Internet Engineering Task Force (IETF)
Request for Comments: 6970
Category: Standards Track
ISSN: 2070-1721

M. Boucadair
France Telecom
R. Penno
D. Wing
Cisco

July 2013

Universal Plug and Play (UPnP) Internet Gateway Device - Port Control Protocol Interworking Function (IGD-PCP IWF)

Abstract

This document specifies the behavior of the Universal Plug and Play (UPnP) Internet Gateway Device - Port Control Protocol Interworking Function (IGD-PCP IWF). A UPnP IGD-PCP IWF is required to be embedded in Customer Premises (CP) routers to allow for transparent NAT control in environments where a UPnP IGD is used on the LAN side and PCP is used on the external side of the CP router.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6970.

Table of Contents

1. Introduction

The Port Control Protocol (PCP) specification [RFC6887] discusses the implementation of NAT control features that rely upon Carrier Grade NAT devices such as a Dual-Stack Lite (DS-Lite) Address Family Transition Router (AFTR) [RFC6333] or NAT64 [RFC6146]. In environments where a Universal Plug and Play Internet Gateway Device (UPnP IGD) is used in the local network, an interworking function between the UPnP IGD and PCP is required to be embedded in the IGD (see the example illustrated in Figure 1).

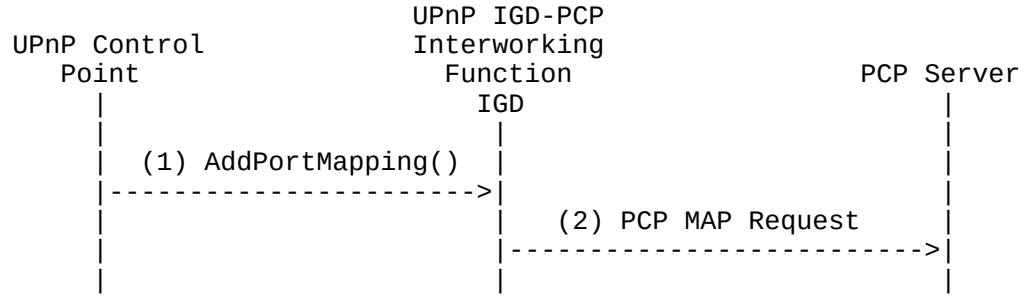

Figure 1: Flow Example

Two configurations are considered within this document:

- No NAT function is embedded in the IGD (Section 5.4). This is required, for instance, in DS-Lite or NAT64 deployments.
- The IGD embeds a NAT function (Section 5.5).

The UPnP IGD-PCP Interworking Function (UPnP IGD-PCP IWF) maintains a local mapping table that stores all active mappings constructed by internal IGD 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 for this document.

Considerations related to co-existence of the UPnP IGD-PCP Interworking Function and a PCP Proxy [PCP-PROXY] are out of scope.

1.1. 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].

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 as adopted by the UPnP Forum [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 device using UPnP to control an IGD (Internet Gateway Device).
- 'IGD' is a router supporting a UPnP IGD. It is typically a NAT or a firewall.
- 'Host' is a remote peer reachable in the Internet.

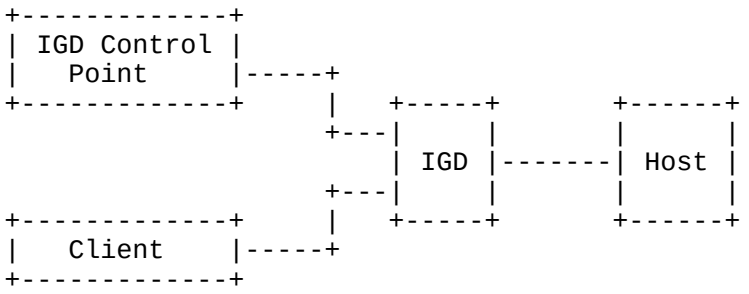

Figure 2: UPnP IGD Model

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

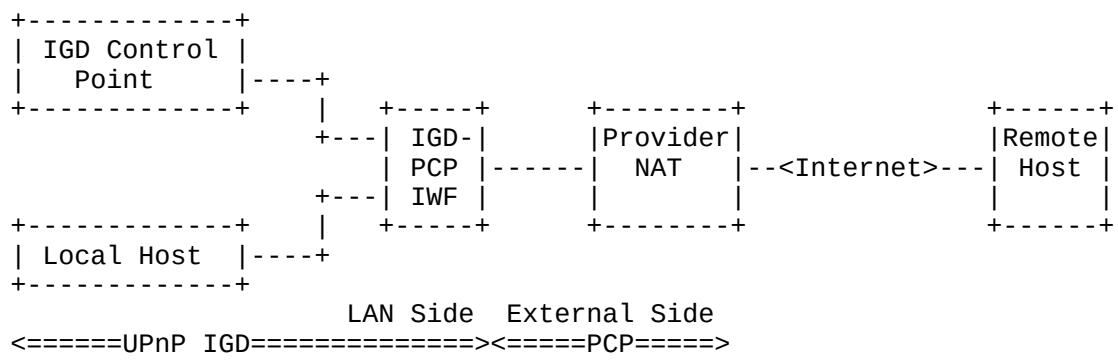

Figure 3: UPnP IGD-PCP Interworking Model

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).

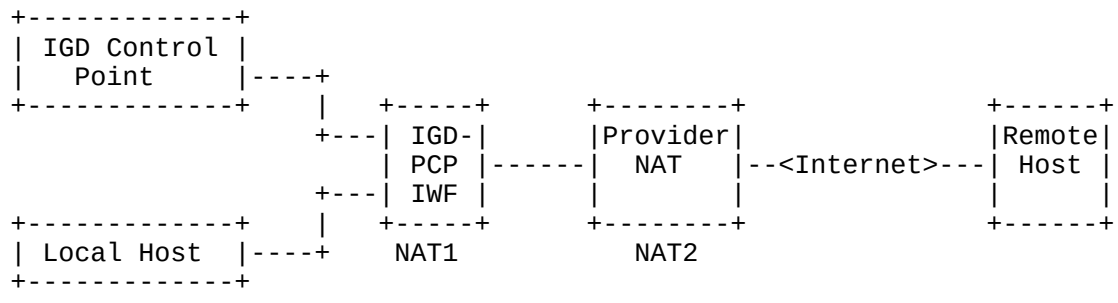

Figure 4: Cascaded NAT Scenario

To ensure successful interworking between a 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 [RFC6887], and a UPnP IGD-PCP Interworking Function are embedded in the IGD. In the rest of the document, "IGD-PCP IWF" refers to the UPnP IGD-PCP Interworking Function, which includes PCP client functionality.

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

The 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 a 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 error messages.

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-IGD-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 of the UPnP IGD-PCP IWF in the case of a failing renewal is currently undefined (see Section 5.9).

IGD:1 doesn't define the behavior in the case of state loss; IGD:2 doesn't require that state be kept 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. Mapped to the Remote Peer IP Address field of the FILTER option.

ExternalPort: External Port Number
Mapped to the Suggested External Port field in MAP messages.

InternalPort: Internal Port Number
Mapped to the Internal Port field in MAP messages.

PortMappingProtocol: Protocol
Mapped to the Protocol field in MAP messages. Note that a 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. Mapped to the Internal IP Address field of the THIRD_PARTY option.

PortMappingDescription: Not supported in base PCP.
If the local PCP client supports a PCP option to convey the description (e.g., [PCP-DESCR-OPT]), 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

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

GetGenericPortMappingEntry(): This request is not relayed to the PCP server.

The 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 [RFC6887] 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 error codes and the corresponding UPnP IGD codes. Error codes specific to IGD:2 are tagged accordingly.

1 UNSUPP_VERSION: 501 "ActionFailed"

2 NOT_AUTHORIZED: IGD:1 718 "ConflictInMappingEntry" / IGD:2 606 "Action not authorized"

3 MALFORMED_REQUEST: 501 "ActionFailed"

4 UNSUPP_OPCODE: 501 "ActionFailed"
[RFC6887] 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"
This error code can be received 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"

7 NETWORK_FAILURE: 501 "ActionFailed"

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

9 UNSUPP_PROTOCOL: 501 "ActionFailed"

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 5.6.2) or 714 "NoSuchEntryInArray" (see Section 5.8).

12 ADDRESS_MISMATCH: 501 "ActionFailed"

13 EXCESSIVE_REMOTE_PEERS: 501 "ActionFailed"

5. Specification of the IGD-PCP IWF

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

This specification assumes that 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 [RFC6887].

5.1. PCP Server Discovery

The IGD-PCP IWF implements one of the discovery methods identified in [RFC6887] (e.g., DHCP [PCP-DHCP-OPT]). 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 communicated with a PCP server), a "501 ActionFailed" error message is returned to the requesting IGD Control Point if the IGD-PCP IWF fails to establish communication with that PCP server. Note that the IGD-PCP IWF proceeds to PCP message validation and retransmission the same way as any PCP client [RFC6887].

5.2. Control of the Firewall

In order to configure security policies to be applied to inbound and outbound traffic, a UPnP IGD can be used to control a local firewall engine. No IGD-PCP IWF is therefore required for that purpose.

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

5.3. Port Mapping Table

The IGD-PCP IWF MUST store locally all the mappings instantiated by internal IGD 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.

Each mapping entry stored in the local mapping table is associated with a lifetime as discussed in [RFC6887]. Additional considerations specific to the IGD-PCP Interworking Function are discussed in Section 5.9.

5.4. Interworking Function without NAT in the IGD

When no NAT is embedded in the IGD, the contents of received WANIPConnection and PCP messages are not altered by the IGD-PCP Interworking Function (i.e., the contents 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 contents of mapping messages received from the IGD Control Point. These messages will contain an IP address and/or port number that 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 as depicted in Figure 4).

The IGD-PCP IWF intercepts all WANIPConnection messages issued by the IGD Control Point. For each such message, the IGD-PCP IWF then generates one or more corresponding requests (see Sections 4.1, 4.2, and 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 contents of the generated WANIPConnection response messages are set as follows:

- The internal IP address and/or port number as initially set by the IGD Control Point and stored in the IGD NAT are used to update the corresponding fields in received PCP responses.

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

- The NAT mapping entry in the IGD is updated with the result of each 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() and AddPortMapping().

5.6.1. AddAnyPortMapping()

When an IGD Control Point issues an AddAnyPortMapping() call, 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).

If the IGD-PCP IWF fails to send the MAP request to its PCP server, it follows the behavior defined in Section 5.1.

Upon receipt of a PCP MAP response from the PCP server, the corresponding UPnP IGD method is returned to the requesting IGD Control Point (the contents of the messages follow 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 IGD 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 IGD Control Point.

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

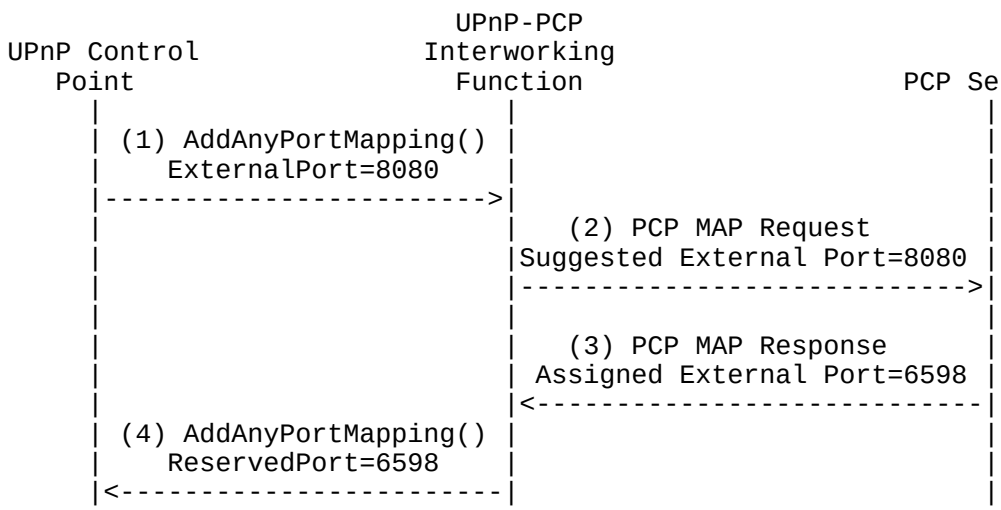

Figure 5: Flow Example: AddAnyPortMapping()

5.6.2. AddPortMapping()

A dedicated option called "PREFER_FAILURE" is defined in [RFC6887] 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 IGD Control Point.

Upon receipt of AddPortMapping() from an IGD Control Point, the IGD-PCP IWF MUST generate a PCP MAP request with all requested mapping information as indicated by the IGD 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 IGD-PCP IWF fails to send the MAP request to its PCP server, it follows the behavior defined in Section 5.1.

