pcp
Internet-Draft
Intended status: Standards Track
Expires: July 9, 2011

R. Maglione
Telecom Italia
D. Cheng
Huawei Technologies

January 5, 2011

RADIUS Extensions for Port Control Protocol
draft-maglione-pcp-radius-ext-00

Abstract

Port Control Protocol (PCP) provides a mechanism to pre-configure a port on a NAT device, a firewall, etc., so that IP packets of applications initiated from network side can be "port forwarded" to the correct user. PCP is a client-server protocol and the PCP client needs to be provisioned with the FQDN of the server. In a broadband network, customer information is usually stored on a RADIUS server and DHC protocol is used to populate user's configuration information. This memo proposes a new RADIUS attribute to carry the FQDN of a PCP server, such that while the PCP server information is configured on a RADIUS server, the information can be conveyed to NAS via RADIUS protocol, and the co-located DHCP/DHCPv6 server can then populate the information to PCP client.

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 July 9, 2011.

Copyright Notice

Copyright (c) 2011 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.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1. Introduction

Port Control Protocol (PCP) [I-D.ietf-pcp-base] provides a mechanism to control how incoming packets are forwarded by upstream devices such as NATs and firewalls. PCP is a client-server protocol where a PCP client may reside on a host, a CPE, etc., which communicates with a PCP server that may reside anywhere in a network.

A PCP client must know the Fully Qualified Domain Name of a PCP server, before it can communicate with the later in order to perform the relevant functions defined by PCP.

The draft [I-D.bpw-pcp-dhcp] defines DHCPv6 and DHCP options which are meant to be used by a PCP client to discover a PCP server name. However, provisioning for name of the PCP server is required on a DHCP/DHCPv6 server before it can populate these information.

Auto-configuration on a DHCP/DHCPv6 is possible in a broadband network, where typically, user profile is maintained on a RADIUS server and RADIUS protocol [RFC2865] is used to convey user related information to other network elements including a host and CPE. [I-D.ietf-radext-ipv6-access] describes a typical broadband network scenario in which the Network Access Server (NAS) acts as the access gateway for the users (hosts or CPEs) and the NAS embeds a DHCPv6 Server function that allows it to locally handle any DHCPv6 requests issued by the clients.

In such environment, PCP server’s name can be configured on a RADIUS server, which then passes the information to a NAS that co-locates with the DHCP/DHCPv6 server, which in turn populates the location of the PCP server.

This memo defines a new RADIUS attribute that can be used to carry the FQDN of a PCP server.

2. Terminology

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].

The following terms are defined in [I-D.ietf-pcp-base]:

- Port forwarding
- PCP

- PCP client
- PCP Server

3. PCP Server Configuration using RADIUS and DHCP/DHCPv6

Figure 1 illustrates how RADIUS protocol works together with DHCPv6, to allow a user (host or CPE) to learn automatically the FQDN of a PCP server in case of a PPP Session that carries IPv6 traffic.

The Network Access Server (NAS) operates as a client of RADIUS and as DHCPv6 Server for DHCPv6 protocol. The NAS initially sends a RADIUS Access Request message to the RADIUS server, requesting authentication. Once the RADIUS server receives the request, it validates the sending client and if the request is approved, the RADIUS server replies with an Access Accept message including a list of attribute-value pairs that describe the parameters to be used for this session. This list may also contain the name of a PCP server. When the NAS receives a DHCPv6 message containing the PCP Server Option, the NAS shall use the name returned in the RADIUS attribute as defined in this memo to populate the DHCPv6 PCP Server option defined in [I-D.bpw-pcp-dhcp]

