

Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 29, 2016

M. Boucadair
France Telecom
R. Parthasarathi
Nokia Networks
November 26, 2015

Port Control Protocol (PCP) for SIP Deployments in Managed Networks
draft-boucadair-pcp-sip-ipv6-07

Abstract

This document discusses how PCP (Port Control Protocol) can be used in SIP deployments in managed networks. This document applies for both IPv4 and IPv6.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on May 29, 2016.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Internet-Draft

PCP & SIP

November 2015

Table of Contents

1.	Introduction	2
2.	PCP Features	4
2.1.	Learn External IP Address and Port Number	4
2.2.	Learn and Set the Lifetime of Mapping Entries	6
2.3.	Allow Unidirectional Media Flows	6
2.4.	Preserve Port Parity	7
2.5.	Preserve Port Contiguity	7
2.6.	Learn PREFIX64	8
2.7.	Compliant with "a=rtcp" Attribute	10
2.8.	DSCP Marking Policy	10
3.	Avoid Crossing CGNs	11
3.1.	Avoid NAT64	11
3.2.	Avoid Crossing DS-Lite AFTR	12
4.	Security Considerations	12
5.	IANA Considerations	12
6.	Acknowledgements	12
7.	References	13
7.1.	Normative References	13
7.2.	Informative References	13
	Authors' Addresses	16

[1.](#) Introduction

The base Port Control Protocol (PCP, [\[RFC6887\]](#)) specification allows to retrieve the external IP address and external port to be conveyed in the SIP signaling messages [\[RFC3261\]](#). Therefore, SIP Proxy Servers do not need to support means to ease the NAT traversal of SIP messages (e.g., [\[RFC5626\]](#), [\[RFC6223\]](#), etc.). Another advantage of using the external IP address and port is this provides a hint to the proxy server there is no need to return a small expire timer (e.g., 60s). In addition, the outbound proxy does not need any further feature to be supported in order to assist the remote endpoint to successfully establish media sessions. In particular, ALGs are not required in the NAT for this purpose and no dedicated functions at the media gateway are needed.

This document discusses how PCP can be used in SIP deployments (including IPv6 considerations).

The benefits of using PCP for SIP deployments are listed below:

- o Avoid embedding an ALG in the middleboxes. Note, ALGs are not recommended since the evolution of the service would depend on the ALG maintenance.

- o Not require any Hosted NAT Traversal function (e.g., [[RFC7362](#)]) to be embedded in the SIP server. Intermediate NATs and firewalls are transparent to the SIP service platform.
- o Avoid overloading the network with keepalive message to maintain the mapping in intermediate middleboxes.

Note, mechanisms such as STUN do not allow to discover the lifetime assigned by the middleboxes; frequent keepalive messages are therefore generated to maintain binding entries on those middleboxes. PCP is superior to those mechanisms as it allows to retrieve the assigned lifetime, and to provide hints to the middleboxes in order to decide which lifetime value is to be assigned for that particular flow.

- o Work without requiring symmetric RTP/RTCP [[RFC4961](#)].
- o Not require symmetric SIP to work (i.e., rport [[RFC3581](#)]).
- o Easily support unidirectional sessions.
- o Does not encounter issues with early media.
- o The combination of PCP and ALTC [[RFC6947](#)] allows to optimize IPv4-IPv6 interworking function resources.
- o Because there is no need for connectivity checks, session establishment delay is not impacted (pairs of ports can be pre-reserved).
- o The binding entries maintained by a flow-aware device (NAT/Firewall) can be associated with a textual description ([[RFC7220](#)]).

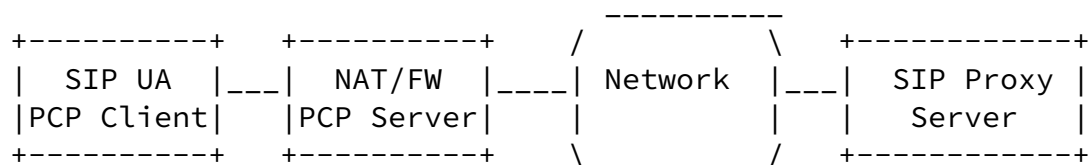
Experimentation results, including SIP flow examples, are documented in [[I-D.boucadair-pcp-nat64-experiments](#)].