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 IGD 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 IGD Control Point with ConflictInMappingEntry as the error code.

The maximum retry limit is implementation-specific; its default value is 2.

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

The IGD Control Point may issue a new request with a different requested external port number. This process is typically repeated by the IGD 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 the corresponding positive answer to the requesting IGD Control Point. This answer terminates the 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 message exchange when the requested external port is not available.

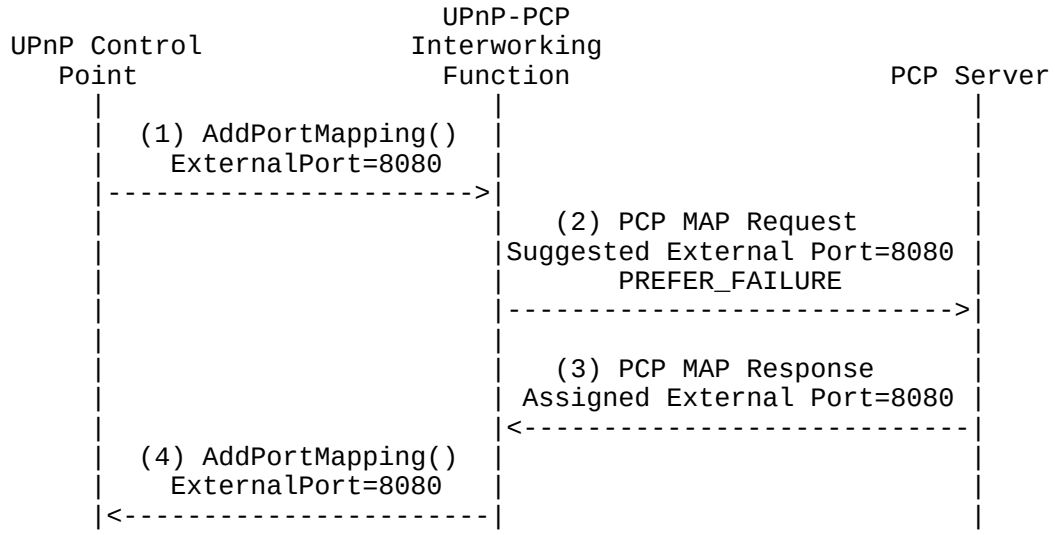

Figure 6: Flow Example (Positive Answer)

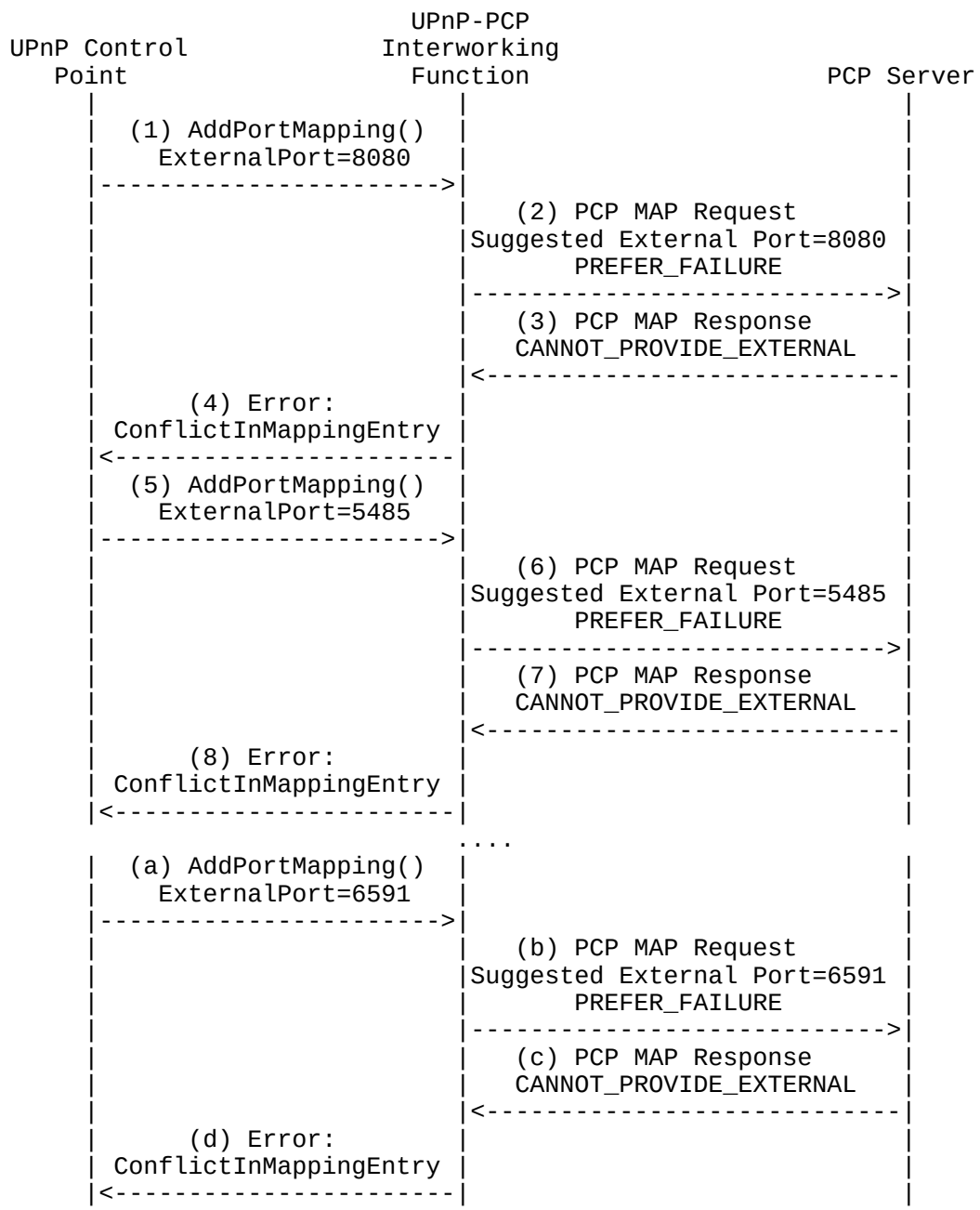

Figure 7: Flow Example (Negative Answer)

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 determine whether a mapping exists.

5.7. Listing One or a Set of Mappings

In order to list active mappings, an IGD 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 an IGD Control Point, the IGD-PCP IWF MUST check first to see if the external port number is used by the requesting IGD Control Point. If the external port is already in use by the requesting IGD Control Point, the IGD-PCP IWF MUST send back the mapping entry matching the request. 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 IGD-PCP IWF fails to send the MAP request to its PCP server, it follows the behavior defined in Section 5.1. 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 IGD 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 IGD Control Point indicating NoSuchEntryInArray as the error code so that the IGD Control Point knows the queried mapping doesn’t exist.

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

An IGD Control Point requests the deletion of one or a list of mappings by issuing DeletePortMapping() or DeletePortMappingRange().

In IGD:2, we assume that 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 is 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 IGD Control Point: "714 NoSuchEntryInArray" for DeletePortMapping() or "730 PortMappingNotFound" for DeletePortMappingRange().

Figure 8 shows an example of an IGD Control Point asking to delete a mapping that is not instantiated in the local table of the IWF.

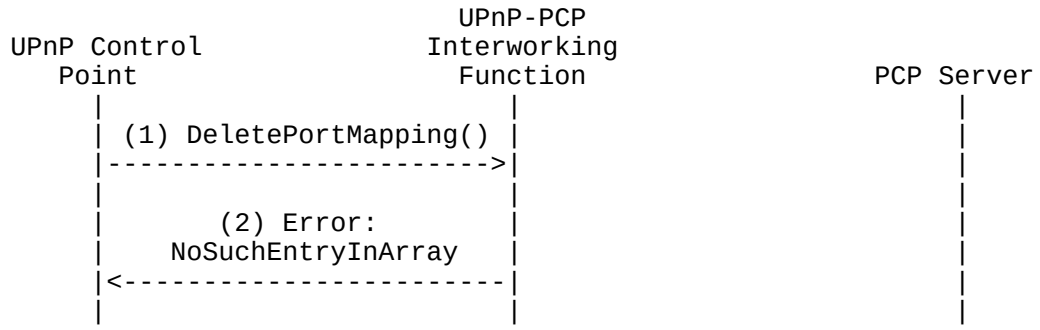

Figure 8: Local Delete (IGD-PCP IWF)

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.

If the IGD-PCP IWF fails to send the MAP request to its PCP server, it follows the behavior defined in Section 5.1.

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 IGD Control Point of 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 message containing the corresponding error cause (see Section 4.3) is sent back to the IGD-PCP IWF.

