PCP Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 29, 2014

M. Boucadair
France Telecom
T. Reddy
Cisco

November 25, 2013

Retrieving the Capabilities of a PCP-controlled Device
draft-boucadair-pcp-capability-03

Abstract

This document extends Port Control Protocol (PCP) with the ability to retrieve the capabilities of PCP-controlled device: CAPABILITY Option.

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 May 29, 2014.

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. CAPABILITY 2
3. PCP Client/Server Behavior 3
4. Option Usage 4
5. Security Considerations 5
6. IANA Considerations 5
7. References 6
7.1. Normative References 6
7.2. Informative References 6
Authors' Addresses 7

1. Introduction

This document extends the base PCP [RFC6887] with a new feature to discover the capabilities of a PCP-controlled device. Retrieving the capabilities of a PCP-controlled device would allow to avoid error, provide a hint why some applications fails, help select the OpCode to issue, etc.

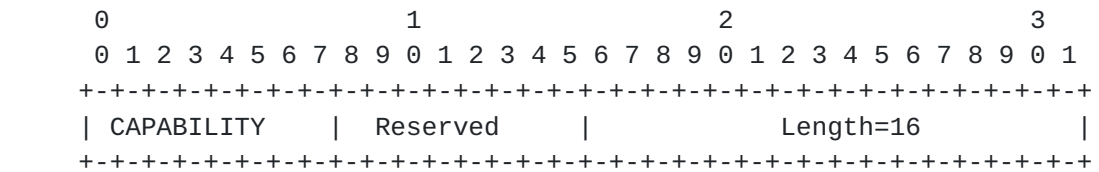
This option can be elected to be defined as a new OpCode.

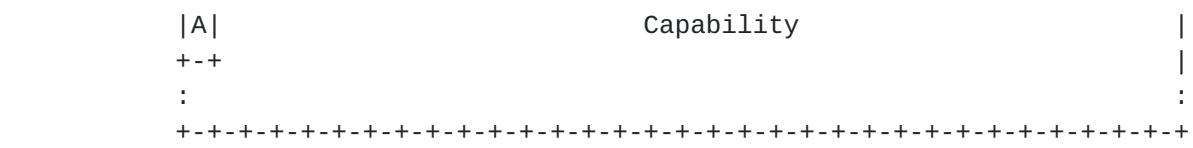
2. CAPABILITY

The CAPABILITY option (Code: TBA, Figure 1) is used by a PCP Server to indicate to a requesting PCP Client the capabilities it supports with regards to port forwarding operations.

One single Capability option is conveyed in the same PCP response message even if several functions are co-located in the same PCP-controlled device (e.g., NAT44 and NAT64, NAT44 and ports set assignment capability, etc.).

This option, when received from a PCP Server, is used by a PCP Client to constraint the content of its requests and therefore avoid errors.





This Option:

Option Name: PCP Capabilities Option (CAPABILITY)
Number: TBA (IANA)
Purpose: Retrieve the capabilities of a PCP-controlled device
Valid for Opcodes: ANNOUNCE, MAP, PEER
Length: 16
May appear in: both request and response
Maximum occurrences: None

Figure 1: Capability option

A-bit when set (i.e., 1) indicates the PCP Server supports authentication. If this bit is set to 0, is indicates plain PCP is supported.

The Capability Field is encoded in 127 bits. Each bit in the Capability bit mask is used to represent the PCP-controlled device capability. Several bits can be set if several functions are co-located in the same device. The following values for the Capability field are:

Bit #: Description
1: NAT44
2: Stateless NAT64 [RFC6145].
4: Stateful NAT64 [RFC6146].
8: A+P Port Range Router [RFC6346]
9: Supports PORT_SET option [I-D.ietf-pcp-port-set].
16: IPv4 firewall.
32: IPv6 Firewall [RFC6092].
64: NPTv6 [RFC6296].
125: DSCP re-marking function.
126: FLOWDATA-aware function ([I-D.wing-pcp-flowdata]).
127: ILNP Translator [RFC6740].

3. PCP Client/Server Behavior

This section specifies the behavior of the PCP Client and the PCP Server to handle the CAPABILITY Option.

The PCP Server MAY be configured to return the CAPABILITY Option even if it is not included in the request.

Once the PCP Client is configured with its PCP Server(s), it MAY issue an ANNOUNCE OpCode which enclose a CAPABILITY Option. Sending the ANNOUNCE OpCode and the CAPABILITY Option allows the PCP Client to determine whether the PCP Server is alive and also to retrieve its capabilities. Based on the received capabilities, the PCP Client may decide to tune its requests (e.g., Section 4) and decide whether all PCP Servers need to be contacted in parallel or only a subset of them should be contacted.

Upon receipt of a PCP request from a PCP Client requiring the PCP Server to enforce an operation beyond its capabilities, the PCP Server MAY return an error code together with the CAPABILITY option.

When a new PCP Server joins the network then it MAY send an ANNOUNCE OpCode with its capabilities (i.e., CAPABILITY Option).

4. Option Usage

Below are provided examples of the CAPABILITY Option usage:

- In an IPv6 network with NPTv6 [RFC6296], Firewalls implementing the PCP Server are on different devices: the 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. PCP Client learns the PCP Server capabilities using CAPABILITY Option. The PCP Client sends MAP PCP request to PCP-controlled NPTv6 device with Internal Port=0 and Protocol=0 (which means 'all ports for all protocols') to find the external IP address. This PCP request has to be sent only once since NPTv6 is stateless and provides a 1:1 relationship between addresses in the "inside" and "outside" prefixes. The PCP Client will send PCP re-request to NTPv6 only before the Assigned Lifetime of the MAP response expires or when the host embedding the PCP Client acquires a new IPv6 address using "inside" prefix. However PCP Client will send MAP/PEER requests to Firewall to create/delete dynamic outbound mapping or use PCP instead of its default application keep-alives to maintain the Firewall state alive.

