PCP Working Group
Internet-Draft
Intended status: Informational
Expires: January 4, 2015

M. Boucadair
France Telecom

July 03, 2014

Port Control Protocol (PCP) Deployment Models
draft-boucadair-pcp-deployment-cases-03

Abstract

This document lists a set of Port Control Protocol (PCP) deployment models.

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 January 4, 2015.

Table of Contents

1. Introduction

This document lists a set of PCP [RFC6887] deployment models.

2. Terminology

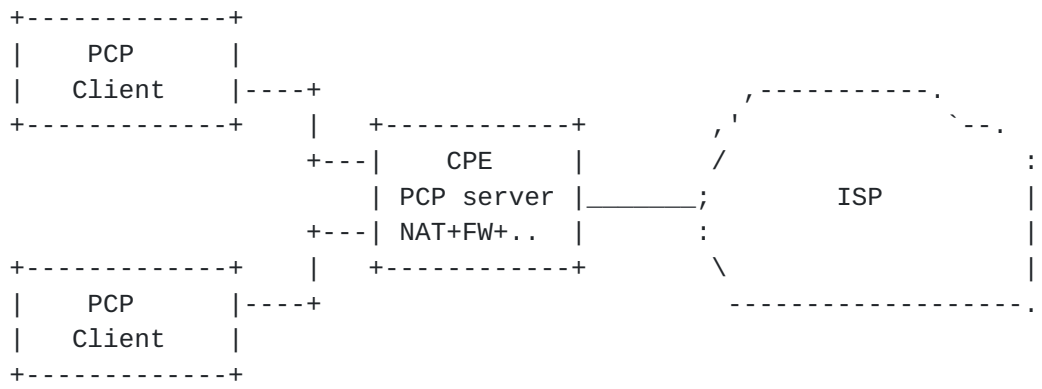
This document makes use of the following terms:

- PCP client denotes a functional element responsible for issuing PCP requests to a PCP server. Refer to [RFC6887].
- PCP server denotes a functional element that receives and processes PCP requests from a PCP client. A PCP server can be co-located with or be separated from the function (e.g., NAT, Firewall) it controls. Refer to [RFC6887].
- PCP proxy refers to a functional elements that is responsible for relaying PCP requests received from PCP client to upstream PCP servers.

3. CPE Models

3.1. Single Homed CPE Model: Local PCP Server

This model assumes PCP is enabled in the LAN side to control functions located in the CPE. The PCP server is reachable with the IP address of the private-faced interface of the CPE. Typical functions that can be controlled by PCP in this model are NAT and firewall.



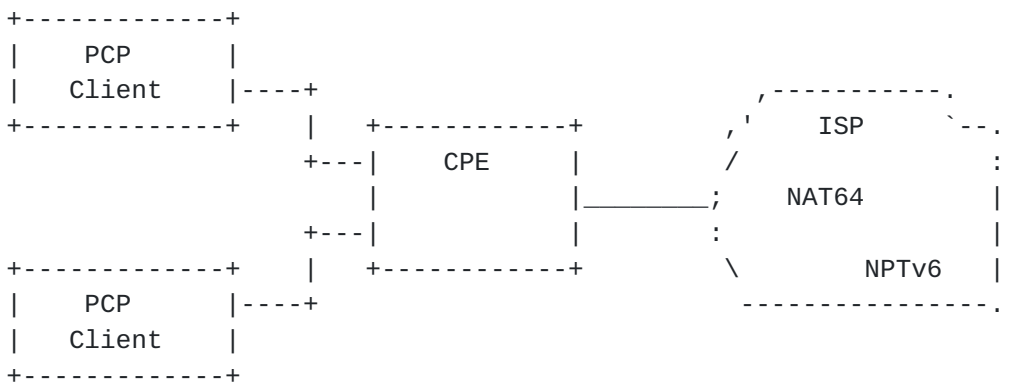
PCP client can be configured with their PCP server using DHCP for instance [I-D.ietf-pcp-dhcp]. If no PCP server is configured, PCP clients assume their default gateway is the PCP server.

This model applies for both residential or corporate markets.

3.2. Single Homed CPE Model: Multiple PCP Servers

This model assumes a customer site is connected to the same ISP's network. One or multiple PCP servers are deployed in the ISP's domain; each of them manage distinct set of functions. In the example shown in the following figure:

- NAT64 device [RFC6146] are used to interwork with IPv4-only devices.
- NPTv6 function [RFC6296] is used for engineering motivation internal to the ISP.



