International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.609.1

(06/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

OSI networking and system aspects – Networking

Managed P2P communications: Peer activity management protocol (PAMP)

Recommendation ITU-T X.609.1

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.

Recommendation ITU-T X.609.1

Managed P2P communications: Peer activity management protocol (PAMP)

Summary

Recommendation ITU-T X.609.1 specifies a peer activity management protocol (PAMP) that runs on two interfaces: 1) an interface between a peer activity management server (PAMS) and a peer; 2) an interface between a PAMS and an overlay management server (OMS). A PAMP is used to deliver peer activity status information with the goal of optimization of the overlay network. Peer activity status information includes both static and dynamic status information. Recommendation ITU-T X.609.1 provides the requirements, protocol operations, and message formats used in each operation for a PAMP.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.609.1	2016-06-13	11	11.1002/1000/12886

Keywords

Managed P2P, PAMP, PAMS, peer activity management.

* 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 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/.

© ITU 2016

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

Page

Recommendation ITU-T X.609.1

Managed P2P communications: Peer activity management protocol (PAMP)

1 Scope

This Recommendation specifies a peer activity management protocol (PAMP). The purpose of a PAMP is to collect and exchange peer activity status information. A PAMP is used among a peer activity management server (PAMS), an overlay management server (OMS), and the peer, which are involved in managed peer-to-peer (P2P) communications.

The scope of this Recommendation covers:

– the requirements of a PAMP based on [ITU-T X.609];

– the protocol operation of a PAMP;

– the messages and parameters used by a PAMP.

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*.
[IETF RFC 7231]	IETF RFC 7231 (2014), *Hypertext Transfer Protocol (HTTP/1.1), Semantics and Content*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 fragment [ITU-T X.609]: A piece of the shared content.

3.1.2 functional entity [b-ITU-T Y.2012]: An entity that comprises an indivisible set of specific functions. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.

3.1.3 managed peer-to-peer [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.

3.1.4 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.

3.1.5 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.

3.1.6 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.

3.1.7 peer status information [ITU-T X.609]: Both dynamic and static status information of a peer. The dynamic status information describes the activity of peer in the participating overlay network. The static status information describes a peer's activity configuration.

3.1.8 reference point [b-ITU-T Y.2012]: A conceptual point at the conjunction of two non-overlapping functional entities that can be used to identify the type of information passing between these functional entities.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 JavaScript object notation (JSON): A lightweight, text-based, language-independent data interchange format.

NOTE – Definition based on that given in [b-IETF RFC 7159].

3.2.2 leech; leecher: A peer possessing none or some of fragments composing the content shared among peers participating in the same overlay network. A leech can upload its fragments to other peers and it can also download fragments from other peers.

3.2.3 seed; seeder: A peer possessing all fragments composing the content shared among peers participating in the same overlay network. A seed can upload fragments to other peers, but it does not download any fragment.

3.2.4 uniform resource identifier (URI): A simple and extensible means for identifying a resource.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CS	Cache Server
DHT	Distributed Hash Table
FE	Functional Entity
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
ID	Identifier
IXS	Index Server
JSON	JavaScript Object Notation
MP2P	Managed Peer-to-Peer
N/A	Not Applicable
OIM	Overlay Information Management
OMS	Overlay Management Server
ONIM	Overlay Network Information Management
PAIM	Peer Activity Information Management
PAM	Peer Activity Management

PAMP	Peer Activity Management Protocol
PAMS	Peer Activity Management Server
P2P	Peer-to-Peer
PIA	Peer Information Analysis
PLM	Peer List Management
PLO	Peer List Optimization
PPIM	Peer Profile Information Management
PPM	Peer Profile Management
REST	Representational State Transfer
RS	Relay Server
RSM	Resource Status Management
TLS	Transport Layer Security
UMS	User Management Server
UNIS	Underlying Network Information Server
VoIP	Voice over Internet Protocol

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 the specification.

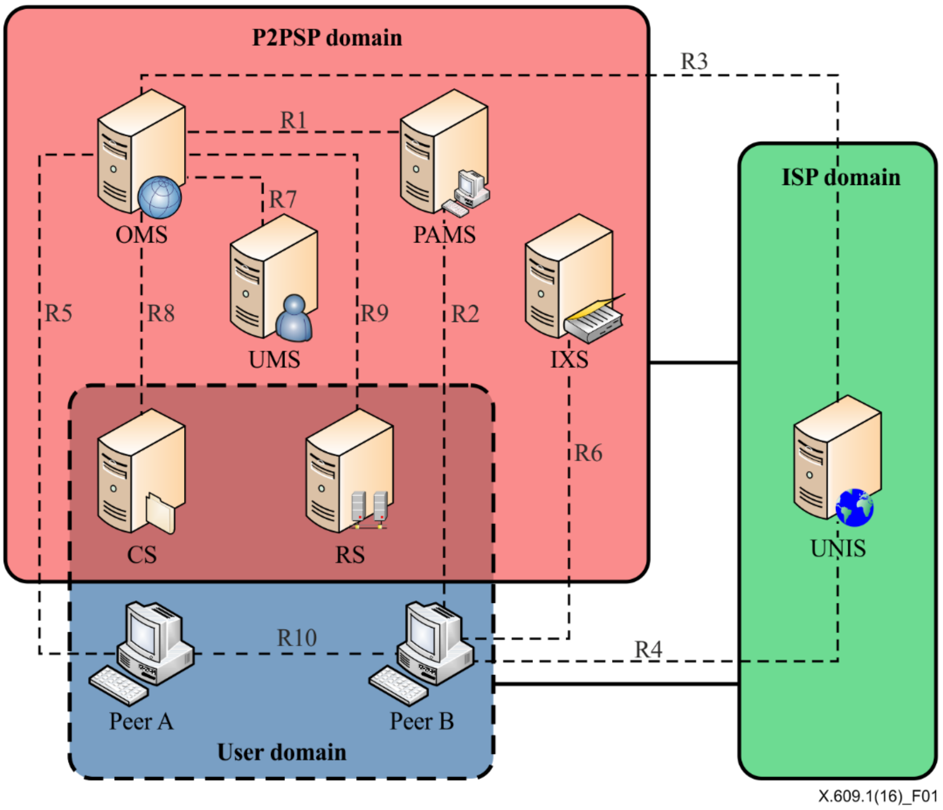
6 Overview

Peer-to-peer (P2P) networking is a decentralized communication, where the participants, called peers, can directly communicate with each other. P2P networking enables one peer's resources to be shared with other peers in the same P2P network. The P2P network is self-organized, composed of peers capable of adapting to the dynamics of a peer without central coordination. P2P networking has been used in various applications, such as file distribution, VoIP and multimedia streaming. However, P2P networking incurs problems such as load concentration on a specific peer and free-riding.

Managed peer-to-peer (MP2P) aims to provide manageability features to the P2P network in order to solve or alleviate concerns about P2P networking.

Peers organizing a P2P network are equally privileged, but may not have the same amount of resources. In other words, a peer with more resources can contribute more than peers with fewer resources. Peers may want to retrieve data from peers with abundant resources. However, this can impose a burden on the specific peer that results in an inefficient P2P network. Thus the amount of burden imposed on each peer needs to be considered when setting up an efficient P2P network. To achieve this, [ITU-T X.609] has defined an entity, called a peer activity management server (PAMS). A PAMS collects peer activity status information from peers. Peer activity status information is based on an abstract view of peer activity in the overlay network. These views provide status information about the overlay network for an overlay management server (OMS) to effectively utilize them. A peer can also utilize this information to select the appropriate peers for retrieving data.

Figure 1 shows reference points among entities for MP2P communications. This Recommendation describes a peer activity management protocol (PAMP) and its related interfaces, denoted as R1 and R2 in Figure 1.



UMS: user profile management server
OMS: overlay management server
PAMS: peer activity management server
RS: relay server
CS: cache server
IXS: index server
UNIS: underlying network information server

Figure 1 – Framework and interface of an MP2P [ITU-T X.609]

A PAMS collects and analyses the status information received from peers. The PAMS can provide analysis results to an OMS to be utilized to set up an overlay network.

Figure 2 shows functional entities (FEs) and their interactions to support PAMP operations.

A PAMS has the following FEs involved in the PAMP:

– a peer activity information management (PAIM) FE manages peer dynamic activity information;

– a peer profile information management (PPIM) FE manages peer static information;

– a peer information analysis (PIA) FE provides peer static/dynamic information to be used by OMS.

An OMS has the following FEs involved in the PAMP:

– an overlay information management (OIM) FE manages information about overlay networks;

– a peer list optimization (PLO) FE calculates optimized peer lists from given peer lists.

A peer has the following FEs involved in the PAMP.

– a resource status management (RSM) FE reports peer activity information to the PAMS;

– a peer profile management (PPM) FE manages peer profiles used in the overlay network;

– an overlay network information management (ONIM) FE manages the overlay network in which the peer is participating;

– a peer list management (PLM) FE manages the list of peers that are participating in the same overlay network.

NOTE 1 – Detailed descriptions of each FE are given in [ITU-T X.609].

NOTE 2 – When a cache server (CS) operates as a virtual peer, the CS uses R2 to communicate with the PAMS.