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), that match 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 IGD 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 IGD-PCP IWF MAY send a positive answer to the requesting IGD Control Point without waiting to receive all the answers from the PCP server.

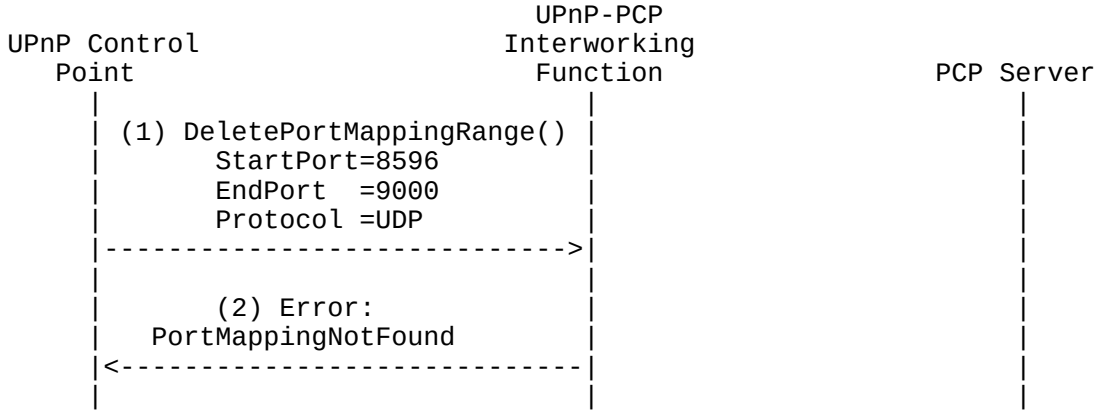

Figure 9: Flow Example: Error Encountered when Processing DeletePortMappingRange()

Figure 10 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.

