

PCP Working Group
Internet-Draft
Intended status: Informational
Expires: March 28, 2013

M. Ait Abdesselam
M. Boucadair
A. Hasnaoui
J. Queiroz
France Telecom
September 24, 2012

PCP NAT64 Experiments
draft-boucadair-pcp-nat64-experiments-00

Abstract

This memo documents a set of PCP experiments conducted in NAT64 environment. Two services are detailed in the document: access to a video server behind NAT64 and SIP-based sessions. Both 3G and Wi-Fi IPv6-only connectivity have been used.

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 March 28, 2013.

Copyright Notice

Copyright (c) 2012 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

Internet-Draft

PCP NAT64 Experiments

September 2012

described in the Simplified BSD License.

Table of Contents

| | | |
|------------------------|--|--------------------|
| 1. | Introduction | 3 |
| 2. | Software Modules & Modifications | 3 |
| 2.1. | PCP Server | 3 |
| 2.2. | NAT64 | 4 |
| 2.3. | PCP Packet Generator | 4 |
| 2.4. | RA Daemon | 5 |
| 2.5. | DNS64 | 5 |
| 2.6. | Wirshark PCP Dissector | 5 |
| 2.7. | SIP Proxy Server | 5 |
| 2.8. | SIP UA | 5 |
| 2.9. | PCP Server Discovery | 6 |
| 2.9.1. | DHCP | 6 |
| 2.9.2. | RA-based approach | 7 |
| 3. | Testbed Setup & Configuration | 7 |
| 3.1. | Handsets | 7 |
| 3.2. | IPv6-only APN for 3G | 8 |
| 3.3. | Wi-Fi Connectivity | 8 |
| 3.4. | Network Topology | 9 |
| 4. | Tested Services | 10 |
| 4.1. | HTTP Webcam Server Behind NAT64 | 11 |
| 4.2. | SIP Use Case | 12 |
| 4.2.1. | Media Sessions | 15 |
| 4.2.2. | IPv6-only to IPv4-only | 15 |
| 4.2.3. | IPv4-only to IPv6-only | 19 |
| 4.2.4. | IPv6-only to IPv6-only | 20 |
| 5. | IANA Considerations | 21 |
| 6. | Security Considerations | 21 |
| 7. | Acknowledgements | 22 |
| 8. | Normative References | 22 |
| | Authors' Addresses | 23 |

Internet-Draft

PCP NAT64 Experiments

September 2012

1. Introduction

This document describes a set of PCP [[I-D.ietf-pcp-base](#)] experiments conducted in the context of NAT64 [[RFC6146](#)]. Both Wi-Fi and 3G configurations have been tested.

The main goals of these experiments are:

- o Port a NAT64 implementation to be controlled using PCP.
- o Integrate a PCP Client in an Android device.
- o Validate the PCP chain in the NAT64 context.
- o Assess the use of PCP for NAT64 traversal and delivery of services behind NAT64.
- o Evaluate the complexity to update applications to invoke PCP service or embed a PCP Client.

Two services are detailed in the document: access to video server behind NAT64 ([Section 4.1](#)) and SIP-based sessions ([Section 4.2](#)).

2. Software Modules & Modifications

The following sub-sections provide more details on the software modules used for the experiments.

2.1. PCP Server

The PCP server used for NAT64 experiments is based on the DS-Lite compliant daemon implementation from ISC. The base functionalities of this PCP Server are listed below:

- o Configurable port range to be used for the external port mapping for both TCP and UDP.
- o Support of MAP and PEER OpCodes.
- o Support of THIRD_PARTY and PREFER_FAILURE Options.

The code has been updated as follows:

- o Add an interactive shell interface with basic commands to: view active mappings, list users, delete a specific user and reset a user's epoch time, etc.
- o Adapt the behavior to be compatible with a NAT64 environment.
- o Support of DESCRIPTION PCP option
[\[I-D.boucadair-pcp-description-option\]](#).
- o Support of PREFIX64 option
[\[I-D.boucadair-pcp-nat64-prefix64-option\]](#).
- o Support of PORT_RESERVATION option [\[I-D.boucadair-pcp-rtp-rtcp\]](#).
- o Establish and maintain a communication channel to control the NAT64 module.

The PCP Server software architecture is shown in Figure 1.

