P2P Streaming Protocol (PPSP) Requirements
draft-ietf-ppsp-reqs-05

Abstract

The objective of the PPSP work is to standardize the key signaling protocols that apply to tracker and peers in a Peer-to-Peer (P2P) streaming system. These protocols are called PPSP. This document enumerates the requirements for the PPSP, which should be considered when designing PPSP.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 10, 2012.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal
Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.
Table of Contents

1. Introduction .............................................. 4
2. Terminology ............................................. 4
3. Overview of PPSP .......................................... 5
4. PPSP Requirements ......................................... 6
   4.1. Basic Requirements ................................. 6
   4.2. PPSP Tracker Protocol Requirements ............. 8
   4.3. PPSP Peer Protocol Requirements ................ 9
5. Security Considerations ................................. 11
6. IANA Considerations ..................................... 12
7. Acknowledgements ........................................ 12
8. References ............................................... 12
   8.1. Normative References .............................. 12
   8.2. Informative References ......................... 12
Authors’ Addresses .......................................... 13
1. Introduction

Peer to Peer (P2P) computing has been successfully used in many fields, from one-to-one communication like Voice over IP (VoIP) and Instance Messaging (IM), to one-to-many communication like streaming, file sharing and gaming. In the streaming area, the popularity of P2P real-time and video on demand (VoD) streaming technology has been demonstrated by PPLive [PPLive], PPStream [PPStream], UUSee [UUSee], Pando [Pando] etc. Take PPLive for example, it has over 5 million online users at the same time for real-time streaming. P2P streaming applications account for more and more Internet traffic. According to statistics in a major Chinese Internet Service Provider (ISP), the traffic generated by P2P streaming applications exceeded 50% of the total backbone traffic during peak time in 2008 [I-D.ietf-ppsp-problem-statement].

Given the increasing integration of P2P streaming into the global content delivery infrastructure, the lack of an open, standard P2P streaming protocol has become a major missing component in the Internet protocol stack. Multiple similar but proprietary P2P streaming protocols result in repetitious development efforts and lock-in effects. More importantly, it leads to substantial difficulties when integrating P2P streaming as a component of a global content delivery infrastructure. For example, proprietary P2P streaming protocols do not integrate well with infrastructure devices such as caches and other edge devices [I-D.ietf-ppsp-problem-statement].

The objective of the PPSP work is to standardize the key signaling protocols that apply to tracker and peers in a P2P streaming system. These protocols are called PPSP. PPSP will serve as an enabling technology, building on the development experiences of existing P2P streaming systems. Its design will allow it to integrate with IETF efforts on distributed resource location, traffic localization, and streaming control mechanisms. It allows effective integration with edge infrastructures such as cache and mobile edge equipment [I-D.ietf-ppsp-problem-statement].

This document enumerates the requirements for the PPSP, which should be considered when designing PPSP.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119] and indicate requirement levels for compliant implementations.
This document uses the following PPSP-related terms, which are defined in [I-D.ietf-ppsp-problem-statement], including:

Chunk, Live streaming, Peer/PPSP peer, PPSP, Swarm, Tracker/PPSP tracker, Video-on-demand (VoD).

Furthermore, the following additional terms will be used:

Peer list: A list of peers which are in a same swarm maintained by the tracker. A peer can fetch the peer list of a swarm from either tracker or other peers to know which peers have the required streaming content.

Peer ID: An identifier of a peer such that other peers or tracker can refer the ID for the peer.

Swarm ID: An identifier of a swarm containing a group of peers sharing a same streaming content.

Chunk ID: An identifier of a chunk in a streaming content.

3. Overview of PPSP

As described in [I-D.ietf-ppsp-problem-statement], the following components are considered in the scope of PPSP:

1) Tracker communication. Tracker communication is a component that enables each peer to get peer list from the tracker and/or provide content availability to the tracker.

2) Peer communication. Peer communication is a component that enables each peer to exchange content availability and request content from other peers.

3) Report. Report is a component that enables peers to report streaming status to the tracker. The information may include swarm IDs to show swarms that the peer is taking active part in, chunk list for each swarm to show the current content availability in the peer, inbound/outbound traffic capacity, amount of neighbor peers, peer health degree, total amount of bytes uploaded/downloaded to neighbour peers, and other streaming parameters.

