

PCP Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 13, 2013

M. Boucadair
France Telecom
R. Penno
D. Wing
Cisco
April 11, 2013

**Universal Plug and Play (UPnP) Internet Gateway Device (IGD)-Port
Control Protocol (PCP) Interworking Function
draft-ietf-pcp-upnp-igd-interworking-08**

Abstract

This document specifies the behavior of the UPnP IGD (Internet Gateway Device)/PCP Interworking Function. A UPnP IGD-PCP Interworking Function (IGD-PCP IWF) is required to be embedded in CP (Customer Premises) routers to allow for transparent NAT control in environments where UPnP IGD is used on the LAN side and PCP on 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 October 13, 2013.

Copyright Notice

Copyright (c) 2013 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	2
2.	Acronyms	3
3.	Architecture Model	4
4.	UPnP IGD-PCP IWF: Overview	5
4.1.	UPnP IGD-PCP: State Variables	6
4.2.	IGD-PCP: Methods	7
4.3.	UPnP IGD-PCP: Errors	8
5.	Specification of the IGD-PCP IWF	9
5.1.	PCP Server Discovery	9
5.2.	Control of the Firewall	9
5.3.	Port Mapping Table	10
5.4.	Interworking Function Without NAT in the IGD	10
5.5.	NAT Embedded in the IGD	10
5.6.	Creating a Mapping	11
5.6.1.	AddAnyPortMapping()	11
5.6.2.	AddPortMapping()	12
5.7.	Listing One or a Set of Mappings	15
5.8.	Delete One or a Set of Mappings: DeletePortMapping() or DeletePortMappingRange()	15
5.9.	Renewing a Mapping	18
5.10.	Rapid Recovery	19
6.	IANA Considerations	20
7.	Security Considerations	20
8.	Acknowledgments	20
9.	References	20
9.1.	Normative References	20
9.2.	Informative References	20
	Authors' Addresses	21

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 (Internet Gateway Device) is used in the local network, an interworking function between UPnP IGD and PCP is

required to be embedded in the IGD (see the example illustrated in Figure 1).

Two configurations are considered:

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

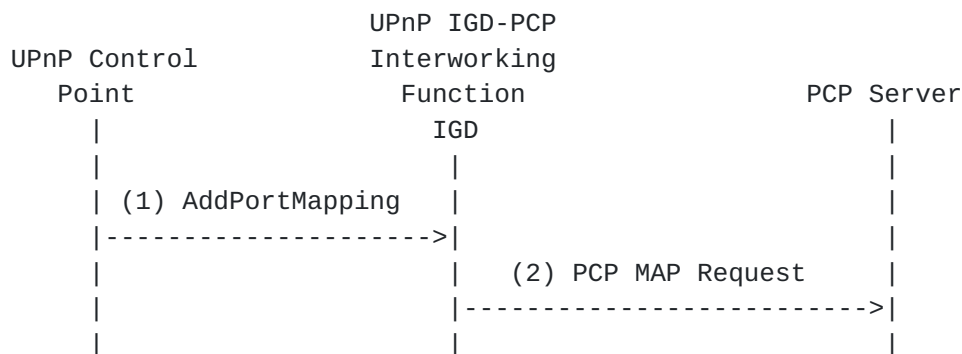


Figure 1: Flow Example

The UPnP IGD-PCP Interworking Function (UPnP IGD-PCP IWF) maintains a local mapping table that stores all active mappings constructed 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 IWF from the IGD and relying on a PCP-only mode are out of scope of this document.

Considerations related to co-existence of the UPnP IGD-PCP Interworking Function and a PCP Proxy [[I-D.ietf-pcp-proxy](#)] are out of scope.

2. Acronyms

This document makes use of the following abbreviations:

DS-Lite - Dual-Stack Lite
 IGD - Internet Gateway Device
 IGD:1 - UPnP Forum's nomenclature for version 1 of IGD [[IGD1](#)]
 IGD:2 - UPnP Forum's nomenclature for version 2 of IGD [[IGD2](#)]
 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 device using UPnP to control an IGD (Internet Gateway Device).
- o 'IGD' is a router supporting UPnP IGD. It is typically a NAT or a firewall.
- o 'Host' is a remote peer reachable in the Internet.

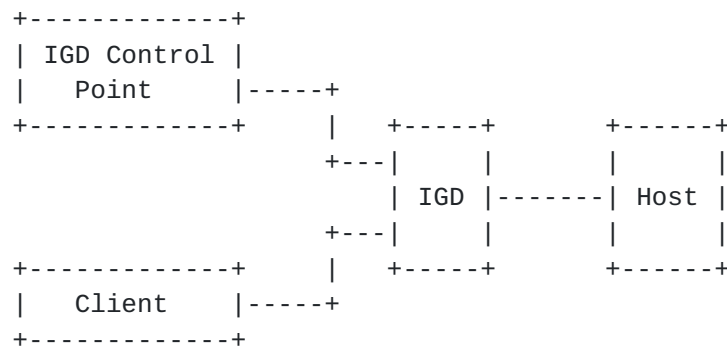


Figure 2: UPnP IGD Model

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 IGD. In such scenarios, Figure 3 shows the updated model.

