PPSP
Internet-Draft
Intended status: Informational
Expires: November 15, 2013

Y. Zhang
Unaffiliated
N. Zong
Huawei Technologies

May 14, 2013

Problem Statement and Requirements of Peer-to-Peer Streaming Protocol (PPSP)
draft-ietf-ppsp-problem-statement-15

Abstract

Peer-to-Peer(P2P for short) streaming systems show more and more popularity in current Internet with proprietary protocols. This document identifies problems of the proprietary protocols, proposes the development of Peer to Peer Streaming Protocol(PPSP) including the tracker and peer protocol, and discusses the scope, requirements and use cases of 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 November 15, 2013.

Table of Contents

1. Introduction

1.1. Backgrounds

Streaming traffic is among the largest and fastest growing traffic on the Internet [Cisco], where peer-to-peer (P2P) streaming contributes substantially. With the advantage of high scalability and fault tolerance against single point of failure, P2P streaming applications are able to distribute large-scale, live and video on demand (VoD) streaming programs to a large audience with only a handful of servers. What's more, along with the players like CDN providers joining in the effort of using P2P technologies in distributing their serving streaming content, there are more and more various players in P2P streaming ecosystem.

Given the increasing integration of P2P streaming into the global content delivery infrastructure, the lack of an open, standard P2P streaming signaling protocol suite becomes a major missing component. Almost all of existing systems use their proprietary protocols. Multiple, similar but proprietary protocols result in repetitious development efforts for new systems, and the lock-in effects lead to substantial difficulties in their integration with other players like CDN. For example, in the enhancement of existing caches and CDN systems to support P2P streaming, proprietary protocols may increase the complexity of the interaction with different P2P streaming applications.

In this document we propose the development of an open P2P Streaming Protocol, which is abbreviated as PPSP, to standardize signaling operations in P2P streaming systems to solve the above problems.

1.2. Requirements Language

The key words "MUST" and "MUST NOT" in this document are to be interpreted as described in RFC 2119 [RFC2119] and indicate requirement levels for compliant implementations.

2. Terminology and concepts

CHUNK: A CHUNK is a basic unit of data organized in P2P streaming for storage, scheduling, advertisement and exchange among peers [VoD]. A CHUNK size varies from several KBs to several MBs in different systems. In case of MBs size CHUNK scenario, a sub-CHUNK structure named piece is often defined to fit in a single transmitted packet. A streaming system may use different granularities for different usage, e.g., using CHUNKs during data exchange, and using a larger unit such as a set of CHUNKs during advertisement.

CHUNK ID: The identifier of a CHUNK in a content stream.

CLIENT: A CLIENT refers to a participant in a P2P streaming system that only receives streaming content. In some cases, a node not having enough computing and storage capabilities will act as a CLIENT. Such node can be viewed as a specific type of PEER.

CONTENT DISTRIBUTION NETWORK (CDN): A CDN is a collection of nodes that are deployed, in general, at the network edge like Points of Presence (POP) or Data Centers (DC) and that store content provided by the original content servers. Typically, CDN nodes serve content to the users located nearby topologically.

LIVE STREAMING: It refers to a scenario where all the audiences receive streaming content for the same ongoing event. It is desired that the lags between the play points of the audiences and streaming source be small.

P2P CACHE: A P2P CACHE refers to a network entity that caches P2P traffic in the network and, either transparently or explicitly, streams content to other PEERs.

PEER: A PEER refers to a participant in a P2P streaming system that not only receives streaming content, but also caches and streams streaming content to other participants.

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 the TRACKER or from other PEERs in order to know which PEERs have the required streaming content.

PEER ID: The identifier of a PEER such that other PEERs, or the TRACKER, can refer to the PEER by using its ID.

PPSP: The abbreviation of Peer-to-Peer Streaming Protocols. PPSP refer to the primary signaling protocols among various P2P streaming system components, including the TRACKER and the PEER.

TRACKER: A TRACKER refers to a directory service that maintains a list of PEERs participating in a specific audio/video channel or in the distribution of a streaming file. Also, the TRACKER answers PEER LIST queries received from PEERs. The TRACKER is a logical component which can be centralized or distributed.

VIDEO-ON-DEMAND (VoD): It refers to a scenario where different audiences may watch different parts of the same recorded streaming with downloaded content.

SWARM: A SWARM refers to a group of PEERs who exchange data to distribute CHUNKs of the same content (e.g. video/audio program, digital file, etc.) at a given time.

SWARM ID: The identifier of a SWARM containing a group of PEERs sharing a common streaming content.

SUPER-NODE: A SUPER-NODE is a special kind of PEER deployed by ISPs. This kind of PEER is more stable with higher computing, storage and bandwidth capabilities than normal PEERs.

3. Problem statement

The problems caused by proprietary protocols for P2P streaming applications are listed as follows.

3.1. Heterogeneous P2P traffic and P2P cache deployment

ISPs are faced with different P2P streaming application introducing substantial traffic into their infrastructure, including their backbone and their exchange/interconnection points. P2P caches are used by ISPs in order to locally store content and hence reduce the P2P traffic. P2P caches usually operate at the chunk or file granularity.

However, unlike web traffic that is represented by HTTP requests and responses and therefore allows any caching device to be served (as long as it supports HTTP), P2P traffic is originated by multiple P2P applications which require the ISPs to deploy different type of caches for the different types of P2P streams.

This increases both engineering and operational costs dramatically.

3.2. QoS issue and CDN deployment

P2P streaming is often criticized due to its worse QoS performance compared to client/server streaming (e.g., longer startup delay, longer seek delay and channel switch delay). Hybrid CDN/P2P is a good approach in order to address this problem [Hybrid CDN P2P].

