PCP Working Group   M. Boucadair
Internet-Draft   France Telecom
Intended status: Standards Track   F. Dupont
Expires: May 24, 2012   Internet Systems Consortium
                                                            R. Penno
                                                     Juniper Networks
                                                             D. Wing
                                                               Cisco
                                                   November 21, 2011

Universal Plug and Play (UPnP) Internet Gateway Device (IGD)-Port Control Protocol (PCP) Interworking Function
draft-ietf-pcp-upnp-igd-interworking-00

Abstract

   This document specifies the behavior of the UPnP IGD (Internet
   Gateway Device)/PCP Interworking Function. An UPnP IGD-PCP
   Interworking Function (IGD-PCP IWF) is required to be embedded in CP
   routers to allow for transparent NAT control in environments where
   UPnP is used in the LAN side and PCP in the external side of the CP
   router.

Requirements Language

   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 [RFC2119].

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

   PCP [I-D.ietf-pcp-base] discusses the implementation of NAT control
   features that rely upon Carrier Grade NAT devices such as DS-Lite
   AFTR [RFC6333] or NAT64 [RFC6146]. Nevertheless, in environments
   where UPnP is used in the local network, an interworking function
   between UPnP IGD and PCP is required to be embedded in the CP router
   (an example is illustrated in Figure 1).

   Two configurations are considered:

   o No NAT function is embedded in the CP router. This is required
      for instance in DS-Lite or NAT64 deployments;

   o The CP router embeds a NAT function.

```
                         UPnP-PCP
    UPnP Control        Interworking
       Point             Function                    PCP Server
         |                   |                            |
         | (1) AddPortMapping |                           |
         |------------------->|                           |
         |                   |   (2) PCP MAP Request      |
         |                   |-------------------------->|
         |                   |                            |
```
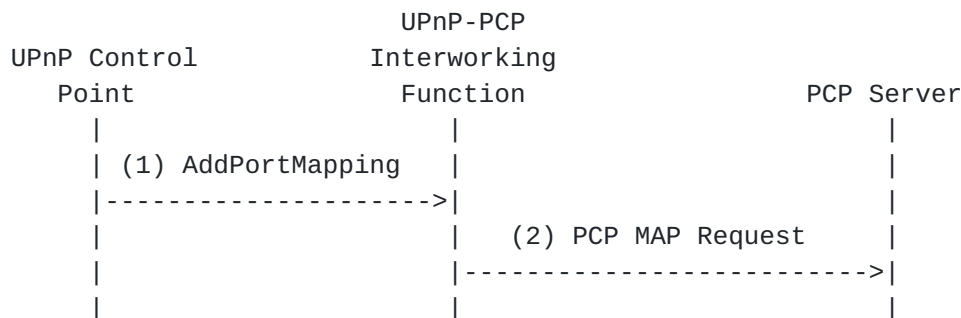
                      Figure 1: Flow Example

   The UPnP IGD-PCP Interworking Function (IGD-PCP IWF) maintains a
   local mapping table which stores all active mappings instructed by
   internal UPnP Control Points. This design choice restricts the
   amount of PCP messages to be exchanged with the PCP Server.

   Triggers for deactivating the UPnP IGD-PCP Interworking Function from
   the CP router and relying on a PCP-only mode are out of scope of this
   document.

2. Acronyms

   This document make use of the following abbreviations:

```
                        CP router  Customer Premise router
                          DS-Lite  Dual-Stack Lite
                              IGD  Internet Gateway Device
                              IWF  Interworking Function
                              NAT  Network Address Translation
                              PCP  Port Control Protocol
                             UPnP  Universal Plug and Play
```

3. Architecture Model

As a reminder, Figure 2 illustrates the architecture model adopted by
UPnP IGD [IGD2]. In Figure 2, the following UPnP terminology is
used:

o Client refers to a host located in the local network.

o IGD Control Point is a UPnP control point using UPnP to control an
   IGD (Internet Gateway Device).

o Host represents a remote peer reachable in the Internet.

```
+-------------+
| IGD Control |
|   Point     |-----+
+-------------+     |    +-----+        +------+
                    +---|     |        |      |
                        | IGD |-------| Host |
                    +---|     |        |      |
+-------------+     |    +-----+        +------+
|   Client    |-----+
+-------------+
```
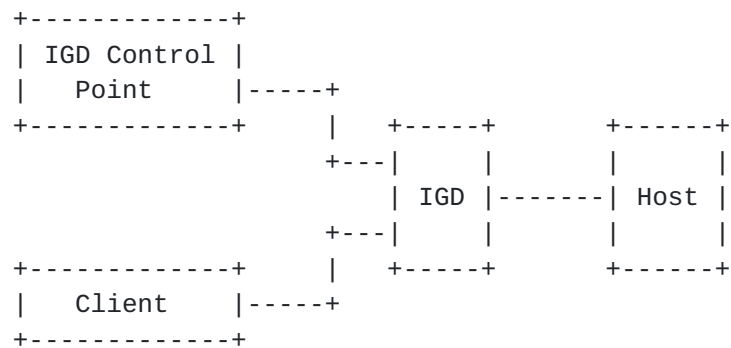
Figure 2: UPnP IGD Model

This model is not valid when PCP is used to control for instance a
Carrier Grade NAT (a.k.a., Provider NAT) while internal hosts
continue to use UPnP. In such scenarios, Figure 3 shows the updated
model.

```
+-------------+
| IGD Control |
|   Point     |----+
+-------------+    |   +-----+      +--------+              +------+
                 +---| IGD-|      |Provider|              |      |
                   | PCP |------|   NAT  |--<Internet>---| Peer |
                 +---| IWF |      |        |              |      |
+-------------+    |   +-----+      +--------+              +------+
| Local Host  |----+
+-------------+
                    LAN Side  External Side
<======UPnP IGD==============><=====PCP=====>
```
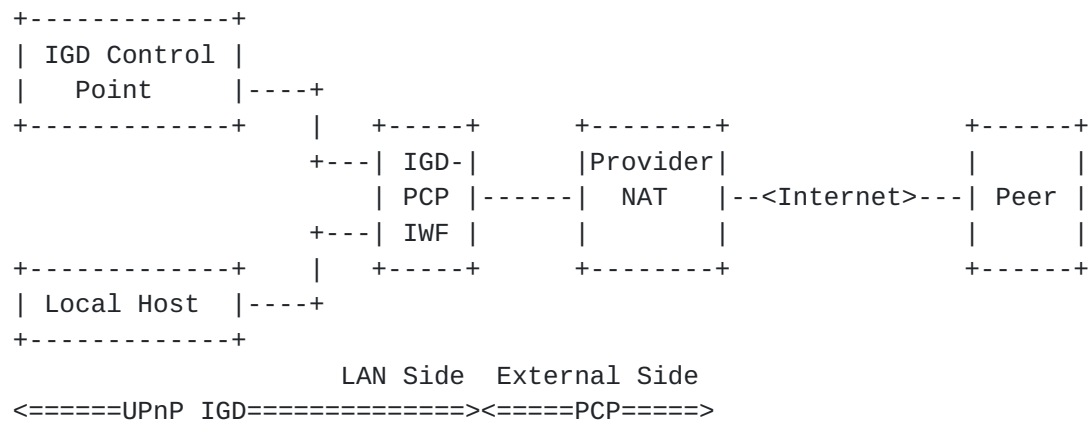
                 Figure 3: UPnP IGD-PCP Interworking Model