Therefore, PPSP includes the PPSP tracker protocol - a signaling protocol between PPSP trackers and PPSP peers, and the PPSP peer protocol - a signaling protocol among PPSP peers.

PPSP tracker protocol will define:
1) Standard format/encoding of information between PPSP peers and PPSP tracker. Some of this exchanged information may be explicitly marked as optional. Exchanged information may include peer list, swarm ID, chunk information, content availability, streaming status including online time, link status, node capability and other streaming parameters.

2) Standard messages between PPSP peers and PPSP trackers defining how PPSP peers report streaming status and request to PPSP trackers, as well as how PPSP trackers reply to the requests.

PPSP peer protocol will define:

1) Standard format/encoding of information among PPSP peers, such as chunk description.

2) Standard messages among PPSP peers defining how PPSP peers advertise chunk availability to each other, as well as the signaling for requesting the chunks among PPSP peers.

This document itemizes requirements for the following aspects of PPSP:

1) Basic requirements to PPSP protocols (peer and tracker protocols), entities (peer and tracker), streaming content, and QoS issues.

2) General requirements to the tracker protocol.

3) General requirements to the peer protocol.

4) Security requirements.

4. PPSP Requirements

4.1. Basic Requirements

PPSP.REQ-1: The tracker and the peer protocols SHOULD be as similar as possible, in terms of design, message formats and flows.

It is desirable that the peer protocol would be an extension to the tracker protocol by adding a few message types, or vice versa.

PPSP.REQ-2: The tracker protocol and the peer protocol SHOULD enable peers to receive streaming content within the required time constraints, i.e., fulfill streaming feature.

PPSP.REQ-3: Each peer MUST have a unique ID (i.e. peer ID) in a
swarm.

It’s a basic requirement for a peer to be uniquely identified in a swarm that other peers or tracker can refer to the peer by ID.

PPSP.REQ-4: The streaming content MUST be uniquely identified by a swarm ID.

A swarm refers to a group of peers sharing the same streaming content. A swarm ID uniquely identifies a swarm. The swarm ID can be used in two cases: 1) a peer requests the tracker for the peer list indexed by a swarm ID; 2) a peer tells the tracker about the swarms it belongs to.

PPSP.REQ-5: The streaming content MUST allow to be partitioned into chunks.

A key characteristic of P2P streaming system is allowing the data fetching from different peers concurrently. Therefore, the whole streaming content must allow to be partitioned into small pieces or chunks for transmission between peers.

PPSP.REQ-6: Each chunk MUST have an unique ID (i.e. chunk ID) in the swarm.

Each chunk must have an unique ID in the swarm such as the peer can understand which chunks are stored in which peers and which chunks are requested by other peers. An example for generating the chunk ID is the buffer map approach [I-D.ietf-ppsp-survey].

PPSP.REQ-7: The tracker protocol and peer protocol are Recommended to be carried over TCP (or UDP, when delivery requirements cannot be met by TCP).

PPSP.REQ-8: The tracker and peer protocol together MUST facilitate acceptable QoS (e.g. low startup delay, low channel/content switching time and minimal end-to-end delay) for both on-demand and live streaming, even for very popular content. The tracker and peer protocol do not include the algorithm required for scalable streaming. However, the tracker and peer protocol SHALL NOT restrict or place limits on any such algorithm.

There are basic QoS requirements for streaming system. Setup time to receive a new streaming channel or to switch between channels should be reasonable small. End to end delay (time between content generation, e.g. camera and content consumption, e.g. user side monitor) will become critical in case of live streaming. Especially in provisioning of sports events, end to end delay of 1 minute and
more are not acceptable.

For instance, the tracker and peer protocols can support carrying QoS related parameters (e.g. video quality, delay requirements) together with the priorities of these parameters, and QoS situation (e.g. performance, available uplink bandwidth) of content providing peers.

There are also some other possible mechanisms, e.g. addition of super peers, in-network storage, request of alternative peer addresses, and the usage of QoS information for an advanced peer selection.

4.2. PPSP Tracker Protocol Requirements

The tracker protocol defines how the peers report and request information to/from the tracker and how the tracker replies to the requests. The tracker discovery and the possible communication between trackers are out of the scope of tracker protocol.

PPSP.TP.REQ-1: The tracker MUST implement the tracker protocol for receiving queries and periodical peer status reports/updates from the peers and for sending the corresponding replies.

PPSP.TP.REQ-2: The peer MUST implement the tracker protocol for sending queries and periodical peer status reports/updates to the tracker and receiving the corresponding replies.

PPSP.TP.REQ-3: The tracker request message MUST allow the requesting peer to solicit the peer list from the tracker with respect to a specific swarm ID.

The tracker request message may also include the requesting peer’s preference parameter, e.g. preferred number of peers in the peer list, or preferred downloading bandwidth. The track will then be able to select an appropriate set of peers for the requesting peer according to the preference.

PPSP.TP.REQ-4: The tracker reply message MUST allow the tracker to offer the peer list to the requesting peer with respect of a specific swarm ID.

PPSP.TP.REQ-5: The tracker SHOULD support generating the peer list with the help of traffic optimization services, e.g. ALTO [I-D.ietf-alto-protocol].

PPSP.TP.REQ-6: The peer status report/update MUST have the ability to inform the tracker about the peer’s activity in the swarm.

PPSP.TP.REQ-7: The chunk availability information of the peer SHOULD
be reported to tracker when tracker needs such information to steer peer selection. The chunk information MUST at least contain the chunk ID.

PPSP.TP.REQ-8: The chunk availability information between peer and tracker MUST be as expressed as compactly as possible.

The peers may report CHUNK AVAILABILITY DIGEST information (i.e. compact expression of chunk availability) to the tracker when possible to decrease the bandwidth consumption for messages in bandwidth constraint environment like mobile network. For example, if a peer has a bitmap like 11111...1(100 continuous 1)xxx..., the 100 continuous "1" can be expressed by one byte with seven bits representing 100 and one bit representing "1". In this example, 100-8=92 bits are saved. Considering the frequency of exchange of CHUNK AVAILABILITY and the fact that many bitmaps have quite a long length of continuous "1" or "0", such compression makes sense.

PPSP.TP.REQ-9: The status of the peer SHOULD be reported to the tracker when tracker needs such information to steer peer selection.

For example, peer status can be online time, physical link status including DSL/WIFI/etc, battery status, processing capability, and other capabilities of the peer. Therefore, the tracker is able to select better candidate peers for streaming.

4.3. PPSP Peer Protocol Requirements

The peer protocol defines how the peers advertise streaming content availability and exchange status with each other. The peer protocol also defines the requests and responses of the chunks among the peers. The first task for this WG will be to decide which signaling and media transfer protocols will be used. The WG will consider existing protocols and, if needed, identify potential extensions to these protocols.

PPSP.PP.REQ-1: The streaming content availability request message MUST allow the peer to solicit the chunk information from other peers in the peer list. The chunk information MUST at least contain the chunk ID. This chunk availability information MUST NOT be passed on to other peer, unless validated (e.g. prevent hearsay and DoS).

PPSP.PP.REQ-2: The streaming content availability reply message MUST allow the peer to offer the information of the chunks in its content buffer. The chunk information MUST at least contain the chunk ID.

PPSP.PP.REQ-3: The streaming content availability request message SHOULD allow the peer to solicit an additional list of peers to that
received from the tracker - with the same swarm ID. The reply
message MUST contain swarm-membership information of the peers that
have explicitly indicated they are part of the swarm, verifiable by
the receiver. This additional list of peers MUST only contain peers
which have been checked to be valid and online recently (e.g. prevent
hearsay and DoS).

It is possible that a peer may need additional peers for certain
streaming content. Therefore, it is allowed that the peer
communicates with the peers in the current peer list to obtain an
additional list of peers in the same swarm.

PPSP.PP.REQ-4: Streaming content availability update message among
the peers MUST be supported by peer protocol. In the push based
model, where peers advocate their own chunk availability proactively,
the content availability request message described in PP.REQ-1 is not
needed. The peer protocol MUST implement either pull-based, push-
based or both.

Due to the dynamic change of the buffered streaming content in each
peer and the frequent join/leave of peers in the swarm, the streaming
content availability among a peer’s neighbours (i.e. the peers known
to a peer by getting the peer lists from either tracker or peers)
always changes and thus requires being updated on time. This update
should be done at least on demand. For example, when a peer requires
finding more peers with certain chunks, it sends a message to some
other peers in the swarm for streaming content availability update.
Alternatively, each peer in the swarm can advertise its streaming
content availability to some other peers periodically. However, the
detailed mechanisms for this update such as how far to spread such
update message, how often to send this update message, etc should
leave to peer algorithms, rather than protocol concerns.

