PCP WG
Internet-Draft
Intended status: Standards Track
Expires: November 25, 2013

R. Maglione
Cisco Systems
D. Cheng
Huawei Technologies
M. Boucadair
France Telecom

May 24, 2013

RADIUS Extensions for Port Control Protocol (PCP)
draft-maglione-pcp-radius-ext-08

Abstract

This document specifies a new Remote Authentication Dial In User Service (RADIUS) attribute to carry a Port Control Protocol (PCP) Server Names. This attribute can be configured on a RADIUS server so that the information can be conveyed to Network Access Server (NAS) via RADIUS protocol, and the co-located Dynamic Host Configuration Protocol (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 November 25, 2013.

Copyright Notice

Table of Contents

1. Introduction 2
2. Terminology 3
3. PCP Server Configuration using RADIUS and DHCPv4/DHCPv6 . . . 4
4. PCP-Server-Name RADIUS Attribute 7
5. Table of attributes 9
6. Security Considerations 9
7. IANA Considerations 9
8. Acknowledgments 9
9. References 9
9.1. Normative References 9
9.2. Informative References 10
Authors' Addresses 10

1. Introduction

Port Control Protocol (PCP) [RFC6887] 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 Customer Premises Equipment (CPE), etc., which communicates with a PCP server that may reside anywhere in a network.

[RFC6887] defines a procedure for the PCP client to communicate with its PCP Server. The IP address of the PCP Server(s) can be configured to the PCP client; if not the PCP client assumes its default router as being its PCP server.

[I-D.ietf-pcp-dhcp] defines DHCPv6 and DHCPv4 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 DHCPv4/ DHCPv6 server before it can populate this information.

Auto-configuration on a DHCPv4/DHCPv6 is possible in a broadband network, where typically, user profile is maintained on a Remote Authentication Dial In User Service (RADIUS) server and RADIUS protocol [RFC2865] is used to convey user-related information to other network elements including a host and CPE. [RFC6911] 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 DHCPv4/DHCPv6 server, which in turn populates the location of the PCP server.

This document defines a new RADIUS attribute that can be used to carry a PCP server name. As defined in [I-D.ietf-pcp-dhcp], a PCP Server Name can be a DNS name, IP literals strings, etc. This document is designed to allow for configuring PCP Server name which can be a DNS name, IP literals or any strings which may be passed to a local name resolution library on the PCP client side. Multiple occurrences of the PCP server name RADIUS attribute is supported.

The proposed RADIUS attribute is designed to accommodate various deployment contexts (e.g., dedicated option per IP connectivity context, single option for dual-stack access, etc.).

The approach described above is already used for providing the FQDN of the AFTR in the DS-Lite scenario [RFC6333] and the equivalent RADIUS attribute for the DS-Lite Tunnel Name is defined [RFC6519].

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 [RFC6887]:

- Port forwarding
- PCP
- PCP client
- PCP Server

The following term is defined in [I-D.ietf-pcp-dhcp]:

- PCP Server Name

3. PCP Server Configuration using RADIUS and DHCPv4/DHCPv6

Figure 1 illustrates an example of how RADIUS protocol works together with DHCPv6, to allow a host to learn automatically the name 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 co-locates with a DHCPv6 Server for DHCPv6. 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 co-located DHCPv6 server receives a DHCPv6 message from a client containing the PCP Server Option, it 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.ietf-pcp-dhcp].

