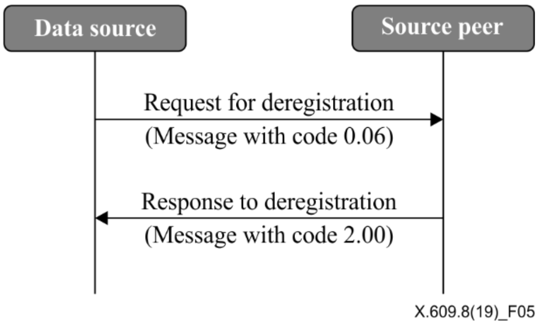

Figure 5 – Procedure for successful deregistration of a data source

Figure 6 shows interactions between a data source and a source peer when the deregistration of the data source failed. The failure may occur if the data source requesting deregistration sends the request to the source peer to which the data source did not register. In such a case, the response from the source peer is required to indicate the reason of failure using a message with a code.

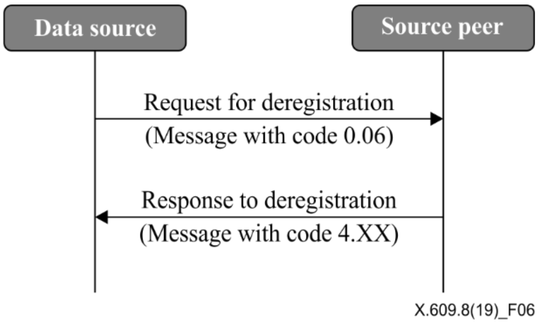

Figure 6 – Procedure for unsuccessful deregistration of a data source

The request for deregistration is not retransmitted even if a response message corresponding to the request did not arrived prior to an expiration time. Instead, the source peer will exclude the data source which sent the missing request message by conducting the procedure for connection management described in clause 7.3.

7.3 Connection management

To detect and recover any problem in connection with a data source and a source peer, LDMP supports connection management. Figure 7 shows the procedure for connection management without any connection problem. Either a data source or a source peer requests its opponent node to send a message, if no message arrived prior to a specific expiration time for message arrival. The request message indicates that a response from a recipient is required. The recipient is then required to respond with a message indicating that the connection has no problem.

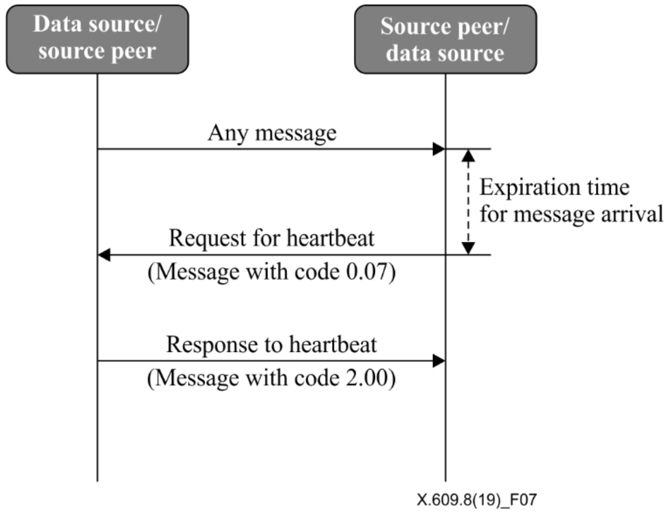

Figure 7 – Procedure for normal connection management

To avoid congestion incurred by excessively frequent exchange of messages for connection management, it is recommended that the expiration time value of the source peer is set to be larger than that of the data source.

As shown in Figure 8, either a data source or a source peer can request for heartbeat until the maximum time for removal is expired. If no message arrived prior to the maximum expiration time, the node which sent the request message will remove the information concerning the opponent node. Data source will conduct the registration procedure as described in clause 7.1 after handling the connection failure in connection management.

