Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 3, 2007

E. Marocco
Telecom Italia
D. Bryan
SIPeerior Technologies Inc.

March 2, 2007

Interworking between P2PSIP Overlays and Conventional SIP Networks
draft-marocco-p2psip-interwork-01

Status of this Memo

Copyright Notice

Abstract

This document describes how user agents registered in P2PSIP overlay networks can interwork with those in conventional SIP networks. Communications between any two user agents will happen through the SIP protocol and the location of SIP servers will follow the usual procedures. However, interworking in some environments may require the support of additional elements; this document also describes such elements and how to locate them in P2PSIP overlays.

Table of Contents

1. Introduction

This document describes how user agents registered in P2PSIP overlay networks [I-D.willis-p2psip-concepts] can interwork with those in conventional SIP networks [RFC3261]. In particular, no assumption is made about the overlay but that it allows clients and peers to insert and retrieve routing information, possibly bound to URIs [RFC3986].

The main goal of peer-to-peer networks is to build distributed systems using resources such as bandwidth, storage and computation power, shared by participating peers. P2PSIP overlay peer protocols, in particular, aim to enable lookup services for clients initiating and managing SIP protocol sessions without relying on central servers.

To enable P2PSIP overlays to fully interwork with conventional SIP networks (i.e. handling sessions either originated or terminated in public domains), some peers must provide more resources than those required for maintaining the overlay through the P2PSIP peer protocol. Indeed, connectivity with public domains requires some peers willing to share their ability to exchange messages with public hosts on the Internet and, even more important, to be registered in the public naming service (DNS) for a fully qualified domain name (FQDN) which uniquely identifies the overlay they participate in.

The purpose of this document is to define the elements which can supply the additional resources required for full interworking, to specify how such elements can register and be located within the overlay, and to describe how user agents (UAs) can establish sessions across overlay boundaries.

1.1. 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 RFC 2119 [RFC2119].

Terminology defined in RFC 3261 [RFC3261] and in P2PSIP concepts draft [I-D.willis-p2psip-concepts] is used without definition.

Conventional SIP Network: A SIP network where location and routing functionalities are provided by centralized elements, as described in RFC 3261 [RFC3261].

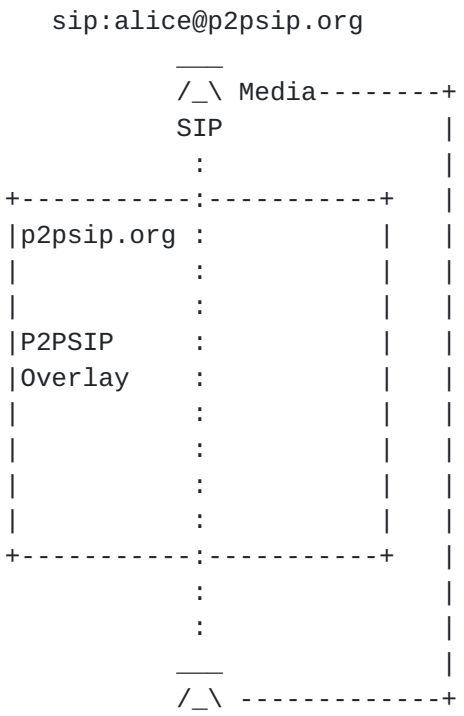
Public SIP Network: A SIP network, either conventional or P2PSIP based, whose user agents can be located using procedures specified in RFC 3263 [RFC3263].

P2PSIP Proxy Peer: An element registered with the P2PSIP overlay which is able to route SIP messages directed to public URLs. If a P2PSIP proxy peer is bound to a FQDN, it can be used also for routing SIP messages directed to UAs in the P2PSIP overlay.

Relay Agent Peer: An element registered with the P2PSIP overlay which provides relayed transport addresses through protocols like TURN [I-D.ietf-behave-turn] and TEREDO [RFC4380] for allowing media streaming between UAs without direct connectivity.

2. Overview

User agents registered in a P2PSIP overlay are able to reach each other through the SIP protocol, with resource location handled by the overlay itself. Figure 1 shows a typical example of the very basic deployment, where the overlay supplies the functionalities which, in canonical networks, are usually provided by registrars and proxies.

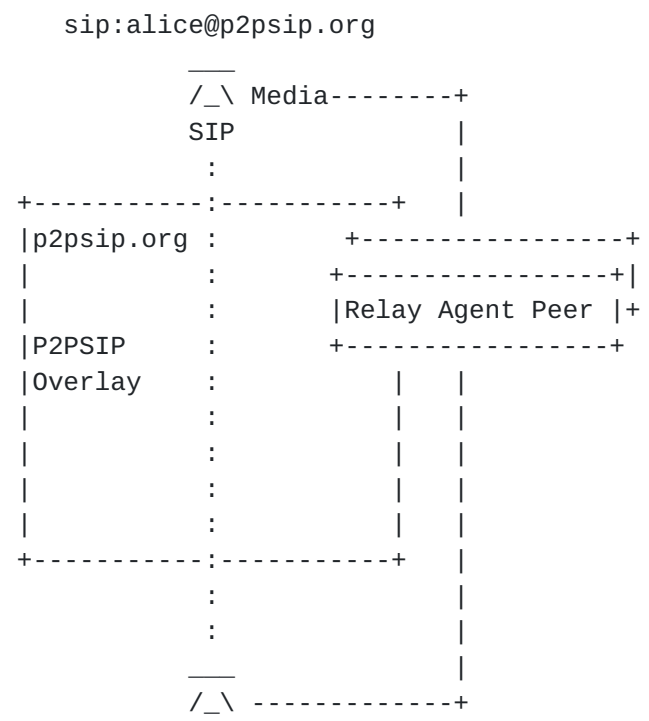


Session between P2PSIP user agents. Media streams flow directly between UAs.

