

PCP Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 25, 2012

T. Reddy
P. Patil
D. Wing
F. Baker
Cisco
June 23, 2012

PCP Server Discovery in IPv6 Multihoming
draft-reddy-pcp-server-discovery-00

Abstract

A multihomed network may have a PCP server on each router connecting to each upstream network, providing firewall or prefix translation functions to hosts in the network. In these networks, a PCP client needs to discover all of those PCP servers and then send PCP requests to them individually.

This document proposes a multicast mechanism to discover PCP servers.

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 December 25, 2012.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
2.	Notational Conventions	3
3.	DISCOVER OpCode	3
3.1.	PCP Server joining a multicast group	4
3.2.	Generating a DISCOVER Request	4
3.3.	Processing a DISCOVER Request	5
3.4.	Processing a DISCOVER Response	5
3.5.	Discover Option Packet Format	6
4.	Operational Considerations	6
5.	Security Considerations	7
6.	IANA Considerations	7
7.	References	7
7.1.	Normative References	7
7.2.	Informative References	8
	Authors' Addresses	8

1. Introduction

Using Port Control Protocol (PCP) [[I-D.ietf-pcp-base](#)] a host can create mappings with its NAT or firewall. PCP expects only one PCP server. In a multihomed network, there may be multiple PCP servers and the PCP client is unaware of all designated PCP Servers in the network. For example, there may be a PCP server integrated into every firewall device connecting to each network. Hence there is a need for PCP client to discover all such PCP Servers with specific functionalities so that the PCP client can make appropriate PCP requests to each one of them.

This document proposes a means by which a PCP client can discover all such PCP servers within the network. Each PCP server in the network joins a certain multicast. Using the new DISCOVER OpCode, defined in this document, each PCP client sends a DISCOVER request to that multicast group address. Each PCP server responds with a DISCOVER response. The PCP client then sends regular unicast PCP request messages (e.g., MAP or PEER OpCodes) to each of those discovered PCP servers.

2. Notational Conventions

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 [[RFC2119](#)].

3. DISCOVER OpCode

DISCOVER : Discover PCP servers listening on specific multicast groups.

PCP Servers SHOULD provide a configuration option to allow administrators to disable DISCOVER support if they wish. PCP

DISCOVER requests are only designed to discover appropriate PCP servers on the network. The request does not offer functionality defined by other Opcodes described in [[I-D.ietf-pcp-base](#)].

The following diagram shows the usage of DISCOVER OpCode, where PCP Server1 and PCP Server2 join the same multicast group (for e.g. ALL-IPv6-FIREWALLS)

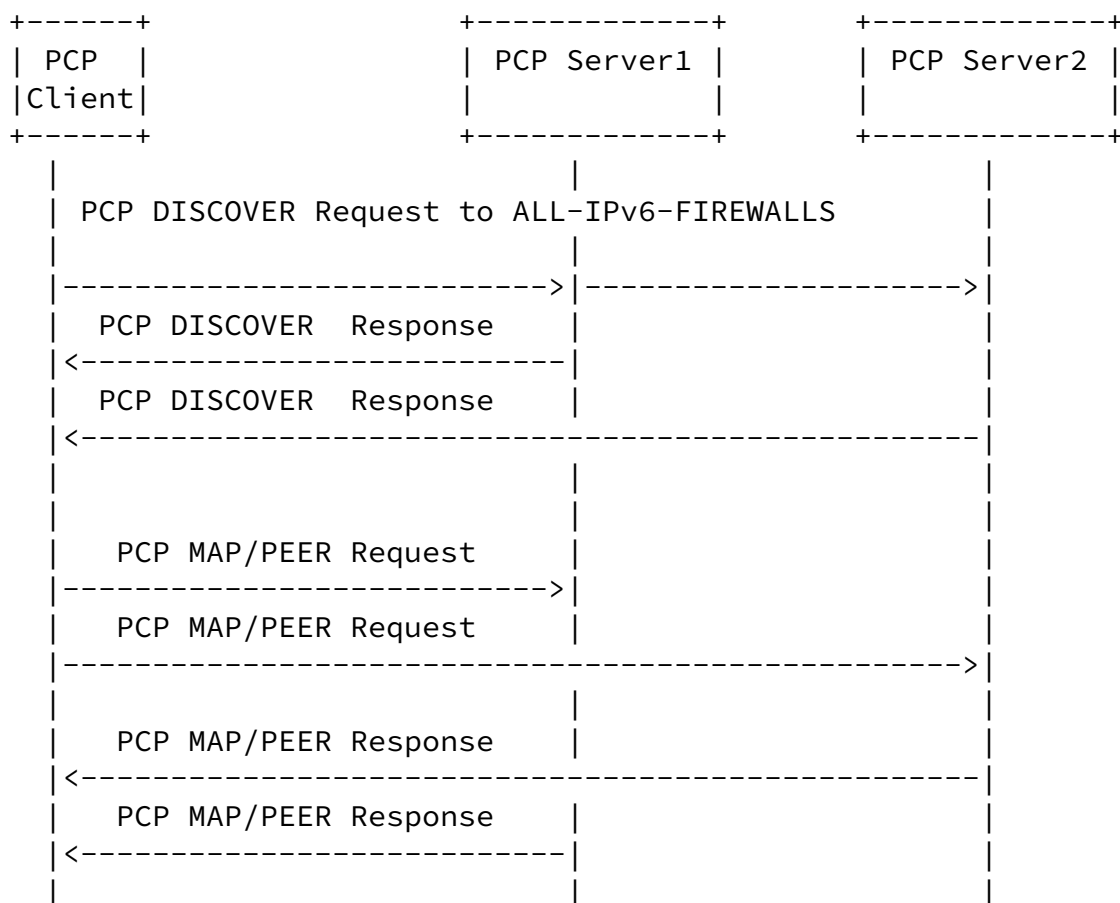


Figure 1: PCP Server Discover

[3.1.](#) PCP Server joining a multicast group

Each PCP server in the network joins a certain multicast group based on other functionalities embedded with it. Consider a scenario in which a firewall also implements a Port Control Protocol (PCP) [[I-D.ietf-pcp-base](#)] Server, in which case it joins a multicast group ALL-IPv6-FIREWALLS.