In deployments where ICE [[RFC5245](#)] is required, PCP can be of great help as discussed in [[I-D.penno-rtcweb-pcp](#)] for the WebRTC case. ICE can be used in the context of SIP over WebSocket [[RFC7118](#)] and WebRTC when deployed within managed networks. Because TURN suffers from limitations in traversing NAT and firewalls over UDP, PCP is a promising solution that can complement ICE in those deployment contexts to soften the experienced high failure rate [[ICEFailure](#)].

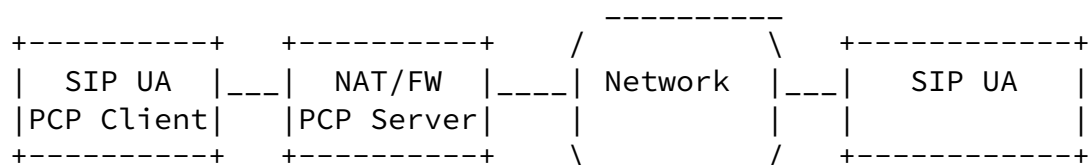
The document targets SIP deployments in managed networks. It can also be used as part of SIP-based services delivery in the context of

network-located residential gateway effort [[WT-317](#)]. Typical deployment scenarios are shown in Figure 1.

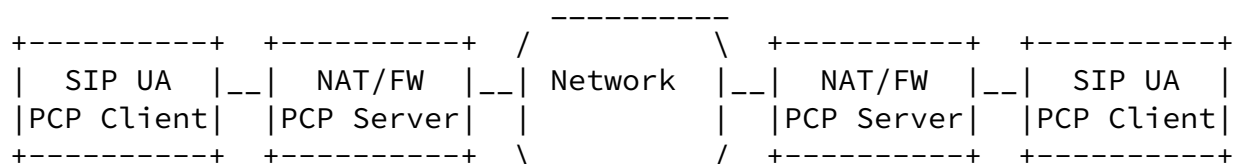
(a) SIP UA behind a NAT/FW communicating with a Proxy Server



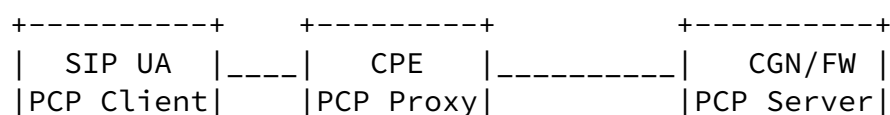
(b) SIP UA behind a NAT/FW communicating with a remote SIP UA



(c) SIP UAs behind a NATs/FWs



(d) SIP UA behind a CPE: PCP Proxy



+-----+ +-----+ +-----+

Figure 1: Typical deployment scenarios

The PCP server can be provisioned using a variety of means (e.g., [RFC7291]) or rely on the discovery method specified in [RFC6887].

This document does not make any assumption whether the PCP client is implemented as an OS service or whether it is integrated in the SIP User Agent (UA). Those considerations are implementation-service.

2. PCP Features

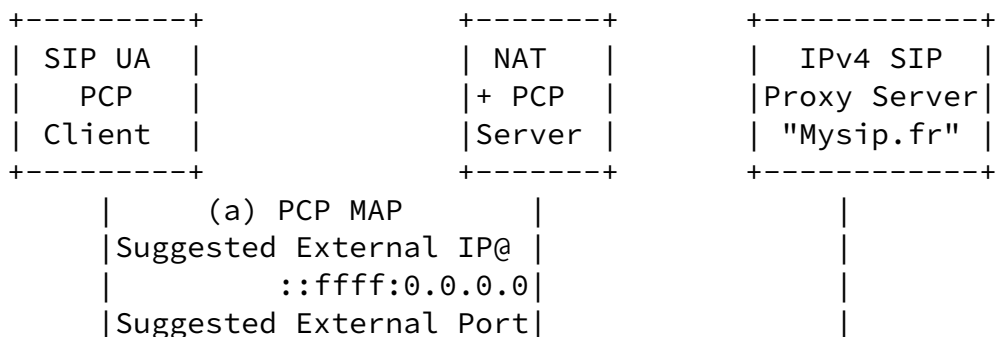
2.1. Learn External IP Address and Port Number

The PCP base specification allows to create mappings in PCP-controlled devices and therefore prepare for receiving incoming

packets. A SIP UA can use PCP to create one mapping for SIP signalling messages and other mappings for media session purposes.