The use of NAT64 and NPTv6 functions is for illustration purposes; other functions can be enabled in the ISP's network side.

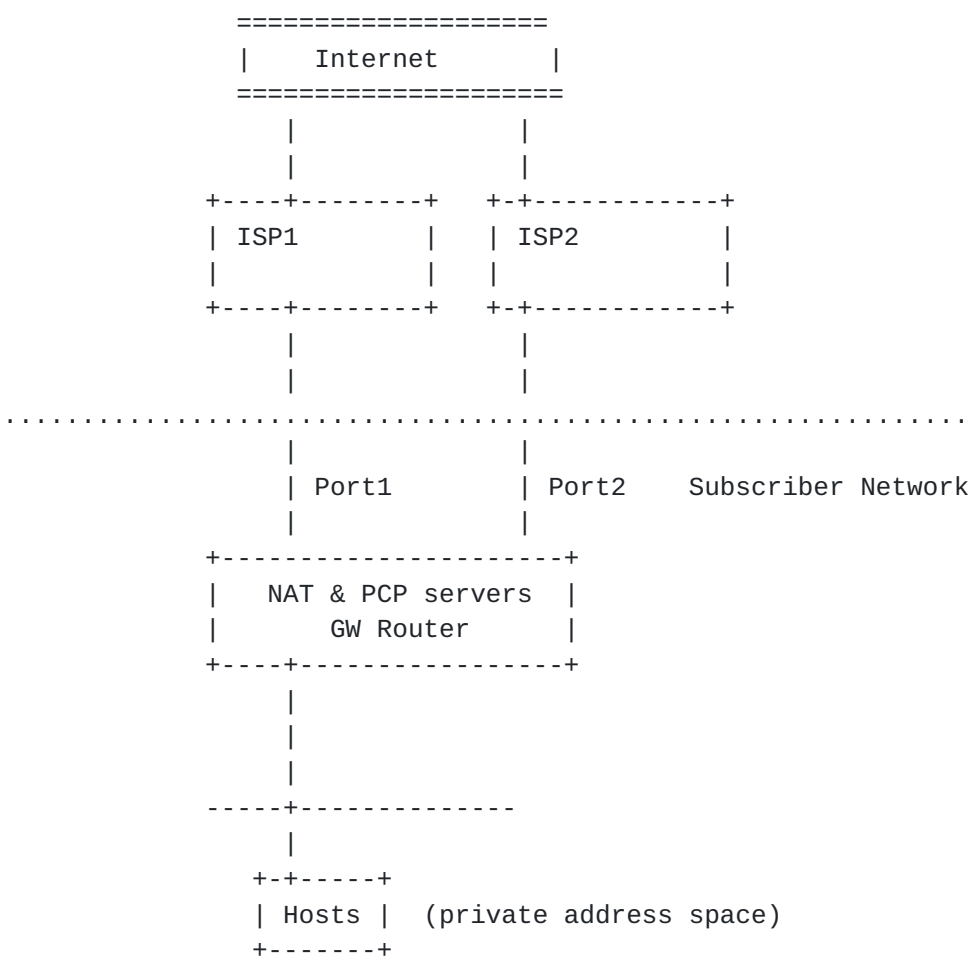
PCP clients located behind the CPE, must discover both the external IPv4 address and port numbers assigned by the NAT64 and the external IPv6 address assigned by the NPTv6. These external addresses are used for example in referrals to indicate to remote peers both the IPv4 address and IPv6 address to reach an internal server deployed in an IPv6-only domain.

The use of a PCP anycast address ([I-D.ietf-pcp-anycast]) is not recommended for this deployment case because two state entries must be created in both NAT64 and NPTv6. Explicit means such as [I-D.ietf-pcp-dhcp] must be used instead to provision IP addresses of available PCP servers.

[I-D.ietf-pcp-dhcp] may be used to provision the IP addresses of these PCP servers, or the CPE must embed a PCP proxy function that must follow [I-D.ietf-pcp-server-selection] to contact all PCP servers.

3.3. Multi-Homed CPE Model: One Single PCP Server

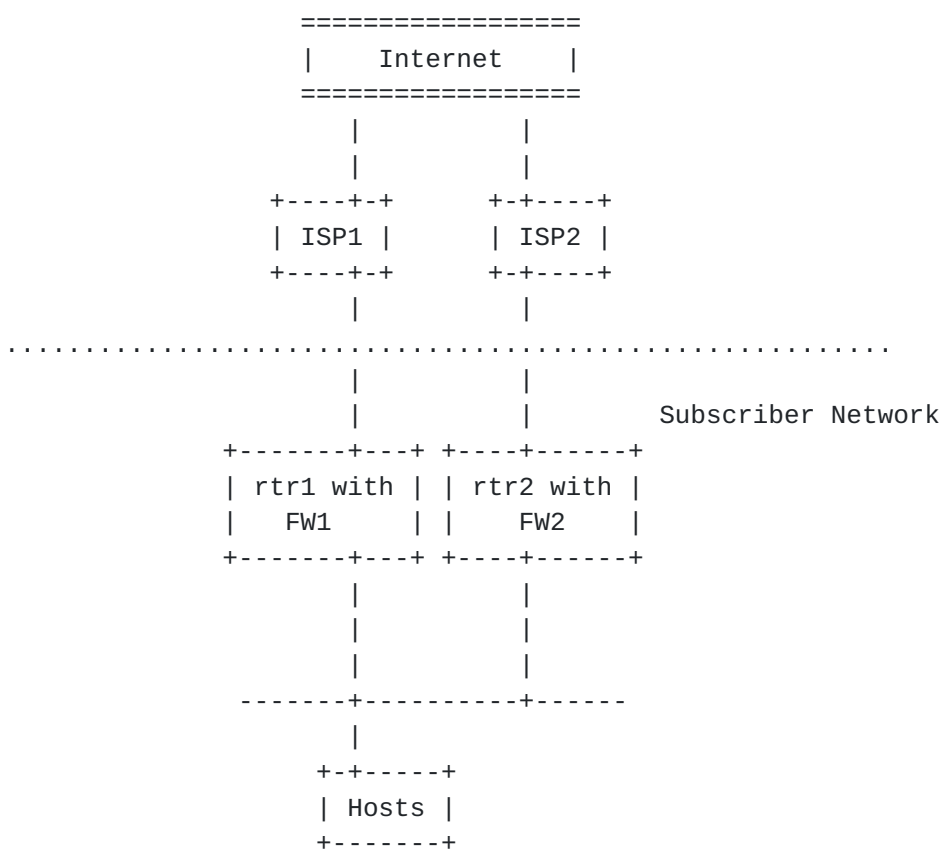
A typical example of this model is shown in the following figure:



Internal PCP clients can interact with one single PCP server.

3.4. Multi-Homed CPE Model: Multiple PCP Servers

A typical example of this model is shown in the following figure:



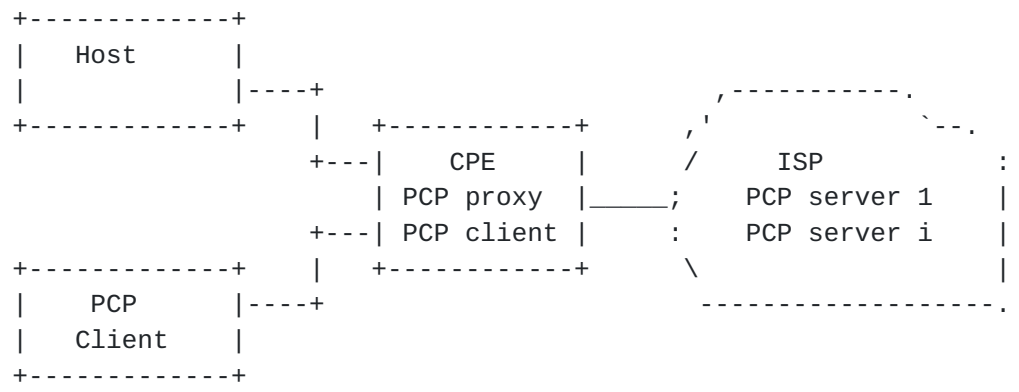
The PCP client must interact with all PCP servers; otherwise complications arise to communicate with remote peers. The procedure defined in [I-D.ietf-pcp-server-selection] is used to contact those servers.

The use of anycast-based model ([I-D.ietf-pcp-anycast]) might induce failures when communicating with external peers (e.g., incoming packets will be dropped by one of the firewalls).