In order to form the hybrid P2P+CDN architecture, the CDN must be aware of the specific P2P streaming protocol in the collaboration. Similarly to what is described in section 3.1, proprietary P2P protocols introduce complexity and deployment cost of CDN.

3.3. Extended applicability in mobile and wireless environment

Mobility and wireless are becoming increasingly important in today's Internet, where streaming service is a major usage. It's reported that the average volume of video traffic on mobile networks has risen up to 50% in the early of 2012 [ByteMobile]. There are multiple prior studies exploring P2P streaming in mobile and wireless networks [Mobile Streaming1] [Mobile Streaming2].

However it's difficult to directly apply current P2P streaming protocols (even assuming we can re-use some of the proprietary ones) in mobile and wireless networks.

Following are some illustrative problems:

First, P2P streaming assumes a stable Internet connection in downlink and uplink direction, with decent capacity and peers that can run for hours. This isn't the typical setting for mobile terminals. Usually the connections are unstable and expensive in terms of energy consumption and transmission (especially in uplink direction). To enable mobile/wireless P2P streaming feasible, trackers may need more information on peers like packet loss rate, peer battery status and processing capability during peer selection compared to fixed peers. Unfortunately current protocols don't convey this kind of information.

Second, current practices often use a "bitmap" message in order to exchange chunk availability. The message is of kilobytes in size and exchanged frequently, e.g., an interval of several seconds or less. In a mobile environment with scarce bandwidth, the message size may need to be shortened or it may require more efficient methods for expressing and distributing chunk availability information, which is different from wire-line P2P streaming.

Third, for a resource constraint peer like mobile handsets or set-top boxes (STB), there are severe contentions on limited resource when using proprietary protocols. The terminal has to install different streaming client software for different usages, e.g., some for movies and others for sports. Each of these applications will compete for the same set of resources even when it is sometimes running in background mode. PPSP can alleviate this problem with the basic idea that the "one common client software with PPSP and different scheduling plug-ins" is better than "different client software running at the same time" in memory and disk consumption.

4. Tasks of PPSP: Standard peer to peer streaming protocols

PPSP is targeted to standardize signaling protocols to solve the above problems that support either live or VoD streaming. PPSP

supports both centralized tracker and distributed trackers. In distributed trackers, the tracker functionality is distributed in decentralized peers. In the following part of this section, the tracker is a logic conception, which can be implemented in a dedicated tracker server or in peers.

The PPSP design includes a signaling protocol between trackers and peers (the PPSP "tracker protocol") and a signaling protocol among the peers (the PPSP "peer protocol") as shown in Figure 1. The two protocols enable peers to receive streaming content within the time constraints.

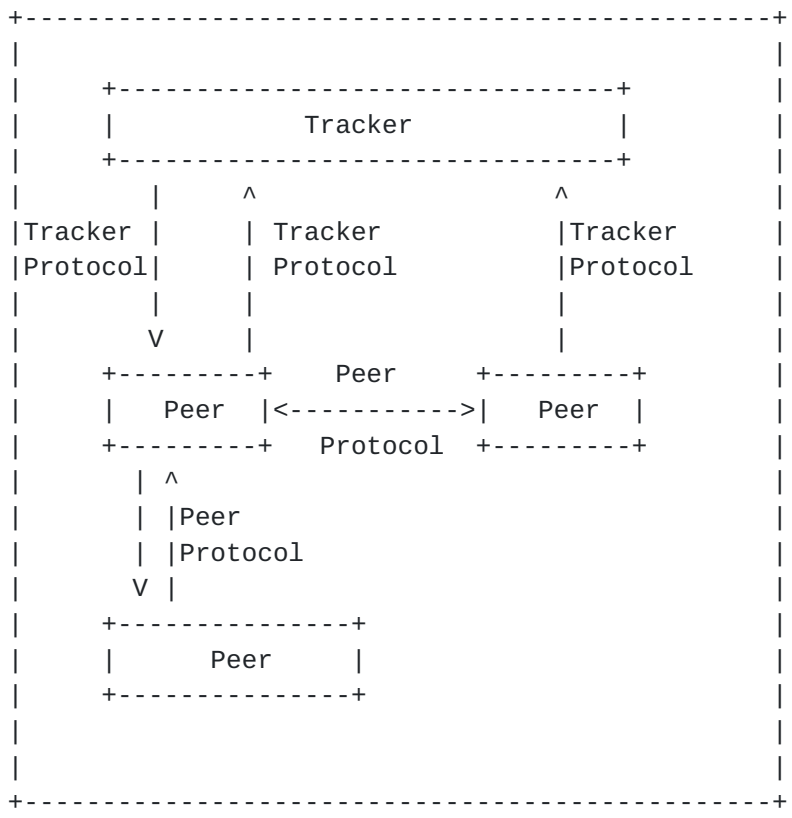


Figure 1 PPSP System Architecture

PPSP design in general needs to solve the following challenges, e.g.

1) When joining a swarm, how does a peer know which peers it should contact for content?

2) After knowing a set of peers, how does a peer contact with these peers? In which manner?

3) How to choose peers with better service capabilities, and how to collect such information from peers?

4) How to improve the efficiency of the communication, e.g. compact on-the-wire message format and suitable underlying transport mechanism (UDP or TCP)?

5) How to improve the robustness of the system using PPSP, e.g. when the tracker fails? How to make the tracker protocol and the peer protocol loose coupled?