The SIP UA uses the external IP address and port number to build SIP headers. In particular, this information is used to build the VIA and CONTACT headers.

Figure 2 shows an example of the flow exchange that occurs to retrieve the external IP address and an external IP address assigned by the NAT, while Figure 2 provides an excerpt of the SIP REGISTER message issued by the SIP UA; only the assigned IP address and port number are present in the SIP headers.



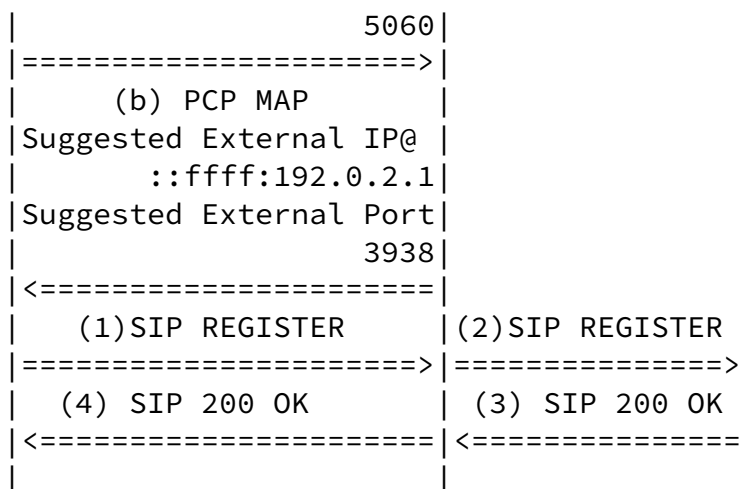


Figure 2: SIP REGISTER Call Flow

SIP Message:

```
REGISTER sip:mysip.fr SIP/2.0
Via: SIP/2.0/UDP 192.0.2.1:3938;branch=z9hG4bK1572043597
From: <sip:client4@mysip.fr:5070>;tag=893886783
To: <sip:client4@mysip.fr:5070>
Call-ID: 1271173454
CSeq: 2 REGISTER
Contact: <sip:client4@192.0.2.1:3938;line=b3433a7df33282d>
    Authorization: Digest username="client4", realm="asterisk",
    nonce="09f75e47", uri="sip:mysip.fr",
    response="826fcff4c6e84ee45fbfa52c351e6316", algorithm=MD5
Max-Forwards: 70
User-Agent: Linphone/3.4.0 (eXosip2/unknown)
Expires: 3600
```

Figure 3: Example of REGISTER messenger

The external IP address and port(s) instantiated for media streams, are used to build the SDP offer/answer. In particular, the "c" line and "m" lines.

[2.2.](#) Learn and Set the Lifetime of Mapping Entries

PCP allows to discover and to set the lifetime of mapping instantiated in intermediate middleboxes.

The discovery of the lifetime of a mapping avoids overloading the network and SIP servers with frequent messages. This is in particular important for cellular devices. According to [\[Power\]](#), the consumption of a cellular device with a keep-alive interval equal to 20 seconds (that is the default value in [\[RFC3948\]](#) for example) is 29 mA (2G)/34 mA (3G). This consumption is reduced to 16 mA (2G)/24 mA (3G) when the interval is increased to 40 seconds, to 9.1 mA (2G)/16 mA (3G) if the interval is equal to 150 seconds, and to 7.3 mA (2G)/14 mA (3G) if the interval is equal to 180 seconds. When no keep-alive is issued, the consumption would be 5.2 mA (2G)/6.1 mA (3G). The impact of keepalive messages would be more severe if multiple applications are issuing those messages (e.g., SIP, IPsec, etc.).

[2.3.](#) Allow Unidirectional Media Flows

As a consequence of instantiating mappings for media/session flows, incoming packets can be successfully forwarded to the appropriate SIP UA. Particularly, unidirectional media flows (e.g., announcement server) will be forwarded accordingly.

