P2PSIP
Internet-Draft
Intended status: Informational
Expires: May 10, 2008

D. Bryan
SIPeerior Technologies, Inc.
E. Shim
Locus Telecom
B. Lowekamp
SIPeerior; William & Mary
S. Dawkins, Ed.
Huawei (USA)
November 7, 2007

Application Scenarios for Peer-to-Peer Session Initiation Protocol (P2PSIP)
draft-bryan-p2psip-app-scenarios-00

Status of this Memo

Copyright Notice

Abstract

This document attempts to identify and classify application scenarios of P2P based SIP. It does not attempt to exhaustively enumerate

these scenarios, and is focused exclusively on scenarios related to real-time IP communication.

Table of Contents

1. Introduction

This document attempts to identify and classify application scenarios for Peer-to-Peer (P2P) based Session Initiation Protocol (SIP) [RFC3261]. Identifying application scenarios will help to understand and clarify requirements of P2PSIP. In particular, these application scenarios will assist the P2PSIP community in identifying commonalities and differences between requirements for different application scenarios, which in turn will help define the near-term scope of specifications and provide a perspective on future specifications.

Only application scenarios related to real-time IP communications, such as VoIP, Instant Messaging (IM), and presence are considered in this document. Application scenarios of other kinds, even if interesting and possibly useful applications of P2PSIP, are out of scope for this document. Thus, application scenarios described herein are application scenarios of P2P IP real-time communications, and P2PSIP is a protocol choice rather than a constraining factor for most of them. In describing application scenarios, no deliberation on implementation is provided. Some of the application scenarios presented may already be implemented or deployed, possibly using proprietary technology.

The list of application scenarios compiled here is by no means a complete list of uses cases of P2PSIP, and further cases would be limited only by the imagination. P2PSIP participants who expect to use P2PSIP technology for application scenarios that don't match any of the combinations of attributes included in this document are invited to contribute descriptions of additional application scenarios to the P2PSIP working group mailing list.

We tried to capture the deployment characteristics of the application scenarios such as whether the nodes will span over multiple physical network administrative domains or whether the ID must be controlled by a central authority. The characteristics are presented as

scenario-attribute tables. The values in the tables are what we think are most likely and we understand there may be similar scenarios with different choices for some attribute values.

Some of these application scenarios, while difficult to implement using a traditional client server SIP (CS SIP) architecture may not require P2P and could be implemented in other ways. While these have often been presented as scenarios calling for P2P communication, the authors recognize that other technologies may also be applicable to these application scenarios.

Since the original iteration of this document, the P2PSIP WG has been

formed and numerous documents have been submitted that include some number of application scenarios. We will not try to enumerate them here. This draft draws from these documents, as well as discussions at the P2PSIP ad-hoc and WG meetings and numerous mailing list and personal conversations of the authors.

2. Terminology

We use terminology defined in RFC 3261 [RFC3261] in this document without further definition.

We use terminology defined in Concepts and Terminology for Peer to Peer SIP [I-D.willis-p2psip-concepts] draft in this document without further definition.

We define the attributes used in the discussion of each application scenario in Section 3.

3. Application Scenario Attributes

The attributes used in the application scenarios matrixes in subsequent sections are explained here.

Application Scenario: The name of an application scenario (previously called a "use case").
Section in Draft: A cross-reference to the section number in this draft where the application scenario is described.

Number of Peers: The number of peers that will be active in an overlay at any given point in time.

Number of Users: The number of users that will be served by an overlay at any given point in time.
Note that if there are more users than peers, this implies that some client protocol is required, whether "client protocol" is a P2PSIP client protocol or the SIP protocol (if the P2PSIP overlay is also providing RFC 3263 [RFC3263]-style routing for unmodified SIP clients).

Overlay spans administrative domains: Whether the overlay spans across multiple physical network administrative domains. If "yes", this makes IP multicast and centralized operations and management unlikely.

Multicast Available: Whether "application-level multicast", "IP multicast", or "link multicast" may be available for a typical overlay.

Note that these are ordered - link multicast implies IP multicast could be available, and IP multicast implies application-level multicast could be available.

P2P Client Support: Whether the overlay need to support a P2P Client protocol, i.e., whether the overlay contains P2P Clients as well as Peers.

Interoperation with CS-SIP: Whether the overlay must also interact with legacy SIP clients and SIP proxies.
Note that one or more peers in the overlay may also act as PSTN gateways.

Non-stop Operation: Whether this application scenarios allows the overlay to become unavailable for periods of time (for example, could an overlay stop operating in order to change DHT algorithms, or would the overlay have to support two DHT algorithms in "ships in the night" mode?)

Centralized Operations and Management: Whether any centralized operations/management entity is responsible for successful operation of the overlay.

Centralized ID Control: Whether ID assignment by central authority is required within an overlay (basically, whether the overlay can be Sybil-attacked - the theory is that if IDs are controlled by a centralized entity, overlay operators simply

remove misbehaving users from the authorization registry).

Supports Anonymous Users: Whether this application scenario allows users to connect to an overlay without providing any identity.

Carrier-Class Robustness: Whether the overlay must provide reliable storage and retrieval in the face of node failure.

NATs within a single overlay Whether the peer protocol must expect to perform NAT traversal as part of normal operation.

DNS available: Whether DNS is available so that peers may perform DNS lookups as part of the overlay JOIN operation.

End-to-end SIP Encryption: Whether this application scenario requires SIP traffic between two peers to be encrypted, so SIP requests and responses are not visible to intermediate peers (peers that forward traffic between two peers that aren't directly connected). In these cases, hop-by-hop TLS encryption, although appropriate when traversing trusted SIP Proxies, is not appropriate when traversing untrusted P2PSIP Peers.

4. Application Scenarios

Application scenarios are grouped according to the characteristics of the network environment in which the end users or devices participating in the P2P overlay are communicating with each other.

4.1. Global Internet Environment

The global Internet environment consists of a large number of autonomous networks with diverse characteristics. Thus, there is no central administration or network control of the physical network on a global scale. Communication paths between two remote devices may span multiple administrative domains and should be assumed to be insecure. Note that most well-known P2P file sharing overlay networks have operated in this environment.

4.1.1. Public P2P VoIP Service Providers

Skype is an outstanding example of a public VoIP service provider using P2P technology among end user devices, although Skype uses a proprietary protocol. Recent research has shown [skypestudy] that

Skype uses a central login server, responsible for management of registered user names. End users are authenticated via a certificate signed by a central server. End user devices are distributed across the global Internet. The number of participating end user devices is very large. A major motivation of using P2P between end user devices for a commercial VoIP service is a reduction in infrastructure and operational costs.

Table 1 provides a high-level overview of this category.

Application Scenario	Public P2P VoIP Service Providers	Open Global P2P VoIP Network
Section in Draft	4.1.1	4.1.2
Number of Peers	hundreds	thousands
Number of Users	millions	millions
Overlay spans administrative domains	no	yes
Multicast Available	no	no
P2P Client Support	yes	yes
Interaction with CS-SIP	yes	yes
Non-stop Operation	yes	yes
Centralized Operations and Management	yes	yes
Centralized ID Control	yes	no
Supports Anonymous Users	no	no
Carrier-Class Robustness	yes	yes
NATs within a single overlay	yes	yes
DNS available	yes	yes
End-to-end SIP Encryption	yes	yes

Public P2P VoIP Service Providers and Open Global P2P VoIP Network

Table 1

4.1.2. Open Global P2P VoIP Network

This is a global P2P VoIP network in which there is no central authority such as a single service provider. Anyone can join and leave the network freely and anyone can implement the software to participate in the overlay network. In such a system, the protocols used must be based on open standards. This P2P VoIP network resembles the global Internet itself in that it has distributed management and growth, enables anyone to reach anyone else in the overlay network, and any device supporting the standard protocols can be used.

Table 1 provides a high-level overview of this category.

4.1.3. Wide Area Networks of Consumer Electronics Devices

Instant messaging application software provides presence, text and media messaging, and file transfer capabilities between online users. As more and more multimedia consumer electronics devices such as cameras, camcorders and televisions become network aware, instant sharing of multimedia content such as photos and video clips between family members and friends will be desirable. VoIP may not be needed on some of these consumer electronics devices, however in other cases such as gaming, voice communication between users may be highly desirable. As consumer electronics providers may desire to provide these capabilities without investing in extensive server capabilities, a global P2P network supporting presence is an important infrastructure component for this application scenario.

Table 2 provides a high-level overview of this category.