4.1. Tasks and design issues of Tracker protocol

The tracker protocol handles the initial and periodic exchange of meta-information between trackers and peers, such as peer list and content information.

Therefore tracker protocol is best modeled as a request/response protocol between peers and trackers, and will carry information needed for the selection of peers suitable for real-time/VoD streaming.

Special tasks for the design of the tracker protocol are listed as follows. This is a high-level task-list. The detailed requirements on the design of the tracker protocol are explicated in section 6.

1) How should a peer be globally identified? This is related to the peer ID definition, but irrelevant to how the peer ID is generated.

2) How to identify different peers, e.g. peers with public or private IP address, peers behind or not behind NAT, peers with IPV4 or IPV6 addresses, peers with different property?

3) The tracker protocol must be light-weight, since a tracker may need to server large amount of peers. This is related to the encoding issue (e.g., Binary based or Text based) and keep-alive mechanism.

4) How can the tracker be able to report optimized peer list to serve a particular content. This is related to status statistic, with which the tracker can be aware of peer status and content status.

PPSP tracker protocol will consider all these issues in the design according to the requirements from both peer and tracker perspective and also taking into consideration deployment and operation perspectives.

4.2. Tasks and design issues of Peer protocol

The peer protocol controls the advertising and exchange of content between the peers.

Therefore peer protocol is modeled as a gossip-like protocol with periodic exchanges of neighbor and chunk availability information.

Special tasks for the design of the peer protocol are listed as follows. This is a high-level task-list. The detailed requirements on the design of the peer protocol are explicated in section 6.

1) How does the certain content be globally identified and verified? Since the content can be retrieved from everywhere, how to ensure the exchanged content between the peers is authentic?

2) How to identify the chunk availability in the certain content? This is related to the chunk addressing and chunk state maintenance. Considering the large amount of chunks in the certain content, light-weight expression is necessary.

3) How to ensure the peer protocol efficiency? As we mentioned in section 3, the chunk availability information exchange is quite frequent. How to balance the information exchange size and amount is a big challenge. What kind of encoding and underlying transport mechanism (UDP or TCP) is used in the messages?

PPSP peer protocol will consider all the above issues in the design according to the requirements from the peer perspective.

5. Use cases of PPSP

This section is not the to-do list for the WG, but for the explanatory effect to show how PPSP could be used in practice.

5.1. Worldwide provision of live/VoD streaming

The content provider can increase live streaming coverage by introducing PPSP in between different providers. This is quite similar to the case described in CDNI [RFC6707][RFC6770].

We suppose a scenario that there is only provider A (e.g., in China) providing the live streaming service in provider B (e.g., in USA) and C (e.g., in Europe)'s coverage. Without PPSP, when a user(e.g. a Chinese American) in USA requests the program to the tracker (which is located in A's coverage), the tracker may generally return to the user with a peer list including most of peers in China, because generally most users are in China and there are only few users in USA. This may affect the user experience. But if we can use the PPSP tracker protocol to involve B and C in the cooperative

provision, as shown in Figure 2, even when the streaming is not hot to attract many users in USA and Europe to view, the tracker in A can optimally return the user with a peer list including B's Super-nodes (SN for short) and C's SN to provide a better user performance. Furthermore User@B and User@C can exchange data (availability) with these local SNs using the peer protocol.