Figure 1

The example in Figure 1 requires that all UAs have direct connectivity with each other. However, since such connectivity is often impeded by environmental constraints introduced by NATs, firewalls or simply by lack of physical links, resources other than those used for maintaining the overlay are generally needed for users to effectively establish multimedia sessions.

Figure 2 shows an example where UAs use the overlay to store and locate locations of relay agent peers (Section 3.2) used to effectiverly exchange data such as media even when NATs are present.

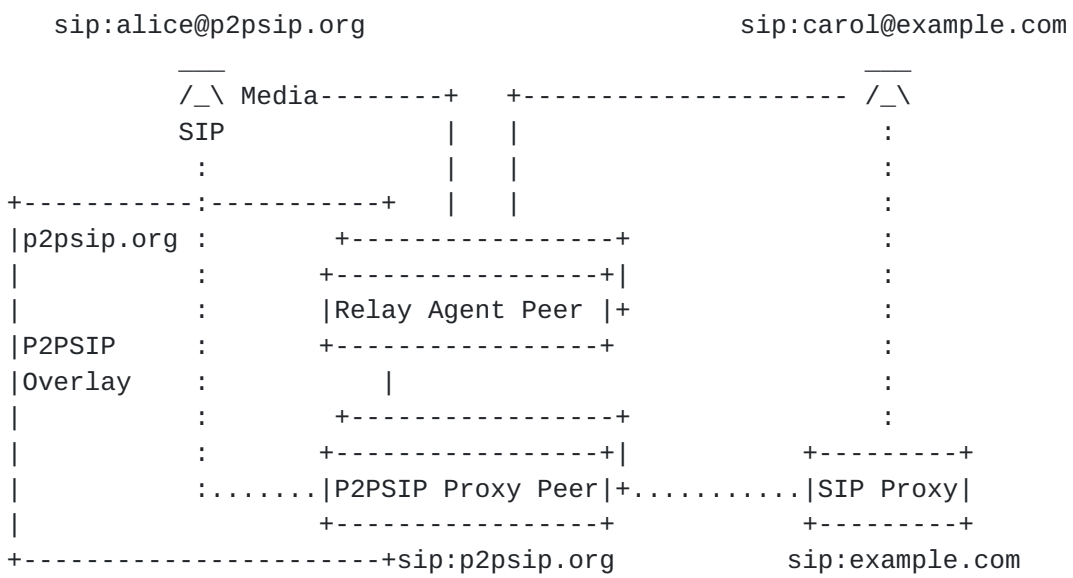


Session between P2PSIP user agents. Media streams are relayed.

Figure 2

Overlays such as those depicted in Figure 1 and Figure 2 can be used only for local communications. Even in network environments where connectivity is not a problem, interworking with non-P2PSIP nodes must be considered. While P2PSIP UAs can initiate sessions with conventional SIP UAs using common resolution procedures defined in RFC 3263 [RFC3263], they cannot be addressed in any way from outside the overlay.

Overlays intended to provide global connectivity must provide interworking with canonical SIP, in addition to providing relaying services amongst the P2PSIP overlay peers. These overlays must provide mechanisms for routing SIP messages to conventional SIP entities in the public Internet and to be located and contacted using standard SIP procedures. Figure 3 shows an example where communication is enabled both within the overlay and across its boundaries, thanks to resources shared by P2PSIP Proxy Peers (Section 3.1).