3.5. PCP Proxy Model

This model assumes no PCP-controlled function is located in the CPE (e.g., DS-Lite case). The upstream PCP server is located in the ISP's network. The PCP server can be deduced from other provisioning parameters (e.g., use the IP address of the AFTR as PCP server); otherwise the IP address (s) must be discovered by other means.

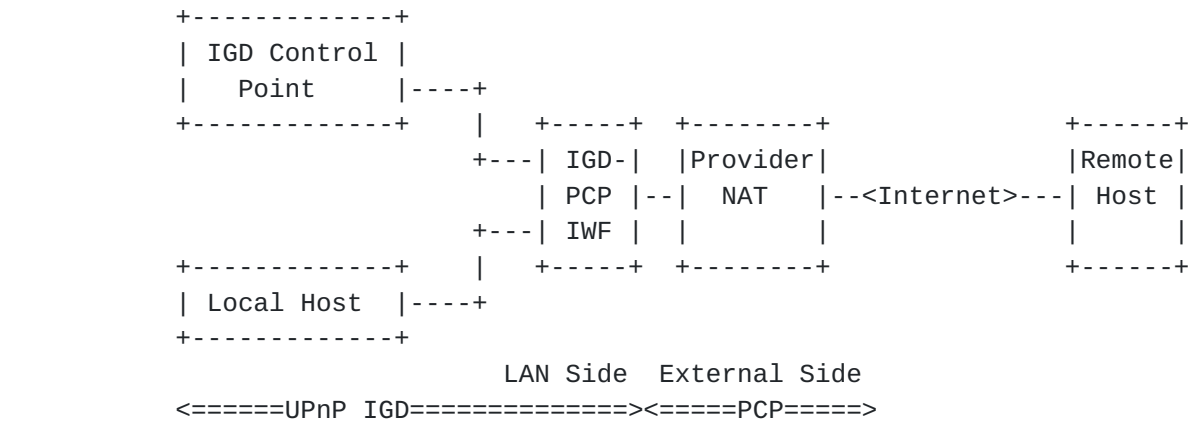
The use of an anycast-based model may not be convenient in some cases (e.g., multiple PCP-controlled devices are deployed; each of them manage a subset of services and state).



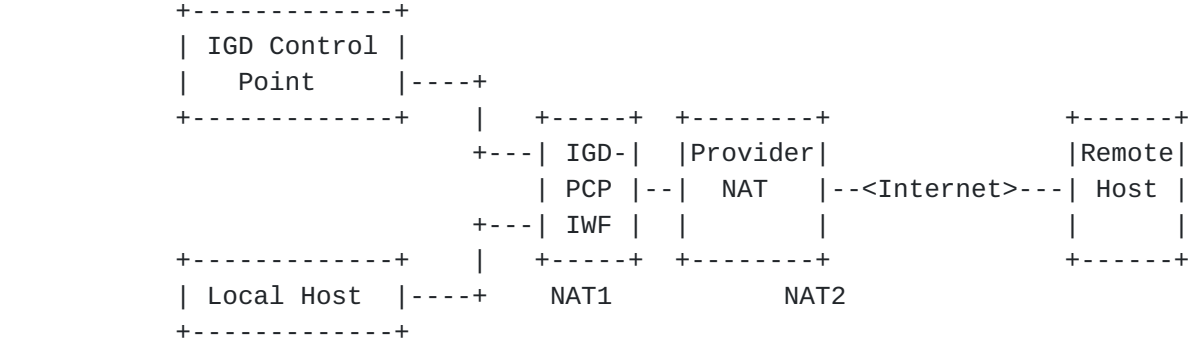
3.6. UPnP IGD-PCP Interworking Model

This model is specified in [RFC6970]. The interworking function must be provisioned with the IP address(es) of remote PCP server(s).

(a)



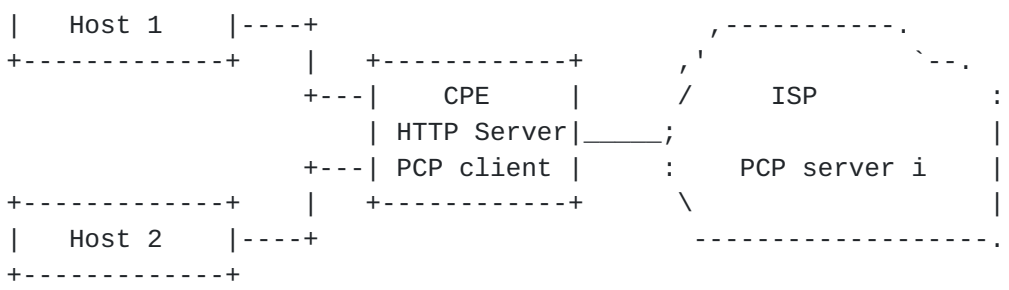
(b)