In the updated model depicted in Figure 3, one or two levels of NAT
can be encountered in the data path. Indeed, in addition to the
Carrier Grade NAT, the CP router may embed a NAT function (Figure 4).

```
+-------------+
| IGD Control |
|   Point     |-----+
+-------------+     |   +-----+      +----+              +------+
                 +---| IGD-|      |    |    |              |Remote|
                   | PCP |-------|NAT2|--<Internet>---| Host |
                 +---| IWF |      |    |    |              |      |
+-------------+     |   +-----+      +----+              +------+
| Local Host  |-----+     NAT1
+-------------+
```
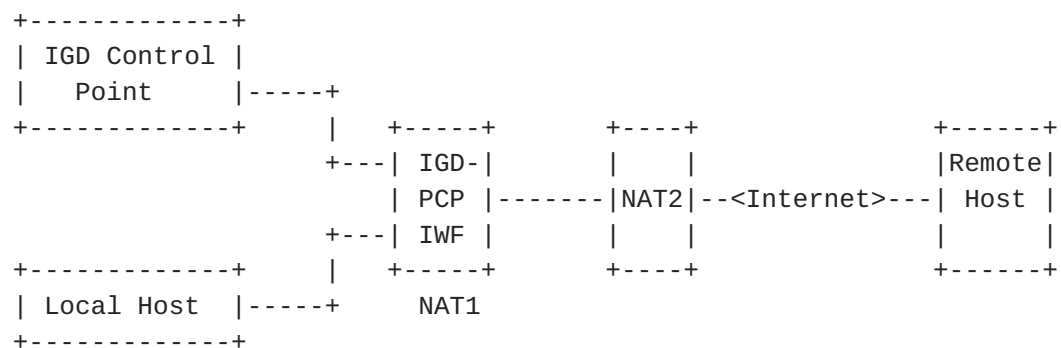
                    Figure 4: Cascaded NAT scenario

To ensure a successful interworking between UPnP IGD and PCP, an
interworking function is embedded in the CP router. In the model
defined in Figure 3, all UPnP IGD server-oriented functions, a PCP
Client [I-D.ietf-pcp-base] and a UPnP IGD-PCP Interworking Function
are embedded in the CP router (i.e., IGD). In the rest of the
document, IGD-PCP Interworking Function refers to PCP Client and UPnP
IGD-PCP Interworking Function.

UPnP IGD-PCP Interworking Function is responsible for generating a
well-formed PCP (resp., UPnP IGD) message from a received UPnP IGD
(resp., PCP) message.

4. **UPnP IGD-PCP Interworking Function: Overview**

Three tables are provided to specify the mapping between UPnP IGD and PCP:

1. Section 4.1 provides the mapping between WANIPConnection State Variables and PCP parameters;

2. Section 4.2 focuses on the correspondence between supported methods;

3. Section 4.3 lists the PCP error messages and their corresponding IGD ones.

Note that some enhancements have been integrated in WANIPConnection as documented in [IGD2].

4.1. **UPnP IGD-PCP: State Variables**

ConnectionType: Not applicable
   Out of scope of PCP but as the controlled device is a NAT the
   default value IP_Routed is very likely used.

PossibleConnectionTypes: Not applicable
   Out of scope of PCP (same comment than for ConnectionType).

ConnectionStatus: Not applicable
   Out of scope of PCP but when it is possible to successfully
   communicate with a PCP Server the Connected value could be
   expected, otherwise Disconnected.

Uptime: Not applicable
   Out of scope of PCP (possible values are the number of seconds
   since a successfull communication was established with a PCP
   Server, or with a state maintained in a stable storage the number
   of seconds since the initialization of the current state).

LastConnectionError: Not applicable
   Out of scope of PCP but expected to be ERROR_NONE in absence of
   errors.

RSIPAvailable: Not applicable
   Out of scope of PCP (expected to be 0, i.e., RSIP not available).

ExternaIPAddress: External IP Address
   Read-only variable with the value from the last PCP response or
   the empty string if none was received yet.

   PortMappingNumberOfEntries: Not applicable
      Managed locally by the UPnP IGD-PCP Interworking Function.

   PortMappingEnabled: Not applicable
      PCP does not support deactivating the dynamic NAT mapping since
      the initial goal of PCP is to ease the traversal of Carrier Grade
      NAT. Supporting such per-subscriber function may overload the
      Carrier Grade NAT.
      On reading the value should be 1, writing a value different from 1
      is not supported.

   PortMappingLeaseDuration: Requested Mapping Lifetime
      In IGD:1 the value 0 means infinite, in IGD:2 its is remapped to
      the IGD maximum of 604800 seconds [IGD2]. PCP allows for a
      maximum value of 65535 seconds.
      The UPnP IGD-PCP Interworking Function simulates long and even
      infinite lifetimes using renewals. The behavior in the case of a
      failing renewal is currently undefined.
      IGD:1 doesn't define the behavior in the case of state lost, IGD:2
      doesn't require to keep state in stable storage, i.e., to make the
      state to survive resets/reboots. Of course the IGD:2 behavior
      should be implemented.

   RemoteHost: Unsupported
      Not yet supported by PCP (part of the firewall features). Note a
      domain name is allowed by IGD:2 and has to be resolved into an IP
      address.

   ExternalPort: External Port Number
      Not wildcard (0) value mapped to PCP external port field in MAP
      messages. The explicit wildcard (0) value is not supported.

   InternalPort: Internal Port Number
      Mapped to PCP internal port field in MAP messages.

   PortMappingProtocol: Transport Protocol
      Mapped to PCP protocol field in MAP messages. Note IGD only
      supports TCP and UDP.

   InternalClient: Internal IP Address
      InternalClient can be an IP address or a domain name. Only an IP
      address scheme is supported in PCP. If a domain name is used
      Point, it must be resolved to an IP address by the Interworking
      Function when relying the message to the PCP Server.

   PortMappingDescription: Not applicable
      Not supported in base PCP. When present in UPnP IGD messages,
      this parameter SHOULD NOT be propagated in the corresponding PCP
      messages. If the local PCP Client support a PCP Option to convey
      the description, this option MAY be used.

   SystemUpdateID (only for IGD:2): Not applicable
      Managed locally by the UPnP IGD-PCP Interworking Function

   A_ARG_TYPE_Manage (only for IGD:2): Not applicable
      Out of scope of PCP (but has a clear impact on security).