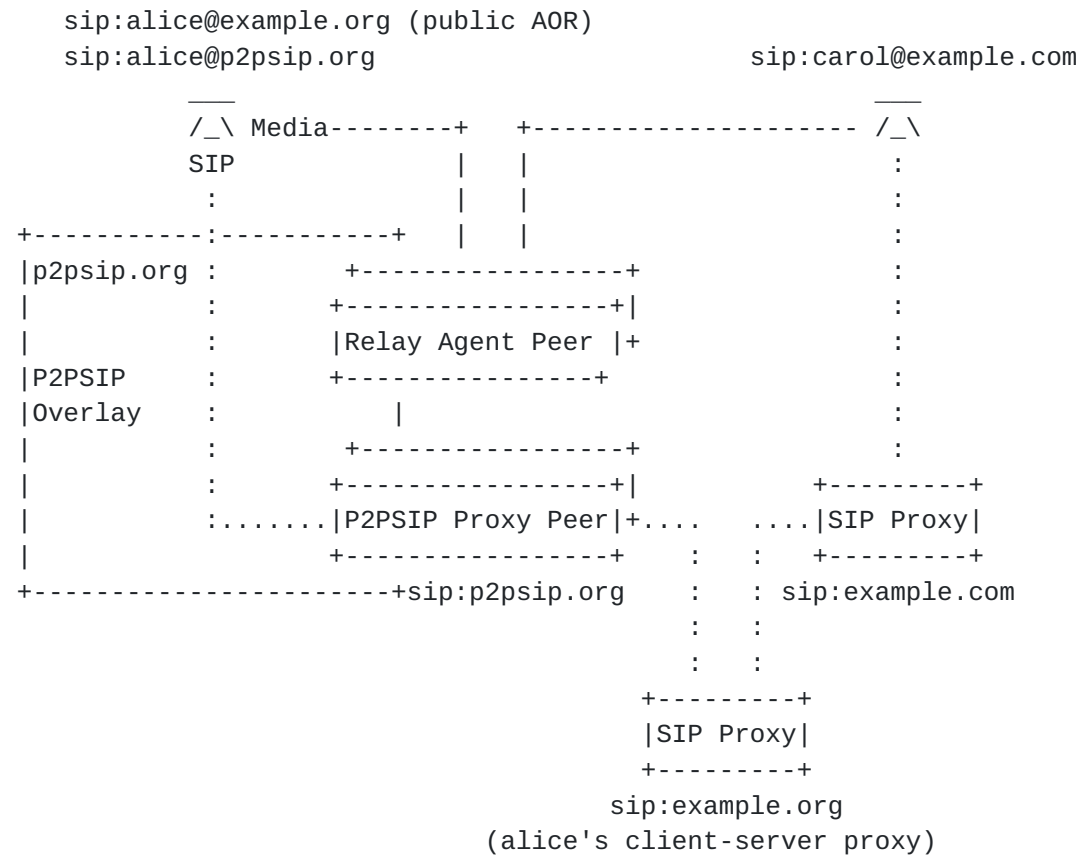
Example of a system connecting a UA in a P2PSIP overlay and one in a conventional SIP network. The user in the P2PSIP overlay is addressed by her local URI and data streams are relayed.

Figure 3

It is worth noting that, in the example in Figure 3, users who register in the overlay MUST have URLs whose host parts match with the FQDN for which overlay's P2PSIP proxy peers are bound to. That is, the P2P overlay identifier for the overlay must be an FQDN. Section 4 defines the detailed procedure for user registration.

Overlays such as the one in Figure 3, which have resources for both relaying data and routing SIP messages to and from public servers can be considered equivalent to conventional SIP networks when viewed from the outside. Such a property is extremely important for P2PSIP UAs which have also an account with conventional SIP providers, but do not have direct connectivity with their servers. Indeed, such UAs, following the usual procedures defined in RFC 3261 [RFC3261], can register their overlay URL as a contact for their conventional SIP address of record (AOR).

Figure 4 shows an example where a user (alice) registers both in an overlay (p2psip.org) and, through P2PSIP proxy peers, with a conventional SIP network (sip:example.org). SIP messages sent by another user (carol) who only knows her conventional SIP URL (sip:alice@example.org) are routed to her conventional SIP proxy (sip:example.org) and, from here, to overlay's P2PSIP proxy peers(sip:p2psip.org) which eventually reach her through the overlay.



Interworking between one UA in a P2PSIP overlay and one in a conventional SIP network. The user in the P2PSIP overlay is addressed by her well known global URI and data streams are relayed

Figure 4

2.1. P2PSIP Overlay Identifier

For overlays which wish to interconnect with existing SIP networks, the P2PSIP overlay identifier MUST be a FQDN. Moreover, some entity (humans or automata) responsible for the overlay MUST be able to manipulate DNS records referring to such identifier for registering and unregistering P2PSIP proxy peers as defined in Section 3.1.

Procedures for selecting overlay identifiers and for manipulating DNS records are outside of the scope of this document.

3. Additional Logical Elements for Interworking

This section describes the network elements which provide the additional resources that P2PSIP overlays need for interworking with conventional SIP networks. Note that these are logical roles, and may (and in fact likely would) be combined into one entity such as a P2PSIP UA. As with the functions in RFC 3261 [RFC3261], we treat them as separate entities in this document for clarity.

3.1. P2PSIP Proxy Peer

A P2PSIP proxy peer, as mentioned in [I-D.willis-p2psip-concepts] (Section 3.1, "What Kinds of P2PSIP Peers and Clients Might Exist?"), is an element which can exchange SIP messages with public domains and provides this function as a service to the overlay it is registered in. In particular, the most important characteristics are the following:

- A P2PSIP proxy peer MUST be able to send SIP requests and receive SIP responses directed to hosts with a public Internet address.

- A P2PSIP proxy peer MUST be able to perform location procedures defined in RFC 3263 [RFC3263]. This implies that it MUST also be able to query the DNS.

- A P2PSIP proxy peer SHOULD have a binding in the DNS so that any resolution for the overlay identifier performed according to location procedures defined in RFC 3263 [RFC3263] returns a list of P2PSIP proxy peers including this node. If such binding doesn't exist for any of the P2PSIP proxy peers, the overlay cannot be reached by public SIP networks.

P2PSIP proxy peer MUST record route on SIP request crossing overlay's boundaries, using the overlay identifier instead of their local address, due to the ephemeral nature of P2PSIP nodes.

3.1.1. Insertion into DNS

The mechanism for registering P2PSIP proxy peers with the DNS is a critical point of the overlay. In fact, if the authorization policies are too permissive, it could be exploited by malicious nodes for denial of service attacks, while, if they are too strict, it could introduce a bottleneck in negation with the peer-to-peer model. Future specifications need to provide mechanisms for managing controlled registration with the DNS, allowing the adoption of different policies in different deployments.

