P2PSIP	C. Jennings	
Internet-Draft	Cisco	
Intended status: Standards Track	B. Lowekamp, Ed.	
Expires: May 1, 2009	SIPeerior Technologies	
	E. Rescorla	
	Network Resonance	
	S. Baset	
	H. Schulzrinne	
	Columbia University	
	October 28, 2008	

TOC

A SIP Usage for RELOAD
draft-ietf-p2psip-sip-00

Status of this Memo

Abstract

This document defines a SIP Usage for REsource LOcation And Discovery (RELOAD), The SIP Usage provides the functionality of a SIP proxy or registrar in a fully-distributed system. The SIP Usage provides lookup service for AoRs stored in the overlay. The SIP Usage also defines GRUUs that allow the registrations to map an AoR to a specific node reachable through the overlay. The Attach method is used to establish a

direct connection between nodes through which SIP messages are exchanged.

Table of Contents

---

1. Overview

TOC

The SIP Usage of RELOAD allows SIP user agents to provide a peer-to-peer telephony service without the requirement for permanent proxy or registration servers. In such a network, the RELOAD overlay itself performs the registration and rendezvous functions ordinarily associated with such servers.
The SIP Usage involves two basic functions:

> **Registration:** SIP UAs can use the RELOAD data storage functionality to store a mapping from their AOR to their Node-ID in the overlay, and to retrieve the Node-ID of other UAs.
>
> **Rendezvous:** Once a SIP UA has identified the Node-ID for an AOR it wishes to call, it can use the RELOAD message routing system to

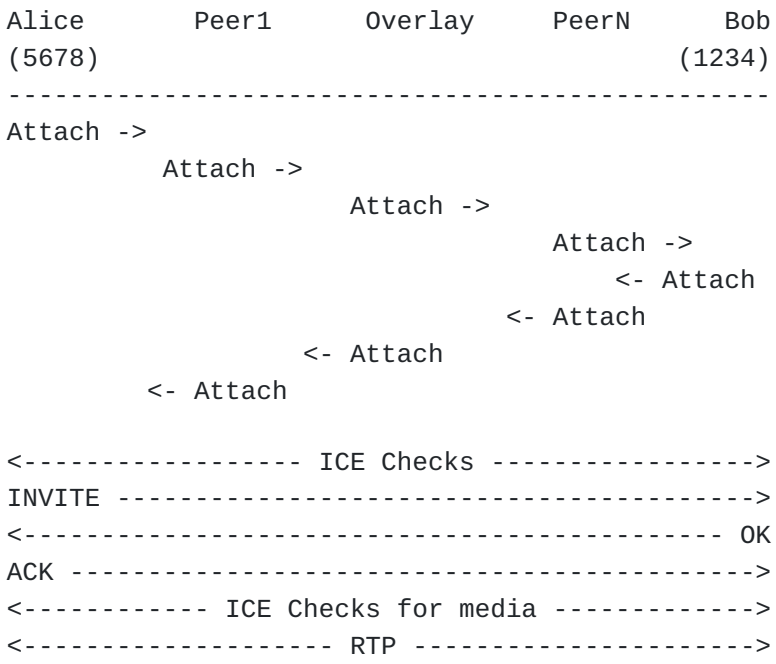
> set up a direct connection which can be used to exchange SIP messages.

For instance, Bob could register his Node-ID, "1234", under his AOR, "sip:bob@dht.example.com". When Alice wants to call Bob, she queries the overlay for "sip:bob@dht.example.com" and gets back Node-ID 1234. She then uses the overlay to establish a direct connection with Bob and can use that direct connection to perform a standard SIP INVITE. The way this works is as follows:

1. Bob, operating Node-ID 1234, stores a mapping from his URI to his Node-ID in the overlay. I.e., "sip:bob@dht.example.com -> 1234".

2. Alice, operating Node-ID 5678, decides to call Bob. She looks up "sip:bob@dht.example.com" in the overlay and retrieves "1234".

3. Alice uses the overlay to route an Attach message to Bob's peer. Bob responds with his own Attach and they set up a direct connection, as shown below.



It is important to note that RELOAD's only role here is to set up the direct connection between Alice and Bob. As soon as the ICE checks complete and the connection is established, then ordinary SIP is used. In particular, the establishment of the media channel for the phone call happens via the usual SIP mechanisms, and RELOAD is not involved.