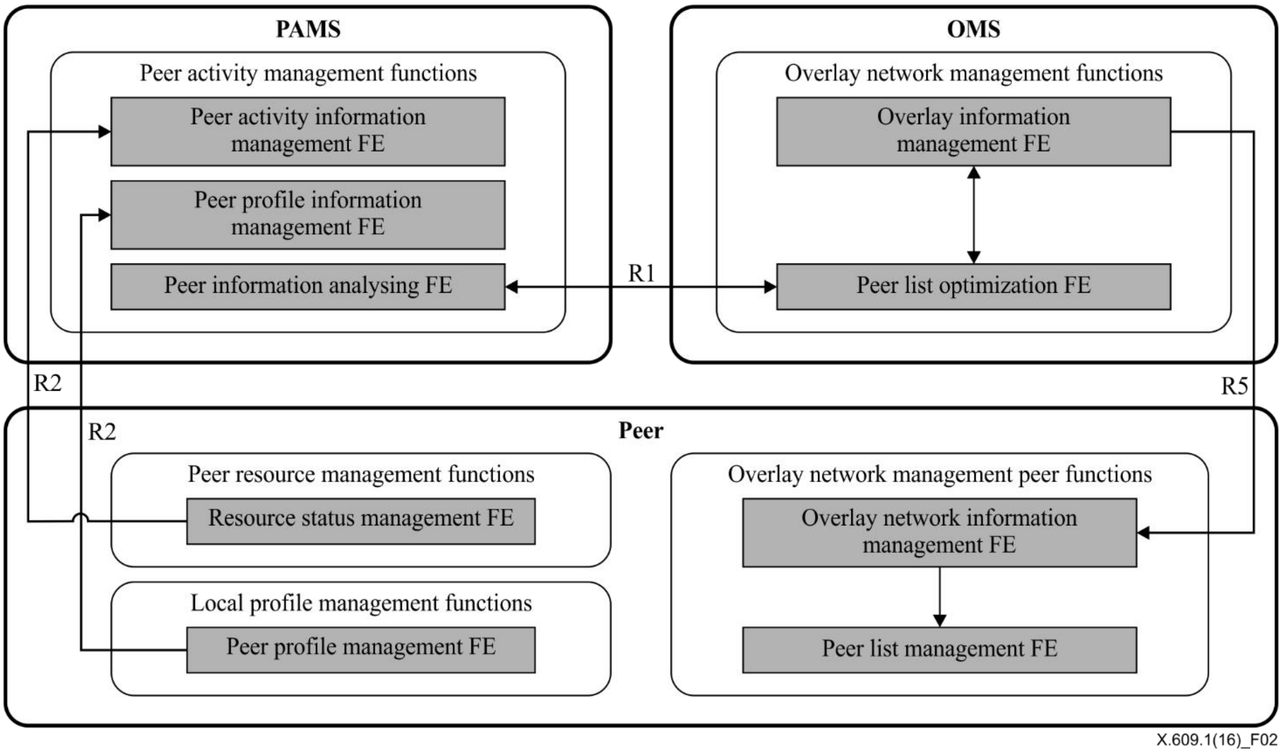

PAMS
Peer activity management functions
Peer activity information management FE
Peer profile information management FE
Peer information analysing FE
R1
OMS
Overlay network management functions
Overlay information management FE
Peer list optimization FE
R2
R2
R5
Peer
Peer resource management functions
Resource status management FE
Local profile management functions
Peer profile management FE
Overlay network management peer functions
Overlay network information management FE
Peer list management FE
X.609.1(16)_F02

Figure 2 – Interactions among FEs to support a PAMP

7 Requirements of a PAMP

This clause describes requirements for a PAMS, OMS, and peer regarding PAMP. The requirements are classified into general requirements and protocol requirements.

7.1 General requirements

This clause describes general requirements to support a PAMP.

[REQ-GEN-01] A PAMS, OMS, and peer are required to support a PAMP.

[REQ-GEN-02] When multiple PAMSs exist, a PAMS is recommended to balance the load among existing PAMSs in order to prevent overload on an individual PAMS.

NOTE – A PAMS can suffer from overload due to PAMP status reports from multiple peers in the managed P2P overlay network.

7.1.1 Identifier

[REQ-ID-01] A peer is required to have a globally unique identifier (ID).

[REQ-ID-02] A fragment is required to have a unique ID in an overlay network.

NOTE – A fragment ID does not need to be globally unique, since it is scoped by the overlay network.

[REQ-ID-03] An overlay network is required to have a globally unique ID.

7.1.2 Message extensibility

[REQ-EXT-01] A PAMP message is required to have an extensible format for further extensions.

7.1.3 Security and privacy

[REQ-SEC-01] A PAMP message is recommended to be delivered securely.

[REQ-SEC-02] A PAMP is required to prevent disclosure of private information about a peer.

[REQ-SEC-03] A PAMP is required not to distribute private information.

7.2 Protocol requirements

This clause describes requirements on protocol operation of PAMP.

7.2.1 Operations

[REQ-OPR-01] A PAMS, OMS, and peer are required to support the following operations.

– Peer registration/deregistration: A process of registering/deregistering a peer to join an overlay network on an OMS.

– Overlay network registration/deregistration: A process of creating/destroying an overlay network by a content provider.

– Peer status report and confirm: A process of reporting peer status to a PAMS.

– Query on peer activity status: A process of querying peer activity status by an OMS or service provider.

7.2.1.1 Peer registration/deregistration

These requirements apply to the peer registration/deregistration to a PAMS.

[REQ-PREG-01] An OMS is required to provide a PAMS address to a peer joining an overlay network.

[REQ-PREG-02] A peer is required to provide a peer ID and an overlay network ID when registering/deregistering on a PAMS.

[REQ-PREG-03] A PAMS is required to provide the result of registration/deregistration to peer.

[REQ-PREG-04] A PAMS is recommended to provide a reporting method in the registration phase.

NOTE – The report can be sent periodically or by event-driven.

7.2.1.2 Overlay network registration/deregistration

[REQ-OREG-01] An OMS is required to provide overlay network ID when registering/deregistering an overlay network on a PAMS.

[REQ-OREG-02] An OMS is recommended to provide the type of content to be served when registering an overlay network on a PAMS.

[REQ-OREG-03] An OMS is required to support deregistration of a specific overlay network.

[REQ-OREG-04] An PAMS is required to provide the result of registration/deregistration to an OMS.

7.2.1.3 Report and confirm

These requirements apply to the process of reporting peer activity status to the PAMS.

[REQ-RPT-01] A peer is required to report its activity status information according to the reporting method obtained during the registration phase.

[REQ-RPT-02] A peer is required to provide a peer ID and an overlay network ID when reporting activity status information.

[REQ-RPT-03] A PAMS is required to send an acknowledgment message for the report message received.

[REQ-RPT-04] A PAMS is recommended to provide a method for verifying the report message.

NOTE – The report from each peer should be cross-checked and verified before being used, since it is possible for a peer to send a fake report message that can corrupt the robustness of an overlay network and incur improper operation of a PAMS.

[REQ-RPT-05] Peer static status information is recommended to include at least the following information:

– maximum uplink capacity;

– maximum downlink capacity;

– maximum number of connections concurrently supportable.

[REQ-RPT-06] A peer dynamic status information report is recommended to include at least the following information:

– sending peer ID;

– receiving peer ID;

– list of fragment ID;

– range of fragment ID;

– size of fragment;

– current participation status (i.e., start, pause, complete);

– connected peer type (i.e., seed, leech, relay server (RS), CS);

– amount of uploaded data;

– amount of downloaded data.

7.2.1.4 Query

These requirements apply to the process of querying status of a peer by an OMS or service provider.

[REQ-QRY-01] An OMS is recommended to support querying of peer status to a PAMS.

[REQ-QRY-02] A service provider is required to support querying of peer status to a PAMS.

NOTE 1 – An OMS/service provider can query a PAMS to provide information about a specific peer or list of peers belonging to a specific overlay network.

NOTE 2 – An OMS/service provider can conduct optimization based on the information received from a PAMS. An OMS/service provider can request a PAMS for an optimized peer list by specifying optimization conditions.

[REQ-QRY-03] A PAMS is required to provide status information about a given peer or list of peers.

7.2.2 Transport protocol

This requirement applies to the transport protocol used in delivery of PAMP messages.

[REQ-TRANS-01] PAMSs, OMSs, and peers are recommended to send messages using a secured transport protocol, such as transport layer security (TLS).

8 Protocol operation

8.1 Basic operations

8.1.1 PAMS discovery

An OMS provides a PAMS address to be used for managing information about peer activity regarding a given overlay network. An OMS can respond with the PAMS address when the peer requests to join the overlay network. The peer connects and registers on the PAMS.

8.1.2 Registration/deregistration

8.1.2.1 Overlay network registration/deregistration

An OMS can establish a new overlay network based on a request from a peer to create one. After the overlay network is established, the OMS can register the newly established overlay network on a PAMS. Steps 2 and 3 of Figure 3 show the procedure for overlay network registration.

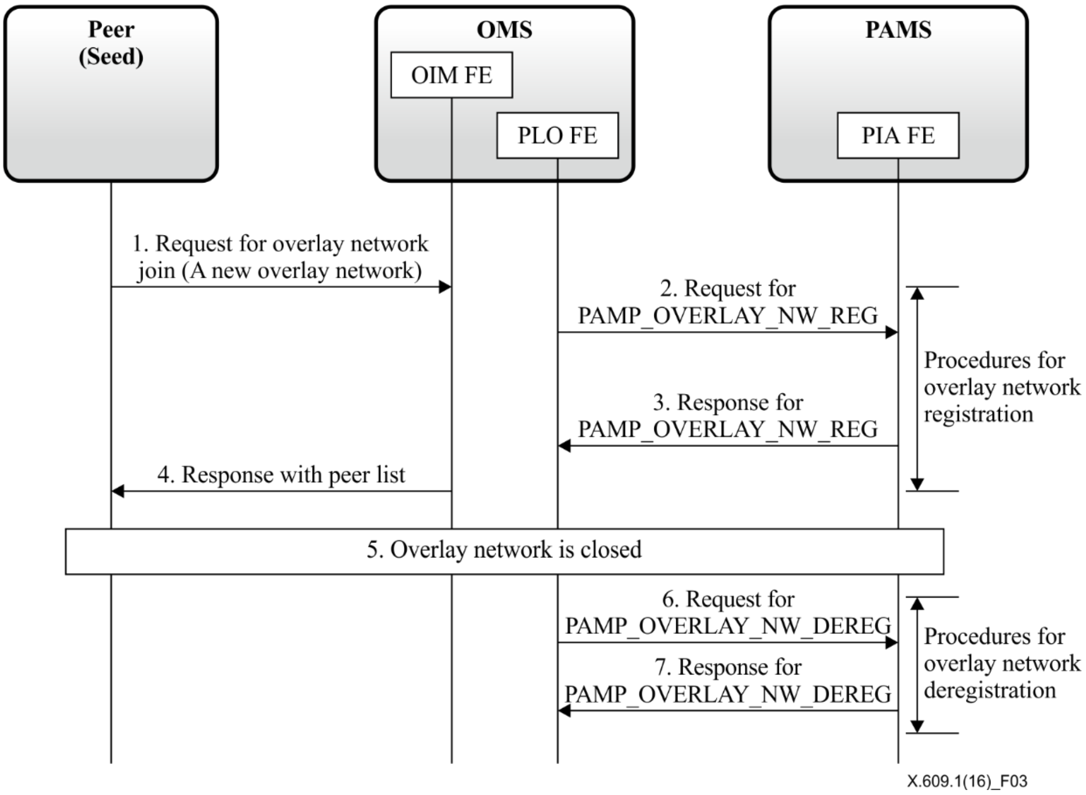

Peer (Seed)
OMS
OIM FE
PLO FE
PAMS
PIA FE
1. Request for overlay network join (A new overlay network)
2. Request for PAMP_OVERLAY_NW_REG
Procedures for overlay network registration
3. Response for PAMP_OVERLAY_NW_REG
4. Response with peer list
5. Overlay network is closed
6. Request for PAMP_OVERLAY_NW_DEREG
Procedures for overlay network deregistration
7. Response for PAMP_OVERLAY_NW_DEREG
X.609.1(16)_F03

Figure 3 – Procedures for overlay network registration/deregistration

An OMS can close the established overlay network, if needed. Then a PAMS does not need to maintain peer activity information regarding the closed overlay network. Steps 2 and 3 of Figure 3 shows the procedures for overlay network deregistration.

8.1.2.2 Peer registration/deregistration

When a peer successfully joins a given overlay network, it can register on a PAMS. If the request is acceptable, the PAMS can respond with the reporting method. The peer reports peer activity status information to the PAMS, according to the reporting method received. Steps 1 and 2 of Figure 4 show the procedures for peer registration.

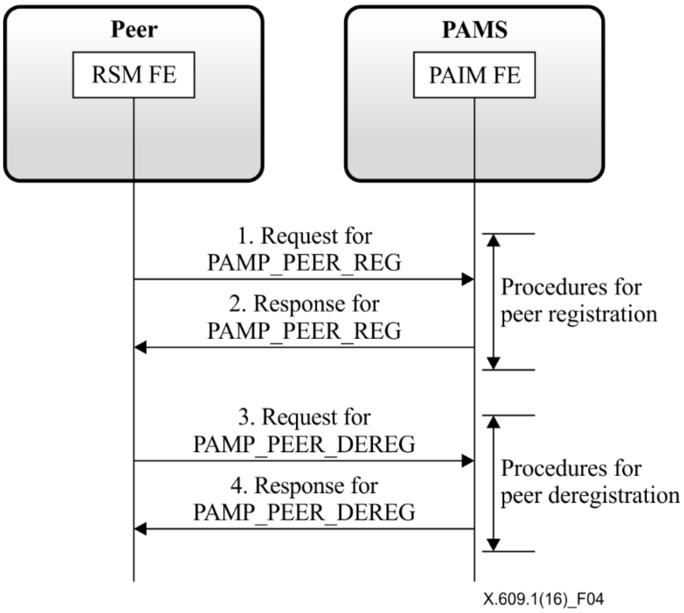

Peer
RSM FE
PAMS
PAIM FE
1. Request for PAMP_PEER_REG
2. Response for PAMP_PEER_REG
Procedures for peer registration
3. Request for PAMP_PEER_DEREG
4. Response for PAMP_PEER_DEREG
Procedures for peer deregistration
X.609.1(16)_F04

Figure 4 – Procedures for peer registration/deregistration

The peer can inform the PAMS of its departure from a specific overlay network through a peer deregistration request. Steps 3 and 4 of Figure 4 show the procedures for peer deregistration.

8.1.3 Peer status query

An OMS can query a PAMS about peer status information. It can request information about either a specific peer or list of peers participating in a specific overlay network. Figure 5 depicts the procedure for a peer status query.

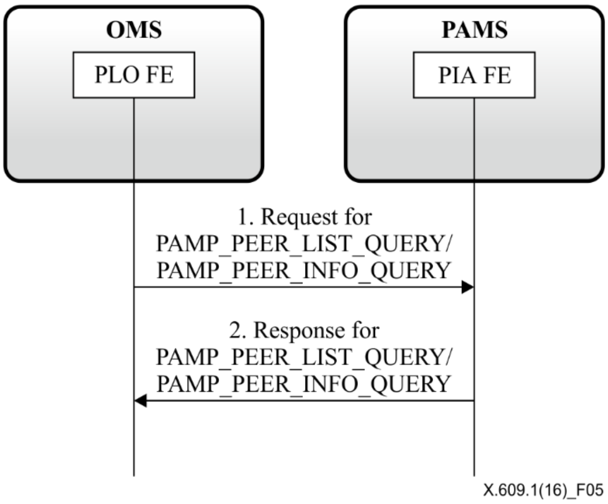

OMS
PLO FE
PAMS
PIA FE
1. Request for PAMP_PEER_LIST_QUERY/ PAMP_PEER_INFO_QUERY
2. Response for PAMP_PEER_LIST_QUERY/ PAMP_PEER_INFO_QUERY
X.609.1(16)_F05

Figure 5 – Procedures for peer status query

8.1.4 Peer status report

A peer reports its status information according to the reporting method from the PAMS during peer registration. The status information is classified into two types. Static status information indicates a profile of a peer that is configured when the peer is initiated. Dynamic status information indicates the peer activity information that is varied dynamically according to peer activity. Figure 6 shows the procedures for peer status reporting.

8.1.4.1 Static status information report

A peer reports static status information after a response during peer registration. A peer sends the PAMS a static status information report whenever its profile is modified.

8.1.4.2 Dynamic status information report

A peer reports dynamic status information report based on the reporting method received during peer registration. Figure 6 assumes that the PAMS requested a peer to report periodically in the reporting method.

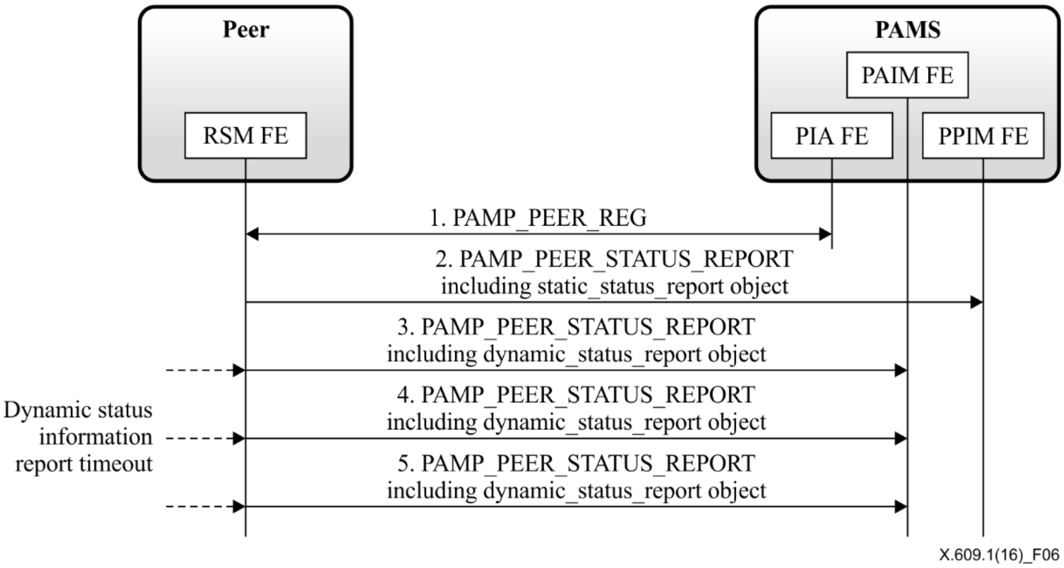

Peer
RSM FE
PAMS
PAIM FE
PIA FE
PPIM FE
1. PAMP_PEER_REG
2. PAMP_PEER_STATUS_REPORT
including static_status_report object
3. PAMP_PEER_STATUS_REPORT
including dynamic_status_report object
4. PAMP_PEER_STATUS_REPORT
including dynamic_status_report object
5. PAMP_PEER_STATUS_REPORT
including dynamic_status_report object
Dynamic status
information
report timeout
X.609.1(16)_F06

Figure 6 – Procedures for peer status reporting

8.2 Extended operations

This clause describes advanced operations utilizing the information stored in the PAMS.

8.2.1 PAMS discovery by DHT

An OMS may not have full knowledge of multiple PAMSs. A distributed hash table (DHT) can be used to discover appropriate PAMS. The procedures for PAMS discovery through DHT are shown in Figure 7.

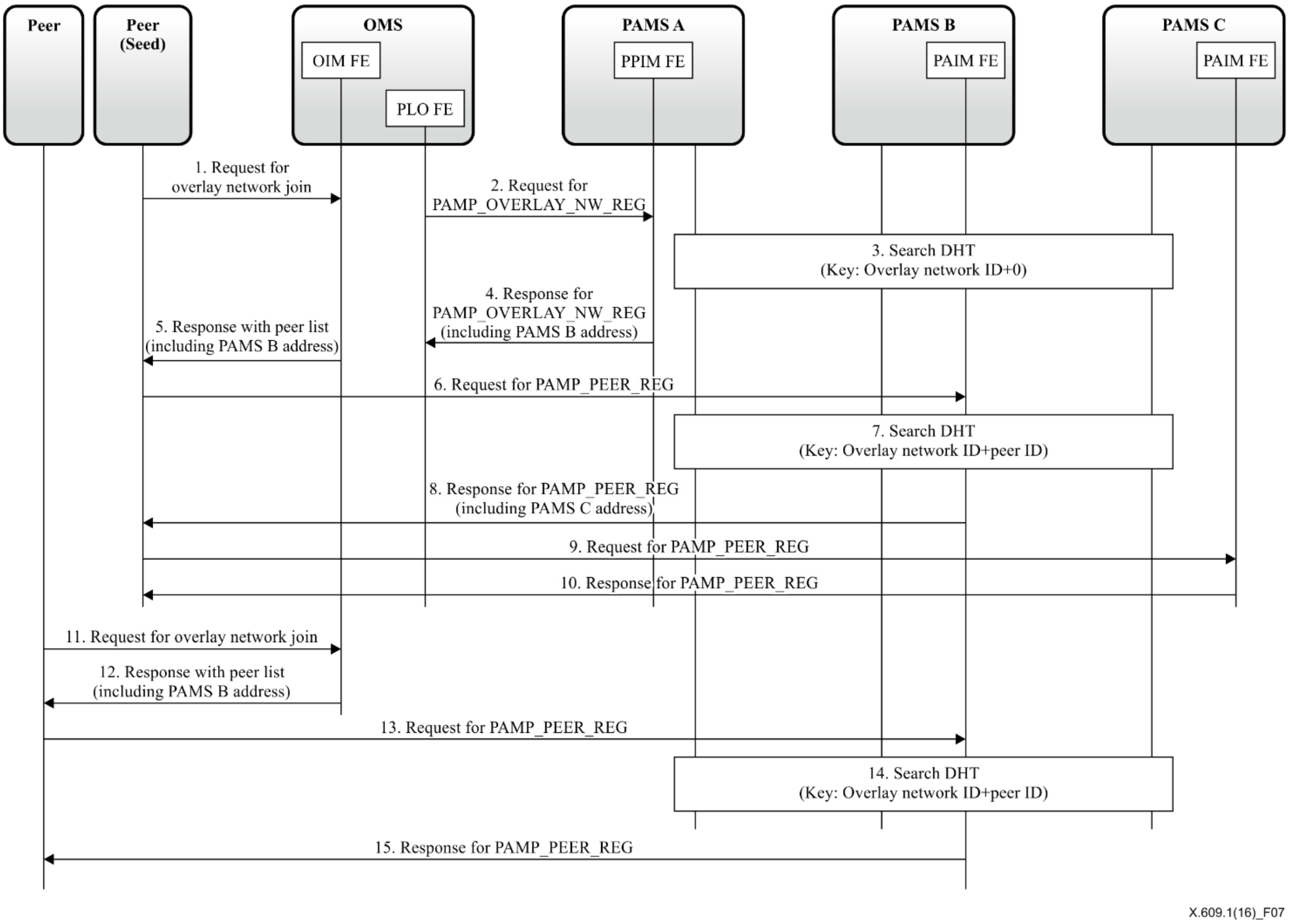

Peer
Peer (Seed)
OMS
OIM FE
PLO FE
PAMS A
PPIM FE
PAMS B
PAIM FE
PAMS C
PAIM FE
1. Request for overlay network join
2. Request for PAMP_OVERLAY_NW_REG
3. Search DHT (Key: Overlay network ID+0)
4. Response for PAMP_OVERLAY_NW_REG (including PAMS B address)
5. Response with peer list (including PAMS B address)
6. Request for PAMP_PEER_REG
7. Search DHT (Key: Overlay network ID+peer ID)
8. Response for PAMP_PEER_REG (including PAMS C address)
9. Request for PAMP_PEER_REG
10. Response for PAMP_PEER_REG
11. Request for overlay network join
12. Response with peer list (including PAMS B address)
13. Request for PAMP_PEER_REG
14. Search DHT (Key: Overlay network ID+peer ID)
15. Response for PAMP_PEER_REG
X.609.1(16)_F07

Figure 7 – Procedures for PAMS discovery through DHT

There can be more than one PAMS in an overlay network. Since a PAMS needs to constantly interact with peers in collecting peer activity information, a PAMS can be added or removed to/from a given overlay network in order to accommodate a large number of peers. However, multiple PAMSs will need to automatically distribute the workload of processing PAIM. This can be achieved by the use of a DHT. However, the detailed procedure for the interoperation of PAMSs is not part of the PAMP and is outside the scope of this Recommendation.

The procedure for PAMS discovery through DHT is as follows. As a peer establishes a new overlay network, an OMS needs information about the bootstrap PAMS. In Figure 7, it is assumed that the OMS is only aware of PAMS A, and the OMS requests information about bootstrap PAMS from PAMS A. The PAMSs interact to find the appropriate PAMS based on a key that is a combination of the overlay network ID and peer ID. In this case, since PAMS A does not have any information about the peer ID, the peer ID is set to "0", and PAMS B can be selected by matching the key in the DHT. As a result of the PAMS selection, the selected PAMS (i.e., PAMS B in Figure 7) generates a resource corresponding to the overlay network. PAMS A responds with the address of PAMS B, and the OMS communicates the address of PAMS B to the peer.

After these steps, every peer joining the overlay network will connect to PAMS B in the peer registration phase. If PAMS B is not the actual PAMS to manage the requesting peer, PAMS B finds the appropriate PAMS based on the DHT with the key comprised of the overlay network ID and peer ID. The address of the PAMS (i.e., PAMS C in Figure 7) will be notified through the response for PAMP_PEER_REG.

8.2.2 Complex query for peer list

When a peer has trouble in getting specific fragment(s), the peer can query an OMS for information about peers possessing such fragment(s). The OMS can interact with the PAMS to get the peer list that satisfies the peer's request. Based on the peer list in the response from the OMS, the peer can get the desired fragment(s). See Figure 8.

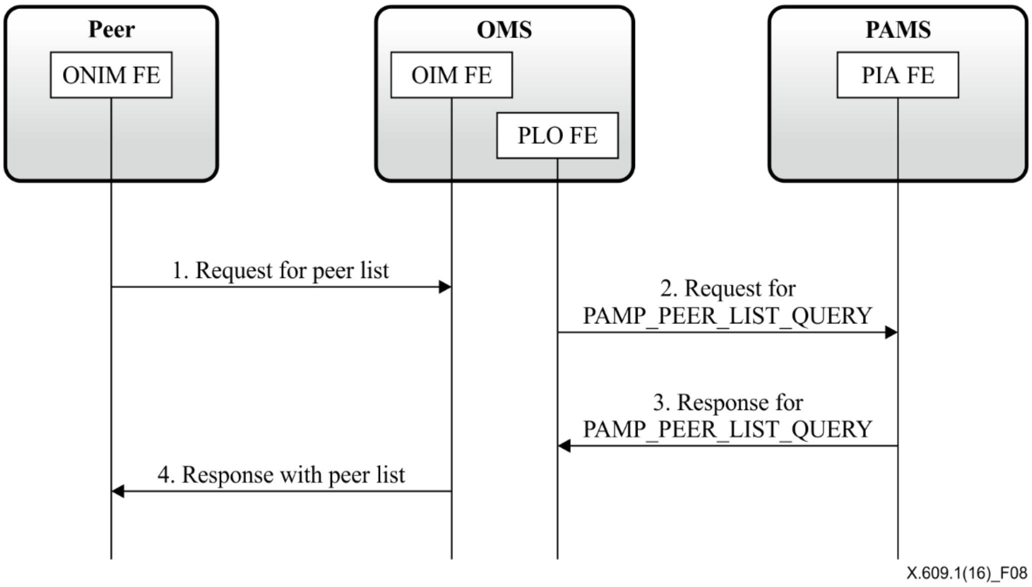

Peer
ONIM FE
OMS
OIM FE
PLO FE
PAMS
PIA FE
1. Request for peer list
2. Request for PAMP_PEER_LIST_QUERY
3. Response for PAMP_PEER_LIST_QUERY
4. Response with peer list
X.609.1(16)_F08

Figure 8 – Procedures for complex query of a peer list

1. A peer sends the OMS a request for the list of peers possessing the desired fragment(s). A list of fragments or range of fragments, including the fragment IDs of the first and the last fragments, are specified in the request for peer list.
2. Upon receiving such request, the OMS sends a message requesting a peer list meeting the criteria to the PAMS. The request can include overlay activity status, maximum number of peers to be responded to, etc.
3. Upon receiving the request from the OMS, the PAMS searches for peers meeting the criteria. The PAMS makes use of the collected peer activity information in order to find the appropriate peers. The PAMS selects the peer possessing the fragments meeting the criteria and responds to the OMS with the selected results.
4. The OMS responds to the peer with the obtained peer list. It is possible for the OMS to exclude a specific peer based on its policy.

8.2.3 Reorganizing overlay network to enhance service quality

A peer can experience low service quality even though it has enough resources to get better quality of service. In such a case, the peer activity information stored in the PAMS can be utilized to increase service quality. Figure 9 assumes that the peer is affected by from low performance, and that the PAMS is aware of this situation through analysis of the dynamic status information reports received.

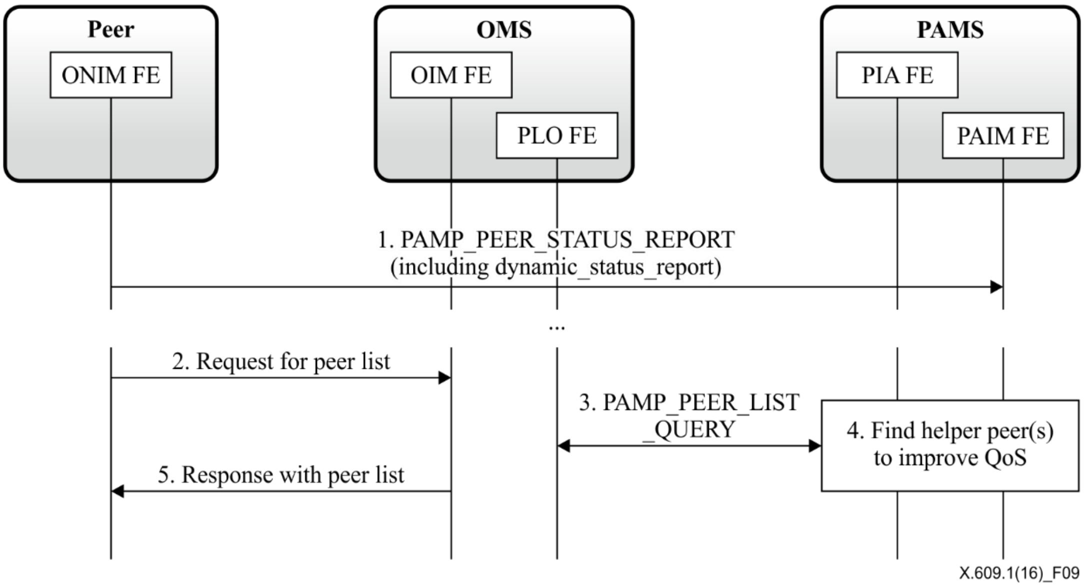


Figure 9 – Procedures for reorganizing an overlay network to enhance service quality

1. The peer periodically reports its activity status information.

2.-4. The peer can periodically request the OMS for the latest peer list. Upon receiving the request, the OMS requests the PAMS for an optimized peer list regarding the requesting peer. The PAMS detects that the requesting peer is affected by low service quality. For example, the PAMS can compare download the speed of the corresponding peer with the maximum download bandwidth. The download speed can be calculated from the amount of downloaded data and report period. The PAMS tries to find an appropriate peer(s) that can assist in improving service quality. For example, the PAMS can use both connection availability and upload availability; connection availability can be calculated from the maximum number of peer connections and the current number of peer connections, while upload availability can be calculated from the maximum upload capacity and current upload speed. The PAMS responds with the peer list containing the helper peer(s).

5. The OMS responds to the peer with the peer list containing helper peer(s). The peer will connect to the helper peers in the peer list received. Eventually, the service quality of the peer will be improved by the received fragment(s) from the helper peer(s).

NOTE – Steps 2. to 5. can be different in a push-based overlay network. In the push-based overlay network, the OMS can control helper peer(s) to send fragment(s) to the target peer.

8.2.4 Providing rarest fragment information in file distribution service

When contents are distributed as sliced fragments in an overlay network, it can become apparent that some fragments are not distributed well over the overlay network. Consequently, many peers are trying to find the peers possessing rare fragments. This may cause delay of completion of file download. Furthermore, the OMS does not provide peers with a list containing every peer, but only a subset. When a peer joins an overlay network, it starts to download sliced fragments with the peers in the peer list. Figure 10 shows an example of fragment distribution status of all peers compared to that of a subset of peers. As shown in the Figure 10, the distribution status of fragments can vary according to the peer list of the overlay network.

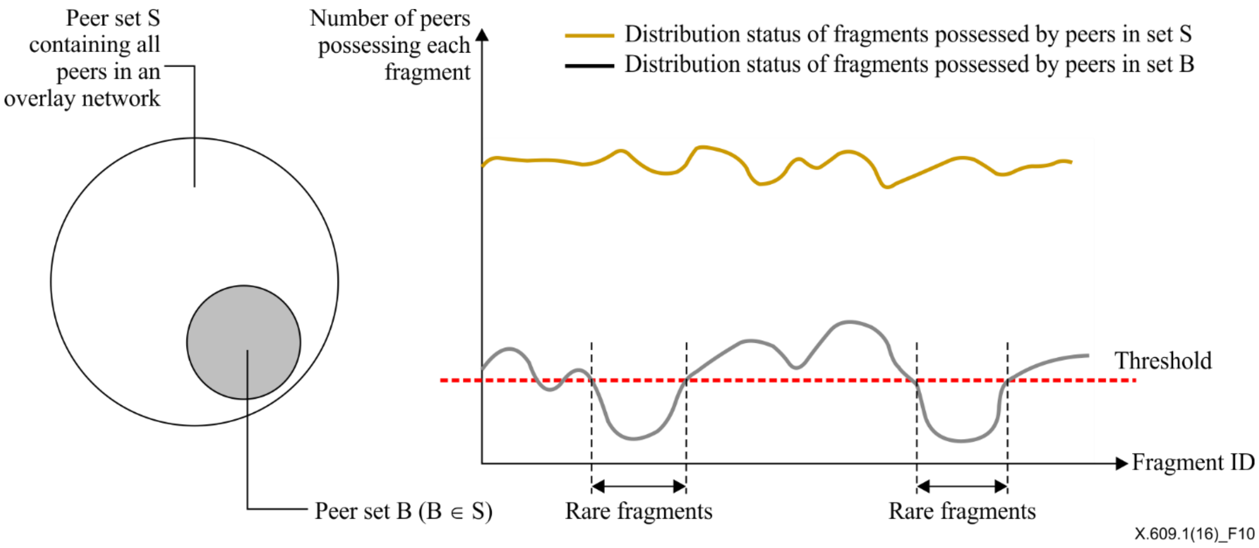


Figure 10 – Example of fragment distribution status for file distribution service

In the case of managed P2P communications, the OMS can analyse the distribution status of fragments, since the PAMS gathers fragment distribution report from peers. By using this information, it is possible to find rare fragments, and the OMS lets those fragments be distributed more actively. Consequently, the distribution performance of the overlay network can be enhanced.

Figure 11 shows a series of communications for providing a rarest fragment list when a peer requests the OMS to send the peer list of a specific overlay network. When a peer receives a peer list along with fragment information, it should request those rarest fragments that have higher priority. Through these procedures, the OMS can boost the distribution of rarest fragments to enhance overall performance. This feature can be used in emergency distribution, such as an urgent patch and emergency alert.

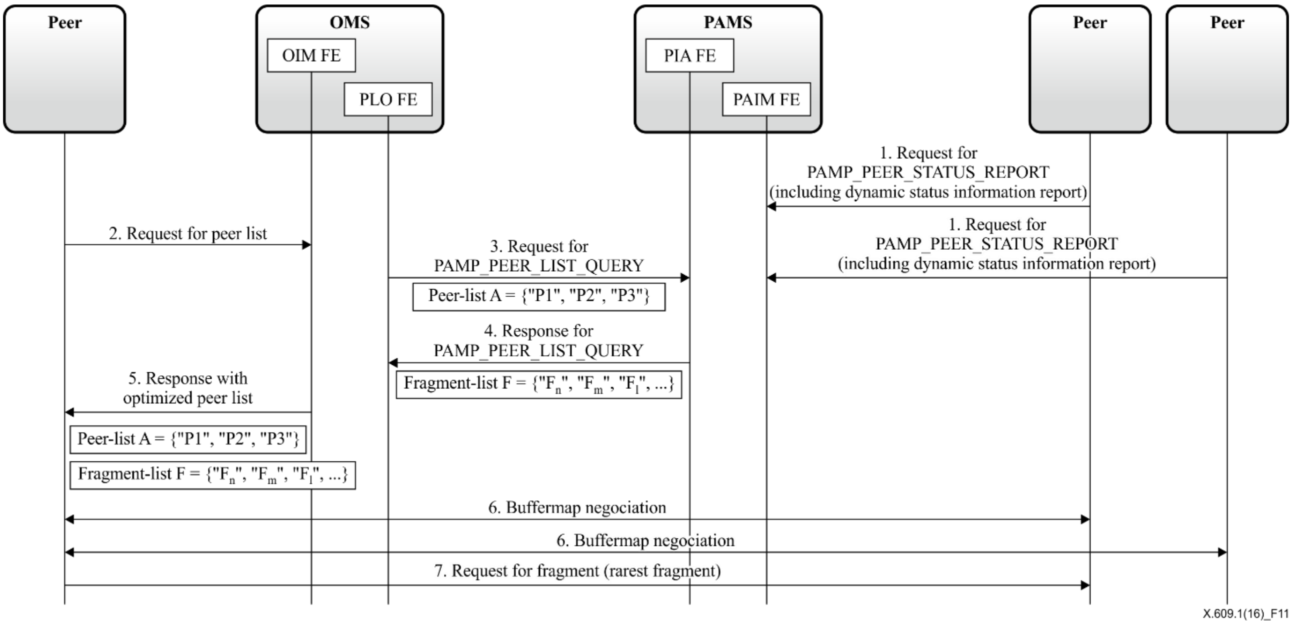

Peer
OMS
OIM FE
PLO FE
PAMS
PIA FE
PAIM FE
Peer
Peer
1. Request for PAMP_PEER_STATUS_REPORT (including dynamic status information report)
1. Request for PAMP_PEER_STATUS_REPORT (including dynamic status information report)
2. Request for peer list
3. Request for PAMP_PEER_LIST_QUERY
Peer-list A = {"P1", "P2", "P3"}
4. Response for PAMP_PEER_LIST_QUERY
Fragment-list F = {"F$_n$", "F$_m$", "F$_l$", ...}
5. Response with optimized peer list
Peer-list A = {"P1", "P2", "P3"}
Fragment-list F = {"F$_n$", "F$_m$", "F$_l$", ...}
6. Buffermap negociation
6. Buffermap negociation
7. Request for fragment (rarest fragment)
X.609.1(16)_F11

Figure 11 – Procedures for providing rarest fragment information

1. Each peer sends a dynamic status information report message to the PAMS on a fragment exchange event. PAMS can find the rarest fragments by analysing the aggregated fragment distribution information.

2. The peer requests a peer list from the OMS. This request is made when a peer joins the overlay network.

3. The OMS sends the PAMS a subset of the peer list and requests information about the rarest fragments that are possessed by the peers in the subset.

NOTE – The PAMS returns ID the list of fragments with a distribution rate less than the predefined threshold. These fragments are assumed to be the rarest. The threshold value changes according to the average fragment distribution rate.

4. The PAMS returns the information about the rarest fragments to the OMS.

5. The OMS returns the peer list along with the fragment information.

6. The peer connects to the peers in the peer list and exchanges a buffermap.

7. When the peer finds a peer that possesses fragment(s) included in the fragment list, it requests the corresponding peer to send that fragment(s) preferably.

8.2.5 Providing differentiated live streaming service

Different from P2P networking-based file distribution, overlay network for live streaming service has one or a small number of sources generating new fragments. To get the latest streaming data, every peer attempts to get the lasted fragments, thus old fragments are rarely exchanged by peers. Also, a starvation problem can occur in this process. Therefore, the OMS can provide a method for scattering peers based on user class, which makes it possible to provide a differentiated service. In MP2P communications, a user management server (UMS) maintains user information and the PAMS is aware of a peer in the overlay network. Figure 12 shows procedures for providing differentiated live streaming based on user class.

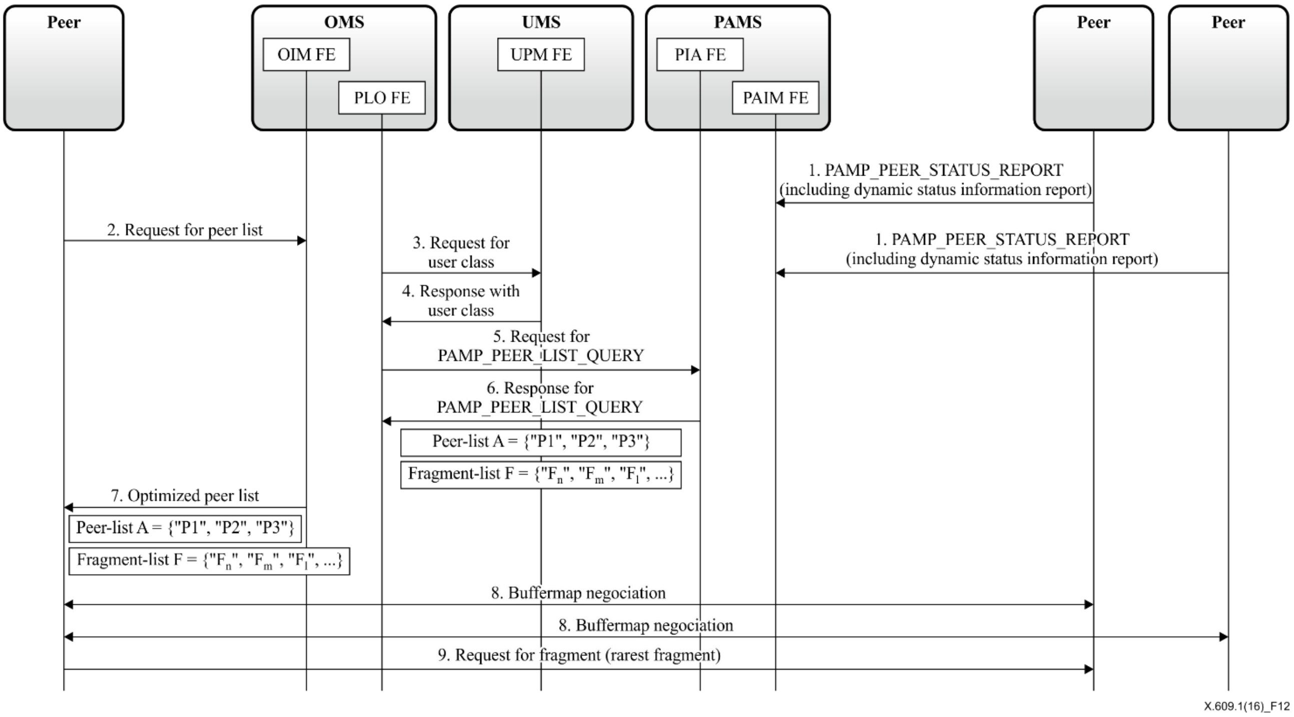

Peer
OMS
OIM FE
PLO FE
UMS
UPM FE
PAMS
PIA FE
PAIM FE
Peer
Peer
1. PAMP_PEER_STATUS_REPORT
(including dynamic status information report)
2. Request for peer list
3. Request for user class
1. PAMP_PEER_STATUS_REPORT
(including dynamic status information report)
4. Response with user class
5. Request for PAMP_PEER_LIST_QUERY
6. Response for PAMP_PEER_LIST_QUERY
Peer-list A = {"P1", "P2", "P3"}
Fragment-list F = {"F_n", "F_m", "F_l", ...}
7. Optimized peer list
Peer-list A = {"P1", "P2", "P3"}
Fragment-list F = {"F_n", "F_m", "F_l", ...}
8. Buffermap negociation
8. Buffermap negociation
9. Request for fragment (rarest fragment)
X.609.1(16)_F12

Figure 12 – Procedures for differentiated streaming service

1. Each peer sends a dynamic status information report message to report of fragment exchanges to the PAMS. The PAMS is aware of fragment distribution status by analysing aggregated fragment distribution information.

2. A peer requests the OMS to send a peer list along with its peer ID.

3. An OMS requests a UMS for class information about the user corresponding to the peer ID. It is assumed that the UMS knows the relationship between the peer ID and user ID.

4. The UMS returns class information.

5. The OMS requests an appropriate fragment list and peer list from the PAMS. In this step, the OMS can provide the PAMS with the subset of peers participating in the overlay network. If not, the PAMS determines the appropriate subset of peers based on its own policy.

6. The PAMS returns an optimized fragment list and peer list for the live streaming service.

NOTE 1 – In an overlay network for streaming, the optimized lists should be made in accordance with the characteristics of the overlay network. Therefore, an OMS needs to register each overlay network with its characteristics on a PAMS for this feature.

NOTE 2 – The PAMS can make use of user class, fragment distribution status, peer list, content-type (e.g., file and stream) to generate an optimized fragment list.

7. The OMS responds to the requesting peer with the peer list and fragment list received from the PAMS.

8. The peer exchanges a buffermap with other peers.

9. When the peer finds a peer possessing fragments(s) included in the fragment list given by the OMS, it requests that peer to send such fragment(s).

8.2.6 Providing peer activity report using digital signature

It is possible for malicious users to forge the activity report, which can lead to corruption of the information gathered in the PAMS. In order to prevent this, a digital signature can be used to guarantee the reliability of reported information. Figure 13 shows a procedure for peer activity reporting using a digital signature. It is assumed that peers and servers have their own asymmetric digital signature using a private key and a public key.

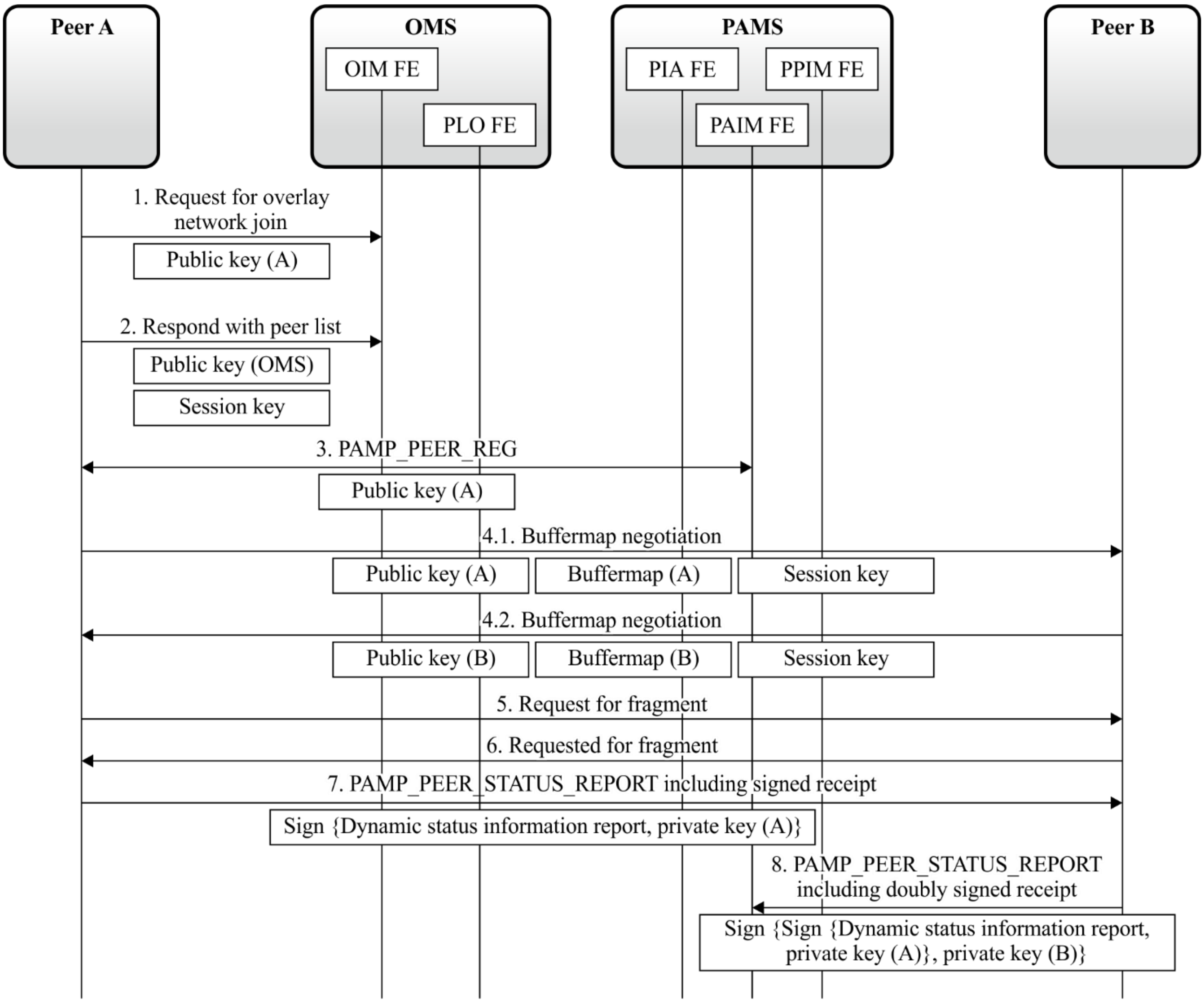

Peer A
OMS
OIM FE
PLO FE
PAMS
PIA FE
PPIM FE
PAIM FE
Peer B
1. Request for overlay network join
Public key (A)
2. Respond with peer list
Public key (OMS)
Session key
3. PAMP_PEER_REG
Public key (A)
4.1. Buffermap negotiation
Public key (A)
Buffermap (A)
Session key
4.2. Buffermap negotiation
Public key (B)
Buffermap (B)
Session key
5. Request for fragment
6. Requested for fragment
7. PAMP_PEER_STATUS_REPORT including signed receipt
Sign {Dynamic status information report, private key (A)}
8. PAMP_PEER_STATUS_REPORT including doubly signed receipt
Sign {Sign {Dynamic status information report, private key (A)}, private key (B)}
X.609.1(16)_F13

Figure 13 – Procedures for peer status report using digital signatures

1. When peer A joins a specific overlay network by interaction with an OMS, it includes its public key in the request message.

2. The OMS returns a peer list with its public key and session key for the overlay network. The session key will be used to check the validation of the session and it is signed with the private key of the service provider to prohibit modifications.

3. After joining the overlay network, the peer informs the PAMS of its peer registration. The request message includes the public key of the peer. The PAMS stores the public key of the peer.

4) Peer A and peer B exchange a buffermap when exchanging their own public keys and session keys. The session key is used to verify whether the peer has valid access rights to the session. The public key is used to verify whether the message with receipt is received from the corresponding peer. The peer manages its own public key and that of the other peer.

5) Peer A requests peer B to send a fragment.

6) Peer B sends the requested fragment to peer A.

7) When peer A receives the requested fragment from peer B, Peer A sends a receipt message to peer B. This receipt message is signed with peer A's private key, and it can be verified by peer B by use of the public key of peer A.

NOTE 1 – If peer A requests other fragments without sending receipt messages, peer B can stop further transmission.

NOTE 2 – If peer B does not receive the receipt message from peer A, peer B can disconnect the connection.

8) If the receipt message received is verified, the RSM FE of peer B signs it with its private key, and sends the confirmed receipt message to the PAMS.

NOTE 3 – When the PAMS receives the confirmed receipt message, it verifies it by use of the public keys of the peers.

9 Messages

This clause describes the format of PAMP messages. For extensibility, PAMP adopts representational state transfer (REST) architecture, and messages are encoded in JavaScript object notation (JSON) [b-IETF RFC 7159].

9.1 Resource element type

This clause provides the format of resource element types used in this Recommendation. A PAMP message consists of one or more resource elements. The grammar used in representing an object defined in this Recommendation is as follows.

- "STRING", "BOOLEAN", and "NUMBER" types are used to indicate string, boolean and number, respectively;
- An array of collective values is enclosed in brackets "[ ]" with values separated by a comma ",";
- Selective options are separated by a vertical bar " | ".

9.1.1 Peer activity management configuration information element

Peer activity management (PAM) configuration information provides the configuration information about PAM. A PAM configuration information element is defined as follows.

```
Object {
   BOOLEAN    pam_enabled;
   STRING           pams_url;
   NUMBER    report_interval;
} pam_conf_info
```

The description of the attributes is as follows.

- *pam_enabled* indicates whether a PAM function is enabled. If the value is set to *true*, the PAM function is enabled;
- *pams_url* is a URL of a PAMS. pam_url is used to indicate the location of the PAMS;
- *report_interval* is a periodic interval in seconds for reporting a dynamic status by the peer.

9.1.2 Overlay network information element

An overlay network information element provides identification information about the overlay network.

The overlay network information element is defined as follows.

```
Object {
   STRING    overlay_network_id;
   STRING     content_type = "FILE"
                   | "STREAM"
                   | other;
```

```
        } overlay_network_information;
```

The description of the attributes is as follows.

– *overlay_network_id* is an ID of the overlay network;

– *content_type* is the type of content shared in the overlay network. The value is set to "FILE", if the overlay network is used to distribute one or more files. The value is set to "STREAM", if the overlay network is used to stream multimedia content. For other purposes, any other string value can be used.

9.1.3 Peer information element

A peer information element provides information about a peer. A peer information element is defined as follows.

```
        Object {
           STRING    peer_id;
           STRING    type = "PEER"
                    |"CS"
                    |"RS"
                    |other;
           STRING    delegation_id;
        } peer_information
```

The description of the attributes is as follows:

– *peer_id* is an ID of a peer;

– *type* indicates the type of peer identified by the value set in *peer_id*. The value is set to "PEER", if the node identified by the value set in *peer_id* is a peer. The value is set to "CS", if the node identified by the value set in *peer_id* is a virtual peer of a CS. The value is set to "RS", if the node identified by the value set in *peer_id* is RS. The value can be set to other values for further extension;

– *delegation_id* is an ID of a peer that delegates a CS to distribute or download content for a given reason.

9.1.4 Fragment event element

A fragment event element provides event information about a fragment. An event means a single event of uploading or downloading a fragment. The fragment event element is defined as follows.

```
        Object {
           STRING        fragment_event_type = "UPLOADED"
                              | "DOWNLOADED";
           STRING        fragment_id;
           BOOLEAN       fragment_integrity;
           STRING        to;
           STRING        from;
        } fragment_event
```

The description of the attributes is as follows.

– *fragment_event_type* indicates the type of event regarding the fragment;

– *fragment_id* is an ID of the fragment;

– *fragment_integrity* indicates the result of an integrity check of the fragment. The value is set to *true*, if the integrity check is passed;

- *to* is the ID of the peer supposed to receive the fragment;
- *from* is the ID of the peer that sent the fragment.

9.1.5 Fragment list element

A fragment list element provides information about fragments. The fragment list element is defined as follows.

```
Object {
   NUMBER  num_of_fragment;
   NUMBER  fragment_size;
   NUMBER   [fragment];
} fragment_list
```

The description of the attributes is as follows.

- *num_of_fragment* indicates the total number of fragments organizing the content shared in an overlay network;
- *fragment_size* indicates the size of the fragment in kilobytes;
- *fragment* is an ID of a fragment.

A fragment_list element can include a list of fragment IDs.

9.1.6 Fragment range element

A fragment range element provides information about a range of fragments. The fragment range element is defined as follows.

```
Object {
   NUMBER   start_fragment_id;
   NUMBER   end_fragment_id;
} fragment_range
```

The description of the attributes is as follows.

- *start_fragment_id* is an ID of the first fragment in the range of fragments;
- *end_fragment_id* is an ID of the last fragment in the range of fragments.

9.1.7 Peer query condition element

A peer query condition element provides information about the condition for querying one or more peers. A peer query condition element is defined as follows.

```
Object {
   STRING   overlay_status = "COMPLETED"
                  |"STARTED";
   NUMBER    max_peer_num;
   STRING   ordering = "UPLOADED"
               | "DOWNLOADED";
               | "LEFT";
STRING  [peer_id];
NUMBER  service_class;
fragment_ list   fragment_list;
fragment_range   fragment_range;
} peer_ query _condition
```

The description of the attributes is as follows.

– *overlay_status* indicates the status of a peer with respect to overlay network participation;

– *max_peer_num* is the maximum number of peers to be responded to;

– *ordering* indicates ordering criteria;

– *peer_id* is an ID of a peer. The listed peers will be ordered according to the value of the ordering attribute;

– *service_class* indicates the service class of a peer;

– *fragment_list* is an object of a fragment_list element;

– *fragment_range* is an object of a fragment_range element.

9.1.8 Peer list element

A peer list element provides information about peers and fragments. A peer list element is defined as follows.

```
    Object {
       STRING   [peer_id];
       fragment_list    fragment_list;
       fragment_range    fragment_range;
    } peer_list
```

The description of the attributes is as follows.

– *peer_id* is an ID of a peer. The array contains an ordered list of peer IDs;

– *fragment_list* is an object of a fragment_list element;

– *fragment_range* is an object of a fragment_range element.

9.1.9 Dynamic status element

A dynamic status element provides information about dynamic status. A dynamic status element is defined as follows.

```
    Object {
       STRING    overlay_event = "STARTED"
                        |"STOPPED"
                        |"COMPLETED";
       STRING          uploaded;
       STRING          downloaded;
       STRING          left;
       fragment_event    [fragment-event];
       fragment_list fragment_list;
       fragment_range fragment_range;
       NUMBER      num_upload_connection;
       NUMBER      num_download_connection;
    } dynamic_status;
```

The description of the attributes is as follows

– *overlay_event* indicates the status of overlay network participation. The value is set to "COMPLETED", if the reporting peer has received entire shared files. The value is set to "STOPPED", if the reporting peer pauses data exchange with other peers. Otherwise, the value is set to "STARTED", after the reporting peer participates in an overlay network;

- *uploaded* is the amount of uploaded data in kilobytes after the previous dynamic status is reported;
- *downloaded* is the amount of downloaded data in kilobytes after the previous dynamic status is reported;
- *left* is the amount of data supposed to be downloaded in kilobytes;
- *fragment_event* is an object of a fragment_event element. A fragment_event contains the events that occurred after the previous dynamic status is reported;
- *fragment_list* is an object of a fragment_list element. The list of fragments possessed by a peer will be reported;
- *num_upload_connection* is the number of allowable connections for uploading;
- *num_download_connection* is the number of allowable connections for downloading.

9.1.10 Static status element

A static status element provides the information about static status. Static status element is defined as follows.

```
Object {
   NUMBER    max_up_bw;
   NUMBER    max_dn_bw;
   NUMBER    max_up_bw_per_net;
   NUMBER    max_dn_bw_per_net;
   NUMBER    max_num_conn_for_up;
   NUMBER    max_num_conn_for_up_per_net;
   NUMBER    max_num_active_net;
} static_status;
```

The description of the attributes is as follows.

- *max_up_bw* is the maximum bandwidth for an uploading fragment in kilobytes;
- *max_dn_bw* is the maximum bandwidth for a downloading fragment in kilobytes;
- *max_up_bw_per_net* is the maximum upload bandwidth for each overlay network in kilobytes;
- *max_dn_bw_per_net* is the maximum download bandwidth for each overlay network in kilobytes;
- *max_num_conn_for_up* is the maximum number of connections for uploading;
- *max_num_conn_for_dn* is the maximum number of connections for downloading.

9.1.11 Peer status element

A peer status element provides information about peer status. A peer status element is defined as follows.

```
Object {
   dynamic_status dynamic_status;
   static_status static_status;
} peer_status;
```

The description of the attributes is as follows.

- *dynamic_status* is an object of a dynamic_status element;
- *static_status* is an object of a static_status element.

9.2 Message format

This clause provides the format of messages for operations explained in clause 8. All operations have request and response messages.

9.2.1 PAMP_OVERLAY_NW_REG

PAMP_OVERLAY_NW_REG is initiated by an OMS to register a new overlay network on a PAMS.

9.2.1.1 Request

The request message format for PAMP_OVERLAY_NW_REG is shown in Table 1.

Table 1 – Request message format for PAMP_OVERLAY_NW_REG

Method	POST
URI	http://{PAMS_ADDRESS}[a]/pams/
Body	overlay_network_information (refer to clause 9.1.2)
[a] {PAMS_ADDRESS} refers to the fully qualified domain name (FQDN) address of the PAMS	

An example of a hypertext transfer protocol (HTTP) request message for PAMP_OVERLAY_NW_REG is as follows.

```
POST /pams/ HTTP/1.1
Host: www.exampleaddress.com
Content-Length: 122
Content-Type: application/json
Accept: application/json
{
   "overlay_network_information" : {
        "overlay_network_id" : "12ekd4kd8",
        "content_type" : "FILE"
   }
}
```

9.2.1.2 Response

The response for PAMP_OVERLAY_NW_REG has response code to indicate the result. Table 2 lists response codes and semantics for PAMP_OVERLAY_NW_REG. This Recommendation follows [IETF RFC 7231] for other response codes.

Table 2 – Response code for PAMP_OVERLAY_NW_REG

Response code and semantics		Body
200	OK The request is accepted and registration is done	pam_conf_info (refer to clause 9.1.1)
401	Unauthorized The request requires user authentication. The OMS may repeat the request with a suitable authorization in the HTTP header	Not applicable (N/A)
406	Conflict The request is denied because an overlay network with the same ID is already registered	N/A

An example of an HTTP response message for PAMP_OVERLAY_NW_REG is as follows.

```
HTTP/1.1 200 OK
Content-Length: 118
Content-Type: application/json
Connection: Closed
{
   "pam_conf" : {
       "pam_enabled" : true,
       "pam_url" : "http://www.examplepams.com/pams/",
       "report_interval" : 10
   }
}
```

9.2.2 PAMP_OVERLAY_NW_DEREG

PAMP_OVERLAY_NW_DEREG is initiated by an OMS to remove a registered overlay network from a PAMS.

9.2.2.1 Request

The request message format for PAMP_OVERLAY_NW_DEREG is shown in Table 3. The request does not include any data in the message body.

Table 3 – Request message format for PAMP_OVERLAY_NW_DEREG

Method	DELETE
URL	http://{PAMS_ADDRESS}[a)]/pams/{NID}[b)]/
Body	N/A

[a)] {PAMS_ADDRESS} refers to the FQDN address of the PAMS.

[b)] {NID} refers to the ID of the overlay network to be deleted.

9.2.2.2 Response

The response for PAMP_OVERLAY_NW_DEREG has response code to indicate the result. Table 4 lists response codes and semantics for PAMP_OVERLAY_NW_DEREG. The response does not include any data in the message body. This Recommendation follows [IETF RFC 7231] for other response codes.

Table 4 – Response code for PAMP_OVERLAY_NW_DEREG

Response code and semantics		Body
200	OK The request is accepted and deregistration is done	N/A
401	Unauthorized The request requires user authentication. The OMS may repeat the request with a suitable authorization in the HTTP header	N/A
404	Not Found The request is denied because there is no responding overlay network with the requested ID	N/A

9.2.3 PAMP_PEER_REG

PAMP_PEER_REG is initiated by a peer after it successfully joins an overlay network.

9.2.3.1 Request

The request message format for PAMP_PEER_REG is shown in Table 5.