P2PSIP proxy peers will generally be located on devices with direct

Internet access. It is NOT RECOMMENDED to insert records in the DNS for P2PSIP proxy peers behind NATs. While NAT traversal mechanisms such as STUN [I-D.ietf-behave-rfc3489bis] and TEREDO [RFC4380] can be used to determine a public address and port which can be registered in the DNS, NAT binding changes are not deterministic and can cause inconsistencies.

3.2. Relay Agent Peer

A relay agent peer is an element which can directly exchange media with hosts on the public Internet. STUN relay servers (previously called TURN servers), specified in the STUN draft [I-D.ietf-behave-turn] and TEREDO [RFC4380] relays are typical examples of relay agents.

Relay agent peers can be located behind some types of NATs if, using traversal mechanisms not based on relay (e.g. STUN [I-D.ietf-behave-rfc3489bis]), they can obtain several public address-port pairs.

3.2.1. Relay Agent Peer Selection

It is extremely difficult to determine apriori which type of relay agent peer fits best for a media session with a particular UA. To avoid this choice, UAs SHOULD find as many relay agent peers as possible and MUST establish media sessions using the ICE [I-D.ietf-mmusic-ice] mechanism so that the most appropriate relay can be chosen at run time.

3.3. Locating the new Elements

P2PSIP UAs often need to locate resources or obtain services provided by P2PSIP proxy peers and relay agent peers. Such lookup is performed directly in the overlay through the P2PSIP client protocol.

One possible way to allow the location of resources within the overlay is to define URI for identifying the elements which provide them. While many mechanisms are possible, we outline a simple possible approach below.

3.3.1. P2PSIP Proxy Peer URI

P2PSIP proxy peers act as SIP servers and are identified by SIP URLs. Such URLs MUST have only the host field set, and its value MUST match the overlay identifier.

For example, the URL which identifies P2PSIP proxy peers registered within the overlay "p2psip.org" could be "sip:p2psip.org".

It is worth noting that the lookups of P2PSIP proxy peers, made in the overlay or in the DNS, are conceptually identical.

3.3.2. Relay Agent Peers URIs

Since relay agent peers can implement different protocols, there will be different URI schemas for identifying each kind. As a general rule, URLs identifying relay agent peers which implement a given protocol, will be formed according to the specific scheme and will have the host field (or the equivalent field) matching the overlay identifier.

While such URI schema do not currently exist, one could use something like "turn:p2psip.org" and "teredo:p2psip.org" identify relay agent peers registered in the overlay "p2psip.org" and implementing TURN and TEREDO protocols respectively.

3.3.3. Impacts on the Overlay

In overlays where the load balancing among all peers utilizes a key-partitioning approach, the lookup of services based on well known URIs would cause dangerous displacements of the overlay traffic. In fact, since many clients and peers need to know the location of a relay agent peer, the peer responsible for a URI which identifies any of those would have to handle much more lookup requests than other peers which store only user records.

4. User Registration

In order to be reachable from a conventional SIP UA, a UA participating in a P2PSIP overlay that supports interworking MUST create a binding in the overlay between its local contact and an URL (i.e. P2PSIP overlay user identifier) as defined in Section 4.1. If the user associated with the UA has another public SIP URI, they MAY register such a URL with the authoritative registrar using a P2PSIP proxy peer as described in Section 4.2.

4.1. Registering with the Overlay

UAs perform registration in the overlay through the P2PSIP client protocol. Such registration consists of an insertion of a P2PSIP overlay user routing record bound to the user identifier.

To support interworking with canonical SIP, the user identifier MUST be a well formed SIP URL, with the host field matching the overlay identifier. The user field MUST be set, and its value will usually be the P2PSIP overlay user identifier.

According to local policies, the user MAY need to enroll and obtain appropriate credentials for their URL before being able to register records for it.

4.2. Registering with a Public SIP Network

Users registered in fully interworking P2PSIP overlays can use P2PSIP proxy peers for sending messages to public SIP networks. This is especially useful for registering bindings for AORs for which the overlay is not authoritative. This mechanism can be used to register the contact for a node participating in a P2PSIP overlay with a well known SIP URI associated with the user that is well known to their usual buddies but outside the overlay.

For registering with a public SIP network, an UA follows these steps:

1. The UA MUST perform user registration as defined in Section 4.1.

2. The UA MUST get the address of a P2PSIP proxy peer performing a lookup as defined in Section 3.3.

3. The UA MUST send a REGISTER message for binding the URL it has registered in the overlay to its public AOR. The message MUST be sent using the P2PSIP proxy peer as an outbound proxy.

5. Examples

5.1. Caller and Callee within the Overlay

The following example refers to the network depicted in Figure 2.