Media never goes over the overlay. After the successful exchange of SIP messages, call peers run ICE connectivity checks for media.
As well as allowing mappings from AORs to Node-IDs, the SIP Usage also allows mappings from AORs to other AORs. For instance, if Bob wanted his phone calls temporarily forwarded to Charlie, he could store the mapping "sip:bob@dht.example.com -> sip:charlie@dht.example.com". When Alice wants to call Bob, she retrieves this mapping and can then fetch Charlie's AOR to retrieve his Node-ID.
The SIP usage allows a RELOAD overlay to be used as a distributed SIP registrar/proxy network augmenting the functionality of [RFC3263] (Rosenberg, J. and H. Schulzrinne, “Session Initiation Protocol (SIP): Locating SIP Servers,” June 2002.). This entails three primary operations:

*Registering one's own AOR with the overlay.

*Looking up a given AOR in the overlay.

*Forming a direct connection to a given peer.

---

2. Terminology

TOC

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.) [RFC2119].
We use the terminology and definitions from Concepts and Terminology for Peer to Peer SIP (Bryan, D., Matthews, P., Shim, E., Willis, D., and S. Dawkins, “Concepts and Terminology for Peer to Peer SIP,” July 2008.) [I-D.ietf-p2psip-concepts] and the RELOAD Base Protocol (Jennings, C., Lowekamp, B., Rescorla, E., Baset, S., and H. Schulzrinne, “REsource LOcation And Discovery (RELOAD) Base Protocol,” October 2008.) [I-D.ietf-p2psip-base] extensively in this document.

---

3. Registering AORs

TOC

In ordinary SIP, a UA registers its AOR and location with a registrar. In RELOAD, this registrar function is provided by the overlay as a whole. To register its location, a RELOAD peer stores a SipRegistration structure under its own AOR. This uses the SIP-REGISTRATION Kind-ID, which is formally defined in Section 7 (SIP-REGISTRATION Kind Definition).

Note:

> GRUUs are handled via a separate mechanism, as described in Section 6 (GRUUs).

As a simple example, if Alice's AOR were "sip:alice@dht.example.com" and her Node-ID were "1234", she might store the mapping "sip:alice@example.org -> 1234". This would tell anyone who wanted to call Alice to contact node "1234".
RELOAD peers MAY store two kinds of SIP mappings:

- From AORs to destination lists (a single Node-ID is just a trivial destination list.)
- From AORs to other AORs.

The meaning of the first kind of mapping is "in order to contact me, form a connection with this peer." The meaning of the second kind of mapping is "in order to contact me, dereference this AOR". This allows for forwarding. For instance, if Alice wants calls to her to be forwarded to her secretary, Sam, she might insert the following mapping "sip:alice@dht.example.org -> sip:sam@dht.example.org".
The contents of a SipRegistration structure are as follows:

```
enum {sip_registration_uri (1), sip_registration_route (2),
   (255)} SipRegistrationType;

select (SipRegistration.type) {
  case sip_registration_uri:
    opaque              uri<0..2^16-1>;

  case sip_registration_route:
    opaque              contact_prefs<0..2^16-1>;
    Destination         destination_list<0..2^16-1>;

  /* This type can be extended */

} SipRegistrationData;

struct {
   SipRegistrationType   type;
   uint16                length;
   SipRegistrationData   data;
} SipRegistration;
```

The contents of the SipRegistration PDU are:

type the type of the registration

length
: the length of the rest of the PDU

data the registration data

- If the registration is of type "sip_registration_uri", then the contents are an opaque string containing the URI.

- If the registration is of type "sip_registration_route", then the contents are an opaque string containing the callee's contact preferences and a destination list for the peer.

RELOAD explicitly supports multiple registrations for a single AOR. The registrations are stored in a Dictionary with the dictionary keys being Node-IDs. Consider, for instance, the case where Alice has two peers:

- her desk phone (1234)

- her cell phone (5678)

Alice might store the following in the overlay at resource "sip:alice@dht.example.com".

- A SipRegistration of type "sip_registration_route" with dictionary key "1234" and value "1234".

- A SipRegistration of type "sip_registration_route" with dictionary key "5678" and value "5678".

Note that this structure explicitly allows one Node-ID to forward to another Node-ID. For instance, Alice could set calls to her desk phone to ring at her cell phone. It's not clear that this is useful in this case, but may be useful if Alice has two AORs.
In order to prevent hijacking, registrations are subject to access control rules. Before a Store is permitted, the storing peer MUST check that:

- The certificate contains a username that is a SIP AOR that hashes to the Resource-ID being stored at.

- The certificate contains a Node-ID that is the same as the dictionary key being stored at.

Note that these rules permit Alice to forward calls to Bob without his permission. However, they do not permit Alice to forward Bob's calls to her. See Section 8.2.2 (Malicious Retargeting) for more on this point.

TOC

4. Looking up an AOR

When a RELOAD user wishes to call another user, starting with a non-GRUU AOR, he follows the following procedure. (GRUUs are discussed in Section 6 (GRUUs)).

1. Check to see if the domain part of the AOR matches the domain name of an overlay of which he is a member. If not, then this is an external AOR, and he MUST do one of the following:

   *Fail the call.

   *Use ordinary SIP procedures.

   *Attempt to become a member of the overlay indicated by the domain part, if that overlay is a RELOAD overlay.)

2. Perform a Fetch for kind SIP-REGISTRATION at the Resource-ID corresponding to the AOR. This Fetch SHOULD NOT indicate any dictionary keys, which will result in fetching all the stored values.

3. If any of the results of the Fetch are non-GRUU AORs, then repeat step 1 for that AOR.

4. Once only GRUUs and destination lists remain, the peer removes duplicate destination lists and GRUUs from the list and forms a SIP connection to the appropriate peers as described in the following sections. If there are also external AORs, the peer follows the appropriate procedure for contacting them as well.

---

5. Forming a Direct Connection

TOC

Once the peer has translated the AOR into a set of destination lists, it then uses the overlay to route Attach messages to each of those peers. The "application" field MUST be 5060 to indicate SIP. If certificate-based authentication is in use, the responding peer MUST present a certificate with a Node-ID matching the terminal entry in the route list. Note that it is possible that the peers already have a RELOAD connection between them. This MUST NOT be used for SIP messages. However, if a SIP connection already exists, that MAY be used. Once the Attach succeeds, the peer sends SIP messages over the connection as in normal SIP.

---

6. GRUUs

TOC

GRUUs do not require storing data in the Overlay Instance. Rather, they are constructed by embedding a base64-encoded destination list in the gr URI parameter of the GRUU. The base64 encoding is done with the alphabet specified in table 1 of RFC 4648 with the exception that ~ is used in place of =. An example GRUU is "sip:alice@example.com;gr=MDEyMzQ1Njc4OTAxMjM0NTY3ODk~". When a peer needs to route a message to a GRUU in the same P2P network, it simply uses the destination list and connects to that peer.
Because a GRUU contains a destination list, it MAY have the same contents as a destination list stored elsewhere in the resource dictionary.
Anonymous GRUUs are done in roughly the same way but require either that the enrollment server issue a different Node-ID for each anonymous GRUU required or that a destination list be used that includes a peer that compresses the destination list to stop the Node-ID from being revealed.

---

7. SIP-REGISTRATION Kind Definition

TOC

The first mapping is provided using the SIP-REGISTRATION Kind-ID:

> **Kind IDs** The Resource Name for the SIP-REGISTRATION Kind-ID is the AOR of the user. The data stored is a SipRegistrationData, which can contain either another URI or a destination list to the peer which is acting for the user.
>
> **Data Model** The data model for the SIP-REGISTRATION Kind-ID is dictionary. The dictionary key is the Node-ID of the storing peer. This allows each peer (presumably corresponding to a single device) to store a single route mapping.
>
> **Access Control** If certificate-based access control is being used, stored data of Kind-ID SIP-REGISTRATION must be signed by a certificate which (1) contains user name matching the storing URI used as the Resource Name for the Resource-ID and (2) contains a Node-ID matching the storing dictionary key.

Data stored under the SIP-REGISTRATION kind is of type SipRegistration. This comes in two varieties:

> **sip_registration_uri** a URI which the user can be reached at.
>
> **sip_registration_route** a destination list which can be used to reach the user's peer.