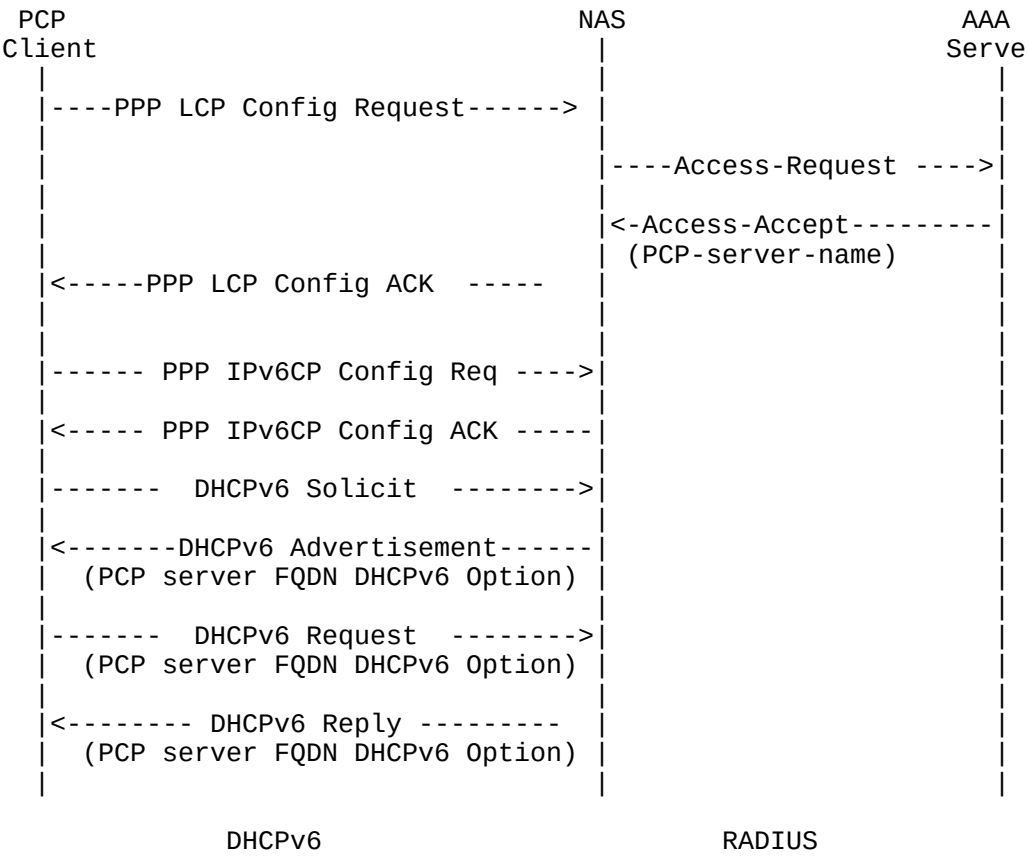


Figure 1: RADIUS and DHCPv6 Message Flow for a PPP Session

The Figure 2 illustrates how the RADIUS protocol and DHCPv6 work together to accomplish PCP client configuration when an IP Session is used to provide connectivity to the user.

The only difference between this message flow and previous one is that in this scenario the interaction between NAS and AAA/ RADIUS Server is triggered by the DHCPv6 Solicit message received by the NAS from the B4 acting as DHCPv6 client, while in case of a PPP Session the trigger is the PPP LCP Config Request message received by the NAS.

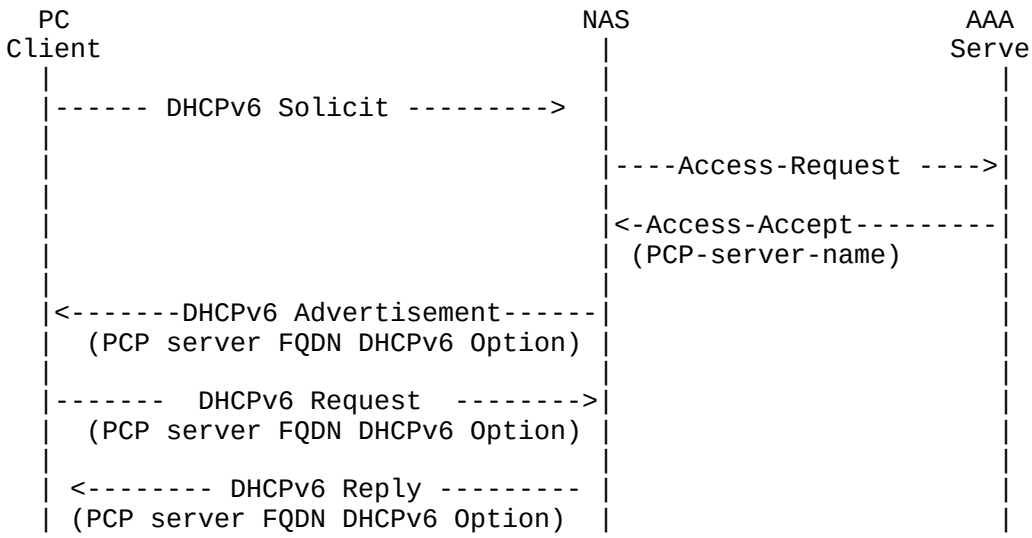


Figure 2: RADIUS and DHCPv6 Message Flow for an IP Session

A similar message flow also applies to the IPv4 scenario when an IP Session is used to provide connectivity to the user (Figure 3).