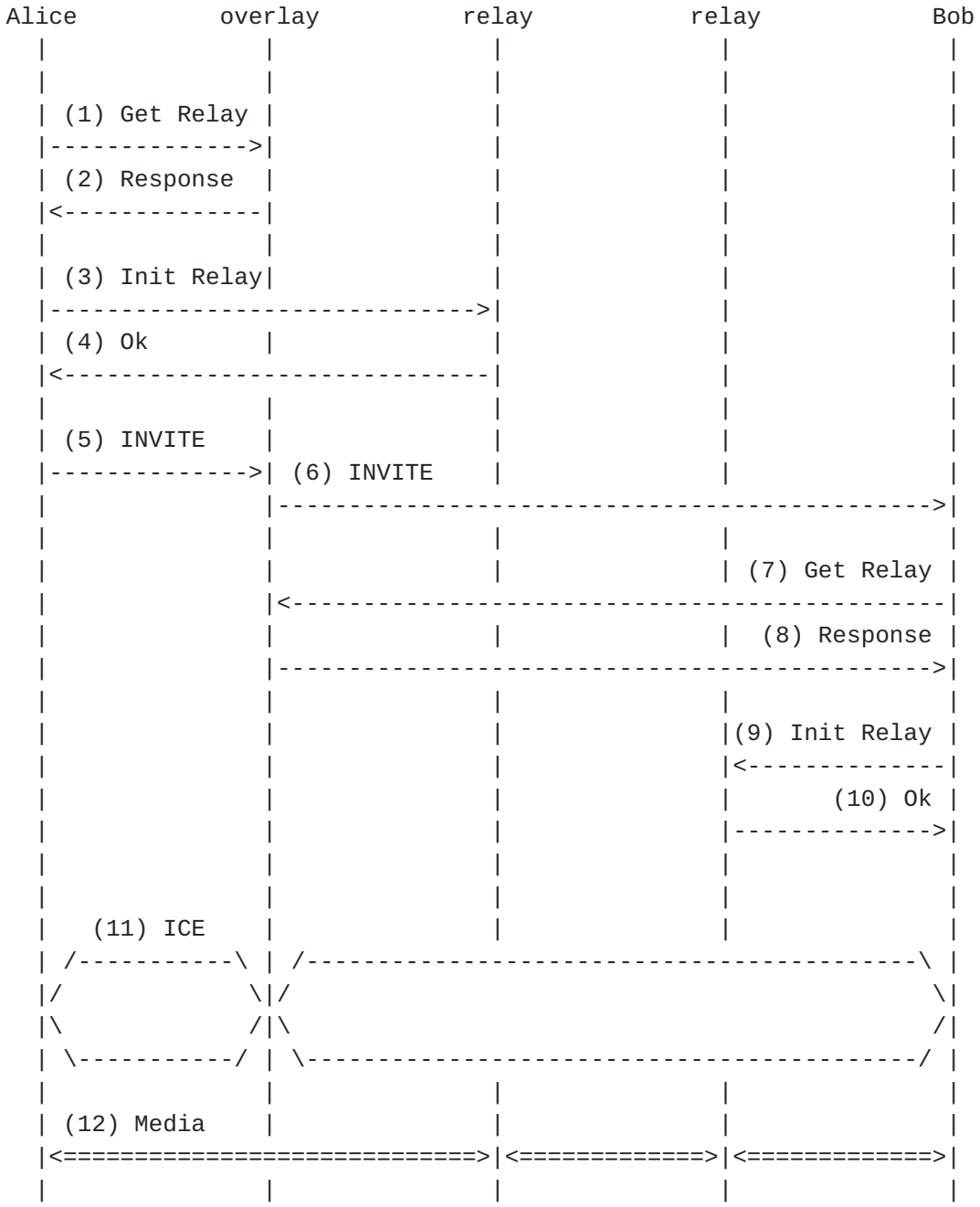


Figure 5

First Alice queries the overlay for discovering the location of some relay agent peers (1-2) and initializes one (3-4) for preparing an ICE candidate. Then she sends an INVITE request with an ICE offer to Bob through the overlay (5-6).

When Bob receives the INVITE, he queries the overlay to obtain the location of some relay agent peers (7-8) and initializes one (9-10) for preparing an ICE candidate. Then the session establishment completes carrying ICE offers and answers and following the signaling path of the first INVITE (11).

Eventually, the media is relayed across both Alice's and Bob's relay agent peers (12).

5.2. Callee within a Public SIP Network

The following example refers to the network depicted in Figure 3.