8. Security Considerations

TOC

8.1. Overview

TOC

RELOAD provides a generic storage service, albeit one designed to be useful for P2PSIP. In this section we discuss security issues that are likely to be relevant to any usage of RELOAD. In Section 8.2 (SIP-Specific Issues) we describe issues that are specific to SIP.
In any Overlay Instance, any given user depends on a number of peers with which they have no well-defined relationship except that they are fellow members of the Overlay Instance. In practice, these other nodes may be friendly, lazy, curious, or outright malicious. No security system can provide complete protection in an environment where most nodes are malicious. The goal of security in RELOAD is to provide strong security guarantees of some properties even in the face of a large number of malicious nodes and to allow the overlay to function correctly in the face of a modest number of malicious nodes.
P2PSIP deployments require the ability to authenticate both peers and resources (users) without the active presence of a trusted entity in the system. We describe two mechanisms. The first mechanism is based on public key certificates and is suitable for general deployments. The second is an admission control mechanism based on an overlay-wide shared symmetric key.

8.2. SIP-Specific Issues

TOC

8.2.1. Fork Explosion

TOC

Because SIP includes a forking capability (the ability to retarget to multiple recipients), fork bombs are a potential DoS concern. However, in the SIP usage of RELOAD, fork bombs are a much lower concern because the calling party is involved in each retargeting event and can therefore directly measure the number of forks and throttle at some reasonable number.

8.2.2. Malicious Retargeting

TOC

Another potential DoS attack is for the owner of an attractive number to retarget all calls to some victim. This attack is difficult to ameliorate without requiring the target of a SIP registration to authorize all stores. The overhead of that requirement would be excessive and in addition there are good use cases for retargeting to a peer without there explicit cooperation.

8.2.3. Privacy Issues

TOC

All RELOAD SIP registration data is public. Methods of providing location and identity privacy are still being studied.

---

9. IANA Considerations

TOC

This section contains the new code points registered by this document. TODO define SIP usage specific kinds, etc here.

---

10. Acknowledgments

TOC

This draft is a merge of the "REsource LOcation And Discovery (RELOAD)" draft by David A. Bryan, Marcia Zangrilli and Bruce B. Lowekamp, the "Address Settlement by Peer to Peer" draft by Cullen Jennings, Jonathan Rosenberg, and Eric Rescorla, the "Security Extensions for RELOAD" draft by Bruce B. Lowekamp and James Deverick, the "A Chord-based DHT for Resource Lookup in P2PSIP" by Marcia Zangrilli and David A. Bryan, and the Peer-to-Peer Protocol (P2PP) draft by Salman A. Baset, Henning Schulzrinne, and Marcin Matuszewski.
Thanks to the many people who contributed including: Michael Chen, TODO - fill in.

---

11. References

TOC

11.1. Normative References

TOC

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC3263]	Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers," RFC 3263, June 2002 (TXT).
[I-D.ietf-p2psip-base]	Jennings, C., Lowekamp, B., Rescorla, E., Baset, S., and H. Schulzrinne, "REsource LOcation And Discovery (RELOAD) Base Protocol," draft-ietf-p2psip-base-00 (work in progress), October 2008 (TXT).

11.2. Informative References

TOC

[I-D.ietf-p2psip-concepts]	Bryan, D., Matthews, P., Shim, E., Willis, D., and S. Dawkins, "Concepts and Terminology for Peer to Peer SIP," draft-ietf-p2psip-concepts-02 (work in progress), July 2008 (TXT).

Appendix A. Change Log

TOC

A.1. Changes since draft-ietf-p2psip-reload-00

TOC

*Split SIP Usage from combined draft into new draft.

Authors' Addresses

TOC

	Cullen Jennings
	Cisco
	170 West Tasman Drive
	MS: SJC-21/2
	San Jose, CA 95134
	USA
Phone:	+1 408 421-9990
Email:	fluffy@cisco.com

	Bruce B. Lowekamp (editor)
	SIPeerior Technologies
	5251-18 John Tyler Highway #330
	Williamsburg, VA 23185
	USA
Email:	bbl@lowekamp.net
	Eric Rescorla
	Network Resonance
	2064 Edgewood Drive
	Palo Alto, CA 94303
	USA
Phone:	+1 650 320-8549
Email:	ekr@networkresonance.com
	Salman A. Baset
	Columbia University
	1214 Amsterdam Avenue
	New York, NY
	USA
Email:	salman@cs.columbia.edu
	Henning Schulzrinne
	Columbia University
	1214 Amsterdam Avenue
	New York, NY
	USA
Email:	hgs@cs.columbia.edu

Full Copyright Statement

TOC

Intellectual Property

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.