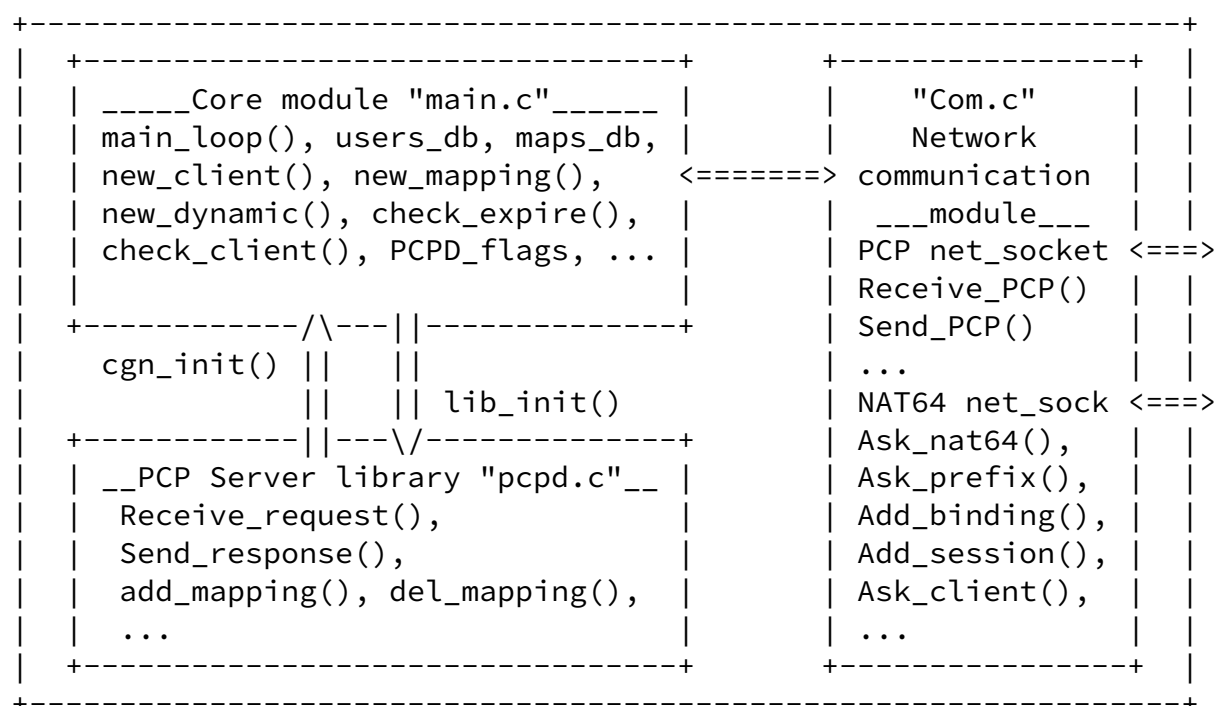


Figure 1: PCP server software architecture.

2.2. NAT64

The NAT64 module is based on the Viagenie's Ecdysis open source implementation for Linux.

The compilation environment is Debian Squeeze 6.0 / Linux Kernel 2.6.32-5-686.

The main modifications we incorporated into Ecdysis module are listed below:

- o Add a management interface to: view mappings, delete mapping, add a new mappings, etc.
- o Add a listening TCP interface for the PCP server.
- o Instantiate/delete mappings when a command is received from the PCP Server module.
- o Packets matching the explicit mapping are handled appropriately.

[2.3.](#) PCP Packet Generator

A basic Android software, denoted as "PCP Packet Generator", has been developed to generate customized PCP requests to be sent to a PCP Server.

This tool allows to set any values for the PCP fields and Options to be used. Received responses are handled, parsed and validated. The content of received PCP requests are shown in a human readable format.

[2.4.](#) RA Daemon

The radvd v1.8.6 (Router Advertisement Daemon) is used to send RA messages for a stateless configuration of IPv6 mobile devices.

[2.5.](#) DNS64

Bind9 v9.9.0 is used as DNS64 server. This PREFIX64 is configured to NAT64 and DNS64: 2001:688:1f94:300a::/96.

A DNS record is created for "mysip.fr", which is used to contact the SIP Proxy Server. DNS64 returns IPv4-embedded IPv6 addresses when resolving "mysip.fr" is: [PREFIX64+sip_serv_ipv4].

AAAA DNS record is created for "mypcp.fr" used to contact the PCP Server. DNS64 reruns the IPv6 address of the NAT64 [2001:688:1f94:3000::2].

[2.6.](#) Wirshark PCP Dissector

The used wireshark version is 1.8.0 running on Linux 2.6.32-5-686.

For PCP, an extension "pcp dissector" has been used to parse PCP packets (with the port 5351 as destination or source port). The recognized opcodes are MAP and PEER. Recognized options are all those conforming to version 18 of [[I-D.ietf-pcp-base](#)].

[2.7.](#) SIP Proxy Server

The used SIP server is Asterisk v1.2 running on a Debian Squeeze 6.0 with Kernel image: 2.6.32-5-686.

The default configuration is used. No extra feature to assist NAT traversal nor IPv6 support were activated.

[2.8.](#) SIP UA

The selected SIP UA for mobile devices is Linphone 1.3.2 for Android. Linphone is based on the eXosip2 C library.

For our experiments, Linphone module has been updated with the main modifications listed below:

- o Add to the GUI a configuration option to set the domain name of the PCP server to be used. Leaving the option field blank disables PCP.
- o If PCP is enabled, a PCP request is sent to instantiate a mapping for the port used for SIP signaling messages (random port is used). The retrieved external IP and port number will be used in the CONTACT and VIA fields of all SIP messages headers. The same request is used to retrieve the PREFIX64 used by the NAT64. The returned PREFIX64 is stored by the UA.
- o If PCP is enabled, for any incoming or outgoing session, two PCP requests are sent to create four bindings for the audio and video RTP and RTCP flows. The allocated external IP and ports are returned in the session description offer/answer.
- o For an incoming call (from IPv4-only network), the IP address included in the INVITE headers and SDP offer is the IPv4 address

- representing the (IPv6) calling host. The PREFIX64 of the NAT64, returned in PCP, is used to synthesize an IPv6 address based on the IPv4 address contained in the SDP offer [[RFC6052](#)].
- o For an outgoing call, the same problem occurs to send the "200 OK" message. The same PREFIX64 is used to construct the IPv4-converted IPv6 address representing the IPv4-only UA.
 - o Other minor GUI modifications.

Linphone has been also patched to support ALTC attribute [[I-D.boucadair-mmusic-altc](#)] (see [Section 4.2.4](#)).

[2.9.](#) PCP Server Discovery

PCP Client needs to implement a method to discover a PCP server not located in the first hop. PCP_SERVER is added automatically to "host" file owing to two methods detailed below:

1. [[I-D.ietf-pcp-dhcp](#)]: DHCPv6 PCP option is used to discover a PCP server name. The DHCPv6 server, when configured to do so, provides the requested PCP server information by including one or more PCP server names option in its response.
2. I-D.boucadair-pcp-nodhcp-discovery specifies Router Advertisement option to learn the PCP Server.

Note these discovery methods are not integrated in Android but are tested using Linux Fedora 15.

[2.9.1.](#) DHCP

[2.9.1.1.](#) DHCP Server

DHCPv6 server from ISC is used to integrate the PCP DHCPv6 option. We modified the configuration file: "inetcdhcp/dhcpd6.conf" to provision a PCP server name to clients.

