PCP Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 29, 2011

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

April 27, 2011

DHCP and DHCPv6 Options for the Port Control Protocol (PCP)
draft-bpw-pcp-dhcp-04

Abstract

This document specifies DHCP (IPv4 and IPv6) options to configure hosts with Port Control Protocol (PCP) Server addresses. The use of IPv4 DHCP or DHCPv6 depends on the PCP deployment scenario.

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 October 29, 2011.

Copyright Notice

Table of Contents

1. Introduction

This document defines IPv4 DHCP [RFC2131] and DHCPv6 [RFC3315] options which can be used to provision PCP Server [I-D.ietf-pcp-base] reachability information; more precisely it defines DHCP options to convey a Fully Qualified Domain Name (FQDN, as per Section 3.1 of [RFC1035]) of PCP Server(s). In order to make use of these options, this document assumes appropriate name resolution means (see Section 6.1.1 of [RFC1123]) are available on the host client.

The use of IPv4 DHCP or DHCPv6 depends on the PCP deployment scenarios.

2. Terminology

This document makes use of the following terms:

- PCP Server: A functional element which 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 [I-D.ietf-pcp-base].
- PCP Client: a PCP software instance responsible for issuing PCP requests to a PCP Server. Refer to [I-D.ietf-pcp-base].
- DHCP refers to both IPv4 DHCP [RFC2131] and DHCPv6 [RFC3315].
- DHCP client (or client) denotes a node that initiates requests to obtain configuration parameters from one or more DHCP servers [RFC3315].
- DHCP server (or server) refers to a node that responds to requests from DHCP clients [RFC3315].

3. Rationale

Both IP Address and Name DHCP options have been defined in previous versions of this document. This flexibility aims to let service providers to make their own engineering choices and use the convenient option according to their deployment context. Nevertheless, DHC WG's position is this flexibility have some drawbacks such as inducing errors. Therefore, only the Name option is maintained within this document.

This choice of defining the PCP Name option rather than the IP address is motivated by operational considerations: In particular,

some Service Providers are considering two levels of redirection: (1) The first level is national-wise is undertaken by DHCP: a regional-specific FQDN will be returned; (2) The second level is done during the resolution of the regional-specific FQDN to redirect the customer to a regional PCP Servers among a pool deployed regionally. Distinct operational teams are responsible for each of the above mentioned levels. A clear separation between the functional perimeter of each team is a sensitive task for the maintenance of the offered services. Regional teams will require to introduce new resources (e.g., new PCP-controlled devices such as Carrier Grade NATs (CGNs, [I-D.ietf-behave-lsn-requirements])) to meet an increase of customer base. Operations related to the introduction of these new devices (e.g., addressing, redirection, etc.) are implemented locally. Having this regional separation provides flexibility to manage portions of network operated by dedicated teams. This two-level redirection can not be met by the IP Address option.

In addition to the operational considerations:

- The use of the FQDN for NAT64 [I-D.ietf-behave-v6v4-xlate-stateful] might be suitable for load-balancing purposes;

- For the DS-Lite case [I-D.ietf-softwire-dual-stack-lite], if the encapsulation mode is used to send PCP messages, an IP address may be used since the AFTR selection is already done via the AFTR_NAME DHCPv6 option [I-D.ietf-softwire-ds-lite-tunnel-option]. Of course, this assumes that the PCP Server is co-located with the AFTR function. If these functions are not co-located, conveying the FQDN would be more convenient.

If the PCP Server is located in a LAN, a simple FQDN such as "pcp-server.local" can be used.

4. Consistent NAT and PCP Configuration

The PCP Server discovered through DHCP must be able to install mappings on the appropriate upstream PCP-controlled device that will be crossed by packets transmitted by the host or any terminal belonging to the same realm (e.g., DHCP client is embedded in a CP router). In case this prerequisite is not met, customers would experience service troubles and their service(s) won’t be delivered appropriately.

Note that this constraint is implicitly met in scenarios where only one single PCP-controlled device is deployed in the network.

5. DHCPv6 PCP Server Option

This DHCPv6 option conveys a domain name to be used to retrieve the IP addresses of PCP Server(s). Appropriate name resolution queries should be issued to resolve the conveyed name. For instance, in the context of a DS-Lite architecture [I-D.ietf-softwire-dual-stack-lite], the retrieved address may be an IPv4 address or an IPv4-mapped IPv6 address [RFC4291], and in the case of NAT64 [I-D.ietf-behave-v6v4-xlate-stateful] an IPv6 address can be retrieved.