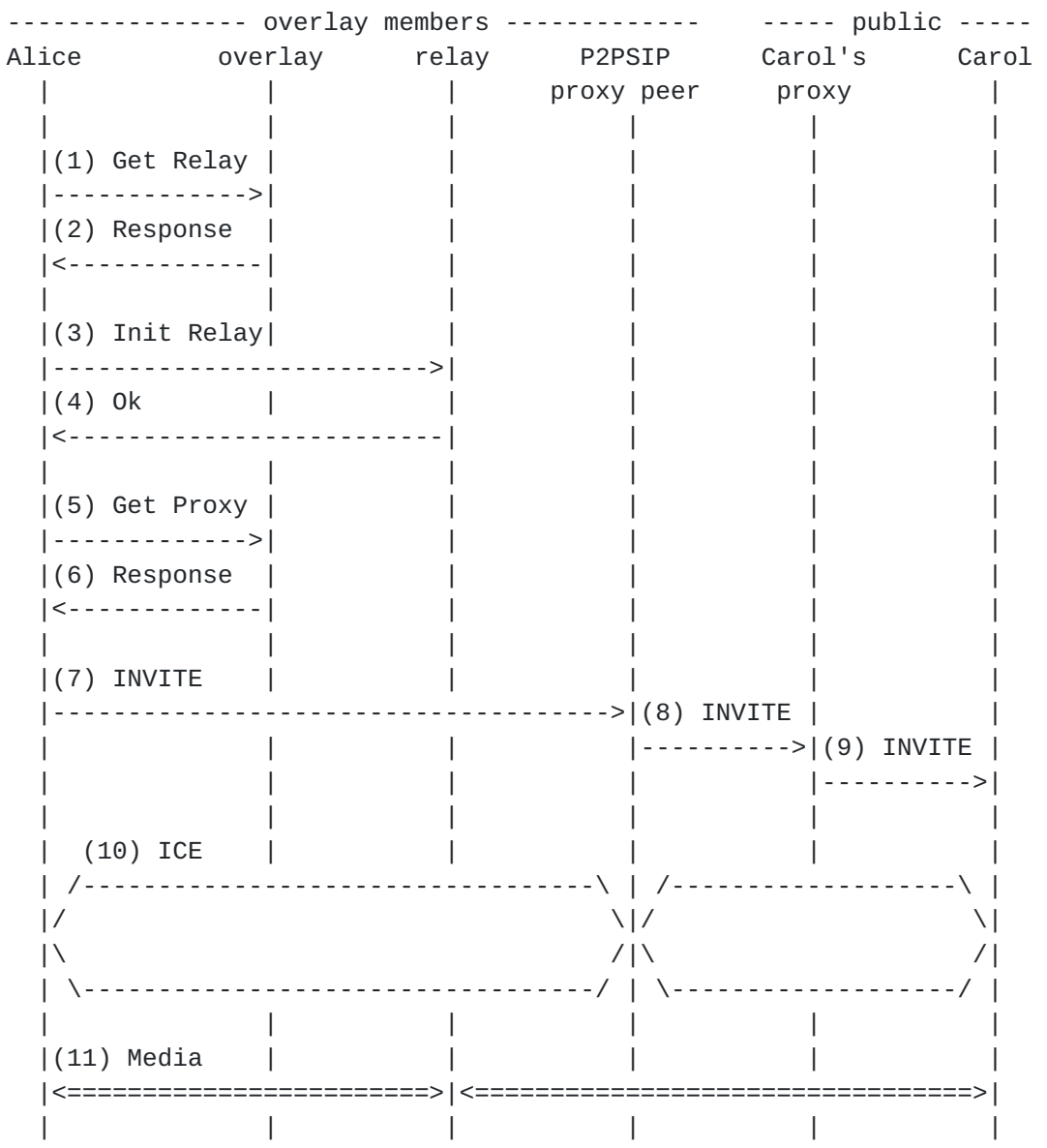


Figure 6

First Alice queries the overlay for discovering the location of one or more relay agent peers (1-2) and initializes one (3-4) for preparing an ICE candidate. Then she queries the overlay requesting the location of some P2PSIP proxy peers (5-6) and sends an INVITE request with an ICE offer to Carol through one of those (7).

The P2PSIP proxy peers performs common location procedures and discovers the address of Carol's authoritative proxy for routing the INVITE. Before sending (8), it adds to the message a Record-Route header with a value equal to the overlay identifier, so that any

other request will reach a P2PSIP proxy peer registered in the same overlay. Carol's location is found by her proxy based on registration information (9).

When Carol receives the INVITE, the session establishment completes carrying ICE offers and answers (if supported) (10).

Media is relayed across Alice's relay agent peer (11).

5.3. Caller within a Public SIP Network

The following example refers to the network depicted in Figure 3.