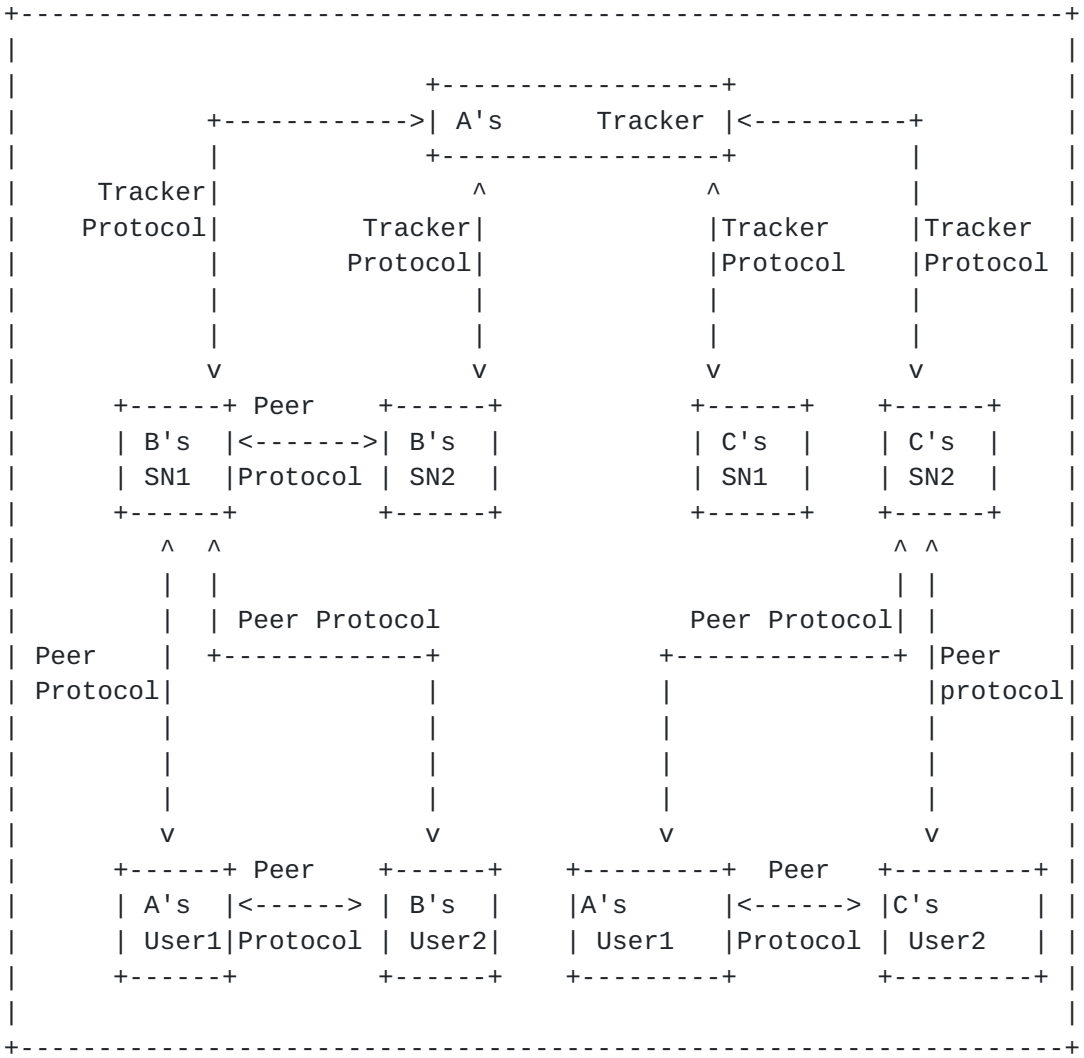


Figure 2 Cooperative Vendors Interaction

5.2. Enabling CDN for P2P VoD streaming

Figure 3 shows the case of enabling CDN to support P2P VoD streaming from different content providers by introducing PPSP inside CDN overlays. It is similar to Figure 2 except that the intermediate SNs are replaced by 3rd party CDN surrogates. The CDN nodes talk with the different streaming systems (including trackers and peers) with the same PPSP protocols.

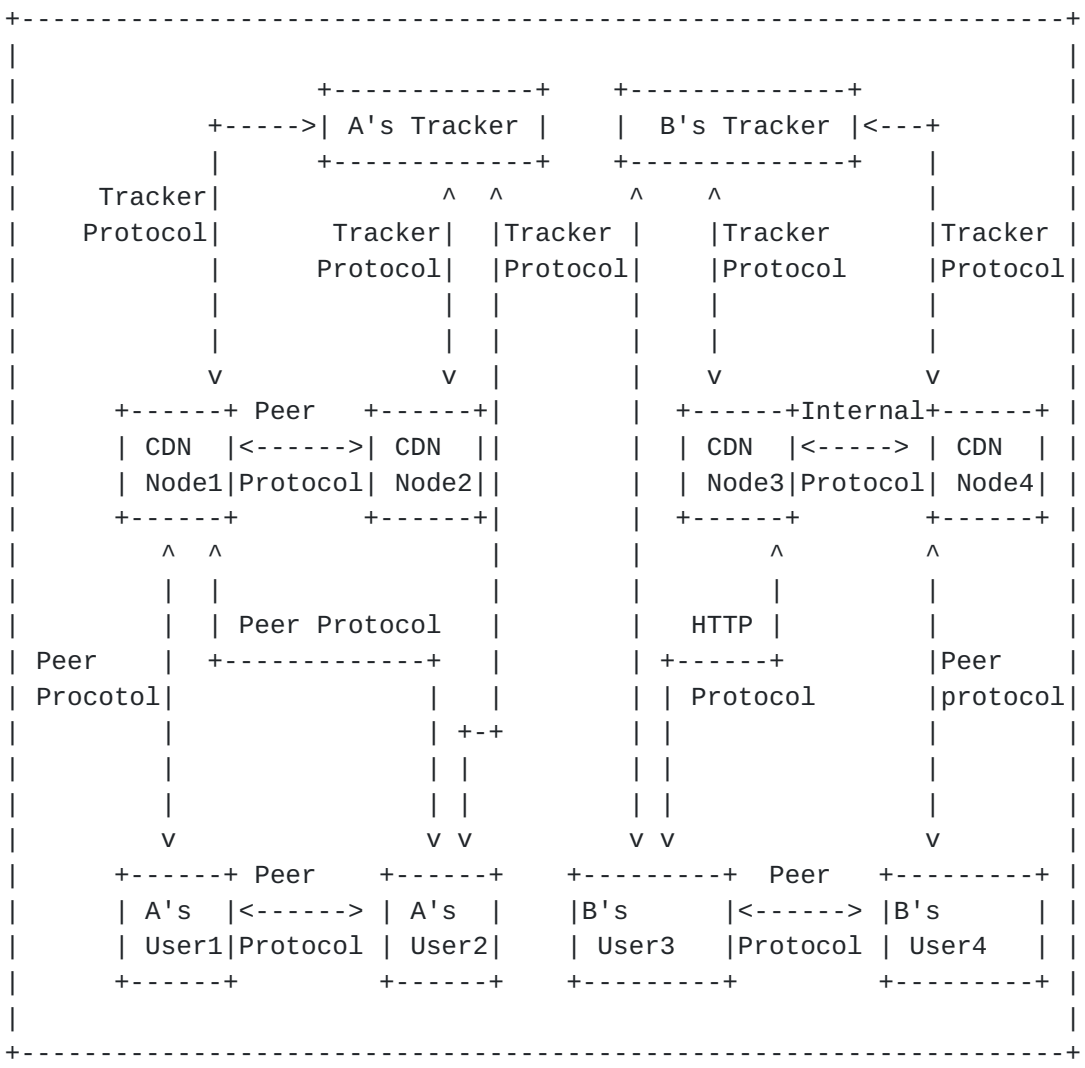


Figure 3 CDN Supporting P2P Streaming

Furthermore the interaction between the CDN nodes can be executed by either existing (maybe proprietary) protocols or the PPSP peer protocol. The peer protocol is useful for building new CDN systems (e.g., operator CDN) supporting streaming in a low cost.

Note that for compatibility reason both HTTP streaming and P2P streaming can be supported by CDN from the users' perspective.

5.3. Cross-screen streaming

In this scenario PC, STB/TV and mobile terminals from both fixed network and mobile/wireless network share the streaming content. With PPSP, peers can identify the types of access networks, average load, peer abilities and get to know what content other peers have even in different networks(potentially with the conversion of the

content availability expression in different networks) as shown in Figure 4.

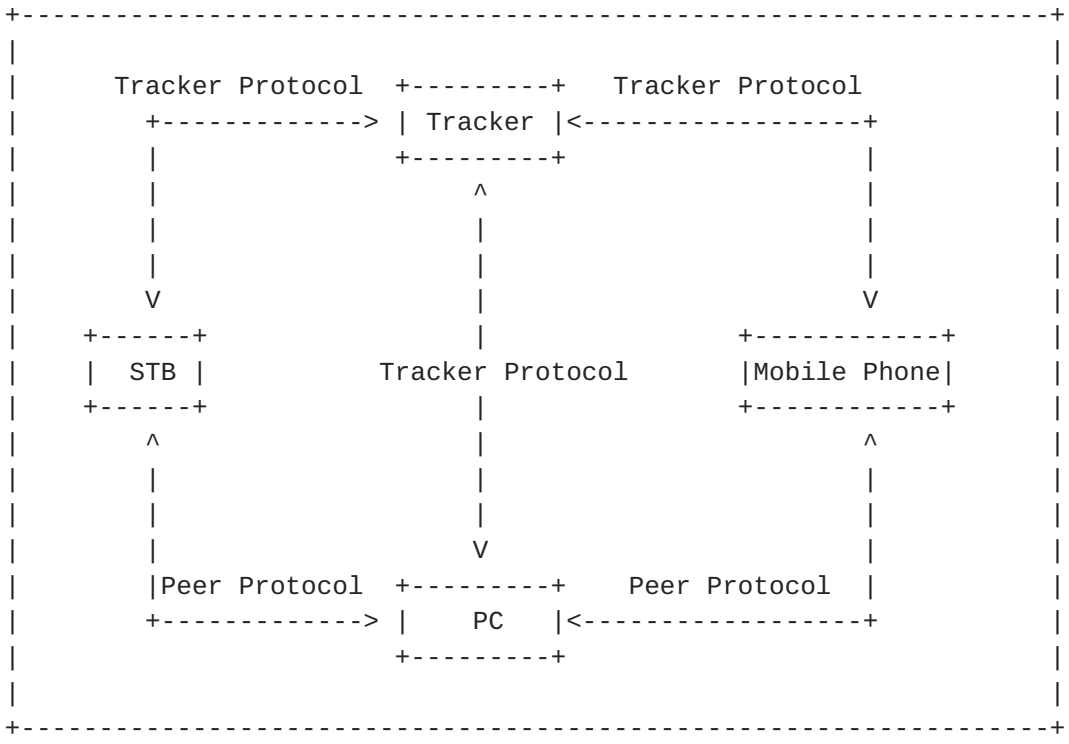
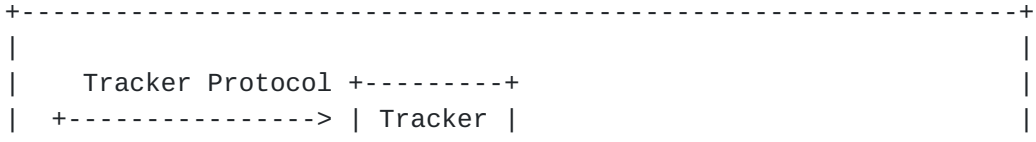


Figure 4 Heterogeneous P2P Streaming with PPSP

Such information will play an important role on selecting suitable peers, e.g., a PC or STB is more likely to provide stable content and a mobile peer within a high-load cell is unlikely to be selected, which may otherwise lead to higher load on the base station.

5.4. Cache service supporting P2P streaming

In Figure 5, when peers request the P2P streaming data, the cache nodes intercept the requests and ask for the frequently visited content (or part of) on behalf of the peers. To do this, it asks the tracker for the peer list and the tracker replies with external peers in the peer list. After the cache nodes exchange data with these peers, it can also act as a peer and report what it caches to the tracker and serve inside requesting peers afterward. This operation greatly decreases the inter-network traffic in many conditions and increases user experience.