A PCP server can join more than one mutlicast groups if it offers multiple functionalities within the same device.

[3.2.](#) Generating a DISCOVER Request

To discover the PCP servers listening on each of the assigned multicast addresses of interest to the PCP client, the PCP client sends a DISCOVER request to each of those multicast addresses.

A Discover Nonce is included in the request by the PCP client. The Discover Nonce is randomly chosen by the PCP client, and is used as part of validation of PCP responses.

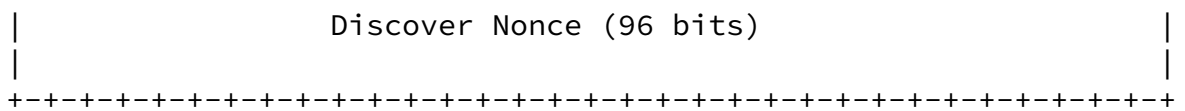
To accommodate packet loss, the request SHOULD be transmitted several times with a random jitter between them to each of the multicast address. It is RECOMMENDED to transmit the DISCOVER Request a total of three times with the first retransmission after 5 seconds plus a random value between 0-2.5 seconds, and again at 10 seconds plus a random value between 0-5 seconds.

Periodic PCP DISCOVER requests should be made to determine the updated list of PCP servers in the network. A PCP client can send DISCOVER messages periodically every 600 seconds to each of the multicast addresses.

[3.3.](#) Processing a DISCOVER Request

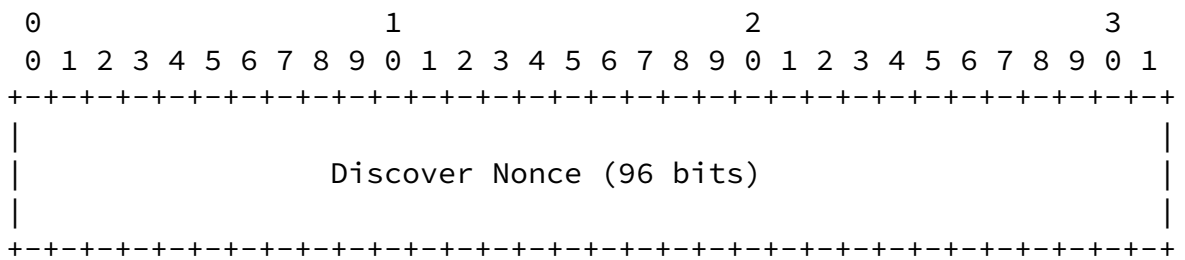
When a PCP server listening on one of the multicast groups as described in [Section 3.1](#) receives a PCP DISCOVER Opcode, after successful parsing and processing, it generates a SUCCESS response with zero Assigned Lifetime. If a PCP DISCOVER Request is received on an unassigned multicast group, it should be ignored.

Each PCP Server sends a separate DISCOVER response with unicast source address signaling to the PCP client that the source IPv6



Discover Nonce: Random value chosen by the PCP client.

The following diagram shows the format of Opcode-specific information in a response packet for the DISCOVER Opcode:



Discover Nonce: Copied from the request.

4. Operational Considerations

This document defines a set of multicast addresses in several scopes. Operationally, the choice of which scope is appropriate is made by the administration. A reasonable default value in system configurations might be Organization-Local (e.g., all firewalls operated by the organization). However, a large organization might well choose Site-Local or Admin-Local, and consider that "site" or "administrative" domain to include the set of Firewalls advertising a default route into a specific part of its network.

5. Security Considerations

The principal security threat in this algorithm is a security threat inherent to IP multicast routing and any application that runs on it. A rogue system can join a multicast group and respond to discovery requests pretending to be PCP servers. Discovery of such rogue systems as PCP servers, in itself, is not a security threat if there is a means for the PCP client to authenticate and authorize the

discovered PCP servers.

In addition, the security considerations in [[I-D.ietf-pcp-base](#)] also apply to this use.

6. IANA Considerations

This note requests of the IANA the assignment of a new PCP Opcode

value	Opcode
-----	-----
TBD	DISCOVER

This note also requests of the IANA the assignment of a set of multicast addresses as described in [Section 2.7](#) of the IP Version 6 Addressing Architecture [[RFC4291](#)] from the registry [[v6mult](#)]. This set of addresses is referred to as "ALL-IPv6-FIREWALLS". One address should be assigned for each of the following scopes: Link-Local, Admin-Local, Site-Local, and Organization-Local.

7. References

7.1. 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-26](#) (work in progress), June 2012.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", [RFC 4291](#), February 2006.

7.2. Informative References

[v6mult] IANA, "IPv6 Multicast Address Space Registry",
December 2011, <[http://www.iana.org/assignments/
ipv6-multicast-addresses/ipv6-multicast-addresses.xml](http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xml)>.

Authors' Addresses

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

Email: tiredddy@cisco.com

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

Email: praspati@cisco.com

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

Email: dwing@cisco.com

Fred Baker
Cisco Systems, Inc.
Santa Barbara, California 93117
USA

Email: fred@cisco.com