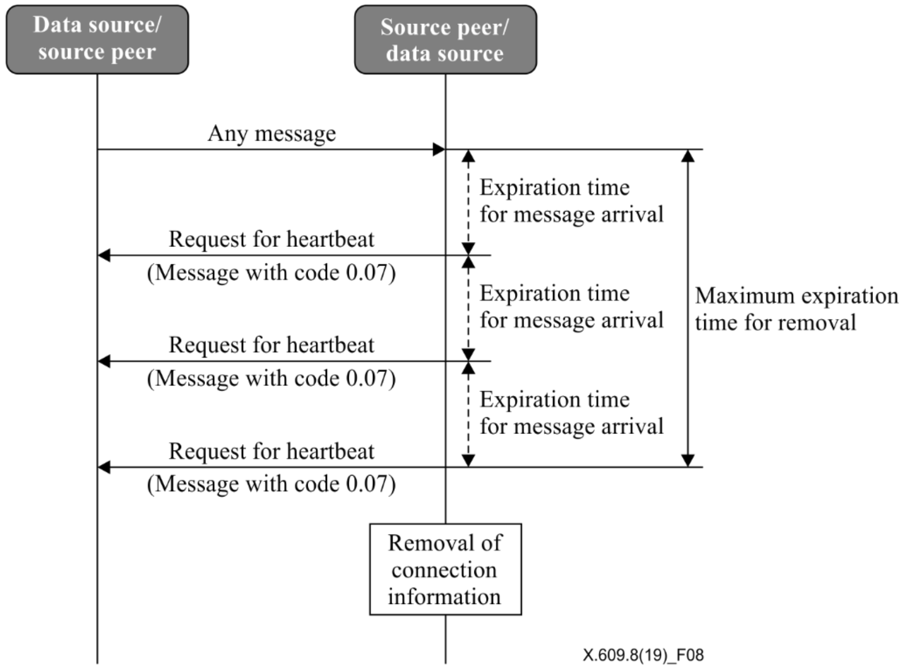

Figure 8 – Procedure for handling failure in connection management

7.4 Post

A data source sends a request for posting data to a source peer, when it needs to post its data on the source peer. The posting data does not need to be reliably delivered and thus it does not need any response from the source peer. For example, a data source sends a certain measured value periodically by posting data.

Figure 9 shows the procedure for posting data. A data source sends a request message to post data, which indicates that the request does not require any response from a recipient.

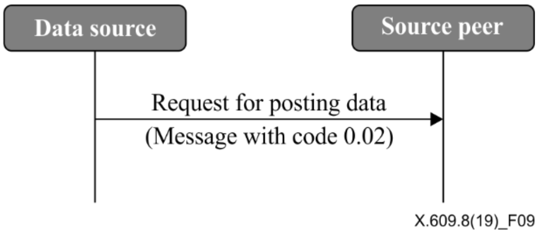

Figure 9 – Procedure for posting data

7.5 Configuration and acquisition

A source peer can configure its data source or acquire specific data from its data source. Figure 10 shows the procedure for configuration and acquisition. These operations require a response from a data source, as the source peer needs to check whether the requested configuration or acquisition has been successfully operated. Thus, the request message and the corresponding response use the same message ID to explicitly show their relationship.

Figure 10 shows the procedure for configuration and acquisition. To acquire specific data, a source peer sends a request message indicating the specific data that it wishes to acquire. The request message indicates that the request requires a response from a recipient. The data source is then required to respond with a message indicating that the response includes the requested data. To configure a data source, a source peer sends a request message configuring the data source. The request message indicates that the request requires a response from a recipient. The data source is then required to respond with a message confirming that the data source is configured as requested. For any error that occurred during configuration or acquisition, the data source responds with a message including the reason of failure.

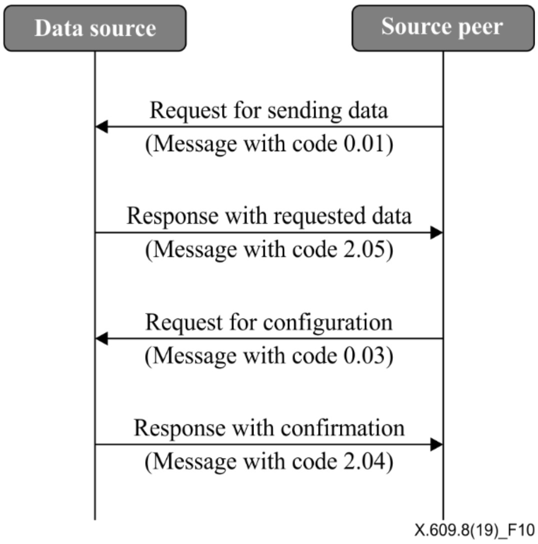

Figure 10 – Procedure for configuration and acquisition

As shown in Figure 11, a source peer can request for configuration or acquisition until the maximum time for removal is expired. If no message arrived prior to the maximum expiration time, the source peer which sent the request message will remove the information concerning the non-responsive data source.