+------------------------------+------------------------------------+

Application Scenario	Wide Area Networks of Consumer Electronics Devices
Section in Draft	4.1.3
Number of Peers	thousands
Number of Users	millions
Overlay spans administrative domains	yes
Multicast Available	no
P2P Client Support	yes
Interaction with CS-SIP	no
Non-stop Operation	no
Centralized Operations and Management	maybe
Centralized ID Control	maybe
Supports Anonymous Users	no
Carrier-Class Robustness	no
NATs within a single overlay	yes
DNS available	yes
End-to-end SIP Encryption	no

Wide Area Networks of Consumer Electronics Devices

Table 2

4.1.4. Multimedia content sharing via Application Layer Multicasting (Content Providers or Ad Hoc)

IP-layer multicasting is not generally available beyond the boundary of single IP subnet. Application layer multicasting has become a plausible alternative to IP-layer multicasting. In application layer multicasting, the nodes that need to receive the content from the same source form a distribution network, typically of a tree-like topology, and relay the received content to other nodes in the distribution network. This technique can be used to multicasting video or audio stream to a number of nodes distributed over the Internet (or across multiple IP subnets).

Note that this application scenario covers two types of deployments - large-scale commercial audio or video distribution/broadcasting services such as Internet radio or TV services ("Content Provider") or to ad-hoc video sharing among a group of friends ("Ad Hoc").

Table 3 provides a high-level overview of this category.

Application Scenario	Multimedia content sharing via Application Layer Multicasting (Content Providers)	Multimedia content sharing via Application Layer Multicasting (Ad Hoc)
Section in Draft	4.1.4	4.1.4
Number of Peers	hundreds	hundreds
Number of Users	thousands	thousands
Overlay spans administrative domains	yes	yes
Multicast Available	application multicast	application multicast
P2P Client Support	yes	yes
Interaction with CS-SIP	no	no
Non-stop Operation	yes	no
Centralized Operations and Management	yes	no
Centralized ID Control	yes	no
Supports Anonymous Users	no	no
Carrier-Class Robustness	yes	no
NATs within a single overlay	yes	yes
DNS available	yes	yes
End-to-end SIP Encryption	yes	no

Multimedia content sharing via Application Layer Multicasting (Content Provider and Ad Hoc)

Table 3

4.2. Environments with Limited Connectivity to the Internet or Infrastructure

When there is no physical network available for stable deployment of client server SIP or an instant deployment of real-time communication systems is required, the P2P approach may be the only feasible solution. Examples of such environment are isolated wireless ad-hoc networks with no connection to the Internet or ad-hoc networks with limited connectivity to the Internet in situations like outdoor public events, emergencies, and battlefields. Any type of manual configuration is difficult to achieve because technical support is not readily available in such environment. In some cases, connectivity to the global Internet may be available, but be very expensive, of limited capacity, or unstable, such as satellite connections. In such cases, it is preferable to localize communications as much as possible, reducing dependency on any infrastructure in the global Internet.

Table 4 provides a high-level overview of this category.

Application Scenario	Ad-Hoc and Ephemeral Groups	Extending the Reach of Mobile Devices	Impeded Access	Local Area Networks of Consumer Electronics Devices
Section in Draft	4.2.1	4.2.2	4.2.3	4.2.4
Number of Peers	tens	hundreds	hundreds	tens
Number of Users	tens	hundreds	hundreds	tens
Spans administrative domains	no	no	yes	no
Multicast Available	link multicast	link multicast	no	link multicast
P2P Client	no	no	no	no

Support Interaction with CS-SIP	no	no	no	no
Non-stop Operation	no	no	no	no
Centralized Operations and Management	no	no	no	no

Centralized ID Control Supports Anonymous Users	no	yes	no	yes
Carrier-Class Robustness	no	no	no	no
NATs within a single overlay	no	no	yes	no
DNS available	no	no	yes	yes
End-to-end SIP Encryption	no	no	yes	no

Environments with Limited Connectivity to the Internet or Infrastructure

Table 4

4.2.1. Ad-Hoc and Ephemeral Groups

Groups of individuals meeting together have need for collaborative communications systems that are ephemeral in nature, have minimum (ideally zero) configuration, and do not depend on connectivity to the Internet. These scenarios require an arbitrary number of users to connect communications devices. These can include cases where Internet connectivity due to remote location, inability to pay for connectivity, or following a natural disaster where service is interrupted.

Example: A group gets together for a meeting, but there is no Internet connectivity. If the users establish a wireless ad hoc

network or have a base station, all users may connect and establish chat sessions using an IM protocol with no need for server configuration.