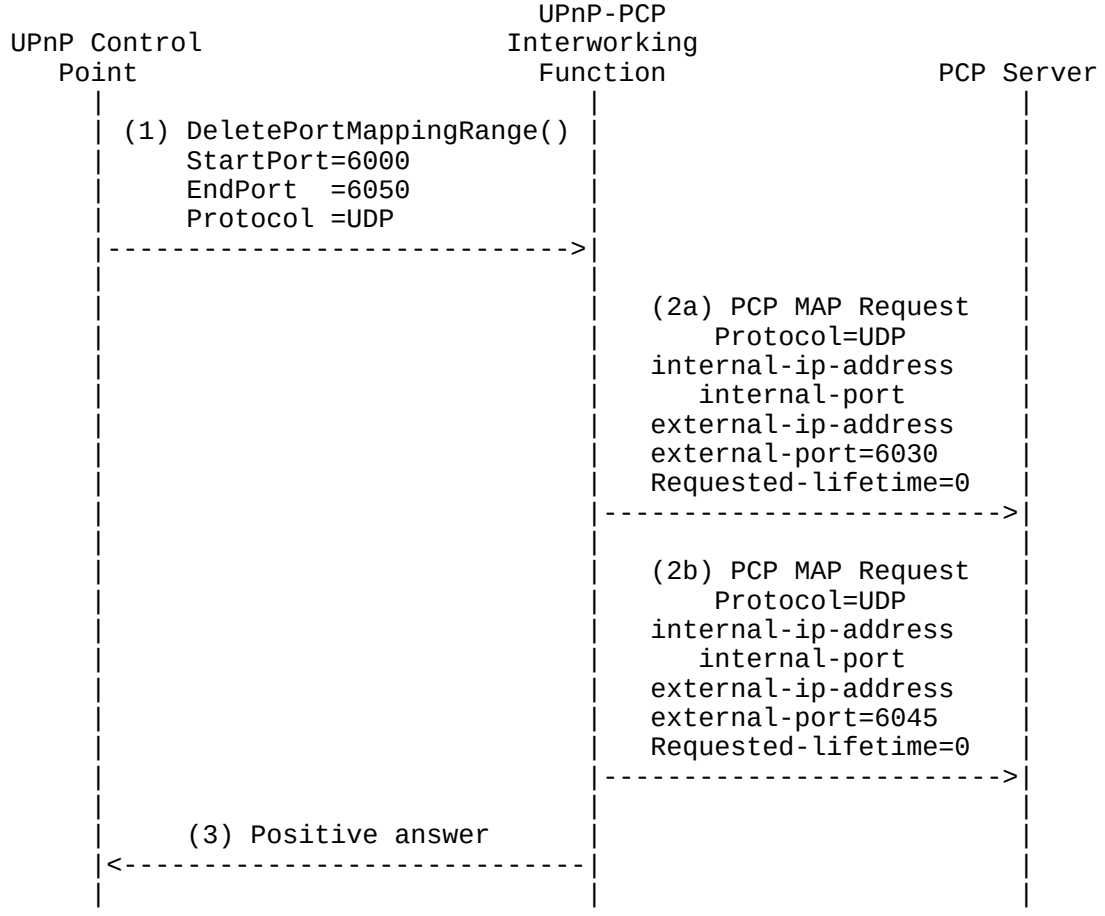

Figure 10: Example of DeletePortMappingRange()

5.9. Renewing a Mapping

Because of the incompatibility of mapping lifetimes between a 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 IGD Control Point with PortMappingLeaseDuration set to the same value as that 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 IGD Control Point.

If an error is encountered during mapping renewal, the IGD-PCP Interworking Function has no means of informing the IGD Control Point of the error.

5.10. Rapid Recovery

When the IGD-PCP IWF is co-located with the DHCP server, the state maintained by the IGD-PCP 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 IGD-PCP IWF MUST delete all the mappings bound to that internal IP address.

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

> Note: If an address change occurs, protocols that are sensitive to address changes (e.g., TCP) will experience disruption.

[RFC6887] defines a procedure for the PCP server to notify PCP clients of changes related to the mappings it maintains. When an unsolicited ANNOUNCE is received, the IGD-PCP 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 IGD-PCP IWF has no means of notifying internal IGD Control Points of any changes of the external IP address and port numbers.

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 IGD-PCP IWF has no means of notifying the internal IGD Control Point of this change.

Further analysis of PCP failure scenarios for the IGD-PCP Interworking Function are discussed in [PCP-FAILURE].

6. Security Considerations

IGD:2 access control requirements and authorization levels SHOULD be applied by default [IGD2]. When IGD:2 is used, operation on behalf of a third party SHOULD be allowed only if authentication and authorization are used [IGD2]. When only IGD:1 is available, operation on 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. The means for preventing a malicious user from creating mappings on behalf of a third party must be enabled as discussed in Section 13.1 of [RFC6887]. In particular, the THIRD_PARTY option MUST NOT be enabled unless the network on which the PCP messages are to be sent is fully trusted -- for example, access control lists (ACLs) installed on the PCP client, the PCP server, and the network between them, so that those ACLs allow only communications from a trusted PCP client to the PCP server.

An IGD Control Point that issues AddPortMapping(), AddAnyPortMapping(), or GetSpecificPortMappingEntry() requests in a shorter time frame will create a lot of mapping entries on the PCP server. The means for avoiding the exhaustion of port resources (e.g., port quota, as discussed in Section 17.2 of [RFC6887]) SHOULD be enabled.

The security considerations discussed in [RFC6887] and [Sec_DCP] should be taken into account.

7. Acknowledgments

The 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 go to him for his thorough reviews and contributions.

8. References

8.1. Normative References

[IGD1] UPnP Forum, "WANIPConnection:1 Service Template Version 1.01", November 2001, <http://upnp.org/specs/gw/UPnP-gw-WANIPConnection-v1-Service.pdf>.

[IGD2] UPnP Forum, "WANIPConnection:2 Service", September 2010, <http://upnp.org/specs/gw/UPnP-gw-WANIPConnection-v2-Service.pdf>.

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

[RFC6887] Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", RFC 6887, April 2013.

8.2. Informative References

[PCP-DESCR-OPT] Boucadair, M., Penno, R., and D. Wing, "PCP Description Option", Work in Progress, May 2013.

[PCP-DHCP-OPT] Boucadair, M., Penno, R., and D. Wing, "DHCP Options for the Port Control Protocol (PCP)", Work in Progress, March 2013.

[PCP-FAILURE] Boucadair, M. and R. Penno, "Analysis of Port Control Protocol (PCP) Failure Scenarios", Work in Progress, May 2013.

[PCP-PROXY] Boucadair, M., Penno, R., and D. Wing, "Port Control Protocol (PCP) Proxy Function", Work in Progress, June 2013.

[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 Service", February 2011, <http://upnp.org/specs/gw/UPnP-gw-DeviceProtection-v1-Service.pdf>.

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