   A_ARG_TYPE_PortListing (only for IGD:2): Not applicable
      Managed locally by the UPnP IGD-PCP Interworking Function

4.2. IGD-PCP: Methods

   Both IGD:1 and IGD:2 methods are listed here.

   SetConnectionType: Not applicable
      Calling this method doesn't make sense in this context. An error
      (IGD:1 501 "ActionFailed" or IGD:2 731 "ReadOnly") may be directly
      returned.

   GetConnectionTypeInfo: Not applicable
      May directly return values of corresponding State Variables.

   RequestConnection: Not applicable
      Calling this method doesn't make sense in this context. An error
      (IGD:1 501 "ActionFailed" or IGD:2 606 "Action not authorized")
      may be directly returned.

   ForceTermination: Notapplicable
      Same than RequestConnection.

   GetStatusInfo: Not applicable
      May directly return values of corresponding State Variables.

   GetNATRSIPStatus: Not applicable
      May directly return values of corresponding State Variables.

   GetGenericPortMappingEntry: Not applicable
      This request is not relayed to the PCP Server. IGD-PCP
      Interworking Function maintains an updated list of active mappings
      instantiated in the PCP Server by internal hosts. See Section 5.8
      for more information.

GetSpecificPortMappingEntry: Not applicable
   Under normal conditions, the IGD-PCP Interworking Function
   maintains an updated list of active mapping as instantiated in the
   PCP Server. The IGD-PCP Interworking Function locally handles
   this request and provides back the port mapping entry based on the
   ExternalPort, the PortMappingProtocol, and the RemoteHost. See
   Section 5.8 for more information.

AddPortMapping: MAP
   We recommend the use of AddAnyPortMapping() instead of
   AddPortMapping(). Refer to Section 5.7.2.

AddAnyPortMapping (for IGD:2 only): MAP
   No issue is encountered to proxy this request to the PCP Server.
   Refer to Section 5.7.1 for more details

DeletePortMapping: MAP with a requested lifetime set to 0
   Refer to Section 5.9.

DeletePortMappingRange (for IGD:2 only): MAP with a lifetime
   positioned to 0
   Individual requests are issued by the IGD-PCP Interworking
   Function. Refer to Section 5.9 for more details

GetExternalIPAddress: Not applicable
   PCP does not support a method for retrieving the external IP
   address. Issuing MAP may be used as a means to retrieve the
   external IP address.
   May directly return the value of the corresponding State Variable.

GetListOfPortMappings: Not applicable
   The IGD-PCP Interworking Function maintains an updated list of
   active mapping as instantiated in the PCP Server. The IGD-PCP
   Interworking Function handles locally this request. See
   Section 5.8 for more information

4.3. UPnP IGD-PCP: Errors

This section lists PCP errors codes and the corresponding UPnP IGD
ones. Error codes specific to IGD:2 are tagged accordingly.

1 UNSUPP_VERSION: 501 "ActionFailed"
  Should not happen.

2 NOT_AUTHORIZED: IGD:1 718 "ConflictInMappingEntry" / IGD:2 606
  "Action not authorized"
  729 "ConflictWithOtherMechanisms" is possible too.

3 MALFORMED_REQUEST: 501 "ActionFailed"

4 UNSUPP_OPCODE: 501 "ActionFailed"
  Should not happen.

5 UNSUPP_OPTION: 501 "ActionFailed"
  Should not happen at the exception of PREFER_FAILURE (this
  option is not mandatory to support but AddPortMapping() cannot be
  implemented without it).

6 MALFORMED_OPTION: 501 "ActionFailed"
  Should not happen.

7 NETWORK_FAILURE: Not applicable
  Should not happen after communication was successfully established
  with a PCP Server. Before the ConnectionStatus State Variable
  must not be set to Connected.

8 NO_RESOURCES: IGD:1 501 "ActionFailed" / IGD:2 728
  "NoPortMapsAvailable"
  Cannot be distinguished from USER_EX_QUOTA.

9 UNSUPP_PROTOCOL: 501 "ActionFailed"
  Should not happen.

10 USER_EX_QUOTA: IGD:1 501 "ActionFailed" / IGD:2 728
  "NoPortMapsAvailable"
  Cannot be distinguished from NO_RESOURCES.

11 CANNOT_PROVIDE_EXTERNAL: 718 "ConflictInMappingEntry"

12 ADDRESS_MISMATCH: 501 "ActionFailed"
  Should not happen.

13 EXCESSIVE_REMOTE_PEERS: 501 "ActionFailed"

5. Specification of the IGD-PCP Interworking Function

   This section covers the scenarios with or without NAT in the CP
   router.

5.1. PCP Server Discovery

   The IGD-PCP Interworking Function implements one of the discovery
   methods identified in [I-D.ietf-pcp-base] (e.g., DHCP
   [I-D.bpw-pcp-dhcp]). The IGD-PCP Interworking Function behaves as a
   PCP Client when communicating with the provisioned PCP Server.

   In order to not impact the delivery of local services requiring the
   control of the local IGD during any failure event to reach the PCP
   Server (e.g., no IP address/prefix is assigned to the CP router),
   IGD-PCP Interworking Function MUST NOT be invoked. Indeed, UPnP
   machinery is used to control that device and therefore lead to
   successful operations of internal services.

   Once the PCP Sever is reachable, the IGD-PCP Interworking Function
   MUST synchronize its state as specified in Section 5.10.

5.2. Control of the Firewall

   In order to configure security policies to be applied to inbound and
   outbound traffic, UPnP IGD can be used to control a local firewall
   engine.

   No IGD-PCP Interworking Function is therefore required for that
   purpose.

5.3. NAT Control in LAN Side

   Internal UPnP Control Points are not aware of the presence of the
   IGD-PCP Interworking Function in the CP router (IGD). Especially,
   UPnP Control Points MUST NOT be aware of the deactivation of the NAT
   in the CP router.

   No modification is required in the UPnP Control Point.

5.4. Port Mapping Tables

   IGD-PCP Interworking Function MUST store locally all the mappings
   instantiated by internal UPnP Control Points in the PCP Server. Port
   Forwarding mappings SHOULD be stored in a permanent storage. If not,
   upon reset or reboot, the IGD-PCP Interworking Function SHOULD
   synchronise its states as specified in Section 5.10.

Upon receipt of a PCP MAP Response from the PCP Server, the IGD-PCP
Interworking Function MUST retrieve the enclosed mapping and MUST
store it in the local mapping table. The local mapping table is an
image of the mapping table as maintained by the PCP Server for a
given subscriber.

5.5. Interworking Function Without NAT in the CP Router

When no NAT is embedded in the CP router, the content of received
WANIPConnection and PCP messages is not altered by the IGD-PCP
Interworking Function (i.e., the content of WANIPConnection messages
are mapped to the PCP messages (and mapped back) according to
Section 4.1).

5.6. NAT Embedded in the CP Router

Unlike the scenario with one level of NAT (Section 5.5), the IGD-PCP
Interworking Function MUST update the content of received mapping
messages with the IP address and/or port number belonging to the
external interface of the CP router (i.e., after the NAT1 operation
in Figure 4) and not as initially positioned by the UPnP Control
Point.

