Universal Plug and Play (UPnP) Internet Gateway Device (IGD)-Port Control Protocol (PCP) Interworking Function
draft-ietf-pcp-upnp-igd-interworking-01

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 IGD 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

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 September 13, 2012.

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 described in the Simplified BSD License.

Table of Contents
1. Introduction ................................................. 4
2. Acronyms ....................................................... 4
3. Architecture Model ........................................... 5
4. UPnP IGD-PCP Interworking Function: Overview ............... 7
   4.1. UPnP IGD-PCP: State Variables .......................... 7
   4.2. IGD-PCP: Methods ....................................... 9
   4.3. UPnP IGD-PCP: Errors .................................. 10
5. Specification of the IGD-PCP Interworking Function .......... 12
   5.1. PCP Server Discovery .................................... 12
   5.2. Control of the Firewall .................................. 12
   5.3. NAT Control in LAN Side ................................. 12
   5.4. Port Mapping Tables ..................................... 12
   5.5. Interworking Function Without NAT in the CP Router ..... 13
   5.6. NAT Embedded in the CP Router ........................... 13
   5.7. Creating a Mapping ...................................... 14
       5.7.1. AddAnyPortMapping() ............................... 14
       5.7.2. AddPortMapping() .................................. 15
   5.8. Listing One or a Set of Mappings: DeletePortMapping() or DeletePortMappingRange() ..................... 19
   5.9. Delete One or a Set of Mappings: DeletePortMapping() or DeletePortMappingRange() ..................... 19
6. IANA Considerations ......................................... 22
7. Security Considerations ..................................... 23
8. Acknowledgments ............................................. 23
9. References .................................................... 23
1. Introduction

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

Two configurations are considered:

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

<table>
<thead>
<tr>
<th>UPnP-PCP UPnP Control</th>
<th>Interworking</th>
<th>PCP Server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(1) AddPortMapping</td>
<td></td>
</tr>
<tr>
<td></td>
<td>---------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(2) PCP MAP Request</td>
</tr>
<tr>
<td></td>
<td></td>
<td>--------------------------</td>
</tr>
</tbody>
</table>

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 makes use of the following abbreviations:
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:

- **Client** refers to a host located in the local network.
- **IGD Control Point** is a UPnP control point using UPnP to control an **IGD** (Internet Gateway Device).
- **IGD** is a router supporting UPnP IGD. It is typically a NAT or a firewall.
- **Host** represents a remote peer reachable in the Internet.

\[\text{Figure 2: UPnP IGD Model}\]

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.

Comment [DT2]: Isn't this the same as the "IGD"? Assuming so, just use one term. Delete "CP router" and replace with IGD throughout.
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).

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. In the rest of the document, IGD-PCP Interworking Function refers to PCP Client and the UPnP IGD-PCP Interworking Function, which includes PCP Client functionality.

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 as 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 successful 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).

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

Comment [DT5]: I find it confusing to have “Not applicable” items in the doc. They should be removed from this document if they’re not applicable. I also observe that some are already omitted (e.g., AutoDisconnectTime, etc.) Rather than adding the rest, just delete all not applicable items.

Comment [DT6]: Not quite. But then this variable should be deleted rather than reworded.

Comment [DT7]: Both of these are wrong. Per the UPnP spec, it’s the uptime of the WAN link. But this variable should be deleted rather than fixed.

Comment [DT8]: I think we should explicitly state that this should be stored on a per control point basis, so that different control points could see different values. Each value comes from the PCP responses for mappings for that control point.
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 it 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 relaying the message to the PCP Server.

Comment [DT9]: These are contradictory. Anything managed by the IWF is by definition applicable.

Comment [DT10]: MUST?

Comment [DT11]: Add a reference to [IGD1]

Comment [DT12]: There seems to be a section missing that would specify how this works. Add as section 5.10.

Comment [DT13]: We should define it to be the same as in the case of state lost in IGD:2.

Comment [DT14]: Should say the IWF MUST support the IGD:2 behavior. (And any requirements for the control point are out of scope)
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 supports 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: Not applicable
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: MAP with PREFER_FAILURE Option
This request is relayed to the PCP Server by issuing MAP with
PREFER_FAILURE Option. It is RECOMMENDED to use a short lifetime
(e.g., 60s).

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 mappings 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 with 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.ietf-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), 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.

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.

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.

Comment [DT24]: Can’t assume there’s only one. See I-D.ietf-PCP-dhcp.

Comment [DT25]: Not sure what this means. Reword. If the control point is asking for a port mapping, then we need to make sure the IWF is invoked and a failure is returned.

Comment [DT26]: Normative language about what the control point does is out of scope for this document.