[2.4.](#) Preserve Port Parity

For deployments relying on classic RTP/RTCP odd/even port numbers assignment scheme, PORT_SET option [\[I-D.ietf-pcp-port-set\]](#) can be used by a SIP UA to request port parity be preserved by the PCP server.

An example is depicted in Figure 4.

2.5. Preserve Port Contiguity

For deployments assuming RTP port number can be deduced from the RTP port number, PORT_SET option [[I-D.ietf-pcp-port-set](#)] can be used by a SIP UA to retrieve a pair of contiguous ports from the PCP server.

A flow example is shown in Figure 4.

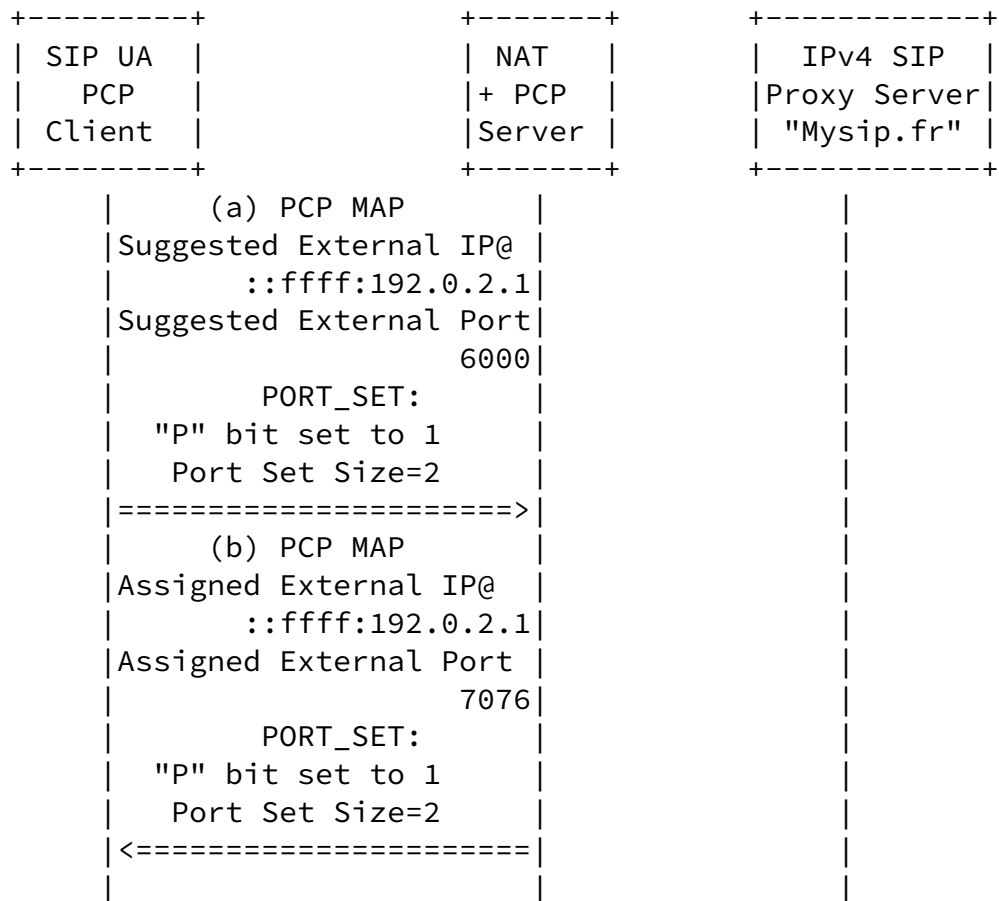


Figure 4: Retrieve a pair of ports that preserves port parity

2.6. Learn PREFIX64

If the SIP UA is located behind a NAT64 device [[RFC6146](#)], the option defined in [[RFC7225](#)] can be used to retrieve the PREFIX64 used by that NAT64 device.

The retrieved prefix will be used to locally build an IPv6-converted IPv4 address ([[RFC6052](#)]) corresponding to the IPv4 address included in the SDP message received from a remote IPv4-enabled SIP UA; the SDP message can be an SDP offer or an answer.