3.7. HTTP-based User Interface

This deployment model relies on the following:

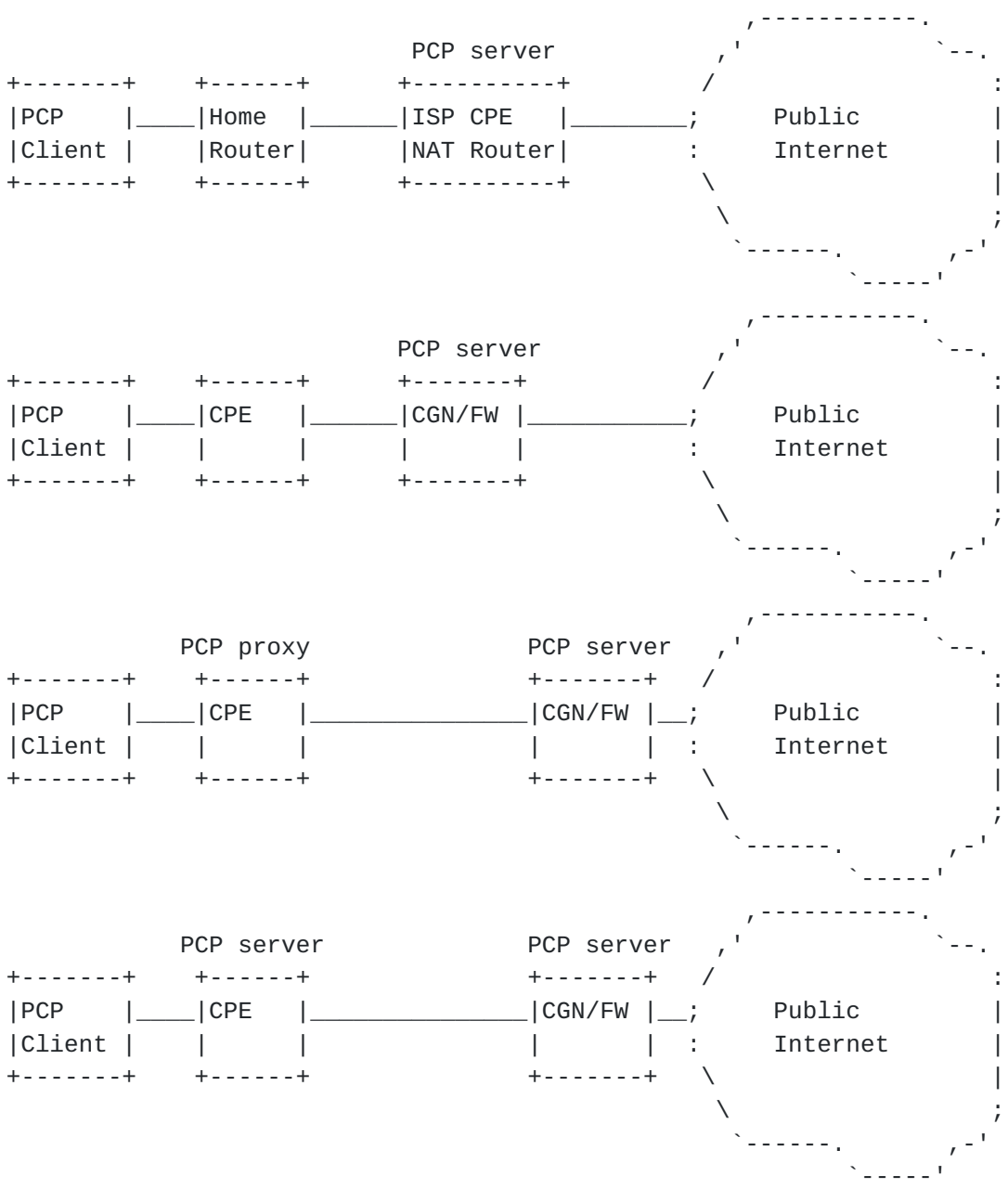
- An HTTP administration based interface (e.g. GUI) is provided to the user to manage its flow-based forwarding rules. This interface is part of the CPE management interface.
- The CPE embeds a PCP client.
- HTTP requests are translated into appropriate PCP requests in order to install the requested state.
- The PCP client uses THIRD_PARTY option.
- The PCP client should be configured with the PCP server that controls the on-path PCP-controlled device for that user.
- One or multiple PCP servers can be deployed. The logic of contacting these PCP servers may be explicitly configured to the PCP client. If not, the procedure defined in [I-D.ietf-pcp-server-selection] is used to contact those PCP servers.
- The use of a well-known address ([I-D.ietf-pcp-anycast]) to reach internal PCP servers might not be convenient if all PCP servers do not manage the same set of mapping entries (e.g., NAT64, NPTv6, IPv6 firewall, etc.).



