Industrial-Strength P2P SIP
draft-matthews-sipping-p2p-industrial-strength-00.txt

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, or will be disclosed, and any of which I become aware will be disclosed, in accordance with RFC 3668.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on August 11, 2005.

Copyright Notice

Copyright (C) The Internet Society (2005). All Rights Reserved.

Abstract

If internet telephony networks based on peer-to-peer and Session Initiation Protocol (SIP) technology are to become as viable as existing centralized telephony services, the peer-to-peer SIP
technology must offer all the features of existing technologies. This
draft lists some features which are in some way "challenging" for
peer-to-peer SIP to support, and proposes a structure for the
resulting protocol suite.

1. Introduction

Peer-to-peer technology offers the promise of being able to replace
centralized services with distributed systems, thus eliminating the
need for a centralized server. Our interest lies in the application
of peer-to-peer technology to telephony networks based on SIP [1].
Specifically, we are interested in constructing peer-to-peer
telephony networks that offer the same feature set as existing
centralized networks, but at a lower cost. The lower cost comes from
eliminating the need to buy and set up central servers.

In order for networks based on peer-to-peer SIP technology
(henceforth called P2P SIP) to become as viable as existing networks,
the new P2P SIP technology must offer the same feature set and
performance as existing technology. We apply the term "industrial-
strength" to P2P SIP technology that meets this goal, in order to
contrast it with other P2P SIP technology that has less-stringent
goals.

Recently, a couple of other drafts [2][3] on P2P SIP technology have
been submitted to the SIPPING working group. The contribution of this
draft is the focus on "industrial-strength" P2P SIP and its
implications.

Specifically, this draft does two things. In section 2, it lists some
features that must be supported by an "industrial-strength" P2P SIP
network. In section 3, it presents a structure for the resulting P2P
SIP protocol suite.

This draft is being discussed on the SIPPING Working Group mailing
list (sipping@ietf.org).

2. Features for "industrial-strength" P2P SIP networks

It may be that there will be different types of P2P SIP networks. One
type that has been mentioned by others is ad-hoc networks,
formed to allow people with similar interests to set up a private
overlay network for communication. These are usually envisioned to be
temporary and/or have a reasonably high membership churn.

We, however, are interested in more permanent networks that replace
existing telephony systems. An example is placing P2P SIP technology
inside phones in an office to give the illusion that the phones are connected to a centralized PBX system. Here the advantage of P2P technology is that there is no need to buy and maintain a centralized PBX server.

For these more permanent P2P SIP networks to be successful, they must duplicate most of the features of existing telephony systems. In particular, some of the necessary features that might be considered more "challenging" are:

- Support for heterogeneous networks
- Support for call handling for an unreachable device
- Support for dividing the network into zones
- Support for network management
- Security

These features are discussed in more detail in the sub-sections below.

2.1. Heterogeneous networks

The P2P SIP network must support a mixture of devices with different attachment bandwidths, storage capacities, network availabilities, and mobility capabilities. For example, the network may consist of a mixture of phones (either soft or hard) that sit on users’ desks and are almost always connected to the network, with some mobile wireless handsets that connect and disconnect frequently and may have lower attachment bandwidths and local storage capacities. The challenge here is to devise protocols that take these different device capabilities into account.

For example, some P2P lookup protocols (like Jxta [4]) assume that devices join and leave the network frequently and are thus optimized for this case. Other P2P protocols (like CAN [5] and Chord [6]) are more concerned with reducing lookup time, and thus device-join and device-leave operations are relatively more expensive.

2.2. Call handling for an unreachable device

The P2P SIP network must support call handling features such as call forwarding and voicemail. The challenge here is to support these features in a P2P network where devices are not always reachable.
For example, consider a handheld SIP phone using WiFi for network connectivity. When the device becomes unreachable because it is out-of-range (or turned off), the phone’s owner might like callers to be forwarded to another number or to be able to leave a voicemail message. How does the system remember this preference when the user’s phone is not available, and how does it store any voicemail message? In a pure P2P system, both pieces of information must be stored on another user’s device. And since that second device might also become unreachable, we must duplicate the information and store copies on a number of devices to ensure that the information (both call treatment information and any received voicemail message) is available when it is needed (e.g., when a call comes in or the user wants to retrieve stored voicemail messages). Here the characteristics of different device comes into account: storing this information on other handheld WiFi devices is likely to result in more messaging and be perhaps less-reliable compared to storing copies on stationary desktop devices.