All WANIPConnection messages issued by the UPnP Control Point (resp.,
PCP Server) are intercepted by the IGD-PCP Interworking Function.
Then, the corresponding messages (see Section 4.1, Section 4.2 and
Section 4.3) are generated by the IGD-PCP Interworking Function and
sent to the provisioned PCP Server (resp., corresponding UPnP Control
Point). The content of PCP messages received by the PCP Server
reflects the mapping information as enforced in the first NAT. In
particular, the internal IP address and/or port number of the
requests are replaced with the IP address and port number as assigned
by the NAT of the CP router. For the reverse path, PCP response
messages are intercepted by the IGD-PCP Interworking Function. The
content of the corresponding WANIPConnection messages are updated:

o The internal IP address and/or port number as initially positioned
   by the UPnP Control Point and stored in the CP router NAT are used
   to update the corresponding fields in received PCP responses.

o The external IP and port number are not altered by the IGD-PCP
   Interworking Function.

o The NAT mapping entry in the first NAT is updated with the result
   of PCP request.

The lifetime of the mappings instantiated in all involved NATs SHOULD
be the one assigned by the terminating PCP Server. In any case, the

lifetime MUST be lower or equal to the one assigned by the
terminating PCP Server.

5.7. Creating a Mapping

Two methods can be used to create a mapping: AddPortMapping() or
AddAnyPortMapping().

AddAnyPortMapping() is the RECOMMENDED method.

5.7.1. AddAnyPortMapping()

When an UPnP Control Point issues a AddAnyPortMapping(), this request
is received by the UPnP Server. The request is then relayed to the
IGD-PCP Interworking Function which generates a PCP MAP Request (see
Section 4.1 for mapping between WANIPConnection and PCP parameters).
Upon receipt of PCP MAP Response from the PCP Server, an XML mapping
is returned to the requesting UPnP Control Point (the content of the
messages follows the recommendations listed in Section 5.6 or
Section 5.5 according to the deployed scenario). A flow example is
depicted in Figure 5.

If a PCP Error is received from the PCP Server, a corresponding
WANIPConnection error code Section 4.3 is generated by the IGD-PCP
Interworking Function and sent to the requesting UPnP Control Point.

```
                              UPnP-PCP
     UPnP Control           Interworking
        Point                 Function                     PCP Server
         |                        |                             |
         |(1) AddAnyPortMapping   |                             |
         |    ExternalPort=8080   |                             |
         |----------------------->|                             |
         |                        |    (2) PCP MAP Request       |
         |                        |requested external port=8080 |
         |                        |---------------------------->|
         |                        |                             |
         |                        |    (3) PCP MAP Response       |
         |                        | assigned external port=6598 |
         |                        |<----------------------------|
         |(4) AddAnyPortMapping   |                             |
         |    ReservedPort=6598   |                             |
         |<-----------------------|                             |
```
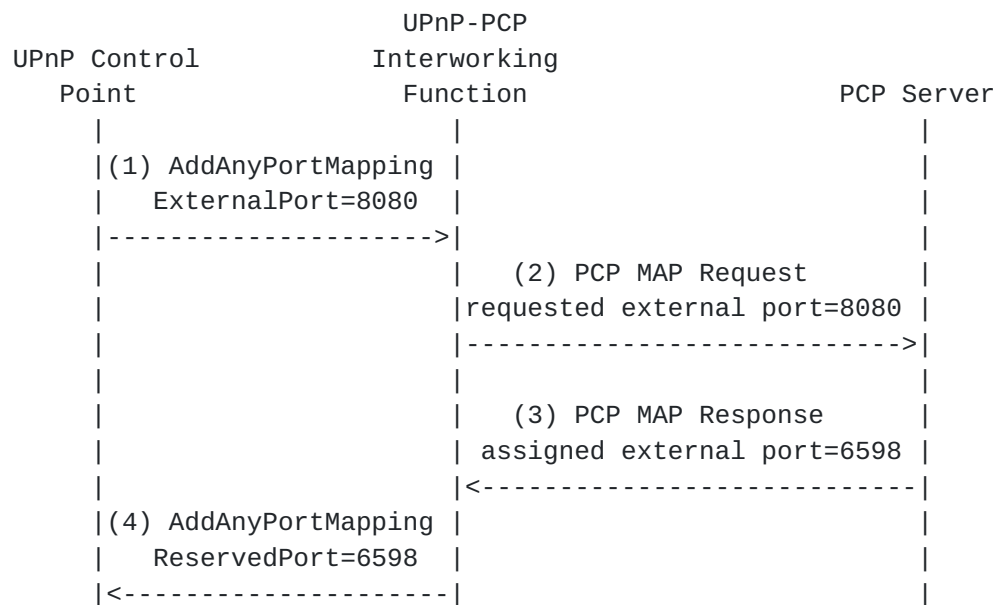
            Figure 5: Flow example when AddAnyPortMapping() is used

5.7.2. AddPortMapping()

   A dedicated option called PREFER_FAILURE is defined in
   [I-D.ietf-pcp-base] to toggle the behavior in a PCP Request message.
   This options is inserted by the IGD-PCP IWF when issuing its requests
   to the PCP Server only if a specific external port is requested by
   the UPnP Control Point. The mapping of wildcard (i.e., 0)
   ExternalPort is not yet defined.