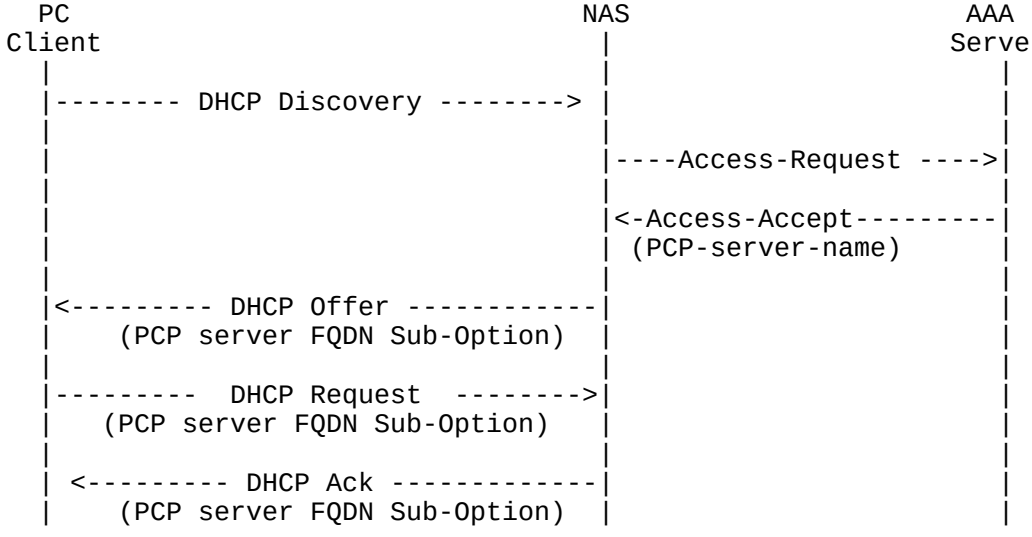


Figure 3: RADIUS and DHCPv4 Message Flow for an IP Session

The scenario with PPP Session and IPv4 only connectivity does not require the DHCP protocol: the whole configuration of the client is performed by PPP. This case is out of scope of this document because in order to complete the configuration of the PCP client a new PPP IPC option would be required.

4. RADIUS Attribute

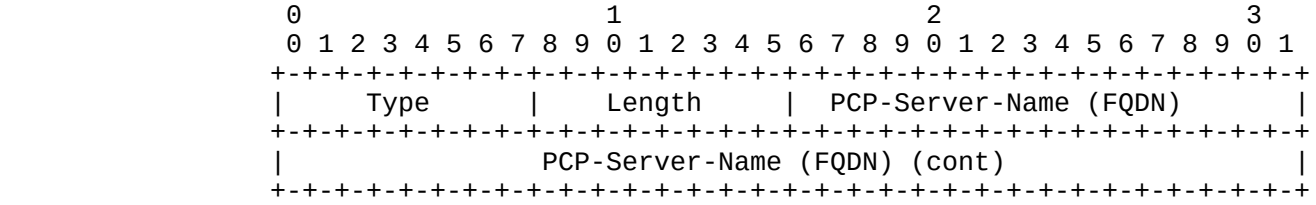
A new RADIUS attribute, called PCP-Server-Name, along with its format is defined below.

Description

The PCP-server-name attribute contains a Fully Qualified Domain Name (FQDN) that refers to a PCP server the client requests to establish a connection to for PCP related service. The NAS shall use the name returned in the RADIUS PCP-server-name attribute to populate the PCP Server FQDN DHCP Sub-Option in IPv4 addressing context, or the PCP Server FQDN DHCPv6 Option in IPv6 addressing context, as determined by the DHCP server [I-D.bpw-pcp-dhcp]

The PCP-server-name attribute MAY appear in an Access-Accept packet, and may also appear in an Accounting-Request packet. In either case, the attribute MUST NOT appear more than once in a single packet. The PCP-server-name MUST NOT appear in any other RADIUS packets.

A summary of the PCP-Server-Name RADIUS attribute format is shown below. The fields are transmitted from left to right.



Type:

TBA1 for PCP-Server-Name.

Length:

This field indicates the total length in octets of this attribute including the Type, the Length fields and the length in octets of the PCP-Server-Name field

PCP-Server-Name:

A single Fully Qualified Domain Name of the PCP-Server. The domain name is encoded as specified in [RFC1035]

5. Table of attributes

The following table provides a guide to which attributes may be found in which kinds of packets, and in what quantity.

Request	Accept	Reject	Challenge	Accounting Request	#	Attribute
0-1	0-1	0	0	0-1	TBA1	PCP-Server-Name

The following table defines the meaning of the above table entries.

0 This attribute MUST NOT be present in packet.
0+ Zero or more instances of this attribute MAY be present in packet.
0-1 Zero or one instance of this attribute MAY be present in packet.

6. Security Considerations

This document has no additional security considerations beyond those already identified in [RFC2865].

7. IANA Considerations

This document requests the allocation of a new Radius attribute types from the IANA registry "Radius Attribute Types" located at http://www.iana.org/assignments/radius-types

PCP-Server-Name - TBA1

8. Normative References

[I-D.bpw-pcp-dhcp]
Boucadair, M., Penno, R., and D. Wing, "DHCP and DHCPv6 Options for Port Control Protocol (PCP)", draft-bpw-pcp-dhcp-00 (work in progress), October 2010.

[I-D.ietf-pcp-base]
Wing, D., "Port Control Protocol (PCP)", draft-ietf-pcp-base-02 (work in progress), January 2011.

[I-D.ietf-radext-ipv6-access]

Lourdelet, B., Dec, W., Sarikaya, B., Zorn, G., and D. Miles, "RADIUS attributes for IPv6 Access Networks", draft-ietf-radext-ipv6-access-02 (work in progress), July 2010.

[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.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

Authors' Addresses

Roberta Maglione
Telecom Italia
Via Reiss Romoli 274
Torino 10148
Italy

Phone:
Email: roberta.maglione@telecomitalia.it

Dean Cheng
Huawei Technologies
2330 Central Expressway
Santa Clara, CA 95050
USA

Phone: +1 408 330 4754
Fax:
Email: Chengd@huawei.com
URI: