

PCP Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 14, 2013

P. Patil
T. Reddy
R. Penno
D. Wing
Cisco

October 11, 2012

Using PCP to control NAT and Firewalls in Multihoming
draft-patil-pcp-multihoming-00

Abstract

This note describes how Port Control Protocol (PCP) can be used to control NATs and Firewalls in multihoming deployments.

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 April 14, 2013.

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.

Internet-Draft

PCP in Multihoming

October 2012

Table of Contents

1.	Introduction	3
2.	Problem Statement	3
3.	IPv6 Multihoming	4
4.	IPv4 Multihoming	4
5.	Other Multihoming use cases	5
5.1.	IPv6 Network-Managed Firewall	6
5.2.	IPv4 Policy based Routing	7
6.	Multiple interfaces and Servers	7
7.	Security Considerations	8
8.	IANA Considerations	8
9.	References	8
9.1.	Normative References	8
9.2.	Informative References	9
	Authors' Addresses	9

1. Introduction

A host can use the Port Control Protocol (PCP) to flexibly manage the IP address and port mapping information on Network Address Translators (NATs) or firewalls, to facilitate communications with remote hosts. In a multihomed network, there may be multiple PCP servers providing Firewall or prefix translation functions to hosts in the network.

This document covers PCP related considerations in IPv4 and IPv6 multihomed networks.

2. Problem Statement

The main problem of a PCP multihoming situation can be succinctly described as 'one client, multiple servers'. PCP-base [[I-D.ietf-pcp-base](#)] does not address how a PCP Client should behave in a situation when it discovers multiple PCP Servers and therefore many questions are open to standardization. For example, if multiple PCP Servers are discovered through the same interface, should the client send PCP requests be sent to all of them? Are there significant differences between a multihoming and high-availability scenarios? If yes, how can a PCP Client determine one versus the other. These are just a few questions related to the problem.

In this document we make the following simplifying assumption:

- o Whenever a PCP Client discovers multiple PCP Servers, it will send requests to all of them in parallel as described in [[I-D.boucadair-pcp-server-selection](#)].
- o There is no requirement that multiple PCP Servers have the same capabilities.
- o PCP Requests to different servers are independent, meaning that

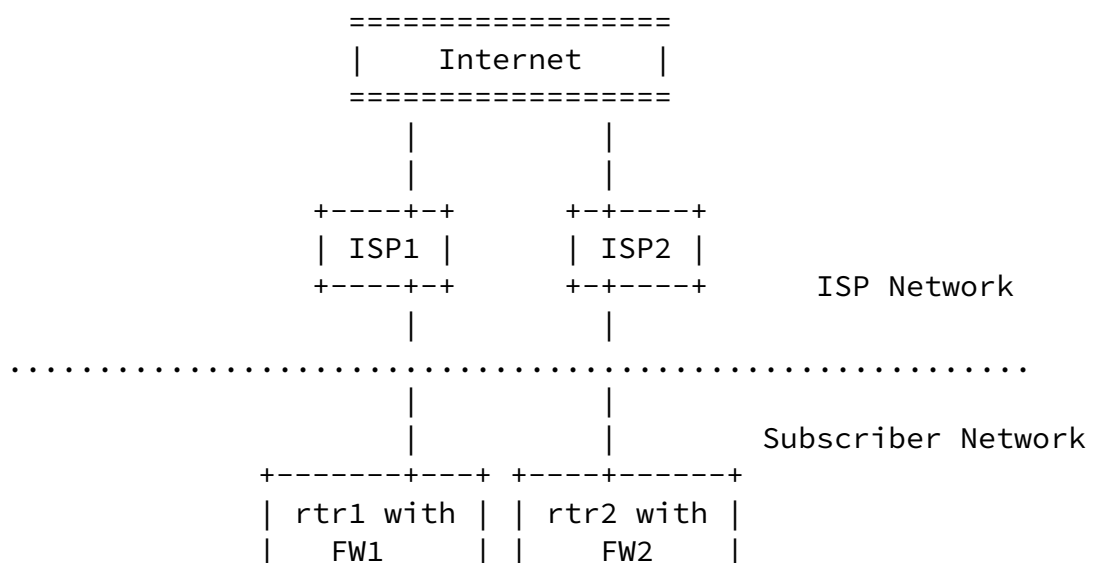
the result of a PCP request to one server does not influence another.

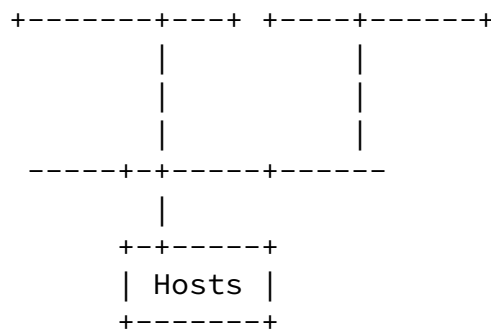
- o If PCP Servers provides NAT, it is out of scope how the client manages ports across PCP Servers. For example, whether PCP Client requires all external ports to be the same or whether there are ports available at all.

In all scenarios below PCP client has a single interface unless explicitly noted otherwise.

3. IPv6 Multihoming

In an IPv6 multihomed network, two or more routers co-located with firewalls are present on a single link shared with the host(s). Each router is in turn connected to a different service provider network and the host in this environment would be offered multiple prefixes and advertised multiple DNS/NTP servers. Consider a scenario in which firewalls within an IPv6 multihoming environment also implement a PCP Server. PCP client learns of the available PCP servers by using DHCP [[I-D.ietf-pcp-dhcp](#)] or any other PCP server discovery technique defined in future specifications. The PCP client will send PCP requests in parallel to each of the PCP Servers as described in [[I-D.boucadair-pcp-server-selection](#)].

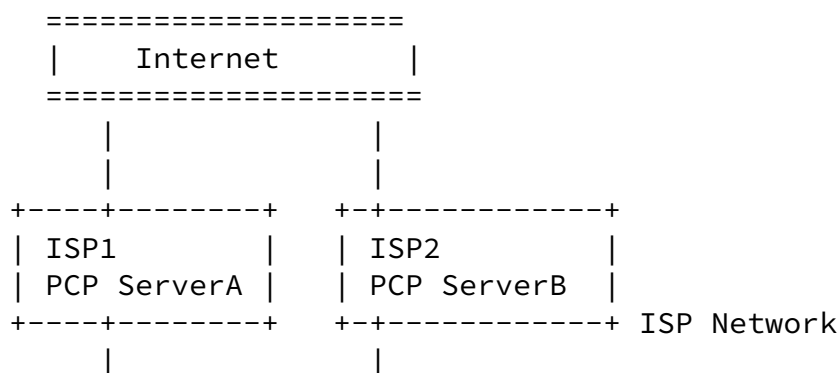




4. IPv4 Multihoming

In an IPv4 multihomed network, the gateway router is connected to different service provider networks. The host is connected to the gateway router and is given a private IPv4 address oblivious to the fact that there are multiple service providers. The Gateway router

will be configured with multiple PCP proxy servers, each corresponding to an upstream PCP server. Each PCP Server is announced independently since it is within a different ISP. PCP client can learn these multiple PCP proxy addresses using DHCP or any other PCP server discovery technique. The PCP client, by sending PCP requests in parallel to both the PCP proxies, will learn the external IP addresses and ports allocated by each of the upstream PCP servers. The Gateway router which implements a PCP Proxy [[I-D.bpw-pcp-proxy](#)], creates local NAT state, modifies the PCP request and forwards it to the PCP server. The incoming PCP response will be updated by the PCP Proxy and forwarded to the PCP client.



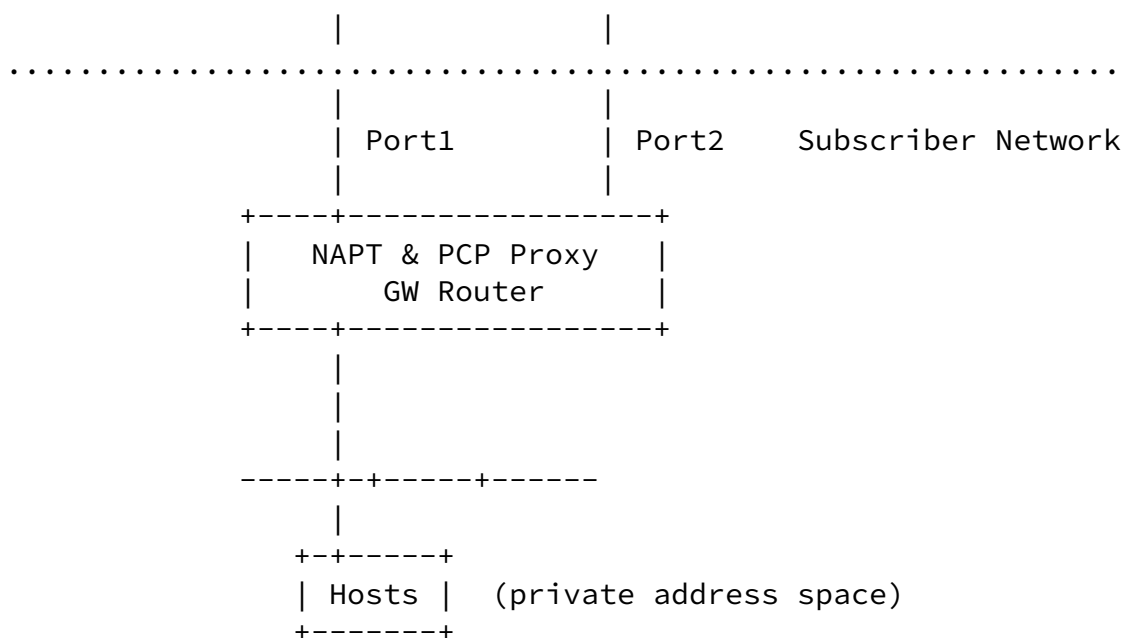
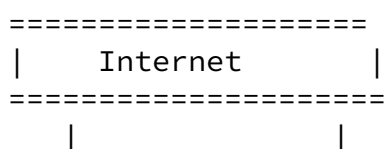


Figure 2: IPv4 Multihomed environment with Gateway Router performing NAT

5. Other Multihoming use cases

5.1. IPv6 Network-Managed Firewall

A network-managed Firewall uses the same techniques as the premises-based firewall, but the firewall service is delivered using a security appliance positioned in the ISP. The requesting router in customer premises may obtain the PCP server addresses from the ISP delegating router, and then pass that configuration information on to the PCP clients through a DHCP server in the requesting router in the customer premises. The PCP client can also learn PCP servers using other PCP server discovery techniques. Each PCP Server is announced independently since it is within a different ISP.



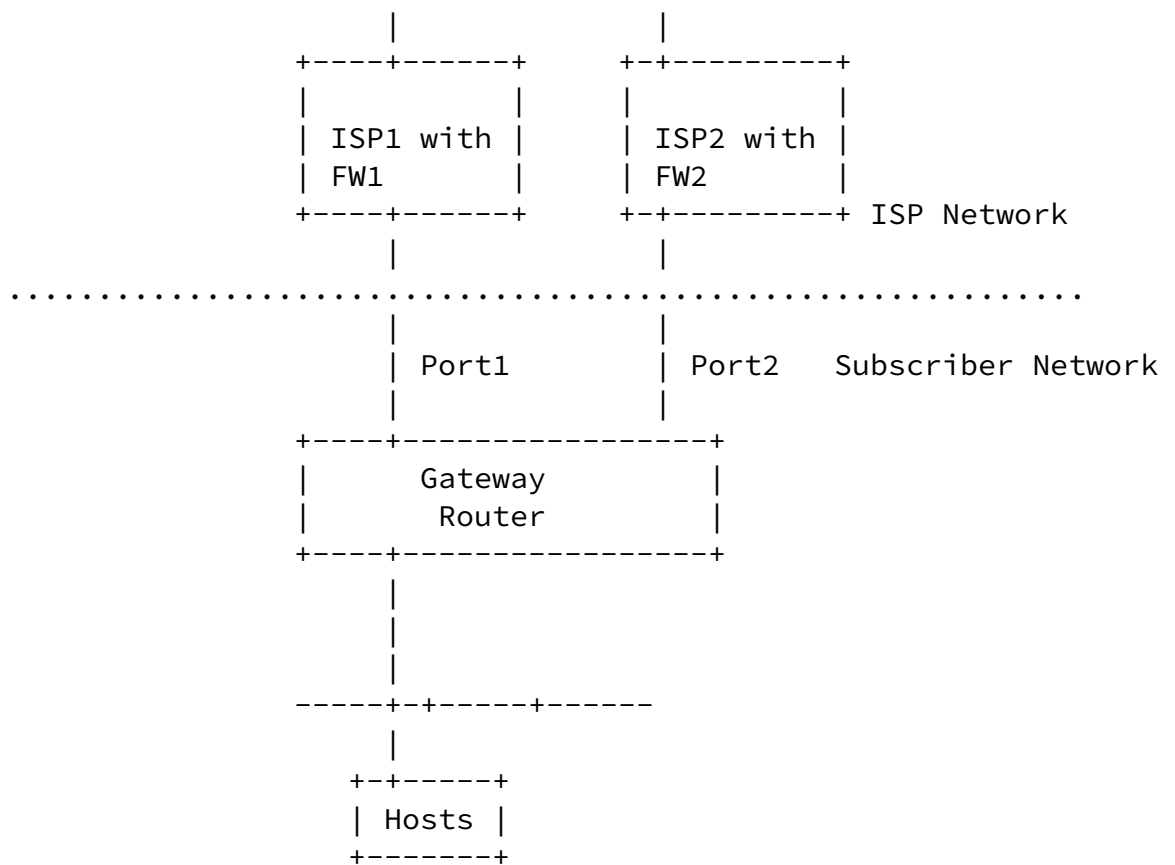


Figure 3: Network-Managed Firewall

When the PCP client sends a PCP request to the PCP server deployed in the ISP and the source address of the PCP request is not the one that is delegated by the upstream ISP, then that PCP request will be dropped at the ISP by its ingress filter rule. Ingress filtering is becoming more popular among ISPs to mitigate the damage of denial-of-service (DoS) attacks as explained in [section 2.1.2 of \[RFC5220\]](#). In IPv6 multihoming the PCP client will eventually learn that the PCP

server responds to only PCP requests with specific source address after few attempts and hence can discard sending PCP requests with wrong source address to the PCP server provided by the ISP.

[5.2.](#) IPv4 Policy based Routing

Policy based Routing (PBR) with multi-homing is typically used in enterprises to route packets from the same source IP address to

different ISP based on configuration policies and match conditions based on source IP address, destination IP address, destination port, DSCP value(s), L4 and L7 protocols (e.g., SIP, RTP, RTSP) etc. For e.g. a site with Dual WAN connections Gold-ISP, Bronze-ISP and uses Gold-ISP for certain traffic only (e.g. Media). In such an environment NAT has different NAT pools and would rely on pre-configured PBR policy to determine which NAT address pool to use when an IP packet comes from an internal host. PCP allows a host to interact with a PCP-controlled NAT device and request an external IP and port. Therefore a PCP Server that controls the NAT device with PBR and receives a PCP request from a PCP client needs to know from which NAT pool to allocate an external IP address and port.

The PCP PEER request would contain the destination IP address, destination port and transport protocol of the remote peer that the PCP client will be trying to communicate with. The PCP MAP request with FILTER option would also contain the destination IP address, transport port but the destination port could be all ports. The NAT device based on the information present in the PCP request can possibly select the NAT pool, create mapping and return the external IP address and port in PCP response.

There is also a possibility that PBR is determined based on other information like L7 protocol, DSCP value(s) that is not conveyed by default in the PCP PEER or MAP with FILTER option. Further In case of PCP MAP request with just the 3-tuple information (internal port, protocol and source IP address), the NAT device does not know which NAT pool to use. Hence if the information conveyed in PCP request is not sufficient to execute the policy then the PCP server will return a new error code (PROVIDE_MORE_DATA) in the PCP response to the PCP client asking it to provide additional information in subsequent PCP requests. The PCP client can then convey more information like DESCRIPTION, DSCP_POLICY using the PCP extensions defined in [\[I-D.boucadair-pcp-extensions\]](#).

[6.](#) Multiple interfaces and Servers

One interesting case for PCP multi-homing is when a end host such as a mobile terminal has multiple interfaces concurrently active, for

example, Wi-Fi and 3G. In this case PCP client would discover

different PCP Servers over different interfaces. Although multiple interfaces are available, an application might choose to use just one based on, for example, bandwidth requirements, and therefore would need to send PCP requests to just one PCP Server.

This scenario requires further discussion. TBD

[7.](#) Security Considerations

Security considerations in [[I-D.ietf-pcp-base](#)] apply to this use.

[8.](#) IANA Considerations

The following PCP result code is to be allocated : PROVIDE_MORE_DATA

[9.](#) References

[9.1.](#) Normative References

[I-D.boucadair-pcp-extensions]

Boucadair, M., Penno, R., and D. Wing, "Some Extensions to Port Control Protocol (PCP)", [draft-boucadair-pcp-extensions-03](#) (work in progress), April 2012.

[I-D.boucadair-pcp-server-selection]

Boucadair, M., Penno, R., and D. Wing, "PCP Server Selection", [draft-boucadair-pcp-server-selection-00](#) (work in progress), September 2012.

[I-D.bpw-pcp-proxy]

Boucadair, M., Penno, R., Wing, D., and F. Dupont, "Port Control Protocol (PCP) Proxy Function", [draft-bpw-pcp-proxy-02](#) (work in progress), September 2011.

[I-D.ietf-pcp-base]

Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", [draft-ietf-pcp-base-28](#) (work in progress), October 2012.

[I-D.ietf-pcp-dhcp]

Boucadair, M., Penno, R., and D. Wing, "DHCP Options for the Port Control Protocol (PCP)", [draft-ietf-pcp-dhcp-05](#) (work in progress), September 2012.

[9.2.](#) Informative References

[RFC5220] Matsumoto, A., Fujisaki, T., Hiromi, R., and K. Kanayama, "Problem Statement for Default Address Selection in Multi-Prefix Environments: Operational Issues of [RFC 3484](#) Default Rules", [RFC 5220](#), July 2008.

Authors' Addresses

Prashanth Patil
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Sarjapur Marthalli Outer Ring Road
Bangalore, Karnataka 560103
India

Email: praspati@cisco.com

Tirumaleswar Reddy
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Sarjapur Marathalli Outer Ring Road
Bangalore, Karnataka 560103
India

Email: tiredy@cisco.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