   Upon receipt of AddPortMapping() from an UPnP Control Point, the IGD-
   PCP Interworking Function first checks if the requested external port
   number is not used by another Internal UPnP Control Point. In case a
   mapping bound to the requested external port number is found in the
   local mapping table, the IGD-PCP IWF MUST send back a
   ConflictInMappingEntry error to the requesting UPnP Control Point
   (see Figure 6).

```
                            UPnP-PCP
     UPnP Control          Interworking
       Point                 Function                  PCP Server
         |                      |                          |
         | (1) AddPortMapping   |                          |
         |    ExternalPort=2356 |                          |
         |--------------------->|                          |
         |                      |                          |
         |      (2) Error:      |                          |
         |ConflictInMappingEntry|                          |
         |<---------------------|                          |
         |                      |                          |
         | (3) AddPortMapping   |                          |
         |    ExternalPort=4586 |                          |
         |--------------------->|                          |
         |                      |                          |
         |      (4) Error:      |                          |
         |ConflictInMappingEntry|                          |
         |<---------------------|                          |
         |                      |                          |
```
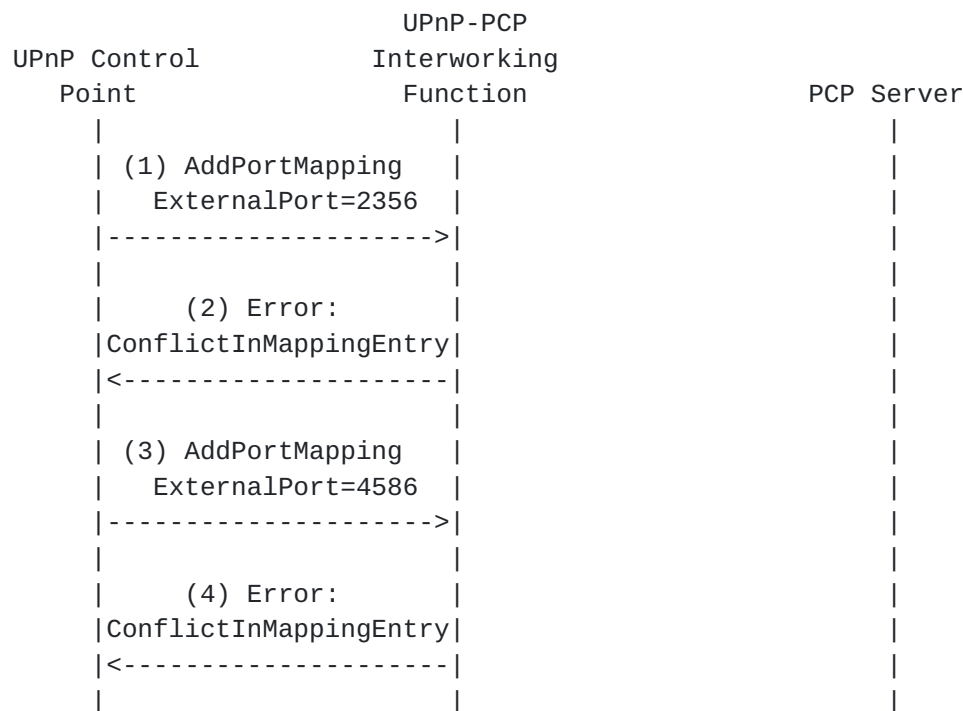
                        Figure 6: IWF Local Behaviour

   This exchange (Figure 6) is re-iterated until an external port number
   that is not in use is requested by the UPnP Control Point. Then, the
   IGD-PCP IWF generates a PCP MAP Request with all requested mapping
   information as indicated by the UPnP Control Point if no NAT is
   embedded in the CP router or updated as specified in Section 5.6. In
   addition, the IGD-PCP IWF inserts a PREFER_FAILURE Option to the
   generated PCP request.

   If the requested external port is in use, a PCP Error message MUST be
   sent by the PCP Server to the IGD-PCP IWF indicating
   CANNOT_PROVIDE_EXTERNAL as the error cause. The IGD-PCP IWF relays a
   negative message to the UPnP Control Point indicating
   ConflictInMappingEntry as error code. The UPnP Control Point re-
   issues a new request with a new requested external port number. This
   process is repeated until a positive answer is received or maximum
   retry is reached.

   If the PCP Server is able to honor the requested external port, a
   positive response is sent to the requesting IGD-PCP IWF. Upon
   receipt of the response from the PCP Server, the returned mapping
   MUST be stored by the IGD-PCP Interworking Function in its local
   mapping table and a positive answer MUST be sent to the requesting
   UPnP Control Point. This answer terminates this exchange.

   Figure 7 shows an example of the flow exchange that occurs when the
   PCP Server satisfies the request from the IGD-PCP IWF. Figure 8
   shows the messages exchange when the requested external port is in
   use.

```
                             UPnP-PCP
     UPnP Control            Interworking
        Point                 Function                     PCP Server
         |                       |                             |
         | (1) AddPortMapping    |                             |
         |    ExternalPort=8080  |                             |
         |---------------------->|                             |
         |                       |    (2) PCP MAP Request       |
         |                       |requested external port=8080 |
         |                       |        PREFER_FAILURE        |
         |                       |---------------------------->|
         |                       |                             |
         |                       |    (3) PCP MAP Response       |
         |                       |  assigned external port=8080 |
         |                       |<----------------------------|
         | (4) AddPortMapping    |                             |
         |    ExternalPort=8080  |                             |
         |<----------------------|                             |
```
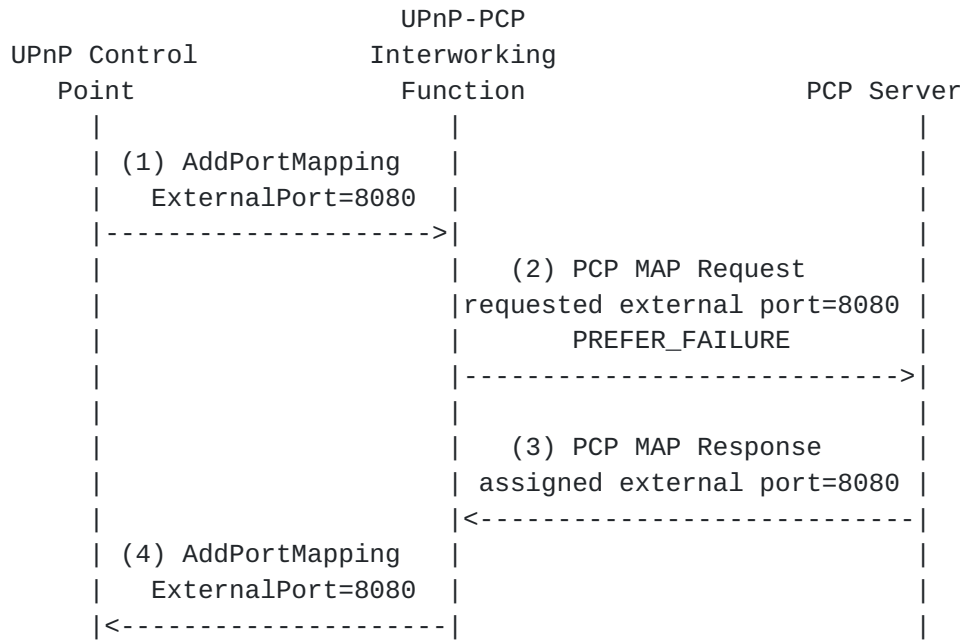
               Figure 7: Flow Example (Positive Answer)

```
                            UPnP-PCP
     UPnP Control          Interworking
        Point                Function                  PCP Server
          |                     |                          |
          | (1) AddPortMapping  |                          |
          |    ExternalPort=8080 |                         |
          |-------------------->|                          |
          |                     | (2) PCP MAP Request      |
          |                     |requested external port=8080 |
          |                     |       PREFER_FAILURE     |
          |                     |------------------------->|
          |                     | (3) PCP MAP Response     |
          |                     |    CANNOT_PROVIDE_EXTERNAL |
          |                     |<-------------------------|
          |      (4) Error:     |                          |
          |ConflictInMappingEntry|                         |
          |<--------------------|                          |
          | (5) AddPortMapping  |                          |
          |    ExternalPort=5485 |                         |
          |-------------------->|                          |
          |                     | (6) PCP MAP Request      |
          |                     |requested external port=5485 |
          |                     |       PREFER_FAILURE     |
          |                     |------------------------->|
          |                     | (7) PCP MAP Response     |
          |                     |    CANNOT_PROVIDE_EXTERNAL |
          |                     |<-------------------------|
          |      (8) Error:     |                          |
          |ConflictInMappingEntry|                         |
          |<--------------------|                          |
                              ....
          | (a) AddPortMapping  |                          |
          |    ExternalPort=6591 |                         |
          |-------------------->|                          |
          |                     | (b) PCP MAP Request      |
          |                     |requested external port=6591 |
          |                     |       PREFER_FAILURE     |
          |                     |------------------------->|
          |                     | (c) PCP MAP Response     |
          |                     |    CANNOT_PROVIDE_EXTERNAL |
          |                     |<-------------------------|
          |      (d) Error:     |                          |
          |ConflictInMappingEntry|                         |
          |<--------------------|                          |
```
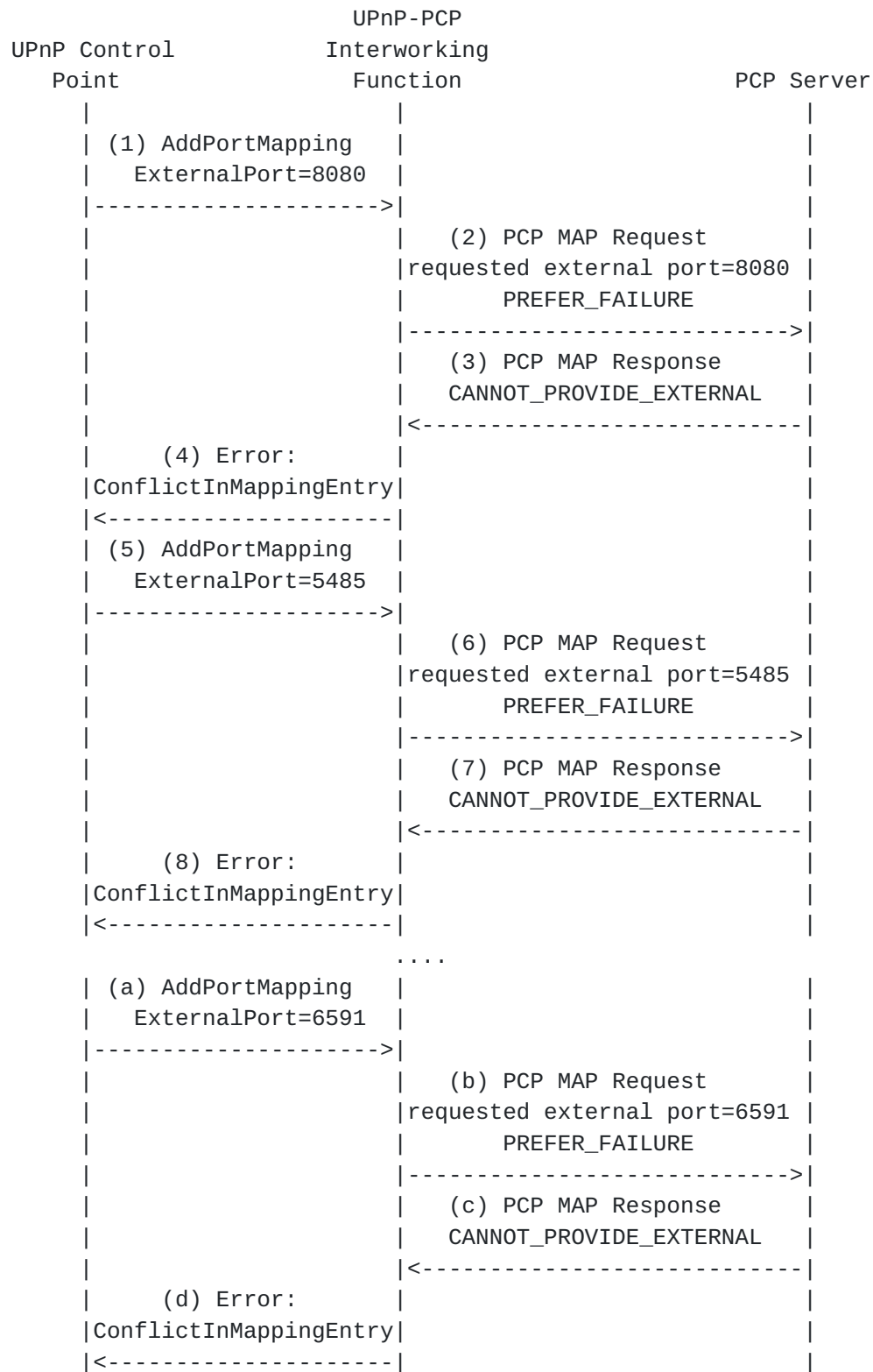
Figure 8: Flow Example (Negative Answer)

[Note: According to some experiments, some UPnP 1.0
implementations,e.g.- uTorrent, simply try the same external port
X times (usually 4 times) and failed. Do we need to add a
clarification about thisin the example above.]

5.8. Listing One or a Set of Mappings

In order to list active mappings, an UPnP Control Point may issue
GetGenericPortMappingEntry(), GetSpecificPortMappingEntry() or
GetListOfPortMappings().

These methods MUST NOT be proxied to the PCP Server since a local
mapping is maintained by the IGD-PCP Interworking Function.

5.9. Delete One or a Set of Mappings: DeletePortMapping() or DeletePortMappingRange()

A UPnP Control Point proceeds to the deletion of one or a list of
mappings by issuing DeletePortMapping() or DeletePortMappingRange().
In IGD:2, we assume the IGD applies the appropriate security policies
to grant whether a Control Point has the rights to delete one or a
set of mappings. When authorization fails, "606 Action Not
Authorized" error code MUST be returned the requesting Control Point.

When DeletePortMapping() or DeletePortMappingRange() is received by
the IGD-PCP Interworking Function, it first checks if the requested
mappings to be removed are present in the local mapping table. If no
mapping matching the request is found in the local table an error
code is sent back to the UPnP Control Point: "714 NoSuchEntryInArray"
for DeletePortMapping() or "730 PortMappingNotFound" for
DeletePortMappingRange().