5.1. Format

The format of the DHCPv6 PCP Server option is shown in Figure 1.

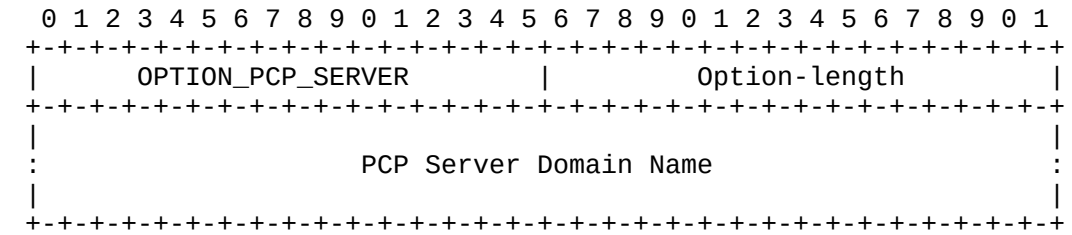

Figure 1: PCP Server FQDN DHCPv6 Option

The fields of the option shown in Figure 1 are as follows:

- Option-code: OPTION_PCP_SERVER (TBA, see Section 9)
- Option-length: Length of the 'PCP Server Domain Name' field in octets.
- PCP Server Domain Name: The domain name of the PCP Server to be used by the PCP Client. The domain name is encoded as specified in Section 8 of [RFC3315]. Any possible future updates to Section 8 of the Section 8 of [RFC3315] also apply to this option.

5.2. Client Behaviour

To discover a PCP Server [I-D.ietf-pcp-base], the DHCPv6 client MUST include an Option Request Option (ORO) requesting the DHCPv6 PCP Server Name option as described in Section 22.7 of [RFC3315] (i.e., include OPTION_PCP_SERVER on its OPTION_ORO). A client MAY also include the OPTION_DNS_SERVERS option on its OPTION_ORO to retrieve a DNS servers list.

If the DHCPv6 client receives more than one OPTION_PCP_SERVER option

from the DHCPv6 server, only the first instance of that option MUST be used.

Upon receipt of an OPTION_PCP_SERVER option, the DHCPv6 client MUST verify that the option length does not exceed 255 octets [RFC1035]). The DHCPv6 client MUST verify the FQDN is a properly encoded as detailed in Section 8 of [RFC3315].

Once the FQDN conveyed in a OPTION_PCP_SERVER option is validated, the included Name is passed to the name resolution library (see Section 6.1.1 of [RFC1123] or [RFC6055]) to retrieve the corresponding IP address (IPv4 or IPv6). If more than one IPv6/IPv4 address are retrieved, the PCP Client MUST use the procedure defined in [I-D.ietf-pcp-base] for address selection.

It is RECOMMENDED to associate a TTL with any address resulting from resolving the Name conveyed in a OPTION_PCP_SERVER DHCPv6 option when stored in a local cache. Considerations on how to flush out a local cache are out of the scope of this document.

5.3. Server Behaviour

A DHCPv6 server MUST NOT reply with a value for the OPTION_PCP_SERVER if the DHCPv6 client has not explicitly included OPTION_PCP_SERVER in its OPTION_ORO.

If OPTION_PCP_SERVER option is requested by the DHCPv6 client, the DHCPv6 server MUST NOT send more than one OPTION_PCP_SERVER option in the response. The DHCPv6 server MUST include only one FQDN in a OPTION_PCP_SERVER option. The DHCPv6 server MUST NOT include an FQDN having a length exceeding 255 octets.

6. IPv4 DHCP PCP Option

6.1. Format

The PCP Server IPv4 DHCP option can be used to configure a FQDN to be used by the PCP Client to contact a PCP Server. The generic format of this option is illustrated in Figure 2.

Because of the depletion of IPv4 DHCP option codes and in order to anticipate future PCP-related IPv4 DHCP options, the proposed option uses a sub-option field.

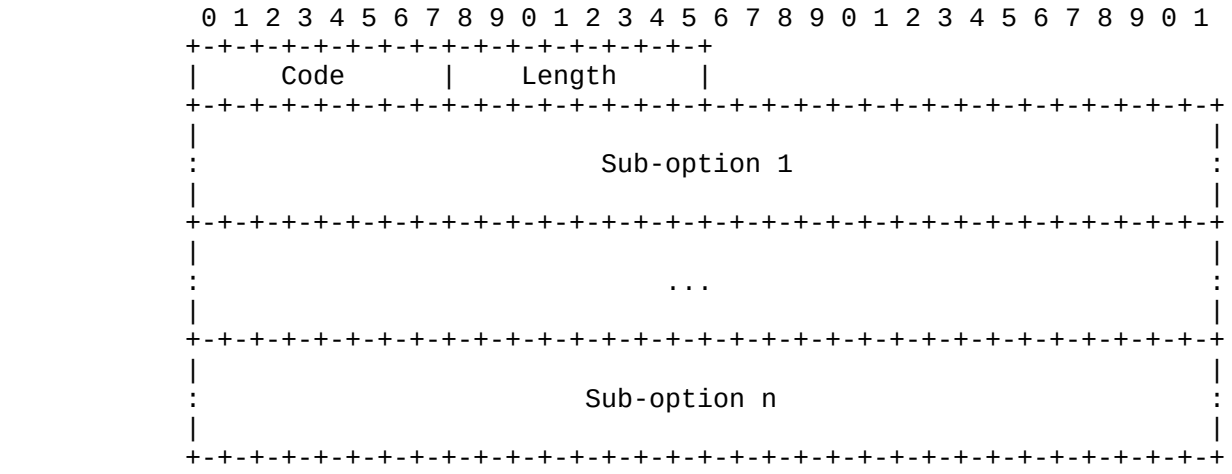

Figure 2: IPv4 DHCP PCP Option

The description of the fields is as follows:

- Code: OPTION_PCP_SERVER (TBA, see Section 9);
- Length: Includes the length of included sub-options in octets; The maximum length is 255 octets.
- One or several sub-options can be included in a PCP IPv4 DHCP option. The format of each sub-option follows the structure shown in Figure 3.

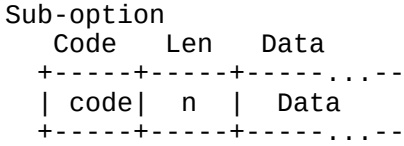

Figure 3: PCP Server sub-option

Only one sub-option is defined in this document:

1: PCP Server Domain Name Sub-option (OPTION_PCP_SERVER_D (Figure 4)). This sub-option includes an FQDN of the PCP Server to be used by the PCP Client when issuing PCP messages.

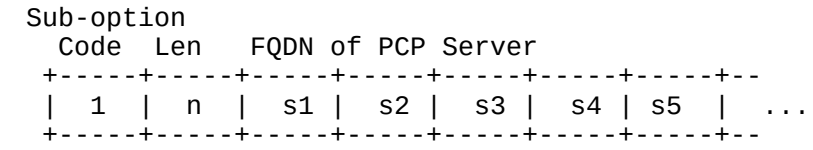

Figure 4: PCP Server FQDN DHCP Sub-option

The fields of the PCP Server Domain Name sub-option shown in Figure 4 are:

- Sub-option Code: 1.
- Len: Length of the "PCP Server Domain Name" field in octets.
- PCP Server Domain Name: The domain name of the PCP Server to be used by the PCP Client. The encoding of the domain name is described in Section 3.1 of [RFC1035].

A side effect of having the sub-option format is the risk to have a large option exceeding the maximum permissible within a single option (254 octets + the length octets). In such case, it is RECOMMENDED to use [RFC3396].

6.2. Server Behaviour

IPv4 DHCP server MUST NOT provide this option, unless the client requested it in Parameter Request List Option.

If OPTION_PCP_SERVER option is requested by the IPv4 DHCP client, the IPv4 DHCP server MUST NOT send more than one OPTION_PCP_SERVER option and more than one OPTION_PCP_SERVER_D sub-option in the response. The IPv4 DHCP server MUST include only one FQDN in a OPTION_PCP_SERVER_D sub-option.

6.3. Client Behaviour

IPv4 DHCP client expresses the intent to get OPTION_PCP_SERVER by specifying it in Parameter Request List Option [RFC2132].