[2.9.1.2.](#) DHCP Client

Setting up the clients is relatively easy. There are several implementations available but we used the DHCPv6 client embedded in Fedora 15.

We modified the configuration file: "etc/dhcp/dhclient6.conf" to request a specific option (PCP OPTION). The same code is used in the client and server sides:

```
#pcp server option option dhcp6.OPTION_PCPSERVER code 156 = string;
```

The client is updated with a script for analyzing, extracting and storing the content of received PCP option.

[2.9.2.](#) RA-based approach

As an alternative to DHCP, we also implemented an RA-based approach to learn the PCP Name of PCP Server(s). This option (called PCPS) contains one or more PCP domain names sharing the Lifetime value.

The router advertisement daemon (radvd-1.8.6) is run by Linux systems acting as IPv6 routers.

An IPv6 host can configure the PCP server of one or more PCPSERVER via RA messages periodically sent by a router or solicited by a Router Solicitation (RS).

[3.](#) Testbed Setup & Configuration

[3.1.](#) Handsets

The used handsets model is:
Samsung Galaxy SII GT-I9100.

The mobile devices have been upgraded to Android ICS 4.0.3 with:

- o Kernel version: 3.0.15-9100XXLPQ-CL223505.
- o Base band version: I9100XXLPQ.

The latest Android version is used to avoid some well known IPv6 issues.

ICS 4 version does not support DHCPv6, and the IPv6 addresses are autoconfigured using RA.

For advanced network utilities, the smartphones have been rooted to unlock access functionalities as setting of DNS server, IP addressing, easiest development/debugging, custom application install, etc.

Busybox is also installed to add more configuration tools.

The "IP WebCam" is a software that turns a mobile Android device into a wireless webcam with multiple viewing options such as a VideoPlayer or web browser by creating an HTTP server that broadcasts video and audio flows by converting it to JavaScript.

URL: <https://play.google.com/store/apps/details?id=com.pas.webcam>

3.2. IPv6-only APN for 3G

An IPv6-only APN from Orange France has been used to assess the PCP behavior over a 3G network.

3.3. Wi-Fi Connectivity

The Wi-Fi IPv6-only environment is set using a 45 Mbps Wireless Access Point Netgear-WG602-v4.

```
+-----ISSUE-----+
|The Android handsets can access to a Wi-Fi IPv6-only network by |
|configuring at first astatic IPv4 address to be used with SSID  |
|network in the Android Wi-Fi configuration menus. Once the device|
|connected to the network and the wlan0 interface got an IPv6 global|
|address (by RA), the IPv4 address can be deleted. This avoids the |
|device to ask automatically for a DHCPv4 server, and allows to    |
|connect to IPv6-only networks. This is a problem due to lack of  |
|global support of IPv6 in Android.                                |
+-----+

```

DHCPv6 is also not supported. The DNS server must be set manually

using the shell command:

```
#setprop net.dns1 dns_serv_address
```

[3.4.](#) Network Topology

Two network topologies are used for the tests. For both configurations, the same NAT64, DNS64 and PCP server are used. NAT64/PCP Server is configured with

- o An IPv4 address pool
- o An IPv6 prefix (/64)
- o Only the handsets change location from 3G network to Wi-Fi local IPv6-only network. /64 is allocated to the handset.
- o A route to the IPv4 default gateway.
- o A route to the IPv6 default gateway.

The network topology is shown in Figure 2.

Internet-Draft

PCP NAT64 Experiments

September 2012

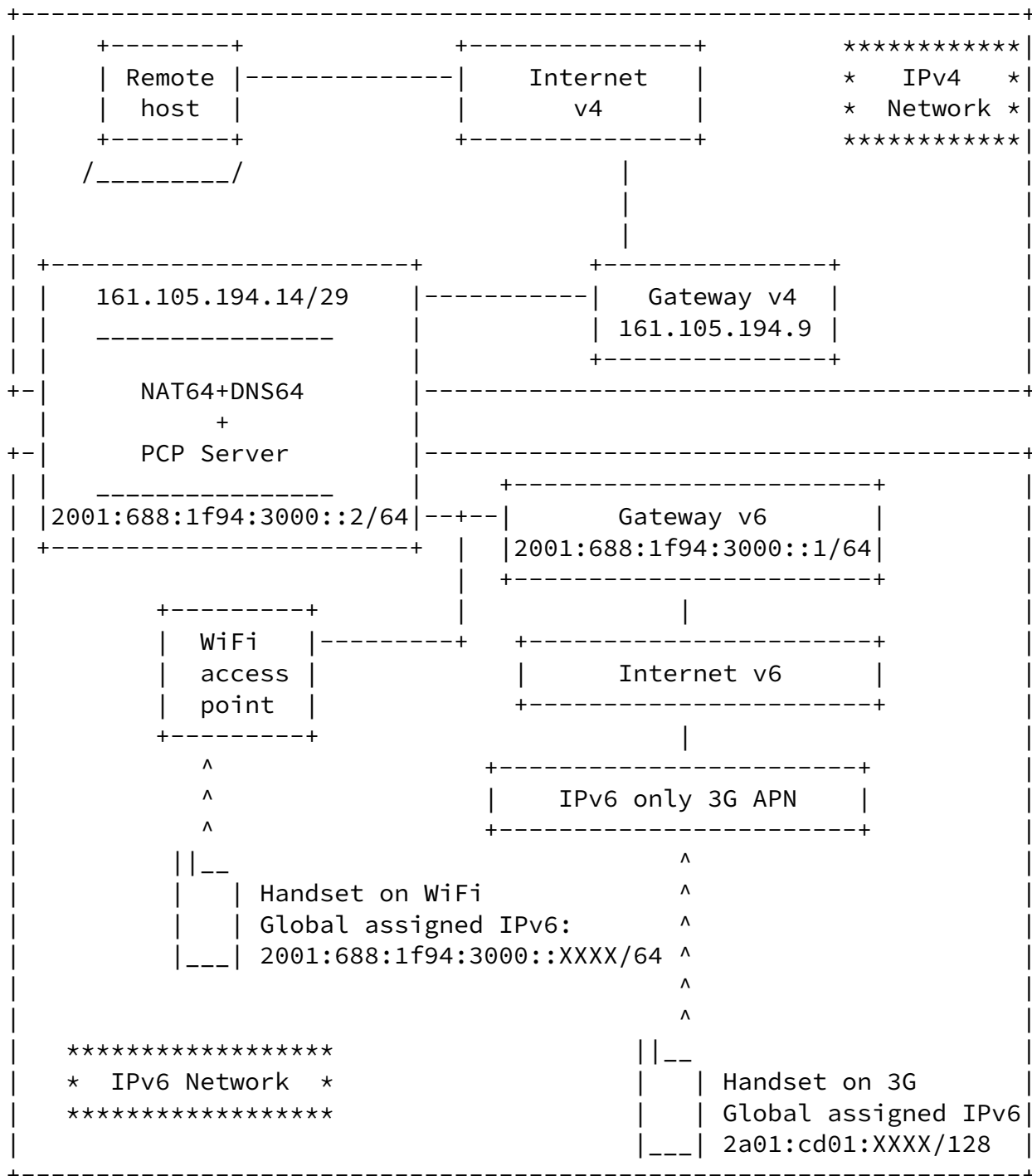


Figure 2: Global testbed topology.

4. Tested Services

Ait Abdesselam, et al. Expires March 28, 2013

[Page 10]

Internet-Draft

PCP NAT64 Experiments

September 2012

4.1. HTTP Webcam Server Behind NAT64

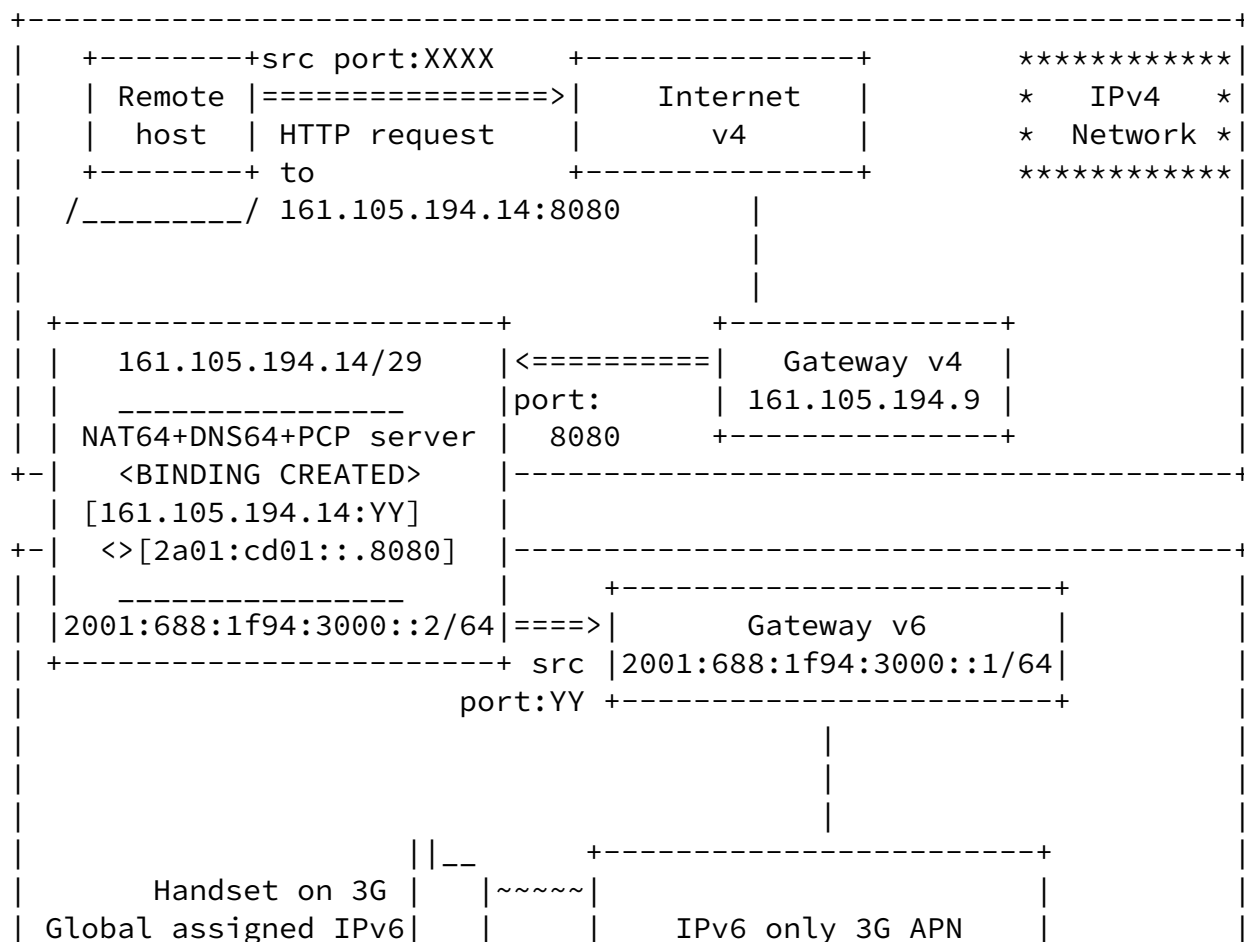
The first tested service is an HTTP server running on a mobile device connected to a IPv6-enabled 3G network, that shows the video flows of the device cam.

The PCP Packet Generator is used to send a MAP request to the PCP server containing the following fields:

```
Client IP: [2a01:cd01:XXXX]
Request Opcode: MAP
Requested internal port: 8080
Suggested external address: [::ffff:0]
Suggested external port: 8080
Lifetime: 3000 sec
Transport protocol: TCP
Description: "HTTP Webcam server service"
```

The PCP response returns the external IPv4 address and the external assigned port to be used to access the HTTP Webcam server.

This example is shown in Figure 3.



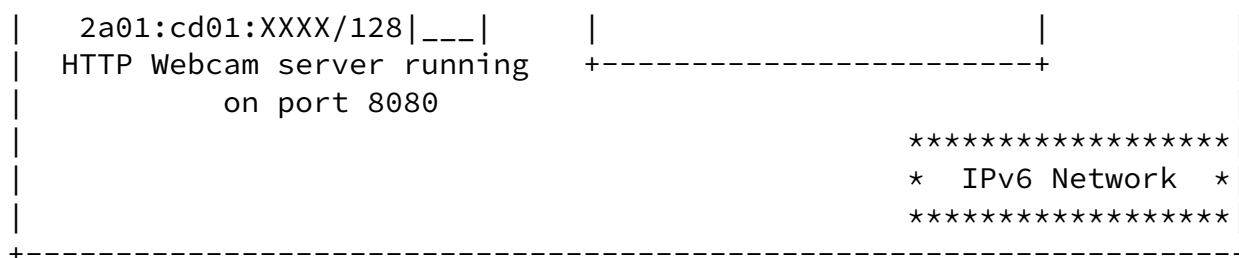


Figure 3: Access to IPv4 server behind NAT64

4.2. SIP Use Case

The registration call flow for the IPv6-only SIP UA is depicted in Figure 4.

In the following examples, port 5070 is used instead of the default SIP port (5060).

At bootstrapping of the SIP UA, it retrieves the PREFIX64 used by the NAT64 and installs a mapping used for SIP registration.

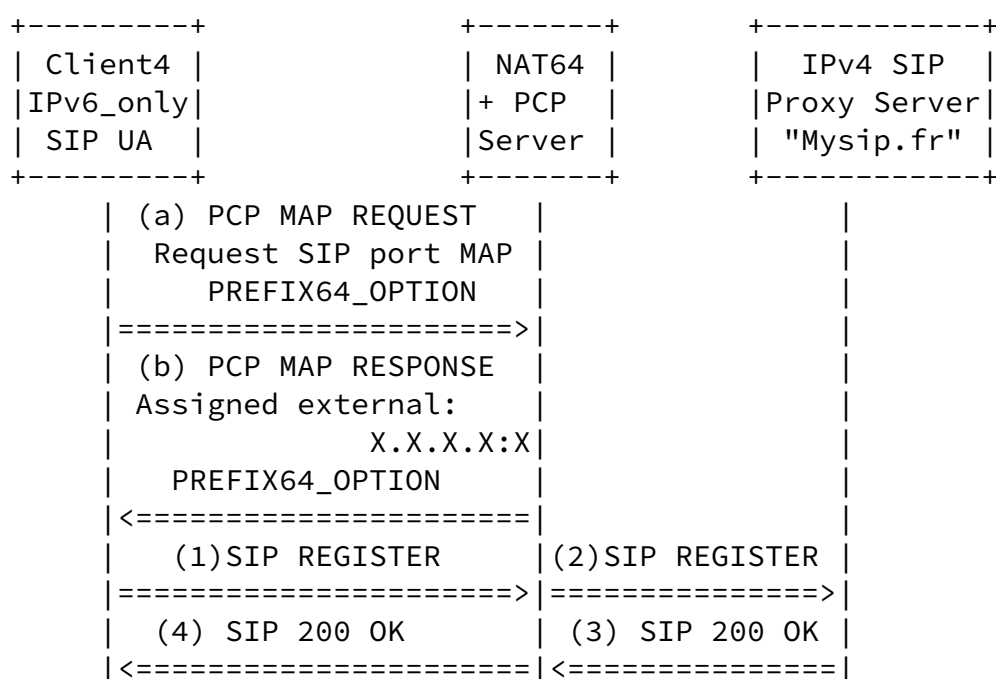


Figure 4: SIP REGISTER

(a) Below is shown the content of the PCP MAP Request issued by Client4 towards the PCP Server:

Source: 2001:688:1f94:3000:289f:db7:e8ae:2988 port: 12345
Destination: 2001:688:1f94:3000::2.5351

PCP Request:

Version: 1

R bit: Request (0)

Opcode: MAP (0x01)

Requested Lifetime: 36000 sec

PCP Client's IP Address: 2001:688:1f94:3000:289f:db7:e8ae:2988
(2001:688:1f94:3000:289f:db7:e8ae:2988)

MAP Request: Protocol: UDP (17)

Internal Port: 3938

Suggested External Port: 3938

Suggested External IP Address: ::ffff:0.0.0.0

Option Code: Unknown (0x7f) Option Length: 12 bytes Data:
000000000000000000000000

(b) The PCP MAP Response received from the PCP Server is shown below:

Source: 2001:688:1f94:3000::2.5153

Destination: 2001:688:1f94:3000:289f:db7:e8ae:2988.12345

PCP Response:

Version: 1

R bit: Response (1)

Opcode: Unknown (0x81)

Result Code: 0

Lifetime: 36000 sec

Epoch Time: 1

MAP Response Protocol: UDP (17)

Internal Port: 3938
Assigned External Port: 3938
Assigned External IP Address: ::ffff:161.105.194.14 (::ffff:
161.105.194.14)
Option Code: PREFIX64 (0x7f) Reserved: 0 Option Length: 12 bytes
Data: 200106881f94300a00000000

(1) Then, the UA uses the retrieved external IP address and port to generate the following SIP REGISTER message:

Source: 2001:688:1f94:3000:289f:db7:e8ae:2988 port: 3938
Destination: 2001:688:1f94:3000::a169:c20d port:5070

SIP Message:

REGISTER sip:mysip.fr SIP/2.0
Via: SIP/2.0/UDP 161.105.194.14:3938;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@161.105.194.14:3938;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

(2) SIP REGISTER is translated by the NAT64 using the PCP-instantiated mapping. This message is then forwarded to the SIP Proxy Server:

Source: 161.105.194.14:3938 (NAT64)
Destination: 161.105.194.13:5070 (SIP Proxy)
Same SIP Message as (1).