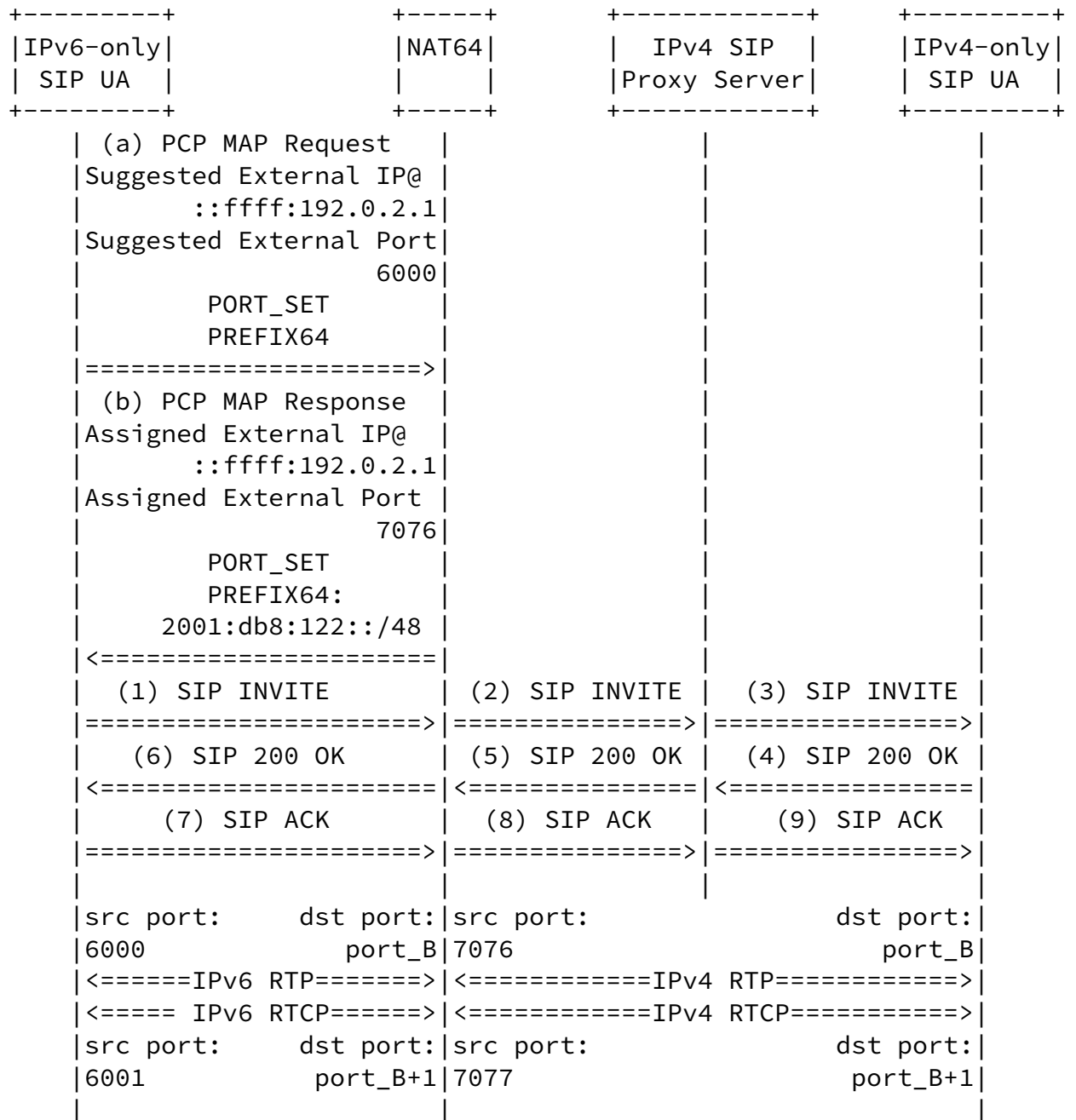


Figure 5: Example of IPv6 to IPv4 SIP-Initiated Session

Figure 6 shows the content of the SIP INVITE message sent by the IPv6-only SIP UA. This message uses the retrieved external IP address and external port numbers in SIP headers and SDP lines. This message is translated by the NAT64 without altering the SIP/SDP content.