If the IPv4 DHCP client receives more than one OPTION_PCP_SERVER option from the IPv4 DHCP server, only the first instance of that option MUST be used. If the selected OPTION_PCP_SERVER includes more than one OPTION_PCP_SERVER_D sub-option, only the first instance of that option MUST be used.

When the PCP Server Domain Name Sub-option is used, the client

invokes the underlying name resolution library (see Section 6.1.1 of [RFC1123] or [RFC6055]) to retrieve the IPv4 address(es) of the PCP server(s).

7. Dual-Stack Hosts

A PCP Server configured using OPTION_PCP_SERVER over IPv4 DHCP is likely to be resolved to IPv4 address(es).

A PCP Server configured using OPTION_PCP_SERVER over DHCPv6 may be resolved to IPv4 address(es) (e.g., DS-Lite [I-D.ietf-softwire-dual-stack-lite]) or IPv6 address(es) (e.g., NAT64 [I-D.ietf-behave-v6v4-xlate-stateful], IPv6 firewall [RFC6092], NPTv6 [I-D.mrw-nat66]).

In some deployment contexts, the PCP Server may be reachable with an IPv4 address but DHCPv6 is used to provision the PCP Client. In such scenarios, a plain IPv4 address or an IPv4-mapped IPv6 address can be configured to reach the PCP Server.

A Dual-Stack host may receive OPTION_PCP_SERVER via both IPv4 DHCP and DHCPv6. The content of these OPTION_PCP_SERVER options may refer to the same or distinct PCP Servers. This is deployment-specific and as such it is out of scope of this document.

8. Security Considerations

The security considerations in [RFC2131], [RFC3315] and [I-D.ietf-pcp-base] are to be considered.

9. IANA Considerations

Authors of this document request the following DHCPv6 option code:

OPTION_PCP_SERVER

Authors of this document request the following IPv4 DHCP option code:

OPTION_PCP_SERVER

Authors of this document request also to create a sub-option registry for OPTION_PCP_SERVER option; a code for the following sub-option is requested:

OPTION_PCP_SERVER_D

10. Acknowledgements

Many thanks to B. Volz, C. Jacquenet, R. Maglione, D. Thaler and T. Mrugalski for their review and comments.

11. References

11.1. Normative References

[I-D.ietf-pcp-base] Wing, D., Cheshire, S., Boucadair, M., and R. Penno, "Port Control Protocol (PCP)", draft-ietf-pcp-base-09 (work in progress), April 2011.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

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

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3396] Lemon, T. and S. Cheshire, "Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)", RFC 3396, November 2002.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

11.2. Informative References

[I-D.ietf-behave-lsn-requirements] Perreault, S., Yamagata, I., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common requirements for IP address sharing schemes", draft-ietf-behave-lsn-requirements-01 (work in progress), March 2011.

[I-D.ietf-behave-v6v4-xlate-stateful]
Bagnulo, M., Matthews, P., and I. Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", draft-ietf-behave-v6v4-xlate-stateful-12 (work in progress), July 2010.

[I-D.ietf-softwire-ds-lite-tunnel-option]
Hankins, D. and T. Mrugalski, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual- Stack Lite", draft-ietf-softwire-ds-lite-tunnel-option-10 (work in progress), March 2011.

[I-D.ietf-softwire-dual-stack-lite]
Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", draft-ietf-softwire-dual-stack-lite-07 (work in progress), March 2011.

[I-D.mrw-nat66]
Wasserman, M. and F. Baker, "IPv6-to-IPv6 Network Prefix Translation", draft-mrw-nat66-16 (work in progress), April 2011.

[RFC1123] Braden, R., "Requirements for Internet Hosts - Application and Support", STD 3, RFC 1123, October 1989.

[RFC6055] Thaler, D., Klensin, J., and S. Cheshire, "IAB Thoughts on Encodings for Internationalized Domain Names", RFC 6055, February 2011.

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

Authors' Addresses

Mohamed Boucadair
France Telecom
Rennes, 35000
France

Email: mohamed.boucadair@orange-ftgroup.com

Reinaldo Penno
Juniper Networks
1194 N Mathilda Avenue
Sunnyvale, California 94089
USA

Email: rpenno@juniper.net

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

Email: dwing@cisco.com