Figure 9 shows an example of UPnP Control Point asking to delete a
mapping which is not instantiated in the local table of the IWF.

```
                              UPnP-PCP
    UPnP Control              Interworking
       Point                  Function                    PCP Server
         |                        |                            |
         |(1) DeletePortMapping   |                            |
         |----------------------->|                            |
         |                        |                            |
         |      (2) Error:        |                            |
         |   NoSuchEntryInArray   |                            |
         |<-----------------------|                            |
         |                        |                            |
```
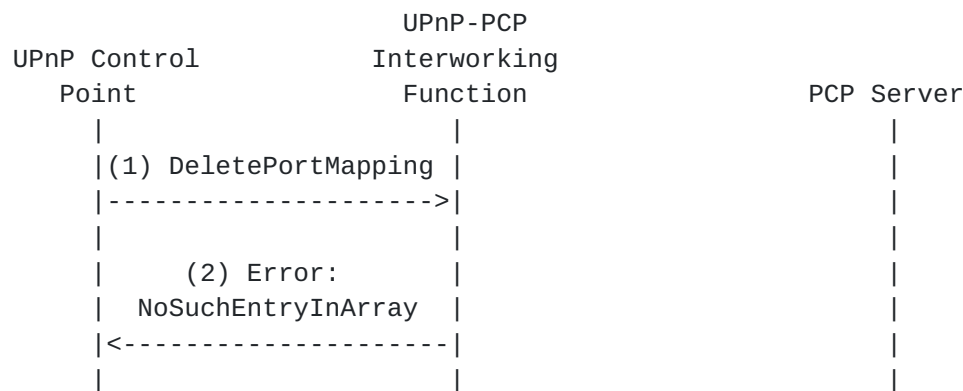
                  Figure 9: Local Delete (IGD-PCP IWF)

If a mapping matches in the local table, a PCP MAP delete request is
generated taking into account the input arguments as included in
DeletePortMapping() if no NAT is enabled in the CP router or the
corresponding local IP address and port number as assigned by the
local NAT if a NAT is enabled in the CP router. When a positive
answer is received from the PCP Server, the IGD-PCP Interworking
Function updates its local mapping table (i.e., remove the
corresponding entry) and notifies the UPnP Control Point about the
result of the removal operation. Once PCP MAP delete request is
received by the PCP Server, it proceeds to removing the corresponding
entry. A PCP MAP delete response is sent back if the removal of the
corresponding entry was successful; if not, a PCP Error is sent back
to the IGD-PCP Interworking Function including the corresponding
error cause (See Section 4.3).

In case DeletePortMappingRange() is used, the IGD-PCP IWF undertakes
a lookup on its local mapping table to retrieve individual mappings
instantiated by the requested Control Point (i.e., authorization
checks) and matching the signalled port range (i.e., the external
port is within "StartPort" and "EndPort" arguments of
DeletePortMappingRange()). If no mapping is found, "730
PortMappingNotFound" error code is sent to the UPnP Control Point
(Figure 10). If a set of mappings are found, the IGD-PCP IWF
generates individual PCP MAP delete requests corresponding to these
mappings (See the example shown in Figure 11).

   [[Discussion note: The IWF can send a positive answer to the
   requesting UPnP Control Point without waiting to receive all the
   answers from the PCP Server. It is unlikely to encounter a
   problem in the PCP leg because the IWF has verified authorization
   rights and also the presence of the mapping in the local table.]]

```
                              UPnP-PCP
    UPnP Control             Interworking
       Point                   Function                   PCP Server
         |                        |                           |
         |(1)DeletePortMappingRange() |                       |
         |      StartPort=8596        |                       |
         |      EndPort  =9000        |                       |
         |      Protocol =UDP         |                       |
         |--------------------------->|                       |
         |                        |                           |
         |        (2) Error:      |                           |
         |    PortMappingNotFound |                           |
         |<-----------------------|                           |
         |                        |                           |
```
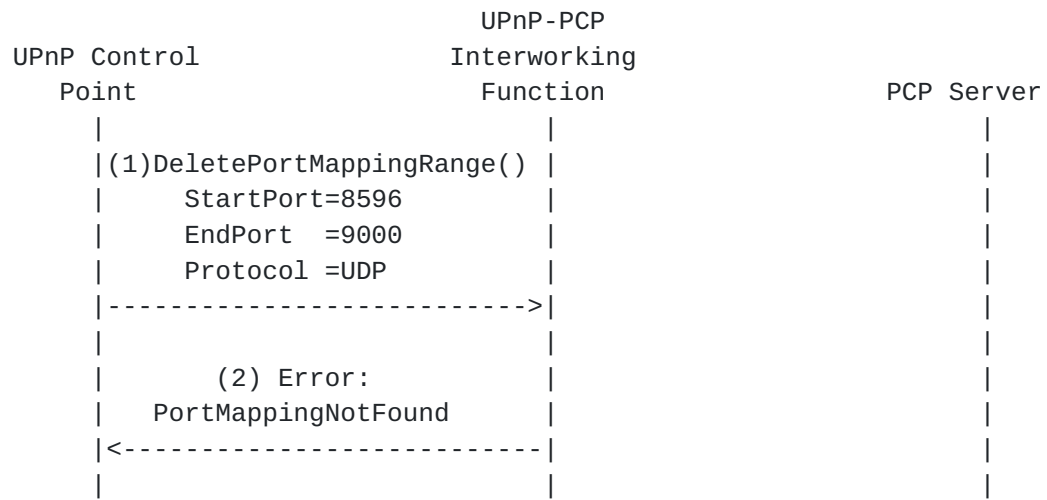
Figure 10: Flow example when an error encountered when processing
DeletePortMappingRange()