Internet-Draft

PCP & SIP

November 2015

```
INVITE sip:13@mysip.fr:5070 SIP/2.0
Via: SIP/2.0/UDP 192.0.2.1:56252;branch=z9hG4bK1876803184
From: <sip:client4@mysip.fr:5070>;tag=631384602
To: <sip:13@mysip.fr:5070> Call-ID: 1377792765 CSeq: 21 INVITE
Contact: <sip:client4@192.0.2.1:56252>
Authorization: Digest username="client4", realm="asterisk",
  nonce="3358d80b", uri="sip:13@mysip.fr:5070",
  response="41442e94f6610e6f383a355a1bdf3e48", algorithm=MD5
Content-Type: application/sdp Allow: INVITE, ACK, CANCEL, OPTIONS,
  BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Max-Forwards: 70
User-Agent: Linphone/3.4.0 (eXosip2/unknown)
Subject: Phone call Content-Length: 443

v=0
o=client4 2487 2487 IN IP4 192.0.2.1
s=Talk c=IN IP4 192.0.2.1
b=AS:256
t=0 0
m=audio 7076 RTP/AVP 111 110 3 101
a=rtpmap:111 speex/16000
a=fmtp:111 vbr=on a=rtpmap:110 speex/8000
a=fmtp:110 vbr=on a=rtpmap:3 GSM/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-11
m=video 9076 RTP/AVP 102 99
a=rtpmap:102 H264/90000
a=fmtp:102 profile-level-id=428014
a=rtpmap:99 MP4V-ES/90000
a=fmtp:99
profile-level-id=3
```

Figure 6: Content of the INVITE message

[2.7.](#) Compliant with "a=rtcp" Attribute

The base PCP specification can be used to retrieve the port number to be singled if "a=rtcp" attribute is in use [[RFC3550](#)].

[2.8.](#) DSCP Marking Policy

PCP can be used to discover the DSCP value to be used when sending real-time flows or to create a mapping that matches a DSCP marking. This can be achieved using the DSCP option defined in [\[I-D.boucadair-pcp-extensions\]](#). DSCP setting value is configured by the network and not the SIP UA.

This feature can be used as an input for DSCP marking in some deployments such as [\[I-D.ietf-tsvwg-rtcweb-qos\]](#).

[3.](#) Avoid Crossing CGNs

[3.1.](#) Avoid NAT64

Because an IPv6-only SIP UA is not aware of the connectivity capabilities of the remote UA, the IPv6-only SIP UA uses the ALTC attribute [\[RFC6947\]](#) to signal the assigned IPv6 address and the IPv4 address learned via PCP.

If the remote SIP UA is IPv6-enabled, IPv6 transfer capabilities will be used to place the session. If the remote SIP UA is IPv4-only, IPv4 transfer capabilities will be used. NAT64 devices will be crossed only if the remote UA is IPv4-only.

Figure 7 provides an except of a SIP INVITE message that encloses both the local IPv6 address and the IPv4 address/port number assigned by a NAT64 device.

```
INVITE sip:13@mysip.fr:5070 SIP/2.0
Via: SIP/2.0/UDP 192.0.2.1:35011;branch=z9hG4bK702695557
From: <sip:client4@mysip.fr:5070>;tag=641336337
To: <sip:13@mysip.fr:5070>
Call-ID: 1532307201
CSeq: 20 INVITE
Contact: <sip:client4@192.0.2.1:35011>
Content-Type: application/sdp
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY,
      MESSAGE, SUBSCRIBE, INFO
Max-Forwards: 70
```

```
User-Agent: Linphone/3.4.0 (eXosip2/unknown)
Subject: Phone call
Content-Length: 538

v=0
o=client4 3867 3867 IN IP4 192.0.2.1
s=Talk
c=IN IP4 192.0.2.1
b=AS:256
t=0 0
m=audio 7056 RTP/AVP 111 110 3 101
a=altc:1 IP6 2001:db8:1f94:3000:6c73:ea54:cef:2730 45678
a=altc:2 IP4 192.0.2.1 7056
```

Figure 7: Content of the INVITE message (with ALTC Attribute)

[3.2.](#) Avoid Crossing DS-Lite AFTR

SIP UAs co-located with the B4 [[RFC6333](#)] or located behind the CPE can behave as dual-stack UAs:

- o Native IPv6 address is assigned locally.
- o The external IPv4 address and port is retrieved using PCP.