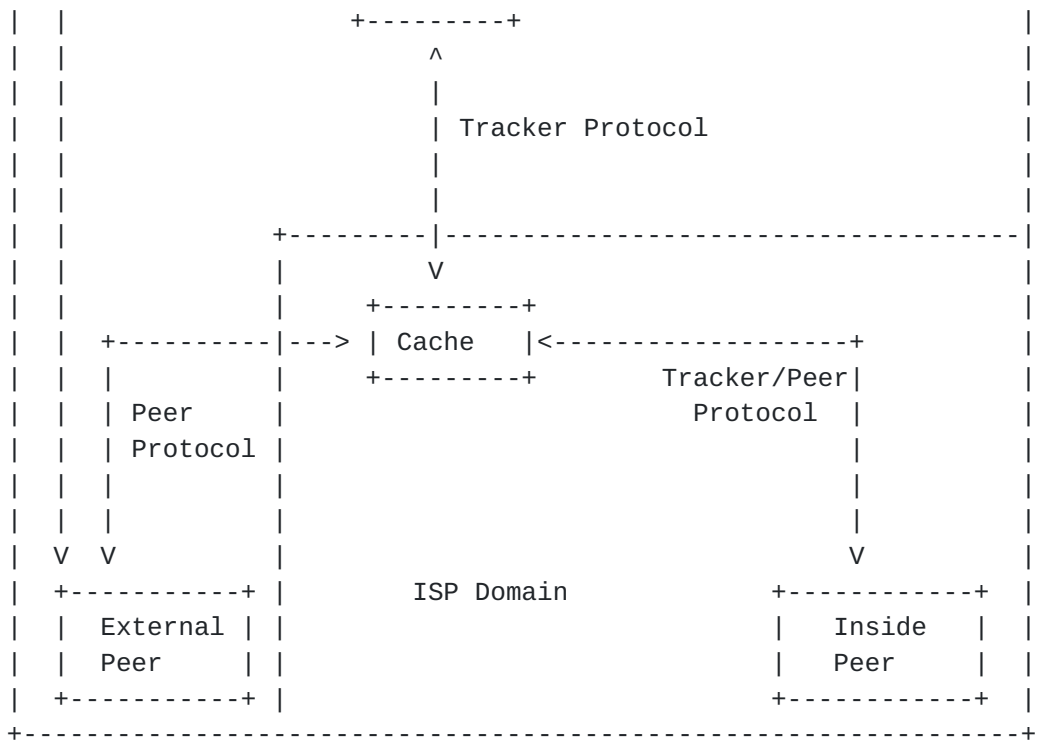


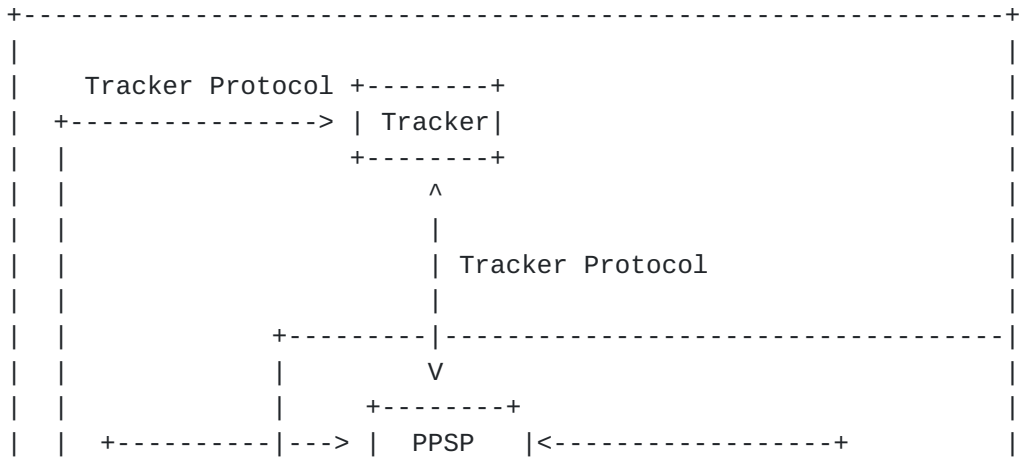
Figure 5 Cache Service Supporting Streaming with PPSP

The cache nodes do not need to update their library when new applications supporting PPSP are introduced, which reduces the cost.

5.5. Proxy service supporting P2P streaming

5.5.1. Home Networking Scenario

For applications where the peer is not co-located with the Media Player in the same device (e.g. the peer is located in a Home Media Gateway), we can use a PPSP Proxy, as shown in figure 6.



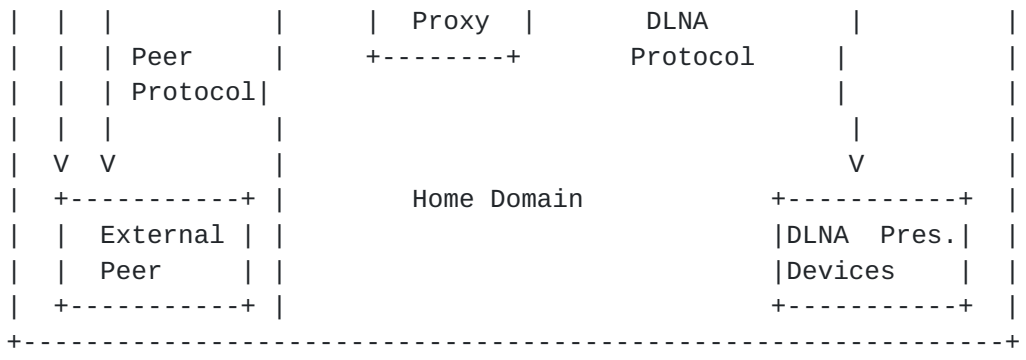


Figure 6 Proxy service Supporting P2P Streaming

As shown in figure 6, the PPSP Proxy terminates both the tracker and peer protocol allowing the legacy presentation devices to access P2P streaming content. In figure 6 the DLNA protocol [DLNA] is used in order to communicate with the presentation devices thanks to its wide deployment. Obviously, other protocols can also be used.

5.5.2. Browser-based HTTP Streaming

P2P Plug-ins are often used in browser-based environment in order to stream content. With P2P plug-ins, HTTP streaming can be turned into a de facto P2P streaming. From the browser (and hence the user) perspective, it's just HTTP based streaming but the PPSP capable plug-in can actually accelerate the process by leveraging streams from multiple sources/peers [P2PYoutube]. In this case the plug-ins behave just like the proxy.