This model can co-exist with the models discussed in Section 3.5 and Section 3.6.

3.8. Cascaded PCP-controlled Nodes Model

This model assumes cascaded PCP-controlled devices are deployed. A typical example is provided below.



This model requires a PCP proxy function [I-D.ietf-pcp-proxy] be deployed in intermediate PCP-controlled devices:

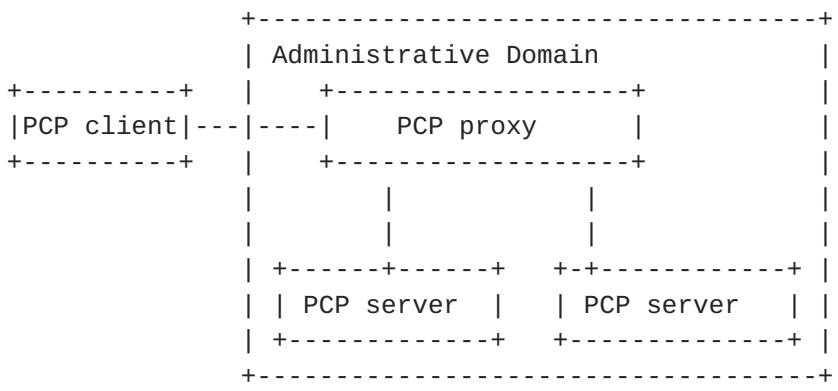
- The PCP client is not aware of the presence of more than one level of PCP servers.
- Each intermediate PCP proxy must contact the appropriate next hop PCP server(s).
- The use of PCP anaycast address may not be appropriate when the PCP server is co-located with the PCP-controlled device.

4. Hide PCP Servers Model

4.1. PCP Proxy Model

In order to hide PCP servers deployed within an administrative domain, an administrative entity may decide to deploy one or more PCP proxies [I-D.ietf-pcp-proxy] in front of PCP clients. A PCP proxy is responsible for relaying PCP requests to the appropriate PCP server(s):

- In order to prevent single failure scenarios, multiple PCP proxies can be hosted within an administrative domain.
- A PCP proxy can be configured with one or multiple PCP servers.
- A PCP proxy can be configured with the logic indicating how it should proceed to contact upstream PCP servers. The PCP proxy will then follow the procedure defined in [I-D.ietf-pcp-server-selection] to contact those PCP servers.
- Internal PCP clients may be configured with the IP address(es) of the appropriate PCP proxy (e.g., [I-D.ietf-pcp-dhcp]).
  - If all PCP proxies interact with the same PCP server(s), the same IP address can be provisioned to PCP clients.
  - If PCP proxies do not interact with the same set of PCP server(s), appropriate IP address(es) are to be returned to each requesting PCP client.



The PCP proxy should not use the PCP anycast address ([I-D.ietf-pcp-anycast]) if available PCP servers do not manage the same PCP-controlled device. Deterministic means should be used instead.

PCP client should not use the PCP anycast address to reach a PCP proxy if deployed PCP proxies do not interact with the same PCP servers. Explicit provisioning means should be preferred.