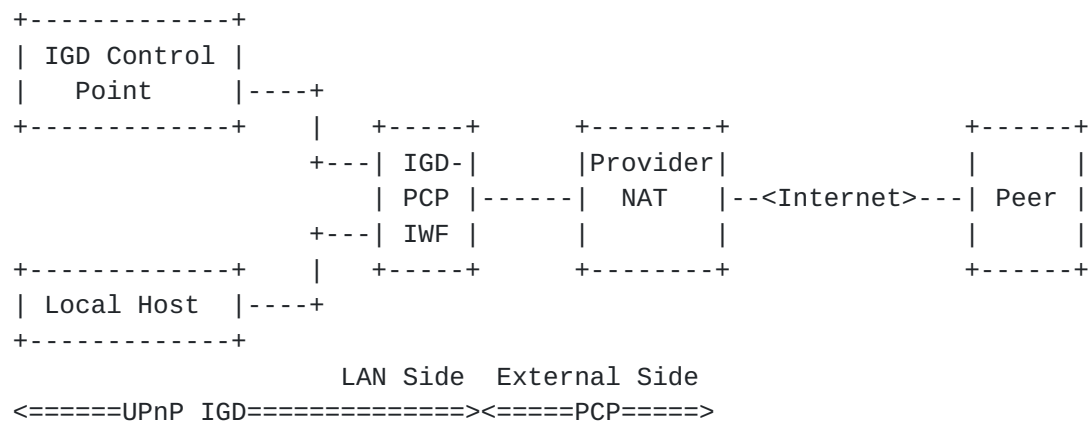


Figure 3: UPnP IGD-PCP Interworking Model

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 IGD may embed a NAT function (Figure 4).

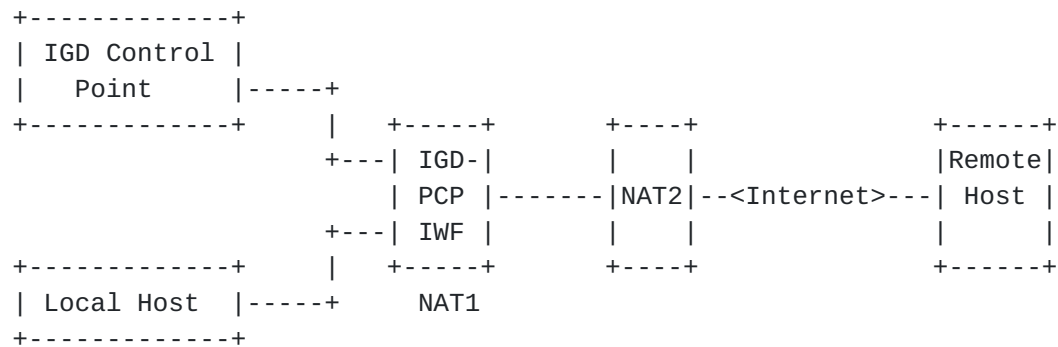


Figure 4: Cascaded NAT scenario

To ensure successful interworking between UPnP IGD and PCP, an interworking function is embedded in the IGD. 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 IGD. In the rest of the document, IGD-PCP IWF refers the UPnP IGD-PCP Interworking Function, which includes PCP Client functionality.

Without the involvement of the IGD-PCP IWF, the UPnP Control Point would retrieve an external IP address and port number having a limited scope and which cannot be used to communicate with hosts located beyond NAT2 (i.e., assigned by the IGD and not the ones assigned by NAT2 in Figure 4).

UPnP IGD-PCP IWF is responsible for generating a well-formed PCP message from a received UPnP IGD message, and vice versa.

4. UPnP IGD-PCP IWF: Overview

Three tables are provided to specify the correspondence 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

Below are listed only the UPnP IGD state variables applicable to the IGD-PCP IWF:

ExternalIPAddress: External IP Address

Read-only variable with the value from the last PCP response or the empty string if none was received yet. This state is stored on a per UPnP Control Point basis.

PortMappingNumberOfEntries: Managed locally by the UPnP IGD-PCP IWF.

PortMappingEnabled:

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.

Only "1" is allowed: i.e., the UPnP IGD-PCP Interworking Function MUST send back an error if a value different from 1 is signaled.

PortMappingLeaseDuration: Requested Mapping Lifetime

In IGD:1 [\[IGD1\]](#) 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 4294967296 seconds.

The UPnP IGD-PCP Interworking Function simulates long and even infinite lifetimes using renewals (see [Section 5.9](#)). The behavior in the case of a failing renewal is currently undefined.

IGD:1 doesn't define the behavior in the case of state loss, IGD:2 doesn't require to keep state in stable storage, i.e., to allow the state to survive resets/reboots. The UPnP IGD-PCP Interworking Function MUST support IGD:2 behavior.

RemoteHost: Remote Peer IP Address

Note that IGD:2 allows a domain name, which has to be resolved to an IP address.

ExternalPort: External Port Number

Mapped to the Suggested External Port in MAP messages.

InternalPort: Internal Port Number

Mapped to the Internal Port field in MAP messages.

PortMappingProtocol: Transport Protocol

Mapped to the Protocol field in MAP messages. Note that UPnP IGD only supports TCP and UDP.

InternalClient: Internal IP Address

Note that IGD:2 allows a domain name, which has to be resolved to an IP address.

PortMappingDescription: Not supported in base PCP.

If the local PCP Client supports a PCP Option to convey the description (e.g., [[I-D.ietf-pcp-description-option](#)]), this option SHOULD be used to relay the mapping description.

SystemUpdateID (IGD:2 only): Managed locally by the UPnP IGD-PCP IWF.

A_ARG_TYPE_PortListing (IGD:2 only): Managed locally by the UPnP IGD-PCP IWF.

[4.2.](#) IGD-PCP: Methods

Both IGD:1 and IGD:2 methods applicable to the UPnP IGD-PCP Interworking Function are listed here.

GetGenericPortMappingEntry: This request is not relayed to the PCP Server.

IGD-PCP Interworking Function maintains a list of active mappings instantiated in the PCP Server by internal hosts. See [Section 5.7](#) for more information.

GetSpecificPortMappingEntry: MAP with PREFER_FAILURE Option

This request is relayed to the PCP Server by issuing a MAP request with the PREFER_FAILURE Option. It is RECOMMENDED to use a short lifetime (e.g., 60 seconds).

AddPortMapping: MAP

See [Section 5.6.2](#).

AddAnyPortMapping (IGD:2 only): MAP

See [Section 5.6.1](#).

DeletePortMapping: MAP with Requested Lifetime set to 0.

See [Section 5.8](#).

DeletePortMappingRange (IGD:2 only): MAP with Requested Lifetime set to 0.

Individual requests are issued by the IGD-PCP IWF. See [Section 5.8](#) for more details.

GetExternalIPAddress: MAP

This can be learned from any active mapping. If there are no active mappings, the IGD-PCP IWF MAY request a short-lived mapping (e.g., to the Discard service (TCP/9 or UDP/9) or some other port). However, once that mapping expires a subsequent implicit or explicit dynamic mapping might be mapped to a different external IP address. See section 11.6 of [[I-D.ietf-pcp-base](#)] for more discussion.

GetListOfPortMappings: See [Section 5.7](#) for more information.

The IGD-PCP Interworking Function maintains a list of active mappings instantiated in the PCP Server. The IGD-PCP Interworking Function handles this request locally.

[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"
- 3 MALFORMED_REQUEST: 501 "ActionFailed"
- 4 UNSUPP_OPCODE: 501 "ActionFailed"
Should not happen. [[I-D.ietf-pcp-base](#)] allows the PCP server to be configured to disable support for the MAP opcode, but the IGD-PCP IWF cannot work in this situation.
- 5 UNSUPP_OPTION: 501 "ActionFailed"
Should not happen except if PREFER_FAILURE is not supported on the PCP server. Note that PREFER_FAILURE 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 has been successfully established with a PCP Server.
- 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" (see
[Section 5.7.2](#)) or 714 "NoSuchEntryInArray" (see [Section 5.8](#)).
- 12 ADDRESS_MISMATCH: 501 "ActionFailed"
Should not happen.
- 13 EXCESSIVE_REMOTE_PEERS: 501 "ActionFailed"
Should not happen, since the IGD-PCP Interworking Function should
not need to use the FILTER option.

5. Specification of the IGD-PCP IWF

This section covers the scenarios with or without NAT in the IGD.

This specification assumes the PCP Server is configured to accept the MAP OpCode.

The IGD-PCP IWF handles the "Mapping Nonce" the same way as any PCP Client [[I-D.ietf-pcp-base](#)].

5.1. PCP Server Discovery

The IGD-PCP IWF 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 provisioned PCP Server(s).

If no IPv4 address / IPv6 prefix is assigned to the IGD or the IGD is unable to determine whether it should contact an upstream PCP Server, the IGD-PCP Interworking Function MUST NOT be invoked.

If the IGD determines that it should establish communication with an upstream PCP server (e.g., because of DHCP configuration or having previously been talking to a PCP server), a "501 ActionFailed" error message is returned to the requesting UPnP Control Point in case the IGD-PCP IWF fails to establish communication with that PCP Server.

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 IWF is therefore required for that purpose.

The use of IGD-PCP IWF to control an upstream PCP-controlled firewall is out of scope of this document.

5.3. Port Mapping Table

The IGD-PCP IWF MUST store locally all the mappings instantiated by internal UPnP Control Points in the PCP Server. All mappings SHOULD be stored in permanent storage.

Upon receipt of a PCP MAP Response from the PCP Server, the IGD-PCP Interworking Function MUST extract 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.

5.4. Interworking Function Without NAT in the IGD

When no NAT is embedded in the 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 PCP messages (and mapped back) according to [Section 4.1](#)).

5.5. NAT Embedded in the IGD

When NAT is embedded in the IGD, the IGD-PCP IWF updates the content of mapping messages received from the UPnP Control Point. These messages will contain an IP address and/or port number which belong to an internal host. The IGD-PCP IWF MUST update such messages with the IP address and/or port number belonging to the external interface of the IGD (i.e., after the NAT1 operation in Figure 4).

The IGD-PCP IWF intercepts all WANIPConnection messages issued by the UPnP Control Point. For each such message, the IGD-PCP IWF then generates one or more corresponding requests (see [Section 4.1](#), [Section 4.2](#) and [Section 4.3](#)) and sends them to the provisioned PCP Server.

Each request sent by the IGD-PCP IWF to the PCP Server MUST reflect the mapping information as enforced in the first NAT. Particularly, the internal IP address and/or port number of the requests are replaced with the IP address and/or port number as assigned by the NAT of the IGD. For the reverse path, the IGD-PCP IWF intercepts PCP response messages and generates WANIPConnection response messages.

The content of the generated WANIPConnection response messages are set as follows:

- o The internal IP address and/or port number as initially set by the UPnP Control Point and stored in the IGD 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 IGD is updated with the result of PCP request.

The lifetime of the mappings instantiated in the IGD SHOULD be the one assigned by the terminating PCP Server. In any case, the lifetime MUST NOT be lower than the one assigned by the terminating PCP Server.

5.6. Creating a Mapping

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

5.6.1. AddAnyPortMapping()

When a UPnP Control Point issues an `AddAnyPortMapping()`, this request is received by the IGD. The request is then relayed to the IGD-PCP IWF 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, the corresponding UPnP IGD method is returned to the requesting UPnP Control Point (the content of the messages follows the recommendations listed in [Section 5.5](#) or [Section 5.4](#) 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 IWF 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 resend the same request to the PCP Server after 30 seconds. If a negative answer is received, the error is then relayed to the requesting UPnP Control Point.

Discussion: Some applications (e.g., uTorrent, Vuze, eMule) wait 90 seconds or more for a response after sending an UPnP request. If a short lifetime error occurs, resending the request may lead to a positive response from the PCP server. UPnP Control Points are therefore not aware of transient errors.

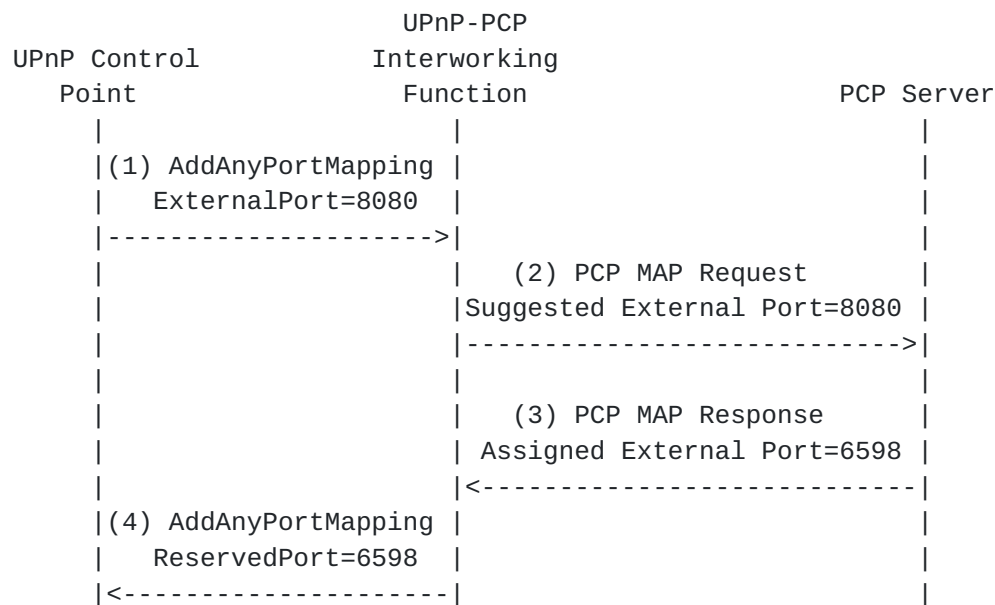


Figure 5: Flow example when AddAnyPortMapping() is used

5.6.2. 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.

Upon receipt of AddPortMapping() from an UPnP Control Point, 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 IGD or updated as specified in Section 5.5. In addition, the IGD-PCP IWF MUST insert a PREFER_FAILURE Option in the generated PCP request.

If the requested external port is not available, the PCP server will send a CANNOT_PROVIDE_EXTERNAL error response:

1. If a short lifetime error is returned, the IGD-PCP IWF MAY resend the same request to the PCP Server after 30 seconds without relaying the error to the UPnP Control Point. The IGD-PCP IWF MAY repeat this process until a positive answer is received or some maximum retry limit is reached. When the maximum retry limit is reached, the IGD-PCP IWF relays a negative message to the UPnP Control Point with ConflictInMappingEntry as the error code.

2. If a long lifetime error is returned, the IGD-PCP IWF relays a negative message to the UPnP Control Point with ConflictInMappingEntry as the error code.

The UPnP Control Point may issue a new request with a different requested external port number. This process is typically repeated by the UPnP Control Point until a positive answer is received or some maximum retry limit is reached.

If the PCP Server is able to create or renew a mapping with the requested external port, it sends a positive response to the IGD-PCP IWF. Upon receipt of the response from the PCP Server, the IGD-PCP IWF stores the returned mapping in its local mapping table, and sends a positive answer to the requesting UPnP Control Point. This answer terminates this exchange.

Figure 6 shows an example of the flow exchange that occurs when the PCP Server satisfies the request from the IGD-PCP IWF. Figure 7 shows the messages exchange when the requested external port is not available.

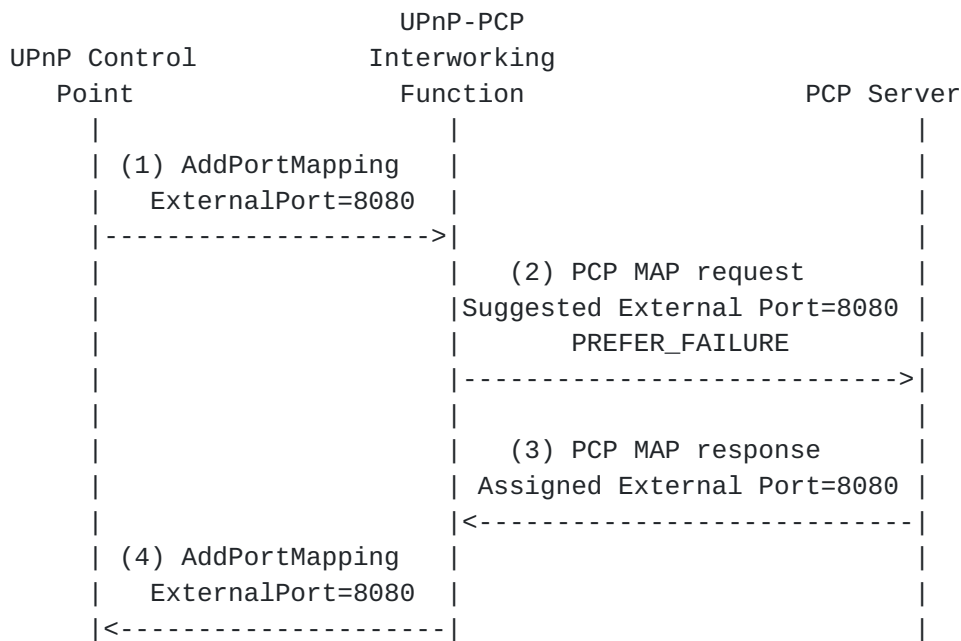
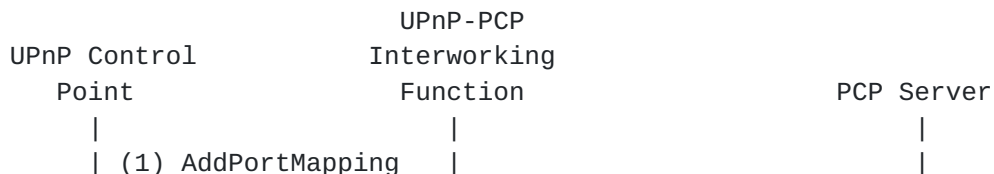


Figure 6: Flow Example (Positive Answer)