6. Requirements of PPSP

This section enumerates the requirements that should be considered when designing PPSP.

6.1. Basic Requirements

PPSP.REQ-1: Each peer MUST have a unique ID (i.e., peer ID).

It's a basic requirement for a peer to be uniquely identified in a P2P streaming system so that other peers or tracker can refer to the peer by ID.

Note that a peer can join multiple swarms with a unique ID, or change swarm without changing its ID.

PPSP.REQ-2: 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-3: The streaming content MUST be partitioned into chunks.

PPSP.REQ-4: Each chunk MUST have a unique ID (i.e. chunk ID) in the swarm.

Each chunk must have a unique ID in the swarm so that the peer can understand which chunks are stored in which peers and which chunks are requested by other peers.

6.2. Operation and Management Requirements

This section lists some operation and management requirements following the checklist presented by Appendix A in [RFC5706].

6.2.1. Operation Considerations

PPSP.OAM.REQ-1: PPSP MUST be sufficiently configurable.

According to basic requirements, when setting up PPSP, content provider should generate chunk IDs and swarm ID for each streaming content. Original content server and tracker are configured and setup. Content provider then should publish this information typically by creating web links.

The configuration should allow the proxy-based and end-client scenarios.

PPSP.OAM.REQ-2: PPSP MUST implement a set of configuration parameters with default values.

PPSP.OAM.REQ-3: PPSP MUST support diagnostic operations.

Mechanisms must be supported by PPSP to verify correct operation. The PPSP tracker should collect the status of the peers including peer's activity, whether it obtained chunks in time, etc. Such information can be used to monitor the streaming behavior of PPSP.

PPSP.OAM.REQ-4: PPSP MUST facilitate achieving quality acceptable to the streaming application.

There are basic quality requirements for streaming systems. Setup time to receive a new streaming channel or to switch between

channels should be reasonably small. End to end delay, which consists of the time between content generation (e.g., a camera) and content consumption (e.g., a monitor), will become critical in case of live streaming especially in provisioning of sport events where end to end delay of 1 minute and more are not acceptable.

For instance, the tracker and peer protocol can carry quality related parameters (e.g. video quality and delay requirements) together with the priorities of these parameters in addition to the measured QoS situation (e.g., performance, available uplink bandwidth) of content providing peers.

PPSP implementations may use techniques such as scalable streaming to handle bandwidth shortages without disrupting playback.

6.2.2. Management Considerations

PPSP.OAM.REQ-5: When management purpose needs to be supported in implementation, PPSP MUST support remote management using standard interface, as well as a basic set of management information.

Due to large-scale peer network, PPSP tracker service or seeders should remotely collect information from peers and expose the information via standard interface for management purpose. Peer information can be collected via PPSP tracker protocol or peer protocol.

The minimum set of management objects should include swarm information such as content characteristics, rate limits, tracking information such as swarm list, log events, peer information such as peer activity, chunk statistics, log event.

PPSP.OAM.REQ-6: PPSP MUST support fault monitoring including peer and server health, as well as streaming behavior of peers.

Peer and server health will at least include node activity and connectivity especially for peers behind NAT. As mentioned in OAM.REQ-4, streaming behavior of peer can be learnt from chunk distribution information.

PPSP.OAM.REQ-7: PPSP MUST support configuration management to define the configuration parameters.

A set of configurable parameters related to chunk generation in PPSP setup stage can be defined by content providers via a management interface to content servers.

PPSP.OAM.REQ-8: PPSP MUST support performance management with respect to streaming performance based on chunk distribution statistics, network load, tracker and peer monitoring.

PPSP.OAM.REQ-9: PPSP MUST support security management. See section of "Security Considerations" in this document.

6.3. PPSP Tracker Protocol Requirements

PPSP.TP.REQ-1: The tracker protocol MUST allow the peer to solicit a peer list in a swarm generated and possibly tailored by the tracker in a query and response manner.

The tracker request message may include the requesting peer's preference parameter (e.g. preferred number of peers in the peerlist) or preferred downloading bandwidth. The tracker will then be able to select an appropriate set of peers for the requesting peer according to the preference.

The tracker may also generate the peer list with the help of traffic optimization services, e.g. ALTO [I-D.ietf-alto-protocol].

PPSP.TP.REQ-2: The tracker protocol MUST report the peer's activity in the swarm to the tracker.

PPSP.TP.REQ-3: The tracker protocol MUST take the frequency of messages and efficient use of bandwidth into consideration, when communicating chunk availability information.

For example, the chunk availability information between peer and tracker can be presented in a compact method, e.g., to express a sequence of continuous "1" more efficiently.

PPSP.TP.REQ-4: The tracker protocol MUST have a provision for tracker to authenticate the peer.

This ensures that only the authenticated users can access the original content in the P2P streaming system.

6.4. PPSP Peer Protocol Requirements

PPSP.PP.REQ-1: The peer protocol MUST allow the peer to solicit the chunk information from other peers in a query and response manner.

PPSP.PP.REQ-2: The chunk information exchanged between a pair of peers MUST NOT be passed to other peers, unless the chunk information is validated (e.g. preventing hearsay and DoS attack).

PPSP.PP.REQ-3: The peer protocol MUST allow the peer to solicit an additional list of peers to that received from the tracker.