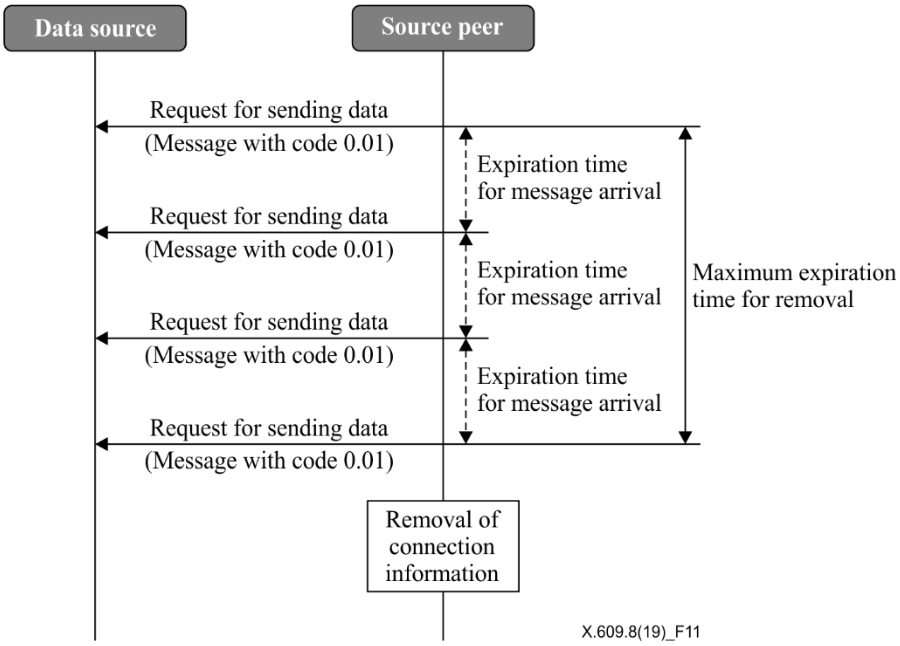

Figure 11 – Procedure for handing non-responsive data source

7.6 Reset

A source peer can request that a data source be reset by sending a request message. Figure 12 shows the procedure for initialization of a data source. The request message indicates that the request does not require any response from a recipient. After reset operation, the data source needs to conduct registration operation, which is described in clause 7.1.

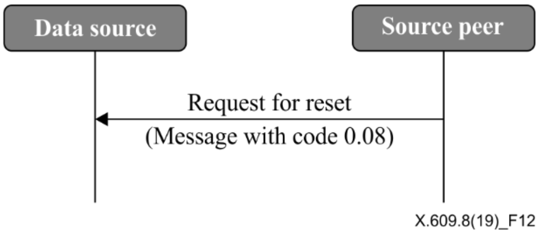

Figure 12 – Procedure for reset

8 Message formats

8.1 Header format

This Recommendation defines a header format in order to be easily adaptable to various wired and wireless environment and also to reduce burden on nodes including data source and source peer. Figure 13 shows the format of the header, which includes 8 bytes of common header and optional payload.

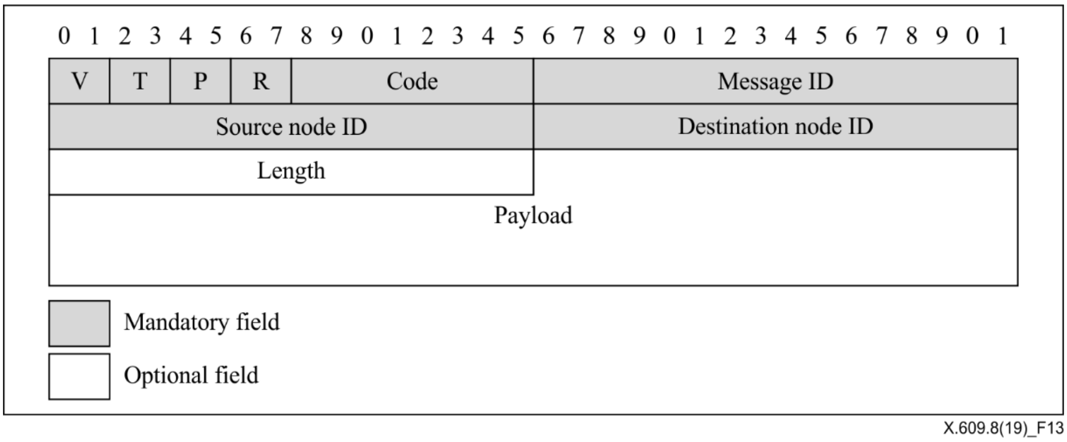

Figure 13 – Common header format

The meaning of each field is as follows:

- V is 2 bits and identifies version, which is set to 1;
- T is 2 bits and identifies type of message delivery:
  - i) 00: this message requires acknowledgement;
  - ii) 01: this message does not require acknowledgement;
  - iii) 10: this message is an acknowledgement;
  - iv) 11: reserved for further use.
- P is 2 bits and identifies the type of a payload:
  - i) 00: this message does not contain any payload;
  - ii) 10: this message contains a binary payload;
  - ii) 01: reserved for further use;
  - iv) 11: this message contains a text payload.
- R is 2 bits and reserved for further use;
- Code is 8 bits and identifies operation for request or response as defined in clause 8.2;
- Message ID is 16 bits and identifies each message. The value starts from a random value and is increased by 1 in round-robin manner for each message;
- Source ID is 16 bits and identifies the origin of this message.
- Destination ID is 16 bits and identifies the recipient of this message.
- Length is 16 bits and is set to the byte length of the payload contained in this message only when P field is set to either "10" or "11";
- Payload is an optional data, and its length is identified by "length" field.

8.2 Code

The message defined in this Recommendation can deliver information only by use of the code field in the message. Among 8 bits, upper 3 bits identify the type of operation including request and response. The remaining 5 bits describe details.

Table 1 shows code values and its meaning for each request operation. Note that the T field of the message is set to "01" if any response from the recipient is required. Otherwise the T field is set to "00".

Table 1 – Code value and its meaning for each request operation

Value	Meaning
0.01	GET
0.02	POST
0.03	PUT
0.05	Registration
0.06	Release
0.07	Heartbeat
0.08	RESET

Table 2 shows code values and its meaning for the acknowledgment as successful result.

Table 2 – Code value and its meaning for acknowledgement as successful result

Value	Meaning
2.00	OK
2.04	Changed
2.05	Content

Table 3 shows code values and its meaning for the acknowledgment as error.

Table 3 – Code value and its meaning for acknowledgement as error

Value	Meaning
4.00	Bad Request
4.01	Unauthorized
4.03	Forbidden
4.04	Not Found
4.05	Method Not Allowed
4.06	Not Acceptable
4.15	Unsupported Content-Format

9 Protocol variables

9.1 Heartbeat time

Heartbeat time is a period to initiate connection management as described in clause 7.3. The default value is 60 seconds, but a smaller value can be used for more precise connection management.

9.2 Retransmission time

Retransmission time is a period to wait for an acknowledgement. If a node does not receive the requested data prior to the expiration of retransmission time, the node will request the data again. The default value is 10 seconds.

9.3 Maximum number of retransmissions

Maximum number of retransmissions is the maximum number of requesting retransmission when a node does not receive the requested data. The default value is 3 times.

Bibliography

[b-ITU-T X.1161] Recommendation ITU-T X.1161 (2008), *Framework for secure peer-to-peer communications.*

[b-ITU-T X.1162] Recommendation ITU-T X.1162 (2008*), Security architecture and operations for peer-to-peer networks.*

[b-ITU-T Y.2206] Recommendation ITU-T Y.2206 (2010*), Requirements for distributed service networking capabilities.*

[b-ISO/IEC TR 20002] ISO/IEC TR 20002 (2012*), Information technology – Telecommunications and information exchange between systems – Managed P2P: Framework.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Environment and ICTs, climate change, e-waste, energy efficiency; 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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, 2020