PPSP.PP.REQ-5: The chunk availability information between peers MUST
be as expressed as compactly as possible.

In PP.REQ-1/2/4, the peers may exchange CHUNK AVAILABILITY DIGEST
information (i.e. compact expression of chunk availability) to with
other peers when possible to decrease the bandwidth consumption for
messages in bandwidth constraint environment like mobile network.

PPSP.PP.REQ-6: The peer status report/update SHOULD be advertised
among the peers to reflect the status of the peer.

Peer status information should be advertised among the peers via the
peer status report/update message. For example, peer status can be
online time, physical link status including DSL/WIFI/etc, battery
status, processing capability, and other capabilities of the peer.
With this information, a peer can select more appropriate peers for streaming.

PPSP.PP.REQ-7: The peers MUST implement the peer protocol for chunk data (not availability information) requests and responses among the peers before the streaming content is transmitted.

5. Security Considerations

The scope of this section is to analyze the security threats and provide the requirements for PPSP.

PPSP.SEC.REQ-1: PPSP MUST support closed swarms, where the peers are authenticated.

This ensures that only the authenticated users can access the original media in the P2P streaming system. This can be achieved by security mechanisms such as user authentication and/or key management scheme.

PPSP.SEC.REQ-2: Confidentiality of the streaming content in PPSP SHOULD be supported and the corresponding key management scheme SHOULD scale well in P2P streaming system.

PPSP.SEC.REQ-3: PPSP MUST provide an option to encrypt the data exchange among the PPSP entities.

PPSP.SEC.REQ-4: PPSP MUST have mechanisms to limit potential damage caused by malfunctioning and badly behaving peers in the P2P streaming system.

Such an attack will degrade the quality of the rendered media at the receiver. For example, in a P2P live video streaming system a polluter can introduce corrupted chunks. Each receiver integrates into its playback stream the polluted chunks it receives from its other neighbors. Since the peers forwards chunks to other peers, the polluted content can potentially spread through much of the P2P streaming network.

PPSP.SEC.REQ-5: PPSP SHOULD support identifying badly behaving peers, and exclude or reject them from the P2P streaming system.

PPSP.SEC.REQ-6: PPSP MUST prevent peers from DoS attacks which will exhaust the P2P streaming system’s available resource.

Given the prevalence of DoS attacks in the Internet, it is important to realize that a similar threat could exist in a large-scale
streaming system where attackers are capable of consuming a lot of resources with just a small amount of effort.

PPSP.SEC.REQ-7: PPSP SHOULD be robust, i.e., when centralized tracker fails the P2P streaming system SHOULD still work by supporting distributed trackers.

PPSP.SEC.REQ-8: Existing P2P security mechanisms SHOULD be re-used as much as possible in PPSP, to avoid developing new security mechanisms.

PPSP.SEC.REQ-9: Integrity of the streaming content in PPSP MUST be supported to provide a peer with the possibility to identify inauthentic media content (undesirable modified by other entities rather than its genuine source). The corresponding checksum distribution and verification scheme SHOULD scale well in P2P streaming system and be robust against distrustful trackers/peers.

6. IANA Considerations

This document presently raises no IANA considerations.

7. Acknowledgements

The authors would like to thank many people for discussing P2P streaming. We would particularly like to thank: Yingjie Gu, Haibin Song, Xingfeng Jiang from Huawei, Hui Zhang, Jan Seedorf, Martin Stiemerling from NEC Labs, Jun Lei from University of Goettingen, James Seng from PPLive, Das Saumitra from Qualcomm, Christian Schmidt from NSN, Akbar Rahman from Interdigital, Lingli Deng from China Mobile, Johan Pouwelse, Arno Bakker and Wesley Eddy.

8. References

8.1. Normative References


8.2. Informative References

[PPLive] "www.pplive.com".

[PPStream] "www.ppstream.com".
Authors’ Addresses

Ning Zong (editor)
Huawei Technologies
Huawei Base, No.101 Software Avenue, Nanjing, China

Phone: +86 25 56624760
Email: zongning@huawei.com

Yunfei Zhang
China Mobile Communication Corporation

Phone: +86 13601032119
Email: zhangyunfei@chinamobile.com

Victor Pascual
Acme Packet
Anabel Segura 10, Madrid 28108, Spain

Email: VPascual@acmepacket.com