This example illustrates the exchanges that occur when the IWF
receives DeletePortMappingRange(). In this example, only two
mappings having the external port number in the 6000-6050 range are
maintained in the local table. The IWF issues two MAP requests to
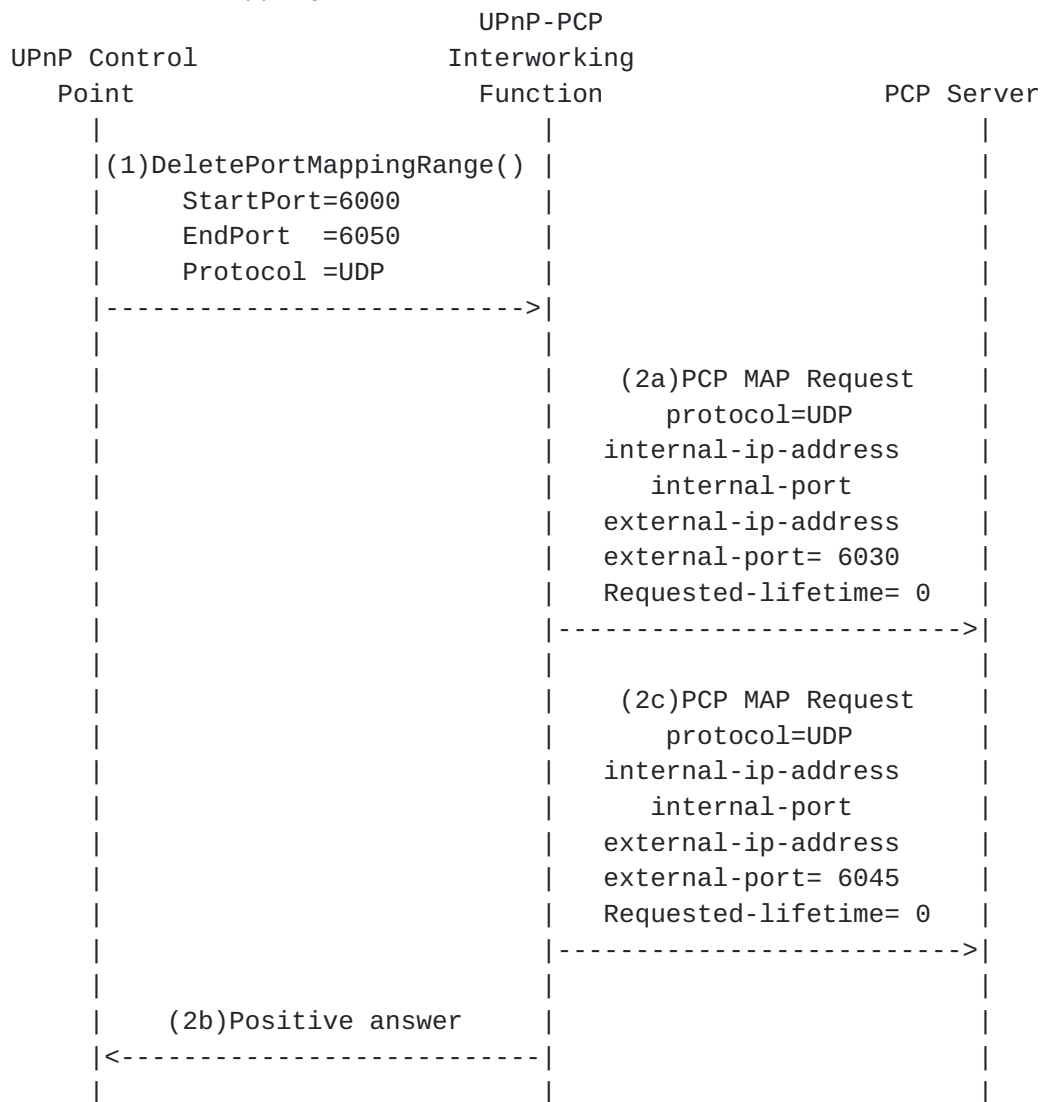delete these mappings.

```
                                    UPnP-PCP
     UPnP Control                 Interworking
        Point                       Function                PCP Server
          |                            |                        |
          |(1)DeletePortMappingRange() |                        |
          |      StartPort=6000        |                        |
          |      EndPort  =6050        |                        |
          |      Protocol =UDP         |                        |
          |--------------------------->|                        |
          |                            |                        |
          |                            |    (2a)PCP MAP Request  |
          |                            |        protocol=UDP     |
          |                            |     internal-ip-address |
          |                            |        internal-port    |
          |                            |     external-ip-address |
          |                            |     external-port= 6030 |
          |                            |     Requested-lifetime= 0 |
          |                            |--------------------------->|
          |                            |                        |
          |                            |    (2c)PCP MAP Request  |
          |                            |        protocol=UDP     |
          |                            |     internal-ip-address |
          |                            |        internal-port    |
          |                            |     external-ip-address |
          |                            |     external-port= 6045 |
          |                            |     Requested-lifetime= 0 |
          |                            |--------------------------->|
          |                            |                        |
          |     (2b)Positive answer    |                        |
          |<---------------------------|                        |
          |                            |                        |
```

              Figure 11: Example of DeletePortMappingRange()

5.10. Mapping Synchronisation

   [[Note: This section needs further discussion among authors]]

   Under normal conditions, since a valid copy of the mapping table is
   stored locally in the CP router, the IGD-PCP Interworking Function
   SHOULD NOT issue any subsequent PCP request to handle a request
   received from an UPnP Control Point to list active mappings.
   Nevertheless, in case of loss of synchronisation (e.g., reboot,

system crashes, power outage, etc.), the IGD-PCP Interworking
Function SHOULD generate a get method to retrieve all active mappings
in the PCP Server and update its local mapping table without waiting
for an explicit request from a UPnP Control Point. Doing so, the
IGD-PCP Interworking Function maintains an updated mapping table.

In case of massive reboot of CP routers (e.g., avalanche restart
phenomenon), PCP request bursts SHOULD be avoided. For this aim, we
recommend the use of a given timer denoted as PCP_SERVICE_WAIT. This
timer can be pre-configured in the CP router or to be provisioned
using a dedicated means such as DHCP. Upon reboot of the CP router,
PCP messages SHOULD NOT be sent immediately. A random value is
selected between 0 and PCP_SERVICE_WAIT. This value is referred to
as RAND(PCP_SERVICE_WAIT). Upon the expiration of
RAND(PCP_SERVICE_WAIT), the CP router SHOULD proceed to its
synchronisation operations (i.e., retrieve all active mappings which
have been instructed by internal UPnP Control Point(s)).

[[Note: per-subscriber quota may be exhausted due to unlimited
lifetime and stale mappings in IGD due to reboots, etc.]]

6. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an
RFC.

7. Security Considerations

IGD:2 authorization framework SHOULD be used. When only IGD:1 is
available, one MAY consider to enforce the default security, i.e.,
operation on the behalf of a third party is not allowed.

This document defines a procedure to instruct PCP mappings for third
party devices belonging to the same subscriber. Identification means
to avoid a malicious user to instruct mappings on behalf of a third
party must be enabled. Such means are already discussed in Section
7.4.4 of [I-D.ietf-pcp-base].

Security considerations elaborated in [I-D.ietf-pcp-base] and
[Sec_DCP] should be taken into account.

8. Acknowledgments

   Authors would like to thank F. Fontaine, C. Jacquenet and X. Deng for
   their review and comments.

9. References

9.1. Normative References

   [I-D.ietf-pcp-base]
              Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P.
              Selkirk, "Port Control Protocol (PCP)",
              draft-ietf-pcp-base-17 (work in progress), October 2011.

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119, March 1997.

9.2. Informative References

   [I-D.bpw-pcp-dhcp]
              Boucadair, M., Penno, R., and D. Wing, "DHCP and DHCPv6
              Options for the Port Control Protocol (PCP)",
              draft-bpw-pcp-dhcp-04 (work in progress), April 2011.

   [IGD2]   UPnP Forum, "WANIPConnection:2 Service (http://upnp.org/
              specs/gw/UPnP-gw-WANIPConnection-v2-Service.pdf)",
              September 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.

   [RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-
              Stack Lite Broadband Deployments Following IPv4
              Exhaustion", RFC 6333, August 2011.

   [Sec_DCP] UPnP Forum, "Device Protection:1", November 2009.

Authors' Addresses

    Mohamed Boucadair
    France Telecom
    Rennes,   35000
    France

    Email: mohamed.boucadair@orange.com

    Francis Dupont
    Internet Systems Consortium

    Email: fdupont@isc.org

    Reinaldo Penno
    Juniper Networks
    1194 N Mathilda Avenue
    Sunnyvale, California 94089
    USA

    Email: rpenno@juniper.net

    Dan Wing
    Cisco Systems, Inc.
    170 West Tasman Drive
    San Jose, California 95134
    USA

    Email: dwing@cisco.com