Example: Following a disaster, the local fire department arrives. Each fire fighter has a wireless handset, and one or more trucks have wireless base stations. When a nearby locality sends additional rescuers, their wireless handsets should be able to instantly join the communications network and communicate, without the need for central configuration.

4.2.2. Extending the Reach of Mobile Devices

[anchor9]

A network of mobile devices can relay traffic between themselves to

reach a base station, even if the base station is out of reach of that device.

Example: A user has a handset for communication that cannot reach a base station. Some other user is within range of both that user and a base station. This intermediate user can serve as a relay for the caller who is out of range. A system might make this feature optional for standard communication and mandatory for E911.

4.2.3. Impeded Access

Certain groups may have their ability to communicate impeded. These users should be able to communicate without the need to connect to any centralized servers, which may be blocked by providers upstream of the user. A fully decentralized system cannot be completely disconnected without removing connectivity at the basic Internet level.

Example: A user wishes to use an IP telephony service to communicate PC to PC with a friend, but the ports commonly used by these services, or the servers used for authentication, are blocked by the ISP because the ISP also offers communications systems and have a vested interest in denying access to external communications systems.

Example: A user with an Internet enabled PDA devices wishes to

connect with colleagues, but traditional services are blocked to ensure that SMS or voice minutes are used (at additional cost) instead.

4.2.4. Local Area Networks of Consumer Electronics Devices

In addition to consumer devices sharing information with other users across the Internet, having devices that can locate each other and exchange information within the local LAN of a particular user may also be an attractive application. In this case, devices could use P2PSIP to locate multimedia resources available on other devices and stream the information between the devices.

Example: A user wishes to share content among consumer electronics devices within a home network.

4.3. Managed, Private Network Environments

A corporate network or a school campus network is an example of the managed, private network environment. Most likely client server SIP can be used and managed for real-time communication applications in these environments. However, in certain scenarios, P2PSIP may be used instead or as a complementary means, to achieve various goals

such as cost and management overhead reduction, scalability, and system robustness.

Table 5 provides a high-level overview of this category.

Application Scenario	Serverless or Small Scale IP-PBX	P2P for Redundant SIP Servers	Failover for Centralized Systems
Section in Draft	4.3.1	4.3.2	4.3.3
Number of Peers	hundreds	hundreds	tens
Number of Users	hundreds	hundreds	tens
Spans administrative domains	no	no	no
Multicast Available	IP multicast	IP multicast	IP multicast

P2P Client Support	no	no	no	
Interaction with CS-SIP	yes	no	yes	
Non-stop Operation	yes	yes	yes	
Centralized Operations and Management	maybe	yes	yes	
Centralized ID Control	self-cert?	yes	yes	
Supports Anonymous Users	no	no	no	
Carrier-Class Robustness	no	yes	yes	
NATs within a single overlay	yes	no	no	
DNS available	no	yes	yes	
End-to-end SIP Encryption	no	no	no	

Managed, Private Network Environments

Table 5

4.3.1. Serverless or Small Scale IP-PBX

Many small enterprises have a need for integrated communications systems. These systems have slightly different requirements than more traditional IP PBXs. For small enterprises, there may be no administrator for these systems, requiring the systems to be essentially self-configuring and/or self-organizing. Additional endpoints should be able to be added with no requirements for configuration on central devices.

These systems should offer the feature sets similar to those of

client server type PBX systems. Connectivity to the PSTN is an important feature for these systems. In addition, they may support features such as call transfer, voice mail, and possibly even other communications modes such as instant messaging or media features such as video or conference services. There are already commercial products of this type.

Example: Small organizations without centralized IT

4.3.2. P2P for Redundant SIP Proxies

Service providers may wish to connect a farm of proxies together in a transparent way, passing resources (user registrations or other call information) between themselves with as little configuration or traffic as possible. Ideally, the redundancy and exchange of information should require a minimum of configuration between the devices. P2P architecture between the proxies allows proxy farms to be organized and operated in this way. With this approach, it is easy to add more proxies with minimal service disruptions and increases the robustness of the system.

Example: a SIP service provider may wish to scale SIP proxies by using a P2PSIP overlay that provides RFC 3263 [RFC3263] request routing services, instead of using either front-end load balancing devices or making the structure of the proxy farm visible outside the proxy farm itself.