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

PPSP.PP.REQ-4: When used for soliciting additional list of peers, the peer protocol MUST contain swarm-membership information of the peers that have explicitly indicated they are part of the swarm, verifiable by the receiver.

PPSP.PP.REQ-5: The additional list of peers MUST only contain peers which have been checked to be valid and online recently (e.g., preventing hearsay and DoS attack).

PPSP.PP.REQ-6: The peer protocol MUST report the peer's chunk availability update.

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 neighbors (i.e. the peers known to a peer by getting the peer list 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 the update message, how often to send this update message, etc. should leave to the algorithms, rather than protocol concerns.

PPSP.PP.REQ-7: The peer protocol MUST take the frequency of messages and efficient use of bandwidth into consideration, when communicating chunk information.

For example, the chunk availability information between peers can be presented in a compact method.

PPSP.PP.REQ-8: The peer protocol MUST exchange additional information, e.g., status about the peers.

This information can be, for instance, information about the access link or information about whether a peer is running on battery or is connected to a power supply. With such information, a peer can select more appropriate peers for streaming.

7. Security Considerations

This document discusses the problem statement and requirements around P2P streaming protocols without specifying the protocols. However we believe it is important for the reader to understand areas of security introduced by the P2P nature of the proposed solution. The main issue is the usage of un-trusted entities (peers) for service provisioning. For example, malicious peers/trackers may:

Originate denial of service (DOS) attacks to the trackers by sending large amount of requests with the tracker protocol;

Originate fake information on behalf of other peers;

Originate fake information about chunk availability;

Originate reply instead of the regular tracker (man in the middle attack);

leak private information about other peers or trackers.

We list some important security requirements for PPSP protocols as below:

PPSP.SEC.REQ-1: PPSP MUST support closed swarms, where the peers are authenticated or in a private network.

This ensures that only the trusted peers can access the original content in the P2P streaming system. This can be achieved by security mechanisms such as peer authentication and/or key management scheme.

Another aspect is that confidentiality of the streaming content in PPSP need to be supported. In order to achieve this, PPSP should provide mechanisms to encrypt the data exchange among the peers.

PPSP.SEC.REQ-2: Integrity of the streaming content in PPSP MUST be supported to provide a peer with the possibility to identify unauthentic content (undesirable modified by other entities rather than its genuine source).

In a P2P live streaming system a polluter can introduce corrupted chunks. Each receiver integrates into its playback stream the

polluted chunks it receives from its neighbors. Since the peers forwards chunks to other peers, the polluted content can potentially spread through the P2P streaming network.

The PPSP protocol specifications will document the expected threats (and how they will be mitigated by each protocol) and also considerations on threats and mitigations when combining both protocols in an application. This will include privacy of the users and protection of the content distribution.

PPSP.SEC.REQ-3: The security mechanisms in PPSP, such as key management and checksum distribution MUST scale well in P2P streaming systems.

8. IANA Considerations

This document has no actions for IANA.

9. Acknowledgements

Thanks to J.Seng, G. Camarillo, R. Yang,C. Schmidt, R. Cruz, Y. Gu, A.Bakker and S. Previdi for contribution to many sections of this draft. Thank you to C. Williams, V. Pascual and L. Xiao for contributions to PPSP requirements section.

We would like to acknowledge the following people who provided review, feedback and suggestions to this document:M. Stiemerling,D. Bryan, E. Marocco, V. Gurbani, R. Even, H. Zhang, D. Zhang, J. Lei, H.Song, X.Jiang, J.Seedorf, D.Saumitra, A.Rahman, J.Pouwelse, W.Eddy, B. Claise, D. Harrington, J. Arkko and all the AD reviewers.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC6707] B. Niven-Jenkins, "Content Distribution Network Interconnection (CDNI) Problem Statement", RFC 6707, Sep 2012.

[RFC6770] G. Bertrand, "Use Cases for Content Delivery Network Interconnection", RFC6770, Nov 2012.

[RFC5706] D. Harrington, "Guidelines for Considering Operations and Management of New Protocols and Protocol Extensions", RFC5706, Nov 2009.

10.2. Informative References

[Cisco] Cisco Visual Networking Index: Forecast and Methodology, 2009-2014, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/ white_paper_c11-481360_ns827_Networking_Solutions_White_Paper.html

[VoD] Y. Huang et al,Challenges,"Design and Analysis of a Large-scale P2P-VoD System", Sigcomm08.

[ByteMobile]http://www.bytemobile.com/news- events/2012/archive_230212.html

[Mobile Streaming1] Streaming to Mobile Users in a Peer-to-Peer Network,J. Noh etal,MOBIMEDIA '09.

[Mobile Streaming2] J.Peltotaloetal.,"A real-time Peer-to-Peer streaming system for mobile networking environment",in Proceedings of the INFOCOM and Workshop on Mobile Video Delivery (MoVID '09).

[Hybrid CDN P2P]D. Xu et al, "Analysis of a CDN-P2Phybrid architecture for cost-effective streaming mediadistribution," SpringerMultimediaSystems, vol.11, no.4, pp.383-399, 2006.

[PPTV] http://www.pptv.com

[PPStream] http://www.ppstream.com

[DLNA] http://www.dlna.org

[P2PYoutube] https://addons.opera.com/en/extensions/details/p2p-youtube/

[I-D.ietf-alto-protocol] R.Alimi et al, "ALTO Protocol", draft-ietf-alto-protocol-13 (work in progress), Sep. 2012.

11. References

Authors' Addresses

Yunfei Zhang
Unaffiliated

Email: hishigh@gmail.com

Ning Zong
Huawei Technologies

Email: zongning@huawei.com