Comment [DT27]: Do you mean "all mappings"? Or is there a difference between "port forwarding" mappings vs some other type?
5.5. Interworking Function Without NAT in the \text{CP} Router\textunderscore \text{IGD}

When no NAT is embedded in the \text{CP} router\textunderscore \text{IGD}, 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 \text{CP} Router\textunderscore \text{IGD}


\begin{itemize}
\item Unlike the scenario with one level of NAT (Section 5.5), when NAT is embedded in the IGD, 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 \text{CP} router\textunderscore \text{IGD} (i.e., after the NAT1 operation in Figure 4) and not as initially positioned by the UPnP Control Point.
\end{itemize}

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 \text{CP} router\textunderscore \text{IGD}. For the reverse path, PCP response messages are intercepted by the IGD-PCP Interworking Function. The content of the corresponding WANIPConnection messages are updated:

\begin{itemize}
\item The internal IP address and/or port number as initially positioned by the UPnP Control Point and stored in the \text{CP} router\textunderscore \text{IGD} NAT are used to update the corresponding fields in received PCP responses.
\item The external IP and port number are not altered by the IGD-PCP Interworking Function.
\item The NAT mapping entry in the first NAT of the \text{CP} router\textunderscore \text{IGD} is updated with the result of PCP request.
\end{itemize}

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.

\begin{itemize}
\item Comment [DT28]: This statement was wrong since 5.5 can happen in a case with NO levels of NAT (just FWs).
\item Comment [DT29]: The IGD might not be the "first" NAT.
\item Comment [DT30]: And how does this apply to devices other than the IGD? You can make a normative statement only about what the IGD does. Also keep in mind that the other devices might have a FW (with a lifetime of state) rather than a NAT.
\end{itemize}
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 an 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 a 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 (see Section 4.3) is generated by the IGD-PCP Interworking Function and sent to the requesting UPnP Control Point. If a short lifetime error is returned (e.g., NETWORK_FAILURE, NO_RESOURCES), the PCP IWF MAY re-send the same request to the PCP Server after 30s. If a negative answer is received, the error is then relayed to the requesting UPnP Control Point.

Justification: Some applications (e.g., uTorrent, Vuzz, Emule) wait approximately 150s, 90s, 90s, respectively for a response after sending an UPnP request. If a short lifetime error occurs, re-sending the requesting may lead to a positive response from the PCP Server. UPnP Control Points are therefore not aware of short lifetime errors that were recovered quickly.

Comment [DT31]: This is a choice made by the control point not the IGD. Normative statements about the control point are out of scope for this doc.
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 option 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 the example shown in Figure 6).
<table>
<thead>
<tr>
<th>UPnP Control Point</th>
<th>Interworking Function</th>
<th>PCP Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) AddPortMapping</td>
<td>ExternalPort=2356</td>
<td></td>
</tr>
<tr>
<td></td>
<td>----------------------</td>
<td>------------</td>
</tr>
<tr>
<td>(2) Error:</td>
<td>ConflictInMappingEntry</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;----------------------</td>
<td>------------</td>
</tr>
<tr>
<td>(3) AddPortMapping</td>
<td>ExternalPort=4586</td>
<td></td>
</tr>
<tr>
<td></td>
<td>----------------------</td>
<td>------------</td>
</tr>
<tr>
<td>(4) Error:</td>
<td>ConflictInMappingEntry</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;----------------------</td>
<td>------------</td>
</tr>
</tbody>
</table>

Some applications use GetSpecificPortMapping() to check whether a mapping exists.

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 MUST generate 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 IGD or updated as specified in Section 5.6.

In addition, the IGD-PCP IWF MUST insert 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. If a short lifetime error is returned, the PCP IWF MAY re-send the same request to the PCP Server after 30s. If a negative answer is received, the IGD-PCP IWF relays a negative message to the UPnP Control Point indicating ConflictInMappingEntry as error code. The UPnP Control Point may re-issue 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

Comment [DT34]: Move to end of this section next to the other "Note:"

Comment [DT35]: Normative statements about the PCP server are out of scope. Change MUST to "will" so it's informational.
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.

![Flow Example (Positive Answer)](image)

Figure 7: Flow Example (Positive Answer)
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 then fail.

Also note that some applications use GetSpecificPortMapping() to check whether a mapping exists before sending an AddPortMapping.

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().

GetGenericPortMappingEntry() and GetListOfPortMappings() methods MUST NOT be proxied to the PCP Server since a local mapping is maintained by the IGD-PCP Interworking Function.

Upon receipt of GetSpecificPortMappingEntry() from an UPnP Control Point, the IGD-PCP IWF MUST check first if the external port number is used by the requesting UPnP Control Point or another Internal UPnP Control Point. If the external port is already in use by the requesting UPnP Control Point, the IGD-PCP IWF MUST send back a positive answer. If the external port is already in use by another UPnP Control Point, the IGD-PCP IWF MUST send back a ConflictInMappingEntry error to the requesting UPnP Control Point. If no mapping is found in the local mapping table, the IWF MUST relay to the PCP Server a MAP request, with short lifetime (e.g. 60s), including a PREFER_FAILURE Option.

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

A UPnP Control Point proceeds to requests the deletion of one or a list of mappings by issuing DeletePortMapping() or DeletePortMappingRange(). In IGDI2, 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.

Comment [DT36]: This is a problem since there may be another external IP address for which it would be fine. I think all that's required is that a given control point see a consistent ExternalIPAddress, but different control points can legitimately see different ones (and always will in a 1:1 case).

Comment [DT37]: This is inconsistent, and should be treated the same way as GetGenericPortMappingEntry and GetListOfPortMappings. That is, it should be able to return something that wouldn’t be returned in the other two.
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 IGD or the corresponding local IP address and port number as assigned by the local NAT if a NAT is enabled in the CP router IGD. 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).

The IWF MAY 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.
### 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.

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

Figure 11: Example of `DeletePortMappingRange()`

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 SHOULD to enforce the default security, i.e., operation on the behalf of a third party is not allowed.

This document defines a procedure to construct 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


9.2. Informative References


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