2.3. Dividing the network into zones

As a network of any type grows larger, any security, stability or scalability problems the network might have tend to get magnified. As a result, the network is often divided into zones to try to keep problems in one part of the network for affecting another part.

An example is the deployment of BGP, which can be considered an early P2P protocol. Here, service providers run one flavor of BGP (iBGP) internally, and another flavor (eBGP) when connecting to other carriers. Moreover, larger service providers often divide up their internal networks (for example, by using BGP confederation or multiple autonomous system (AS) numbers) to achieve greater scalability and to try to restrict problems to a portion of their network.

We believe that any "industrial-strength" P2P SIP protocol suite will need ways to divide the network up into zones.

Note that dividing a network into zones may also make it easier to support heterogeneous networks.

2.4. Network Management

The P2P SIP network must provide a way for an authorized administrator to perform typical network management functions, such as:
2.5. Security

Security in an "industrial-strength" P2P SIP network is very important, perhaps even more important than in ad-hoc networks.

Other documents ([2][3]) have discussed various security issues in P2P SIP networks. Here we mention some of the additional security issues raised by the features discussed in this draft:

- If a voicemail message is left for Alice when Alice’s phone is not available, then the message must be stored somewhere on the network. This will involve storing a copy (or part of a copy) in the phones of various users. If Bob is one of those users, then Bob should not be able to hear it or tamper with it.

- Say Alice sets her desktop phone’s call handling preferences so that most missed calls get redirected to voicemail, but calls from certain friends get redirected to her mobile phone. If Charlie (who is not on Alice’s list of friends) phones Alice, then he should not be able to learn the address of her mobile phone (unless Alice wishes it).

And, of course, anyone who attempts to do network management operations must be authenticated.

3. Structure of the P2P SIP protocol suite

Based on the above feature set, we suggest the P2P SIP protocol suite be divided into the following parts:

- P2P layer
- SIP layer
The P2P layer provides basic P2P services for registering and locating nodes and resources. This should be a generic P2P layer that can be used for many different P2P applications. This layer needs to take the capabilities of different devices into account, but should need no special knowledge of P2P SIP.

The SIP layer includes SIP and any extensions (e.g., SIMPLE). This layer is basically the SIP protocol and extensions as they are today -- little or no changes should be required.

The Call Services layer provides the protocols that support call forwarding, voicemail, and similar services. This layer builds upon the services of the P2P and SIP layers and defines protocols as necessary. In essence, this is glue layer that takes the independent P2P and SIP layers and brings them together into the cohesive whole we call P2P SIP.

Structuring P2P SIP in this manner has the following properties:

- It leaves the SIP layer basically untouched. This maintains two often-cited advantages of SIP over H.323: simplicity and narrow focus.
- It leaves the P2P layer independent of SIP. Thus the P2P layer can evolve independently of SIP, and can be used for other applications that run on the devices in the network that have nothing to do with SIP.

By way of analogy, consider the relationship between SIP and SDP. Though SDP is commonly used with SIP, there is nothing in the SIP protocol that gives SDP any special consideration, and it is easy to substitute another protocol in place of SDP. The above structure supports the same relationship between SIP and P2P.

4. Security Considerations

See section 2.5.

5. Acknowledgments

We thank Eric Cooper, Mahshad Koohgoli, and Jim Stelzig for useful discussions leading up to this draft.
6. Informative References


Authors’ Addresses

Philip Matthews
Nimcat Networks
1135 Innovation Drive
Ottawa, Ontario K2K 3G7
Email: matthews@nimcatnetworks.com

Behrouz Poustchi
Nimcat Networks
1135 Innovation Drive
Ottawa, Ontario K2K 3G7
Email: poustchi@nimcatnetworks.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be 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. By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which I become aware will be disclosed, in accordance with RFC 3668.
Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.