P2PSIP
Internet-Draft
Intended status: Informational
Expires: January 3, 2008

D. Bryan
SIPeerior Technologies, Inc.
E. Shim
Locus Telecom
B. Lowekamp
SIPeerior; William & Mary

July 2, 2007

Use Cases for Peer-to-Peer Session Initiation Protocol (P2P SIP) draft-bryan-p2psip-usecases-00

Status of this Memo

Copyright Notice

Abstract

This document attempts to identify and classify use cases of P2P based SIP. It does not attempt to exhaustively enumerate these cases, and is focused exclusively on cases related to real-time IP communication.

Table of Contents

1. Introduction

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

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

Some of these use cases, 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 use cases.

Since the original iteration of this document, the P2PSIP WG has been formed and numerous documents have been submitted that include some number of use cases. We will not try to enumerate them here. This draft draws from these documents, as well as discussions at the P2P SIP ad-hoc and WG meetings and numerous mailing list and personal conversations of the authors. The list of use cases compiled here is by no means a complete list of uses cases of P2P SIP, and further cases would be limited only by the imagination.

2. Terminology

In this document, words which are normally key words, such as "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are used COLLOQUIALLY and are not intended to be interpreted as described in RFC2119 [RFC2119].

We use the terminology and definitions from the Concepts and

Terminology for Peer to Peer SIP [I-D.willis-p2psip-concepts] draft in this document without further definition. Terminology defined in RFC3261 [RFC3261] is used without definition.

3. Use Cases

Use cases 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.

3.1. 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.

3.1.1. Public P2P VoIP Service Providers

Skype is an outstanding example of a public VoIP service provider using P2P technology among end user devices, although using 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 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.

3.1.2. 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.

3.1.3. Presence Using Multimedia Consumer Electronics Devices

Presence is a useful and important feature for instant messaging and VoIP applications. Well-known instant messaging application software provides presence, text and media messaging, and supports file transfer 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 presence that enables instant content sharing will be required for many types of consumer electronics devices. A global P2P network supporting presence is an important infrastructure component for this use case.

3.1.4. Multimedia content sharing via Application Layer Multicasting

IP-layer multicasting is not generally available beyond the boundary of single IP subnet. Application layer multicasting has become a fausible 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). This can be used to realize large-scale commercial audio or video distribution/ broadcasting services such as Internet radio or TV services or to ad-hoc video sharing among a group of friends.

3.2. Security Demanding Environments

There are situations where, despite having connectivity to the Internet or even to client server SIP infrastructure such as SIP proxies, users may not like to use the infrastructure because of security concerns or may not be allowed to use the infrastructure. Such situations are referred to here as involving a security demanding environment. Maintaining privacy of communication and secrecy of identities are important in this environment and the P2P architecture's distributed nature may be more attractive than a client server approach.

3.2.1. 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.

Examples: 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 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.

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.

3.2.2. Anonymous Communications

Users occasionally have need to communicate among themselves in a completely anonymous fashion, whether due to political persecution, need for secrecy for commercial reasons, or threats of violence. In such a case, the need for a self organizing, server-less system is imperative. Users on such a system could communicate with reduced risk of the system being monitored or their identities discovered. As with the impeded access scenario, the only way to disable such networks would be to completely disable Internet connectivity.

3.2.3. Security Conscious Small Organizations

Certain security conscious small organizations may have need for communications systems that allow members of the organization to communicate directly with one another regardless of their location, with encryption, and without any connectivity to or use of servers, either internal or external to the organization. For these organizations, traditional client-server SIP implementations and more importantly hosted solutions for communications are unacceptable. These entities need a system to facilitate such communications without central servers. Note that these users may overlap with the anonymized communications case also described in this document.

Examples: Organizations who are developing technology that might be of interest to a hosted service provider, but because of small size may have no desire or time to maintain centralized servers. Organizations with security needs that preclude any traffic flowing through a central server such as military, national security, or intelligence organizations.

3.3. 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.

3.3.1. 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.

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.

3.3.2. Emergency First Responder Networks

Following a large scale disaster such as a tsunami, earthquake, hurricane, or terrorist attack, access to traditional communications devices of any kind -- Internet, cellular, or traditional PSTN -- may be compromised. Recent events have shown that current first responder radio systems cannot be relied upon to interoperate effectively. A network of devices that can grow organically as responders arrive, requiring only wireless access, is required. As more personnel show up, they should be able to join the network, locate other personnel, and communicate without any centralized configuration required.

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.

3.3.3. Extending the Reach of Mobile Devices

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.

3.3.4. Deployments in the Developing World

Certain locations in the developing world have limited, intermittent, or non-existent connectivity to the Internet. These locations also typically lack experienced people with the specialized skills needed to administer or maintain centralized SIP proxies. Even DNS servers may not exist. A communications system that is able to function reliably for internal communications, even in the presence of degraded or absent connectivity, is clearly needed. Such a system must also scale easily with little or no configuration and ideally should interface easily to existing communications systems when connectivity is available.

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.

3.4. 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 environment. However, in certain scenarios, P2P SIP may be used instead or as a complementary means, to achieve various goals such as cost and management overhead reduction, scalability, and system robustness.

3.4.1. 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

3.4.2. 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. A P2P architecture between the proxies allows proxy farms to be organizing 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.

3.4.3. 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 P2P SIP 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.

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.

4. Acknowledgments

The following persons have contributed use case suggestions 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.

5. Security Considerations

The security requirements of the various use-cases vary tremendously. They should be discussed in more detail in this document.

6. IANA Considerations

This document has no IANA Considerations.

7. References

7.1. 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.

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

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

7.2. 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.

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

Full Copyright Statement

Intellectual Property

Acknowledgment

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