To avoid unnecessary invocation of AFTR resources, ALTC attribute is used to signal both IPv4 and IPv6 addresses. If the remote SIP UA is IPv6-enabled, IPv6 transfer capabilities will be used to place the session (i.e., the flows will avoid crossing the DS-Lite AFTR device). If the remote SIP UA is IPv4-only, IPv4 transfer capabilities will be used. AFTR devices will be crossed only if the remote UA is IPv4-only.

[4.](#) Security Considerations

PCP-related security considerations are discussed in [[RFC6887](#)].

Security considerations related to the discovery of PREFIX64 are discussed in [Section 7 of \[RFC7225\]](#) and those related to retrieving a set of ports are discussed in Section 7 of [[I-D.ietf-pcp-port-set](#)].

An attacker that wants to intercept media flows, without requiring intercepting SIP signalling message, can insert a fake PCP server that will influence the content of SIP messages so that an illegitimate node is inserted in the media path. Such behavior is not desirable. Means to prevent the PCP client from discovering illegitimate PCP servers must be enforced. Within the context of this document, the network on which the PCP messages are to be sent is fully trusted. For example, access control lists (ACLs) can be installed on the PCP client, PCP server, and the network between them, so those ACLs allow only communications from a trusted PCP client to the PCP server.

[5.](#) IANA Considerations

This document does not require any action from IANA.

[6.](#) Acknowledgements

Many thanks for T. Reddy and S. Kiesel for their review.

[7.](#) References

[7.1.](#) Normative References

- [RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", [RFC 3261](#), DOI 10.17487/RFC3261, June 2002, <<http://www.rfc-editor.org/info/rfc3261>>.
- [RFC3581] Rosenberg, J. and H. Schulzrinne, "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing", [RFC 3581](#), DOI 10.17487/RFC3581, August 2003, <<http://www.rfc-editor.org/info/rfc3581>>.
- [RFC6887] Wing, D., Ed., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", [RFC 6887](#), DOI 10.17487/RFC6887, April 2013,

<<http://www.rfc-editor.org/info/rfc6887>>.

7.2. Informative References

[I-D.boucadair-pcp-extensions]

Boucadair, M., Penno, R., and D. Wing, "Some Extensions to Port Control Protocol (PCP)", [draft-boucadair-pcp-extensions-03](#) (work in progress), April 2012.

[I-D.boucadair-pcp-nat64-experiments]

Abdesselam, M., Boucadair, M., Hasnaoui, A., and J. Queiroz, "PCP NAT64 Experiments", [draft-boucadair-pcp-nat64-experiments-00](#) (work in progress), September 2012.

[I-D.ietf-pcp-port-set]

Qiong, Q., Boucadair, M., Sivakumar, S., Zhou, C., Tsou, T., and S. Perreault, "Port Control Protocol (PCP) Extension for Port Set Allocation", [draft-ietf-pcp-port-set-13](#) (work in progress), October 2015.

[I-D.ietf-tsvwg-rtcweb-qos]

Dhesikan, S., Jennings, C., Druta, D., and P. Jones, "DSCP and other packet markings for WebRTC QoS", [draft-ietf-tsvwg-rtcweb-qos-05](#) (work in progress), October 2015.

[I-D.penno-rtcweb-pcp]

Penno, R., Reddy, T., Wing, D., and M. Boucadair, "PCP Considerations for WebRTC Usage", [draft-penno-rtcweb-pcp-00](#) (work in progress), May 2013.

[ICEFailure]

Telemetry Dashboard, "WEBRTC_ICE_SUCCESS_RATE", March 2015, <http://telemetry.mozilla.org/#filter=beta%2F36%2FWEBRTC_ICE_SUCCESS_RATE%2Fsaved_session%2FFirefox&aggregates=multiselect-all!Submissions&evoOver=Builds&locked=true&sanitize=true&renderhistogram=Graph>.