4.3.3. Failover for Centralized Systems

A traditional centralized SIP server, such as used in an IP-PBX, forms a single point of failure of an otherwise fault-independent network. Relying on P2PSIP as a backup to the centralized server allows the communications system to continue functioning normally in the event of planned or unplanned service interruptions of the central IP-PBX. When combined with a low-configuration P2PSIP PBX, this can provide a simple, standalone communications system for the developing world that allows local communication even when Internet

connectivity is severed.

Example: A small company has a central IP-PBX. When that device experiences a failure, the handsets are able to transparently

continue operation for the 24 hours it takes to obtain a replacement switch.

Example: A village in the developing world has connectivity that is limited by weather (microwave connection) or is solar powered. It would be desirable for intra-village communication to continue to function in the absence of Internet connectivity.

5. Changes from draft-bryan-p2psip-usecases-00

This draft builds on the analysis done for an earlier draft, draft-bryan-p2psip-usecases-00, now expired. For ease of reference, Table 6 shows the mapping of use cases described in draft-bryan-p2psip-usecases-00 onto the application scenarios described in this document.

Use Case	Section in Use Cases Draft	Application Scenario
Public P2P VoIP Service Providers	3.1.1	(no change)
Open Global P2P VoIP Network	3.1.2	(no change)
Presence Using Multimedia Consumer Electronics Devices	3.1.3	Split into (Content Provider) and (Ad Hoc) scenarios
Multimedia content sharing via Application Layer Multicasting	3.1.4	(no change)
Impeded Access	3.2.1	(no change)
Anonymous Communications	3.2.2	Became an attribute of other scenarios
Security Conscious Small Organizations	3.2.3	Became an attribute of other scenarios
Ad-Hoc and Ephemeral Groups	3.3.1	(no change)
Emergency First Responder Networks	3.3.2	Merged with Ad-Hoc and Ephemeral Groups
Extending the Reach of Mobile Devices	3.3.3	(no change)

Deployments in the Developing World	3.3.4	Merged with Failover
Serverless or Small Scale IP-PBX	3.4.1	(no change)
P2P for Redundant SIP Servers	3.4.2	(no change)
Failover for Centralized Systems	3.4.3	(no change)

Changes from draft-bryan-p2psip-usecases-00

Table 6

6. Acknowledgments

The following persons have contributed application scenarios or ideas to this document:

Cullen Jennings, Philip Matthews, Henry Sinnreich, Adam Roach, Robert Sparks, Kundan Singh, Henning Schulzrinne, K. Kishore Dhara, and Salman A. Baset.

7. Security Considerations

The security requirements of the various application scenarios vary tremendously. They should be discussed in more detail in this document.

8. IANA Considerations

This document has no IANA Considerations.

9. References

9.1. Normative References

[I-D.willis-p2psip-concepts]
Willis, D., "Concepts and Terminology for Peer to Peer SIP", draft-willis-p2psip-concepts-04 (work in progress), March 2007.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston,

Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC3263] Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

9.2. Informative References

[skypestudy] Baset, S. and H. Schulzrinne, "An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol", Technical Report, Department of Computer Science, Columbia University 0309-04, September 2004.

Editorial Comments

[anchor9] Spencer has misgivings about "Extending the Reach of Mobile Devices", based on (1) relaying at the link layer or at the network layer would make more sense, and would work for devices that do not support P2PSIP, and (2) although small networks might work well enough when peers simply forward a request "around the overlay", in larger networks the problem space morphs from forwarding traffic in *the* direction of a destination to routing traffic in the *best* direction to the destination - a much harder problem.

Authors' Addresses

David A. Bryan
SIPeerior Technologies, Inc.
3000 Easter Circle
Williamsburg, VA 23188
USA

Phone: +1 757 565 0101
Email: dbryan@sipeerior.com

Eunsoo Shim
Locus Telecommunications, Inc.
2200 Fletcher Ave. 6th FL
Fort Lee, NJ 07024
USA

Email: eunsoo@locus.net

Bruce B. Lowekamp
SIPeerior; William & Mary
3000 Easter Circle
Williamsburg, VA 23188
USA

Phone: +1 757 565 0101
Email: lowekamp@sipeerior.com

Spencer Dawkins (editor)
Huawei Technologies (USA)
1547 Rivercrest Blvd.
Allen, TX 75002
USA

Phone: +1 214 755 3870
Email: spencer@mcsr-labs.org

Full Copyright Statement

Intellectual Property

found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).