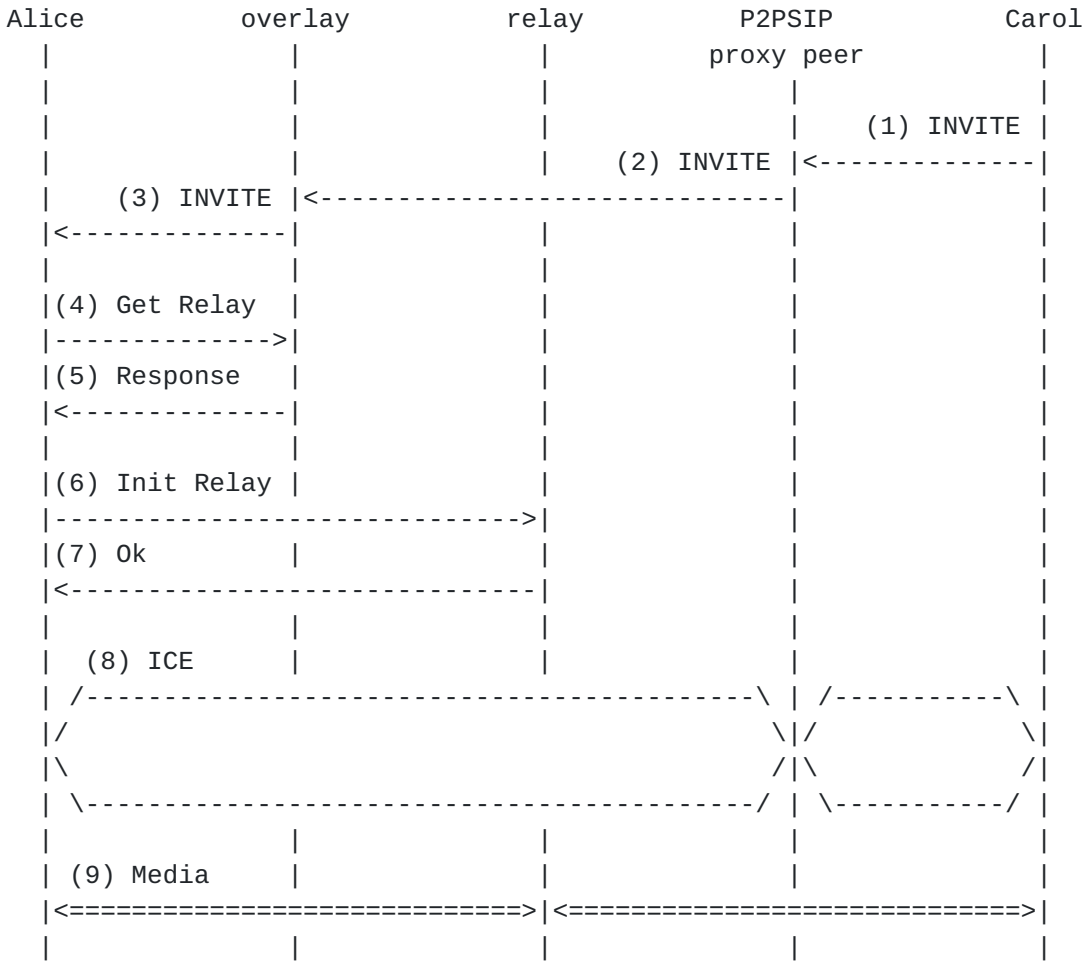


Figure 7

When Carol wants to contact Alice (using the address bound to the P2P

overlay identifier), she performs a conventional SIP location procedure (RFC3263) and finds the address of one or more P2PSIP proxy peers for the overlay. Carol then sends an INVITE message addressed to Alice to any one of the set of such addresses (1). The P2PSIP proxy peer routes the INVITE to Alice through the overlay (2-3) using the overlay's resource location and routing mechanisms.

When Alice receives the INVITE, she queries the overlay to discover the location of one or more relay agent peers (4-5) and initializes one for preparing an ICE candidate (or an answer, if the INVITE didn't declare to support ICE) (6-7).

Then the session establishment completes carrying ICE offers and answers (if the INVITE declared to support it) (8).

Finally, media is relayed across Alice's relay agent peer (9).

5.4. Callee Registered in a Public Network from an Overlay

The following example refers to the network depicted in Figure 3.