(3) A positive response is generated by the SIP Proxy Server as shown

below:

Source: 161.105.194.13:5070 (SIP Proxy)
Source: 161.105.194.14:3938 (NAT64)


```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 161.105.194.14:
      3938;branch=z9hG4bK1572043597;received=161.105.194.14
From: <sip:client4@mysip.fr:5070>;tag=893886783
To: <sip:client4@mysip.fr:5070>;tag=as0b92321f
Call-ID: 1271173454
CSeq: 2 REGISTER
Server: Asterisk PBX 1.6.2.9-2+squeeze6
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE,
      NOTIFY, INFO
Supported: replaces, timer
Expires: 3600
Contact: <sip:client4@
      161.105.194.14:3938;line=b3433a7df33282d>;expires=3600
```

(4) 200 OK message is translated by the NAT64 using the PCP-instantiated mapping:

```
Source: 2001:688:1f94:3000::a169:c20d.5070
Destination: 2001:688:1f94:3000:289f:db7:e8ae:2988.3938
Same SIP message as (3).
```

At the end of this procedure, IPv6-only SIP UA is able to place and receive session requests.

PREFIX64 retrieved during this phase is used to build IPv4-embedded IPv6 addresses when receiving an IPv4 address in an SDP offer/answer.

[4.2.1.](#) Media Sessions

Both audio and video sessions are supported. The audio codecs used for these experiments are: speex 16 KHz, speex 8Khz, and gsm. The used video codecs are H264 and MPEG4.

[4.2.2.](#) IPv6-only to IPv4-only

Figure 5 and Figure 6 illustrate the exchanges which occur when initiating a SIP session from an IPv6-only UA to an IPv4-only SIP UA.

PCP exchanges take place at the bootstrapping of the SIP UA to reserve one or two pair of ports (one for audio and another one for video).

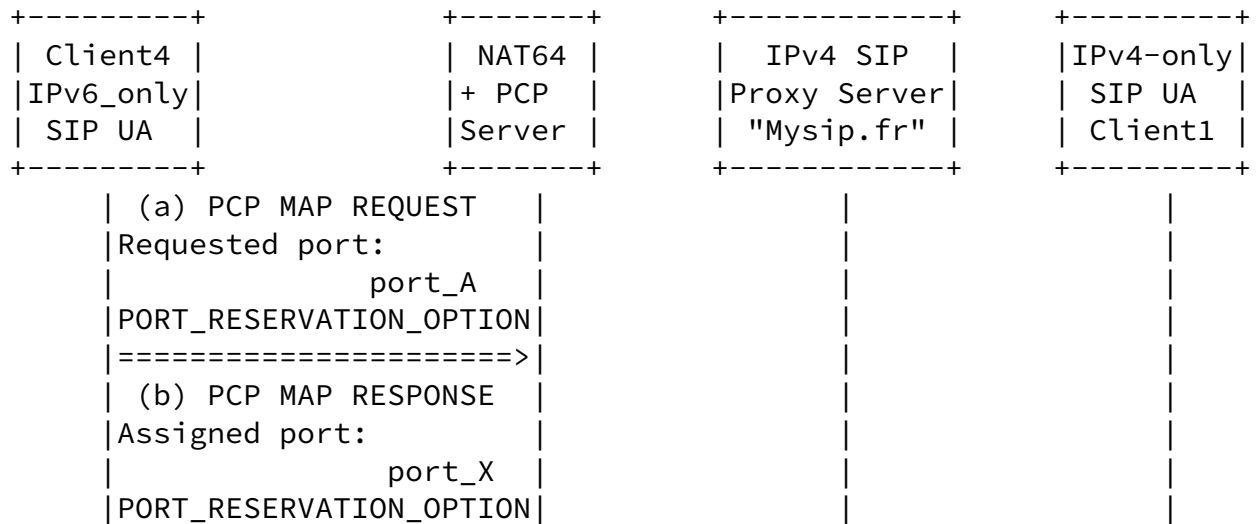


Figure 5: Use PCP to reserve a pair of ports

(a) The following PCP MAP Request is issued from Client4 towards the PCP Server:

Source: 2001:688:1f94:3000:289f:db7:e8ae:2988.12345

Destination: 2001:688:1f94:3000::2.5351

PCP Request:

Version: 1

R bit: Request (0)

Opcode: MAP (0x01)

Requested Lifetime: 36000 sec

PCP Client's IP Address: 2001:688:1f94:3000:289f:db7:e8ae:2988
(2001:688:1f94:3000:289f:db7:e8ae:2988)

MAP Request: Protocol: UDP (17)

Internal Port: 7076

Suggested External Port: 7076

Suggested External IP Address: ::ffff:0.0.0.0

Option Code: RTP (0x84) Option Length: 0 bytes Data: (NULL)

This request aims to reserve a pair of ports preserving parity and contiguity.