Table 5 – Request message format for PAMP_PEER_REG

Method	POST
URI	http://{PAMS_ADDRESS}[a)]/pams/{NID}[b)]/peer/
Body	peer_information (refer to clause 9.1.3)

[a)] {PAMS_ADDRESS} refers to the FQDN address of the PAMS.

[b)] {NID} refers to the ID of the overlay network to be deleted.

An example of an HTTP request message for PAMP_PEER_REG is as follows.

```
POST /pams/12ekd4kd8/peer/ HTTP/1.1
Host: www.exampleaddress.com
Content-Length: 117
```

```
Content-Type: application/json
Accept: application/json
{
   "peer_information" : {
      "peer_id" : "8djdhd",
      "type" : "PEER"
   }
}
```

9.2.3.2 Response

The response for PAMP_PEER_REG has response code to indicate the result. Table 6 lists response codes and semantics for peer network registration. This Recommendation follows [IETF RFC 7231] for other response codes.

Table 6 – Response code for PAMP_PEER_REG

Response code and semantics		Body
200	OK The request is accepted and registration is done	pam_conf_info[a] (refer to clause 9.1.1)
404	Not Found The request is denied because there is no responding overlay network with the requested ID	N/A
409	Conflict The request is denied because an overlay network with the same ID is already registered	N/A

[a] When the PAMS responds for peer registration, it does not set a *pam_enabled* object in *pam_conf_info*.

An example of an HTTP response message for PAMP_PEER_REG is as follows.

```
HTTP/1.1 200 OK
Content-Length: 118
Content-Type: application/json
{
   "pam_conf_info" : {
      "pams_url" : "http://www.examplepams.com/pams/",
      "report_interval" : 10
   }
}
```

9.2.4 PAMP_PEER_DEREG

PAMP_PEER_DEREG is initiated by a peer to remove itself from a PAMS.

9.2.4.1 Request

The request message format for PAMP_PEER_DEREG is shown in Table 7. The request does not include any data in the message body.

Table 7 – Message format for PAMP_PEER_DEREG request

Method	DELETE
URL	http://{PAMS_ADDRESS}[a]/pams/{NID}[b]/peers/{PID}[c]
Body	N/A
[a] {PAMS_ADDRESS} refers to the FQDN address of the PAMS. [b] {NID} refers to the ID of the overlay network to be deleted. [c] {PID} refers to the ID of the peer to be deleted.	

9.2.4.2 Response

The response for PAMP_PEER_DEREG has response code to indicate the result. Table 8 lists response codes and semantics for peer deregistration. The response does not include any data in the message body. This Recommendation follows [IETF RFC 7231] for other response codes.

Table 8 – Response code for PAMP_PEER_DEREG

Response code and semantics		**Body**
200	OK The request is accepted and deregistration is done	N/A
401	Unauthorized The request requires user authentication. The PAMS may repeat the request itself with a suitable authorization in the HTTP header	N/A
404	Not Found The request is denied because there is no responding peer with the requested ID	N/A

9.2.5 PAMP_PEER_STATUS_REPORT

A peer sends two types of report. A dynamic status information report includes status information as a result of peer activity and is reported according to the period received when the peer registers itself on a PAMS. A static status information report includes profile information for peer activity and is assembled after peer registration or after a change in a peer profile.

9.2.5.1 Request

The request can include both a dynamic and a static status report. For example, the first request after peer registration includes both reports and then the peer can send a request including a dynamic status report for each period. The request message format for PAMP_PEER_STATUS_REPORT is shown in Table 9.

Table 9 – Request message format for PAMP_PEER_STATUS_REPORT

Method	PUT
URI	http://{PAMS_ADDRESS}[a)]/pams/{NID}[b)]/peer/{PID}[c)]/
Body	peer_status (refer to clause 9.1.11)
[a)] {PAMS_ADDRESS} refers to the FQDN address of the PAMS. [b)] {NID} refers to the ID of the overlay network to be deleted. [c)] {PID} refers to the ID of the peer sending the report.	

An example of an HTTP request message for PAMP_PEER_STATUS_REPORT is as follows.

```
PUT /pams/18374u/peer/8djdhd HTTP/1.1
Host: www.exampleaddress.com
Content-Length: 797
Content-Type: application/json
Accept: application/json
{
   "peer_status " : {
      "dynamic_status": {
         "overlay_event": "STARTED",
         "uploaded":10000,
         "downloaded":50000,
         "left":50000,
         "fragment_event" : [
            {
              "fragment_event_type": "UPLOADED",
              "fragment_id":"12345",
              "fragment_integrity":true,
              "to":"8djd18"
            },{
              "fragment_event_type": "UPLOADED",
              "fragment_id":"12346",
              "fragment_integrity":true,
              "to":"8djd18"
            }],
         "num_upload_connection":10,
         "num_download_connection":10
      },
      "static_status": {
         "max_up_bw":1000,
         "max_dn_bw":5000,
         "max_up_bw_per_net":100,
         "max_dn_bw_per_net":500,
         "max_num_conn_for_up":50,
         "max_num_conn_for_up_per_net":50,
                "max_num_active_net":20
            }
        }
    }
```

9.2.5.2 Response

The response for PAMP_PEER_STATUS_REPORT has response code to indicate the result. Table 10 lists response codes and semantics for PAMP_PEER_STATUS_REPORT. The response does not include any data in the message body. This Recommendation follows [IETF RFC 7231] for other response codes.

Table 10 – Response code for PAMP_PEER_STATUS_REPORT

Response code and semantics		Body
200	OK The report has succeeded	N/A
404	Not Found The request is denied because there is no corresponding peer/overlay network	N/A

9.2.6 PAMP_PEER_LIST_QUERY

PAMP_PEER_LIST_QUERY is initiated by an OMS to retrieve a peer list from a PAMS.

9.2.6.1 Request

The request message format for PAMP_PEER_LIST_QUERY is shown in Table 11.

Table 11 – Request message format for PAMP_PEER_LIST_QUERY

Method	GET
URI	http://{PAMS_ADDRESS}[a)]/pams/{NID}[b)]/peer
Body	peer_query_condition (refer to clause 9.1.7)[c)]

[a)] {PAMS_ADDRESS} refers to the FQDN address of the PAMS.

[b)] {NID} refers to the ID of the overlay network to be deleted.

[c)] When an OMS queries a peer list, *num_of_fragment* and *fragment_size* in a *fragment_list* object are not set.

An example of an HTTP request message for PAMP_PEER_LIST_QUERY is as follows.

```
GET /pams/1283jdd/peer HTTP/1.1
Host: www.exampleaddress.com
Content-Length: 461
Content-Type: application/json
Accept: application/json
{
   "peer_query_condition" : {
       "overlay_status" : "COMPLETED",
       "max_peer_num" : 10 ,
       "ordering" : "UPLOADED",
       "peer_id": ["8djd18", "8djd20"],
       "service_class": 1,
       "fragment_list" : {
            "fragment" : [100, 102]
        },
        "fragment_range":
        {
             "start_fragment_id":0,
             "end_fragment_id":99
        }
   }
}
```

9.2.6.2 Response

The response for PAMP_PEER_LIST_QUERY has response code to indicate the result. Table 12 lists response codes and semantics for PAMP_PEER_LIST_QUERY. This Recommendation follows [IETF RFC 7231] for other response codes.

Table 12 – Response code for PAMP_PEER_LIST_QUERY

Response code and semantics		Body
200	OK The request has succeeded and this response contains a peer list	peer_list (refer to clause 9.1.8)
401	Unauthorized The request requires user authentication. The peer may repeat the request with a suitable authorization in the HTTP header	N/A
409	Conflict The request is denied because there is no corresponding overlay network with the requested ID	N/A

An example of an HTTP response message for PAMP_PEER_LIST_QUERY is as follows.

```
HTTP/1.1 200 OK
Content-Length: 255
Content-Type: application/json

"peer_list" : {
   "peers" :  ["peerd", "peerb", "peerc"],
   "fragment_list" : {
       "num_of_fragment": 3,
       "fragment_size": 100,
       "fragment" : [101,105,108]
    },
    "fragment_range" : {
           "start_fragment_id": 1,
           "end_fragment_id": 99
    }
}
```

9.2.7 PAMP_PEER_INFO_QUERY

PAMP_PEER_INFO_QUERY is initiated by an OMS to retrieve peer information from a PAMS.

9.2.7.1 Request

The request message format for PAMP_PEER_INFO_QUERY is shown in Table 13. The request does not include any data in the message body.

Table 13 – Message format for PAMP_PEER_INFO_QUERY

Method	GET
URL	http://{PAMS_ADDRESS}[a)]/pams/{NID}[b)]/peers/{PID}[c)]
Body	N/A

[a)] {PAMS_ADDRESS} refers to the FQDN address of the PAMS.

[b)] {NID} refers to the ID of the overlay network to be deleted.

[c)] {PID} refers to the ID of the peer sending the report.

9.2.7.2 Response

The response for PAMP_PEER_INFO_QUERY has response code to indicate the result. Table 14 lists response codes and semantics for PAMP_PEER_INFO_QUERY. This Recommendation follows [IETF RFC 7231] for other response codes.

Table 14 – Response code for PAMP_PEER_INFO_QUERY

Response code and semantics		Body
200	OK The request is succeeded and response contains peer list	peer_status [a)] (refer to clause 9.1.11)
401	Unauthorized The request requires user authentication. The peer may repeat the request with a suitable authorization in the HTTP header	N/A
409	Conflict The request is denied because there is no responding peer with the requested ID	N/A

[a)] When a PAMS responds to a peer information query, a *fragment_event* object of the *dynamic_report* object is not set

An example of an HTTP response message for PAMP_PEER_INFO_QUERY is as follows.

```
HTTP/1.1 200 OK
Content-Length: 658
Content-Type: application/json
{
   "peer_status " : {
      "dynamic_status": {
          "overlay_event": "STARTED",
          "uploaded":10000,
          "downloaded":50000,
          "left":50000,
          "fragment_list" : {
            "num_of_fragment": 3,
            "fragment_size": 100,
            "fragment" : [101,105,108]
          },
         "fragment_range" : {
             "start_fragment_id":0,
             "end_fragment_id":99
          },
          "num_upload_connection":10,
          "num_download_connection":10
      },
      "static_status": {
          "max_up_bw":1000,
          "max_dn_bw":5000,
          "max_up_bw_per_net":100,
          "max_dn_bw_per_net":500,
          "max_num_conn_for_up":50,
          "max_num_conn_for_up_per_net":50,
          "max_num_active_net":20
      }
   }
}
```

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.2012]	Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation 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.*
[b-IETF RFC 7159]	IETF RFC 7159 (2014), *The JavaScript Object Notation (JSON) Data Interchange Format*.

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	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	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 and next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016