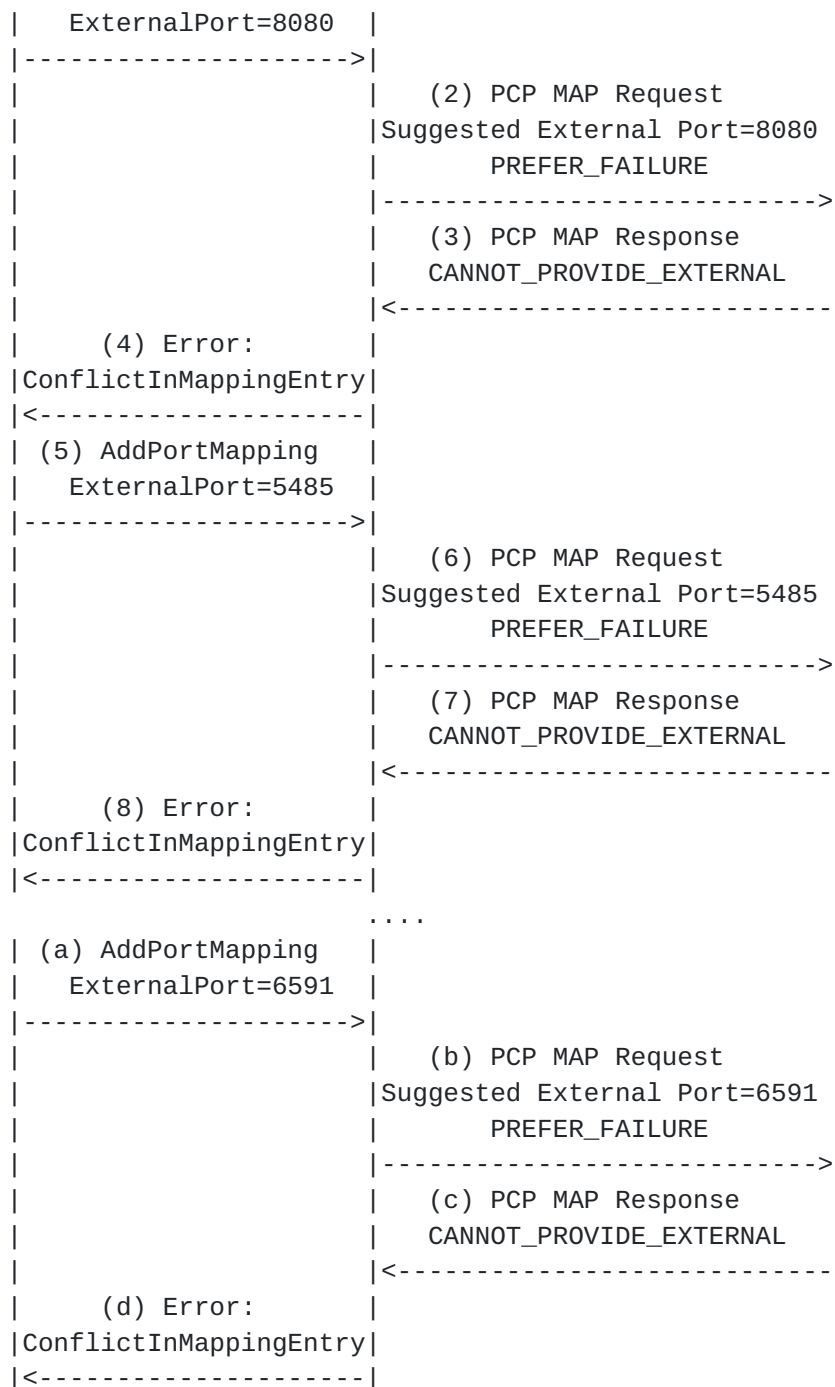


Figure 7: Flow Example (Negative Answer)

Note: According to some experiments, some UPnP 1.0 Control Point implementations, e.g., uTorrent, simply try the same external port a number of times (usually 4 times) and then fail if the port is in use. Also note that some applications use `GetSpecificPortMappingEntry()` to check whether a mapping exists.

5.7. Listing One or a Set of Mappings

In order to list active mappings, a 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 IWF.

Upon receipt of `GetSpecificPortMappingEntry()` from a UPnP Control Point, the IGD-PCP IWF MUST check first if the external port number is used by the requesting 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 not, the IGD-PCP IWF MUST relay to the PCP Server a MAP request, with short lifetime (e.g., 60 seconds), including a `PREFER_FAILURE` Option. If the requested external port is in use, a PCP error message will be sent by the PCP Server to the IGD-PCP IWF indicating `CANNOT_PROVIDE_EXTERNAL` as the error cause. Then, the IGD-PCP IWF relays a negative message to the UPnP Control Point. If the port is not in use, the mapping will be created by the PCP Server and a positive response will be sent back to the IGD-PCP IWF. Once received by the IGD-PCP IWF, it MUST relay a negative message to the UPnP Control Point indicating `NoSuchEntryInArray` as the error code so that the UPnP control point knows the queried mapping doesn't exist.

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

A UPnP Control Point requests 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 determine whether a Control Point has the rights to delete one or a set of mappings. When authorization fails, the "606 Action Not Authorized" error code MUST be returned to the requesting Control Point.

When `DeletePortMapping()` or `DeletePortMappingRange()` is received by the IGD-PCP IWF, 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 8 shows an example of a UPnP Control Point asking to delete a mapping which is not instantiated in the local table of the IWF.

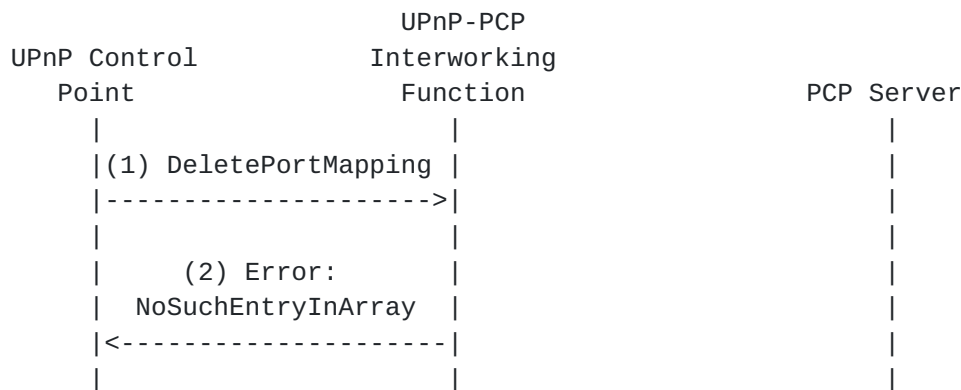


Figure 8: Local Delete (IGD-PCP IWF)

If a mapping matches in the local table, a PCP MAP delete request is generated. If no NAT is enabled in the IGD, the IGD-PCP IWF uses the input arguments as included in `DeletePortMapping()`. If a NAT is enabled in the IGD, the IGD-PCP IWF instead uses the corresponding IP address and port number as assigned by the local NAT.

When a positive answer is received from the PCP Server, the IGD-PCP IWF updates its local mapping table (i.e., removes the corresponding entry) and notifies the UPnP Control Point about the result of the removal operation. Once the PCP MAP delete request is received by the PCP Server, it removes the corresponding entry. A PCP MAP SUCCESS 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 IWF including the corresponding error cause (see [Section 4.3](#)).

If `DeletePortMappingRange()` is used, the IGD-PCP IWF does a lookup in its local mapping table to retrieve individual mappings instantiated by the requesting Control Point (i.e., authorization checks) and matching the signaled port range (i.e., the external port is within the "StartPort" and "EndPort" arguments of `DeletePortMappingRange()`). If no mapping is found, the "730 PortMappingNotFound" error code is sent to the UPnP Control Point (Figure 9). If one or more mappings are found, the IGD-PCP IWF generates individual PCP MAP delete requests corresponding to these mappings (see the example shown in Figure 10).

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.

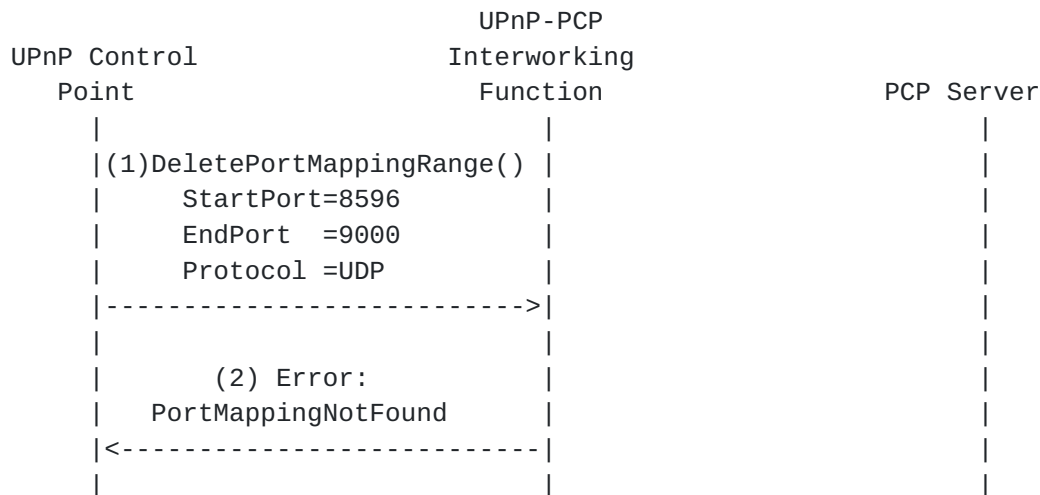


Figure 9: Flow example when an error encountered when processing DeletePortMappingRange()

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.

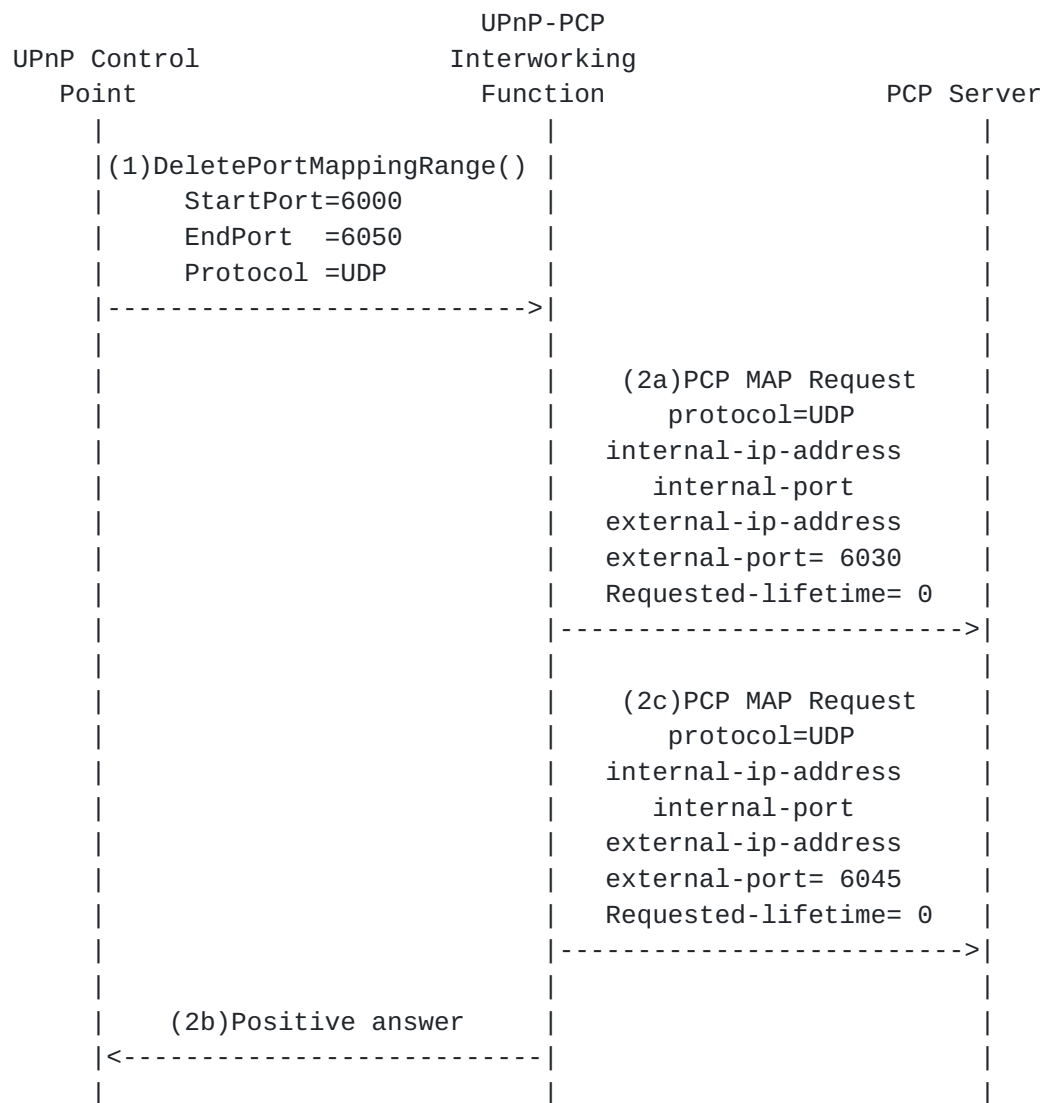


Figure 10: Example of DeletePortMappingRange()

5.9. Renewing a Mapping

Because of the incompatibility of mapping lifetimes between UPnP IGD and PCP, the IGD-PCP IWF MUST simulate long and even infinite lifetimes. Indeed, for requests having a requested infinite **PortMappingLeaseDuration**, the IGD-PCP IWF MUST set the **Requested Lifetime** of the corresponding PCP request to 4294967296. If **PortMappingLeaseDuration** is not infinite, the IGD-PCP IWF MUST set the **Requested Lifetime** of the corresponding PCP request to the same value as **PortMappingLeaseDuration**. Furthermore, the IGD-PCP Interworking Function MUST maintain an additional timer set to the initial requested **PortMappingLeaseDuration**. Upon receipt of a positive answer from the PCP server, the IGD-PCP IWF relays the corresponding UPnP IGD response to the requesting UPnP Control Point.

with `PortMappingLeaseDuration` set to the same value as the one of the initial request. Then, the IGD-PCP IWF MUST periodically renew the constructed PCP mapping until the expiry of `PortMappingLeaseDuration`. Responses received when renewing the mapping MUST NOT be relayed to the UPnP Control Point.

In case an error is encountered during mapping renewal, the IGD-PCP Interworking Function has no means to inform the UPnP Control Point.

5.10. Rapid Recovery

When the IWF is co-located with the DHCP server, the state maintained by the IWF MUST be updated using the state in the local DHCP server. Particularly, if an IP address expires or is released by an internal host, the IWF MUST delete all the mappings bound to that internal IP address.

Upon change of the external IP address of the IWF, the IWF MAY renew the mappings it maintained. This can be achieved only if a full state table is maintained by the IWF. If the port quota is not exceeded in the PCP server, the IWF will receive a new external IP address and port numbers. The IWF has no means to notify the change of the external IP address and port to internal UPnP Control Points. Stale mappings will be maintained by the PCP Server until their lifetime expires.

[I-D.ietf-pcp-base] defines a procedure for the PCP Server to notify PCP Clients about changes related to the mappings it maintains. When an unsolicited ANNOUNCE is received, the IWF makes one or more MAP requests with the `PREFER_FAILURE` option to re-install its mappings. If the PCP server cannot create the requested mappings (signaled with the `CANNOT_PROVIDE_EXTERNAL` error response), the IWF has no means to notify the change of the external IP address and port to internal UPnP Control Points.

Unsolicited PCP MAP responses received from a PCP Server are handled as any normal MAP response. If a response indicates that the external IP address or port has changed, the IWF has no means to notify the internal UPnP Control Point of this change.

Further analysis of PCP failure scenarios for the IGD-PCP Interworking Function are discussed in [[I-D.boucadair-pcp-failure](#)].

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

The IGD:2 authorization framework SHOULD be used [[IGD2](#)]. When only IGD:1 is available, operation on the behalf of a third party SHOULD NOT be allowed.

This document defines a procedure to create PCP mappings for third party devices belonging to the same subscriber. Means to prevent a malicious user from creating mappings on behalf of a third party must be enabled as discussed in Section 13.1 of [[I-D.ietf-pcp-base](#)].

The security considerations discussed 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, X. Deng, G. Montenegro, D. Thaler, R. Tirumaleswar, P. Selkirk, T. Lemon, V. Gurbani, and P. Yee for their review and comments.

F. Dupont contributed to previous versions of this document. Thanks to him for his thorough reviews and contribution.

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-29](#) (work in progress), November 2012.
- [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.boucadair-pcp-failure]
Boucadair, M. and R. Penno, "Port Control Protocol (PCP) Failure Scenarios", [draft-boucadair-pcp-failure-05](#) (work in progress), February 2013.

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

Boucadair, M., Penno, R., and D. Wing, "PCP Description Option", [draft-ietf-pcp-description-option-00](#) (work in progress), March 2013.

[I-D.ietf-pcp-dhcp]

Boucadair, M., Penno, R., and D. Wing, "DHCP Options for the Port Control Protocol (PCP)", [draft-ietf-pcp-dhcp-07](#) (work in progress), March 2013.

[I-D.ietf-pcp-proxy]

Boucadair, M., Penno, R., and D. Wing, "Port Control Protocol (PCP) Proxy Function", [draft-ietf-pcp-proxy-02](#) (work in progress), February 2013.

[IGD1] UPnP Forum, , "WANIPConnection:1 Service (<http://www.upnp.org/specs/gw/UPnP-gw-WANIPConnection-v1-Service.pdf>)", November 2001.

[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

Reinaldo Penno
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134
USA

Email: repenno@cisco.com

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

Email: dwing@cisco.com