(b) PCP MAP Response from PCP Server to Client4:

Internet-Draft

PCP NAT64 Experiments

September 2012

Destination: 2001:688:1f94:3000:289f:db7:e8ae:2988.12345

Source: 2001:688:1f94:3000::2.5153

PCP Response:

Version: 1

R bit: Response (1)

Opcode: Unknown (0x81)

Result Code: 0

Lifetime: 36000 sec

Epoch Time: 1

MAP Response Protocol: UDP (17)

Internal Port: 7076

Assigned External Port: 7076

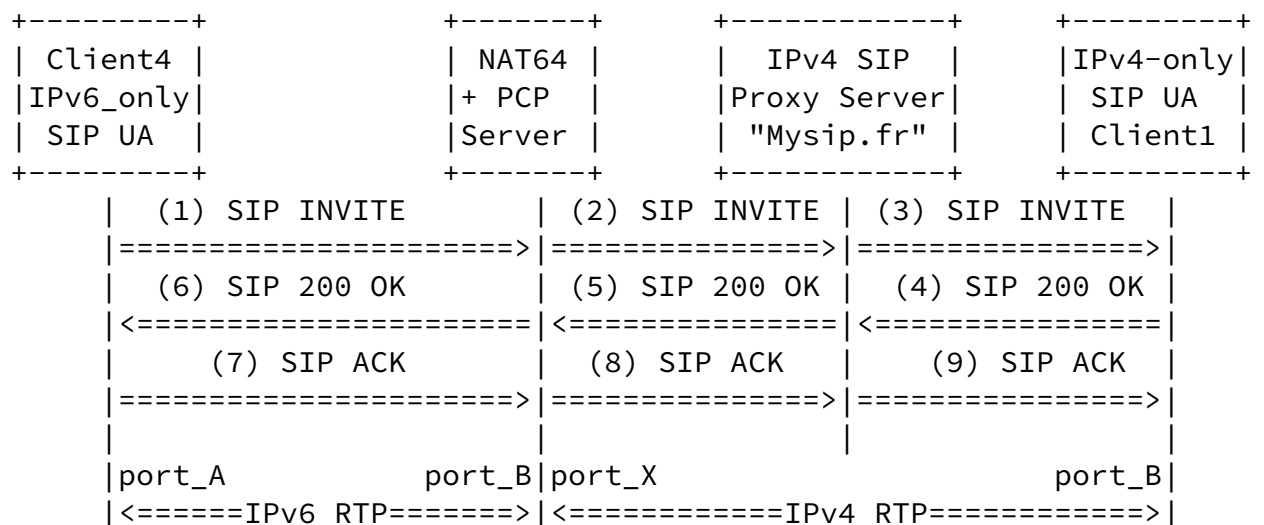
Assigned External IP Address: ::ffff:161.105.194.14 (::ffff:
161.105.194.14)

Option Code: RTP (0x84) Option Length: 0 bytes Data: (NULL)

At the end of this procedure, two external ports are reserved in the NAT64: 7076 and 7077.

In this example, the PCP Server honors the requested external port. If the requested port was in use, an alternative pair of ports would be assigned.

Figure 6 illustrates the messages exchanged to establish a session between an IPv6-only UA and a remote IPv4-only UA.



| | |
|------------------------|-----------------------|
| <===== IPv6 RTCP=====> | <=====IPv4 RTCP=====> |
| port_A+1 | port_B+1 port_X+1 |
| | port_B+1 |

Figure 6: IPv6 to IPv4 SIP Session

(1, 2, 3) Below is shown the content of the SIP INVITE message sent by Client4. This message uses the external IP address and port in SIP headers and SDP lines. This message is translated by the NAT64

without altering the SIP/SDP content.

```

INVITE sip:13@mysip.fr:5070 SIP/2.0
Via: SIP/2.0/UDP 161.105.194.14:56252;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@161.105.194.14:56252>
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 161.105.194.14
s=Talk c=IN IP4 161.105.194.14
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

```

(4, 5, 6) The content of the 200 OK message is shown below:

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 161.105.194.14:
    56252;branch=z9hG4bK1876803184;received=161.105.194.14
From: <sip:client4@mysip.fr:5070>;tag=631384602
To: <sip:13@mysip.fr:5070>;tag=as3d61114e
Call-ID: 1377792765 CSeq: 21 INVITE
Server: Asterisk PBX 1.6.2.9-2+squeeze6 Allow: INVITE, ACK, CANCEL,
    OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO Supported: replaces,
    timer
Contact: <sip:13@161.105.194.13>
Content-Type: application/sdp Content-Length: 414
```