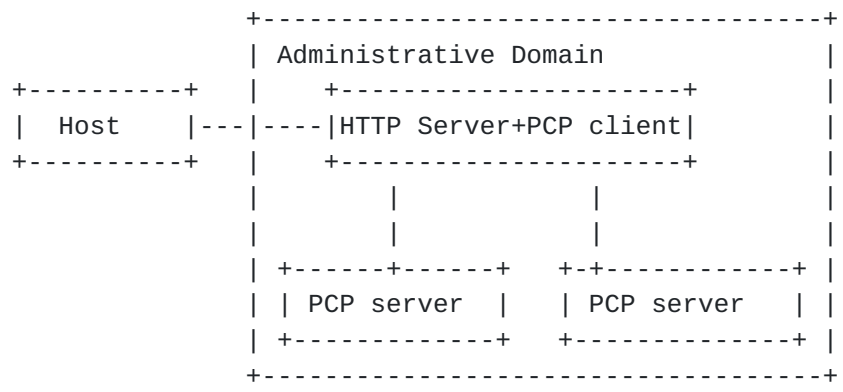
If the PCP proxy is reachable using the PCP anycast address, available PCP servers must not be reachable using the same PCP anycast address.

4.2. HTTP-Triggered PCP Client Model

Another deployment model to hide the identity of back-end PCP servers is to rely on HTTP to invoke the PCP service. This model can be used by operators to accommodate cases where a PCP client implementation is not available at the customer side (e.g., unmanaged CPE model).

The deployment model relies on the following:

- An HTTP administration based interface (e.g. GUI) is provided to the user to manage its flow-based forwarding rules.
- The HTTP user interface can be part of a CPE management interface or be provided as part of the customer care portal.
- The HTTP server embeds also a PCP client.
- HTTP requests are translated into appropriate PCP requests in order to install the requested state.
- The PCP client uses THIRD_PARTY option.
- The PCP client should be configured with the PCP server that controls the on-path PCP-controlled device for that user.
- One or multiple PCP servers can be deployed. The logic of contacting these PCP servers may be explicitly configured to the PCP client. If not, the procedure defined in [I-D.ietf-pcp-server-selection] is used to contact those PCP servers.
- The use of a well-known address ([I-D.ietf-pcp-anycast]) to reach internal PCP servers might not be convenient if all PCP servers do not manage the same set of mapping entries (e.g., NAT64, NPTv6, IPv6 firewall, etc.).



5. Separated PCP Server & PCP-controlled Device Model

This model assumes the PCP server is not co-located with the PCP-controlled device. Moreover:

- In order to prevent single failure scenarios, multiple PCP servers can be hosted within an administrative domain.
- A PCP server can control one or many PCP-controlled devices.
- Multiple PCP servers can be enabled; each of them manages a set of PCP-controlled devices.
- Internal PCP clients are configured with the IP address(es) of the appropriate PCP server.
    - If all PCP servers interact with the same PCP-controlled devices, the same PCP server's IP address can be provisioned to PCP clients.
    - If PCP servers do not interact with the same set of PCP-controlled devices, PCP server IP address(es) are to be returned to each requesting PCP client.

Note, PCP is not used between the PCP server and the PCP-controlled device. Other protocols (e.g., H.248) can be used for that purpose.

6. Security Considerations

PCP-related security considerations are discussed in [RFC6887].

7. IANA Considerations

This document does not require any action from IANA.

8. References

8.1. Normative References

[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

[I-D.ietf-pcp-anycast]
Kiesel, S., Penno, R., and S. Cheshire, "PCP Anycast Address", draft-ietf-pcp-anycast-01 (work in progress), February 2014.

[I-D.ietf-pcp-dhcp]
Boucadair, M., Penno, R., and D. Wing, "DHCP Options for the Port Control Protocol (PCP)", draft-ietf-pcp-dhcp-13 (work in progress), April 2014.

[I-D.ietf-pcp-proxy]
Perreault, S., Boucadair, M., Penno, R., Wing, D., and S. Cheshire, "Port Control Protocol (PCP) Proxy Function", draft-ietf-pcp-proxy-05 (work in progress), February 2014.

[I-D.ietf-pcp-server-selection]
Boucadair, M., Penno, R., Wing, D., Patil, P., and T. Reddy, "PCP Server Selection", draft-ietf-pcp-server-selection-03 (work in progress), April 2014.

[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.

[RFC6296] Wasserman, M. and F. Baker, "IPv6-to-IPv6 Network Prefix Translation", RFC 6296, June 2011.

[RFC6970] Boucadair, M., Penno, R., and D. Wing, "Universal Plug and Play (UPnP) Internet Gateway Device - Port Control Protocol Interworking Function (IGD-PCP IWF)", RFC 6970, July 2013.

Author's Address

Mohamed Boucadair
France Telecom
Rennes 35000
France

Email: mohamed.boucadair@orange.com