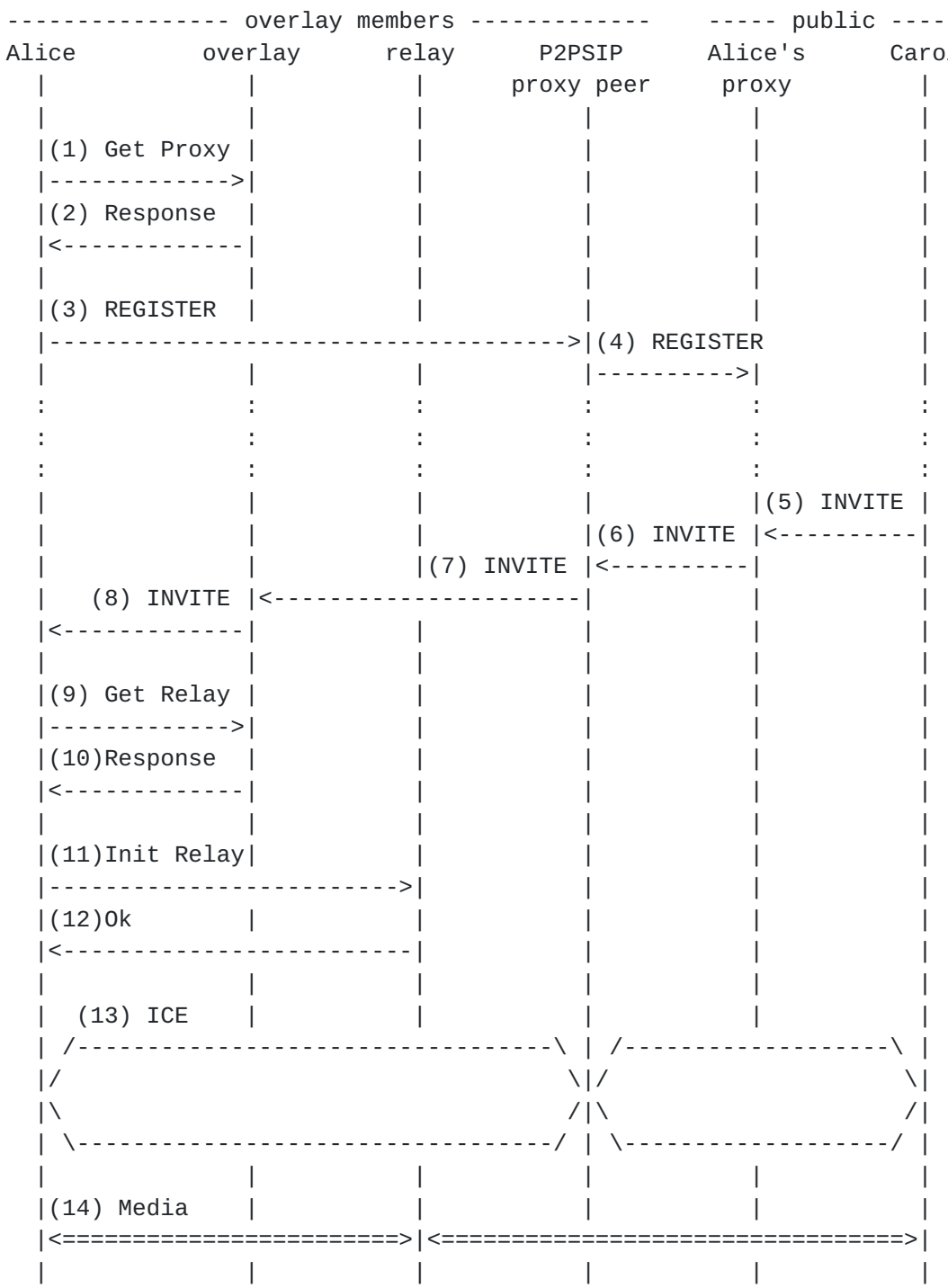


Figure 8

Right after registering in the overlay, Alices queries the location of some P2PSIP proxy peers (1-2) and sends a REGISTER request to her public SIP server through one of them, binding the URL registered in

the overlay to her public AOR (4-3).

When Carol wants to contact Alice, she sends an INVITE request addressed to her public SIP proxy (5). The proxy finds in its local database the binding with the URL registered in the overlay, so it performs a conventional SIP location procedure (RFC3263) for the overlay identifier (i.e. the domain of the URL) and finds the address of one or more P2PSIP proxy peers. Then it routes the INVITE message to any of those (6), which in turn routes the INVITE to Alice through the overlay (7-8) using the overlay's resource location and routing mechanisms.

When Alice receives the INVITE, she queries the overlay to discover the location of one or more relay agent peers (9-10) and initializes one for preparing an ICE candidate (or an answer, if the INVITE didn't declare to support ICE) (11-12).

Then the session establishment completes carrying ICE offers and answers (if the INVITE declared to support it) (13).

Finally, media is relayed across Alice's relay agent peer (14).

6. Security Considerations

Besides the security issues already raised in SIP [2] and other P2PSIP work, the interconnection model based on "well known" URIs is vulnerable to spoofing attacks. More work, or the application of existing SIP work on identity should applied to this to mitigate this risk.

Another security issue is the registration of P2PSIP proxy peers with a public DNS; it could be either a point of failure, if registration policies are too permissive, or a threat to the peer-to-peer model, if they are too restrictive. Mechanisms must allow for nodes to be entered and removed, in a secure fashion. This work is related to and likely to use dynamic DNS.

In a full interworking scenario identity assertion is critically important; this document shows how it could be achieved proxying regular authentication to traditional SIP domains. Mechanisms such as issuing certificates to assert and validate user identities should be used.

7. Open Issues

1. We need to define a mechanism for authenticating, inserting and removing DNS records for the overlay. Need to work with dynamic DNS group to address this.

2. Service location based on well-known URIs impacts the overlay load-balance, especially if it is based on key partitioning among peers.

3. Clients route SIP messages addressed to external hosts directly to P2PSIP proxy peers, without involving the overlay. We should define in details how and why this works, but there are some implications on the P2PSIP client protocol to be defined. If the overlay is supposed to let also conventional SIP user agents work, such routing must be done directly by peers.

4. URI schemes for relay agent peers are not defined and are also needed for things besides interworking. Is it feasible to define URNs for those protocols for which a URI schema does not exist?

5. As security/identity mechanisms for P2PSIP (certificate based or otherwise) emerge, they should be worked into this document.

8. Changes

8.1. Changes from 00

Introduced the issue of the P2PSIP proxy peer registration with the DNS outside "Security Considerations".

Introduced the issue of load-balancing when lookup is based on well-known URIs.

Included the example showing registration with public SIP networks.

9. References

9.1. Normative References

[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.

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

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

9.2. Informative References

[I-D.ietf-behave-rfc3489bis] Rosenberg, J., "Simple Traversal Underneath Network Address Translators (NAT) (STUN)", draft-ietf-behave-rfc3489bis-04 (work in progress), July 2006.

[I-D.ietf-behave-turn] Rosenberg, J., "Obtaining Relay Addresses from Simple Traversal of UDP Through NAT (STUN)", draft-ietf-behave-turn-01 (work in progress), June 2006.

[I-D.ietf-mmusic-ice] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", draft-ietf-mmusic-ice-09 (work in progress), June 2006.

[I-D.willis-p2psip-concepts] Willis, D., Bryan, D., Matthews, P., and E. Shim, "Concepts and Terminology for Peer to Peer SIP", draft-willis-p2psip-concepts-00 (work in progress), June 2006.

[RFC4380] Huitema, C., "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)", RFC 4380, February 2006.

Authors' Addresses

Enrico Marocco
Telecom Italia
Via G. Reiss Romoli, 274
Turin 10148
Italy

Phone: +39 011 228 5029
Email: enrico.marocco@telecomitalia.it

David Bryan
SIPeerior Technologies, Inc. and College of William and Mary
3000 Easter Circle
Williamsburg, VA 23188
USA

Phone: +1.757.565.0101
Email: dbryan@SIPeerior.com

Full Copyright Statement

Intellectual Property

Acknowledgment

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