```
v=0
o=root 1210300728 1210300728 IN IP4 161.105.194.13
c=IN IP4 161.105.194.13 b=CT:384
t=0 0
m=audio 13238 RTP/AVP 3 110 111 101
a=rtpmap:3 GSM/8000
a=rtpmap:110 speex/8000
a=rtpmap:111 G726-32/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16 a=ptime:20
a=sendrecv
m=video 14466 RTP/AVP 102 99
a=rtpmap:102 H264/90000
a=rtpmap:99 MP4V-ES/90000
```

a=sendrecv

When this message is received by the IPv6-only UA, the IPv6-only UA uses PREFIX64 to build the IPv4-embedded IPv6 address corresponding to the IPv4 address included in the SDP response. RTP/RTCP flows are sent to that IPv6 address.

[4.2.3.](#) IPv4-only to IPv6-only

Figure 7 shows the messages exchanged to establish a SIP session initiated from an IPv4-only UA.

In this scenario, PREFIX64 is used to handle the SDP offer received by the IPv6-only UA from the IPv4-only UA. The IPv6-only UA uses PREFIX64 to build the IPv4-embedded IPv6 address corresponding to the IPv4 address included in the SDP offer. RTP/RTCP flows are sent to that IPv6 address.

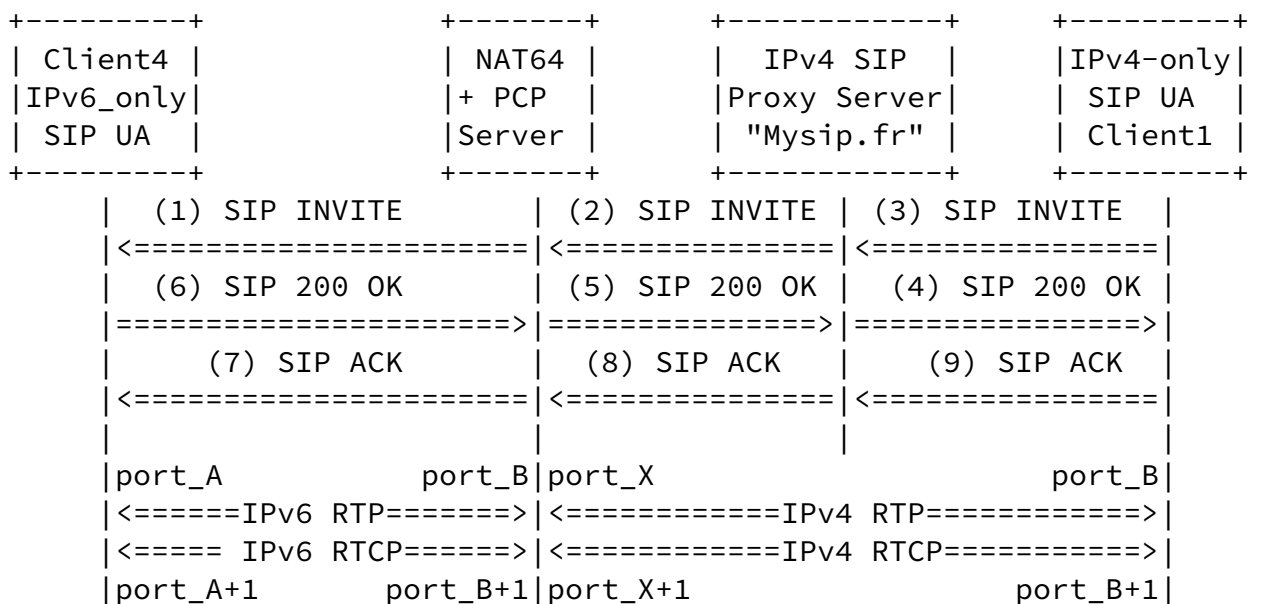


Figure 7: IPv4 to IPv6 SIP Session

[4.2.4.](#) IPv6-only to IPv6-only

Two scenarios have been tested:

1. The behavior of the IPv6-only UA is similar to the one described in [Section 4.2.2](#): in this scenario, NAT64 is involved in the RTP exchanges between IPv6-only UAs.
2. In order to remove the NAT64 from the path, the Linphone module was patched to support ALTC attribute [[I-D.boucadair-mmusic-altc](#)]. Figure 8 shows an example of INVITE message generated by the IPv6-only SIP UA. The remote IPv6-only UA will use the IPv6 altc line to generate its response. As a consequence, IPv6 will be used to exchange RTP flows.

```
INVITE sip:13@mysip.fr:5070 SIP/2.0
Via: SIP/2.0/UDP 161.105.194.14:35011;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@161.105.194.14:35011>
Content-Type: application/sdp
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE,
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 161.105.194.14
s=Talk
c=IN IP4 161.105.194.14
b=AS:256
t=0 0
m=audio 7056 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 9056 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
a=altc: IP6 2001:688:1f94:3000:6c73:ea54:cef:2730 45678
a=altc: IP4 161.105.194.14 7056
```

Figure 8: PCP+ALTC Attribute

[5.](#) IANA Considerations

No request is made to IANA.

[6.](#) Security Considerations

This document does not introduce any security issue in addition to

what is discussed in [[I-D.ietf-pcp-base](#)].

[7.](#) Acknowledgements

Special thanks to X. Deng for porting Linphone to support ALTC attribute.

Many thanks to the authors of PCP Server (ISC) and NAT64 (Viagenie) modules.

8. Normative References

[I-D.boucadair-mmusic-altc]

Boucadair, M., Kaplan, H., Gilman, R., and S. Veikkolainen, "Session Description Protocol (SDP) Alternate Connectivity (ALTC) Attribute", [draft-boucadair-mmusic-altc-05](#) (work in progress), April 2012.

[I-D.boucadair-pcp-description-option]

Boucadair, M., Penno, R., and D. Wing, "PCP Description Option", [draft-boucadair-pcp-description-option-01](#) (work in progress), September 2012.

[I-D.boucadair-pcp-nat64-prefix64-option]

Boucadair, M., "Learn NAT64 PREFIX64s using PCP", [draft-boucadair-pcp-nat64-prefix64-option-02](#) (work in progress), September 2012.

[I-D.boucadair-pcp-rtp-rtcp]

Boucadair, M. and S. Sivakumar, "Reserving N and N+1 Ports with PCP", [draft-boucadair-pcp-rtp-rtcp-04](#) (work in progress), April 2012.

[I-D.ietf-pcp-base]

Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", [draft-ietf-pcp-base-27](#) (work in progress), September 2012.

[I-D.ietf-pcp-dhcp]

Boucadair, M., Penno, R., and D. Wing, "DHCP Options for the Port Control Protocol (PCP)", [draft-ietf-pcp-dhcp-05](#) (work in progress), September 2012.

[RFC6052]

Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", [RFC 6052](#),

October 2010.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", [RFC 6146](#), April 2011.

Authors' Addresses

Mehdi Ait Abdesselam
France Telecom
Issy Les Moulineaux
France

Email: mehdi.aitabdesselam@orange.com

Mohamed Boucadair
France Telecom
Rennes, 35000
France

Email: mohamed.boucadair@orange.com

Amina Hasnaoui
France Telecom
Issy Les Moulineaux,
France

Email: amina.hasnaoui@orange.com

Jaqueline Queiroz
France Telecom
Issy Les Moulineaux
France

Phone:

Email: jaqueline.queiroz@orange.com