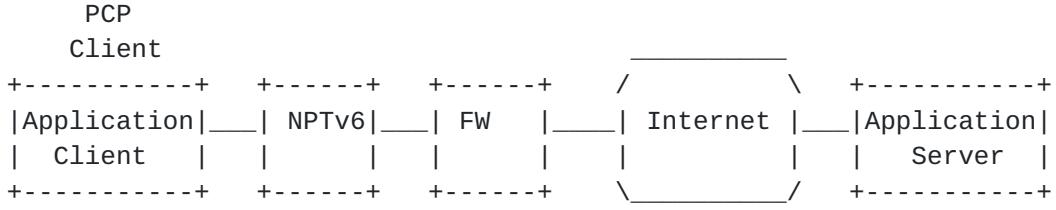


Figure 2: NPTv6 and FW not collocated with PCP server Capability

- In a network with NAT64 [RFC6146], Firewall implementing PCP servers are on different devices: IPv6-only PCP Client can send

PREFIX64 PCP Option [I-D.ietf-pcp-nat64-prefix64] only to the PCP-controlled NAT64 device to learn the Prefix64(s) used to build IPv4-embedded IPv6 addresses.

- Multiple PCP-controlled devices: See Figure 3 the example of a network deploying several techniques to ensure interconnection with IPv4, provide IPv6-only connectivity, etc. Of course, one can argue this configuration is no realistic.

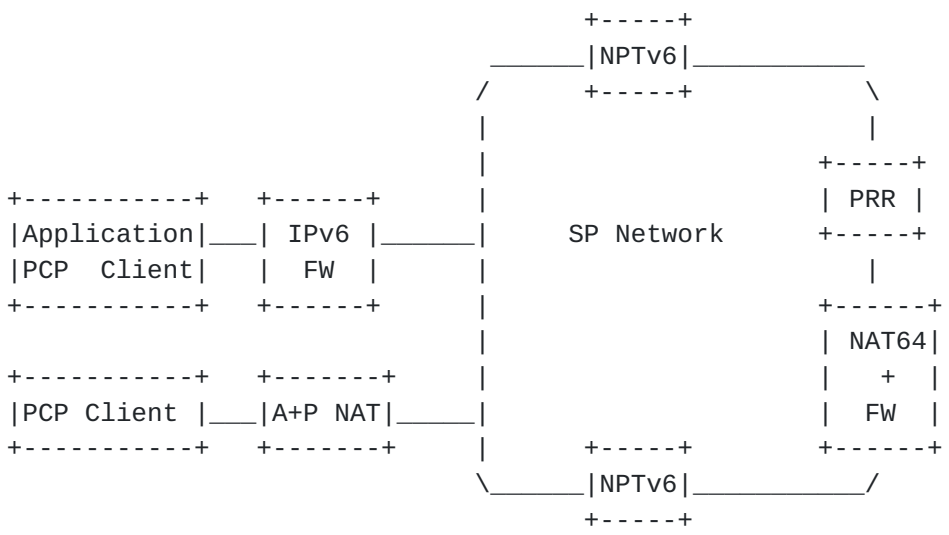


Figure 3: Multiple PCP-controlled devoce

- In a IPv6 network with ILNP translator [RFC6740], Firewall implementing PCP servers are on different devices. PCP client needs to send PCP request only to the PCP-controlled ILNP translator to find Global Locators associated with Internal Locators.
- When the PCP-controlled device is a PRR, the PCP Client should use PORT_SET [I-D.ietf-pcp-port-set] option.

5. Security Considerations

Security considerations discussed in [RFC6887] must be considered.

6. IANA Considerations

The following PCP Option Code is to be allocated in the optional-to-process range (the registry is maintained in http://www.iana.org/assignments/pcp-parameters/pcp-parameters.xml#options):

CAPABILITY

A sub-registry is required to track the set of capabilities of PCP-controlled devices.

7. References

7.1. Normative References

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

[RFC6145] Li, X., Bao, C., and F. Baker, "IP/ICMP Translation Algorithm", RFC 6145, April 2011.

[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.

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

7.2. Informative References

[I-D.ietf-opsawg-firewalls]
Baker, F. and P. Hoffman, "On Firewalls in Internet Security", draft-ietf-opsawg-firewalls-01 (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-09 (work in progress), November 2013.

[I-D.ietf-pcp-nat64-prefix64]
Boucadair, M., "Learning NAT64 PREFIX64s using PCP", draft-ietf-pcp-nat64-prefix64-04 (work in progress), July 2013.

[I-D.ietf-pcp-port-set]
Qiong, Q., Boucadair, M., Sivakumar, S., Zhou, C., Tsou, T., and S. Perreault, "Port Control Protocol (PCP) Extension for Port Set Allocation", draft-ietf-pcp-port-set-04 (work in progress), November 2013.

[I-D.wing-pcp-flowdata]
Wing, D., Penno, R., and T. Reddy, "PCP Flowdata Option", draft-wing-pcp-flowdata-00 (work in progress), July 2013.

[RFC6092] Woodyatt, J., "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service", RFC 6092, January 2011.

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

[RFC6346] Bush, R., "The Address plus Port (A+P) Approach to the IPv4 Address Shortage", RFC 6346, August 2011.

[RFC6740] Atkinson,, RJ., "Identifier-Locator Network Protocol (ILNP) Architectural Description", RFC 6740, November 2012.

Authors' Addresses

Mohamed Boucadair
France Telecom
Rennes 35000
France

Email: mohamed.boucadair@orange.com

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

Email: tireddy@cisco.com