[Power]

Haverinen, H., Siren, J., and P. Eronen, "Energy Consumption of Always-On Applications in WCDMA Networks", April 2007, <<http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4212635>>.

- [RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, [RFC 3550](#), DOI 10.17487/RFC3550, July 2003, <<http://www.rfc-editor.org/info/rfc3550>>.
- [RFC3948] Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec ESP Packets", [RFC 3948](#), DOI 10.17487/RFC3948, January 2005, <<http://www.rfc-editor.org/info/rfc3948>>.
- [RFC4961] Wing, D., "Symmetric RTP / RTP Control Protocol (RTCP)", [BCP 131](#), [RFC 4961](#), DOI 10.17487/RFC4961, July 2007, <<http://www.rfc-editor.org/info/rfc4961>>.
- [RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", [RFC 5245](#), DOI 10.17487/RFC5245, April 2010, <<http://www.rfc-editor.org/info/rfc5245>>.
- [RFC5626] Jennings, C., Ed., Mahy, R., Ed., and F. Audet, Ed., "Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)", [RFC 5626](#), DOI 10.17487/RFC5626, October 2009, <<http://www.rfc-editor.org/info/rfc5626>>.
- [RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", [RFC 6052](#), DOI 10.17487/RFC6052, October 2010, <<http://www.rfc-editor.org/info/rfc6052>>.
- [RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", [RFC 6146](#), DOI 10.17487/RFC6146, April 2011, <<http://www.rfc-editor.org/info/rfc6146>>.

- [RFC6223] Holmberg, C., "Indication of Support for Keep-Alive", [RFC 6223](#), DOI 10.17487/RFC6223, April 2011, <<http://www.rfc-editor.org/info/rfc6223>>.

- [RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", [RFC 6333](#), DOI 10.17487/RFC6333, August 2011, <<http://www.rfc-editor.org/info/rfc6333>>.
- [RFC6947] Boucadair, M., Kaplan, H., Gilman, R., and S. Veikkolainen, "The Session Description Protocol (SDP) Alternate Connectivity (ALTC) Attribute", [RFC 6947](#), DOI 10.17487/RFC6947, May 2013, <<http://www.rfc-editor.org/info/rfc6947>>.
- [RFC7118] Baz Castillo, I., Millan Villegas, J., and V. Pascual, "The WebSocket Protocol as a Transport for the Session Initiation Protocol (SIP)", [RFC 7118](#), DOI 10.17487/RFC7118, January 2014, <<http://www.rfc-editor.org/info/rfc7118>>.
- [RFC7220] Boucadair, M., Penno, R., and D. Wing, "Description Option for the Port Control Protocol (PCP)", [RFC 7220](#), DOI 10.17487/RFC7220, May 2014, <<http://www.rfc-editor.org/info/rfc7220>>.
- [RFC7225] Boucadair, M., "Discovering NAT64 IPv6 Prefixes Using the Port Control Protocol (PCP)", [RFC 7225](#), DOI 10.17487/RFC7225, May 2014, <<http://www.rfc-editor.org/info/rfc7225>>.
- [RFC7291] Boucadair, M., Penno, R., and D. Wing, "DHCP Options for the Port Control Protocol (PCP)", [RFC 7291](#), DOI 10.17487/RFC7291, July 2014, <<http://www.rfc-editor.org/info/rfc7291>>.
- [RFC7362] Iovov, E., Kaplan, H., and D. Wing, "Latching: Hosted NAT Traversal (HNT) for Media in Real-Time Communication", [RFC 7362](#), DOI 10.17487/RFC7362, September 2014, <<http://www.rfc-editor.org/info/rfc7362>>.
- [WT-317] Broadband Forum, "Network Enhanced Residential Gateway (NERG)", 2015, <<https://www.broadband-forum.org/technical/technicalwip.php>>.

Authors' Addresses

Mohamed Boucadair
France Telecom
Rennes 35000
France

Email: mohamed.boucadair@orange.com

Parthasarathi Ravindran
Nokia Networks
Manyata Embassy Business park
Bangalore, Karnataka 560045
India

Email: partha@parthasarathi.co.in

