Ad-Hoc Conferencing in the Session Initiation Protocol (SIP)
draft-camarillo-sipping-adhoc-conferencing-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, and any of which I become aware will be disclosed, in accordance with RFC 3667.

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 September 25, 2004.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

This document describes how to create a conference using SIP ad-hoc methods and a URI list. In particular, we describe a mechanism that allows a client to provide a conference server with the initial list of participants for an ad-hoc conference.
Table of Contents

1. Introduction ......................................................... 3
2. Terminology ......................................................... 3
3. Providing a Conference Server with a URI List .................. 3
4. URI List Format ...................................................... 3
5. Conference Server Behavior ......................................... 4
6. Example ............................................................... 4
7. Security Considerations ............................................ 5
8. Acknowledges .......................................................... 6
   Normative References ................................................. 6
   Informational References ............................................ 7
   Authors' Addresses .................................................. 7
   Intellectual Property and Copyright Statements ................... 8
1. Introduction

Section 4.5 of [3] describes how to create a conference using ad-hoc SIP [2] methods. The client sends an INVITE request to a conference factory URI, and receives the actual conference URI, which contains the "IsFocus" feature tag, in the Contact header field of a response (typically a 200 OK).

Once the client obtains the conference URI, it can add participants to the newly created conference in several ways, which are described in [3].

Some environments have tough requirements regarding conference establishment time. So, they require the client to be able to request the creation of an ad-hoc conference and to provide the server with the initial set of participants in a single operation. This document describes how to meet this requirement using the mechanism to transport URI lists in SIP messages described in [4].

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [1] and indicate requirement levels for compliant implementations.

3. Providing a Conference Server with a URI List

A client that wants to include the set of initial participants in its initial INVITE to create an ad-hoc conference MAY add a "list" parameter (defined in [4]) to the conference factory URI and MUST place the resulting URI in the Request-URI. The "list" parameter MUST contain a pointer to a URI list that contains the participants that the client wants the server to INVITE. The following is an example of a Request-URI with a "list" parameter.

sip:conf-factory@example.com;list="cid:cn35t8jf02@example.com"

4. URI List Format

As described in [4], the default format for URI lists in SIP is the XCAP resource list format [5]. Still, specific services need to describe which information clients should include in their URI lists, as described in [4].
Conferencing UAs SHOULD use flat lists (i.e., no hierarchical lists), SHOULD NOT use any entry's attributes but "uri", and SHOULD NOT include any elements inside entries but "display-name" elements.

A conference factory application receiving a URI list with more information than what we have just described SHOULD discard all the extra information.

5. Conference Server Behavior

On reception of an INVITE with a URI list as described in Section 3, a conference server MUST follow the rules described in [3] to create ad-hoc conferences. Once the ad-hoc conference is created, the conference server SHOULD attempt to add the participants in the URI list to the conference as if their addition had been requested using any of the methods described in [3] (e.g., using CPCP [6]).

Once the conference server has created the ad-hoc conference and has attempted to add the initial set of participants, the conference server behaves as a regular conference server and MUST follow the rules in [3].

Note that the status code in the response to the INVITE does not provide any information about whether or not the conference server was able to bring the users in the URI list into the conference. That is, a 200 (OK) means that the conference was created successfully, that the client that generated the INVITE is in the conference, and that the server understood the URI list. If the client wishes to obtain information about the status of other users in the conference it SHOULD use general conference mechanisms, such as the conference package [7].

6. Example

The following is an example of an INVITE request, which carries a URI list in its body, sent by a UA to a conference factory application.

```
INVITE sip:conf-fact@example.com;list=cid:cn35t8jf02@example.com SIP/2.0
Via: SIP/2.0/TCP client.chicago.example.com
    ;branch=z9hG4bKhjhsBass83
Max-Forwards: 70
To: Conf Factory <sip:conf-fact@example.com>
From: Carol <sip:carol@chicago.example.com>;tag=32331
Call-ID: d432fa84b4c76e66710
CSeq: 1 INVITE
Contact: <sip:carol@client.chicago.example.com>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER,
```
SUBSCRIBE, NOTIFY
Allow-Events: dialog
Accept: application/sdp, message/sipfrag,
application/resource-lists+xml
Content-Type: multipart/mixed;boundary="boundary1"
Content-Length: xxx

--boundary1
Content-Type: application/sdp
Content-Length: xxx

v=0
o=carol 2890844526 2890842807 IN IP4 chicago.example.com
s=Example Subject
c=IN IP4 192.0.0.1
t=0 0
m=audio 20000 RTP/AVP 0
a=rtpmap:0 PCMU/8000
m=video 20002 RTP/AVP 31
a=rtpmap:31 H261/90000

--boundary1
Content-Type: application/resource-lists+xml
Content-Length: 315
Content-ID: <cn35t8jf02@example.com>

<?xml version="1.0" encoding="UTF-8"?>
<resource-lists xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <list>
    <entry uri="sip:bill@example.com" />
    <entry uri="sip:joe@example.com" />
    <entry uri="sip:ted@example.com" />
    <entry uri="sip:bob@example.com" />
  </list>
</resource-lists>
--boundary1--

Figure 1: INVITE request

7. Security Considerations

This document discusses ad-hoc setup of SIP conferences using a list. Both conferencing and lists have specific security requirements which will be summarized here. Conferences generally have authorization rules about who may or may not join a conference, what type of media may or may not be used, etc. This information is used by the focus to admit or deny participation in a conference. It is recommended that
these types of authorization rules be used to provide security for a SIP conference.

For this authorization information to be used, the focus needs to be able to authenticate potential participants. Normal SIP mechanisms including Digest authentication and certificates can be used. These conference specific security requirements are discussed further in the requirements and framework documents.

For conference creation using a list, there are some additional security considerations. In some cases, the list of potential participants may need to be kept private. The use of TLS transport or S/MIME can be used to prevent a third party from viewing this information. In addition, a focus may have policies that limit the number of participants in the list, as a very long list could be used in a denial of service attack to place a large burden on the focus to send a large number of INVITEs. Other list related security considerations are discussed in the list framework document.

8. Acknowledges

Cullen Jennings provided useful comments on this document.

Normative References


Informational References


Authors' Addresses

Gonzalo Camarillo
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

EMail: Gonzalo.Camarillo@ericsson.com

Alan Johnston
MCI
100 South 4th Street
St. Louis, MO 63102
USA

EMail: alan.johnston@mci.com
Internet-Draft            Ad-Hoc Conferencing                 March 2004

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 IETF's procedures with respect to rights in IETF 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.

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 (2004). 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.