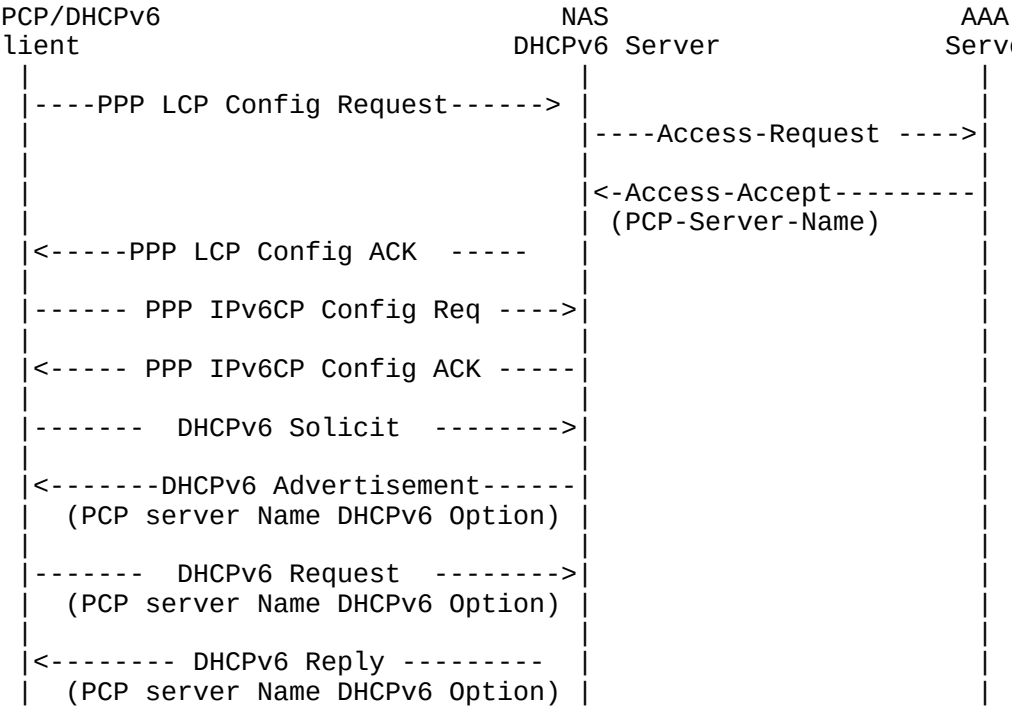


Figure 1: RADIUS and DHCPv6 Message Flow for a PPP Session

The Figure 2 illustrates how the RADIUS protocol and DHCPv6 work together to accomplish PCP client configuration when DHCPv6 is used to provide connectivity to a requesting host.

The 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 DHCPv6 client, while in case of a PPP Session the trigger is the PPP LCP Config Request message received by the NAS.

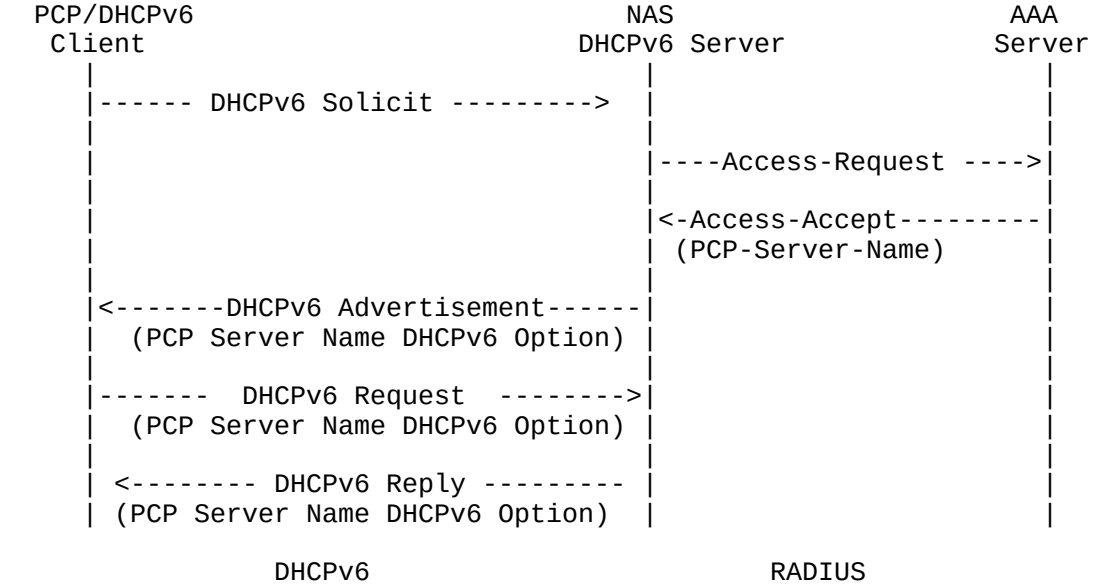


Figure 2: RADIUS and DHCPv6 Message Flow for an IP Session

In the scenario depicted in Figure 2 the Access-Request packet SHOULD contain a Service-Type attribute (6) with the value Authorize Only (17); thus, according to [RFC5080], the Access-Request packet MUST contain a State attribute that it obtains from the previous authentication process.

In both scenaiors mentioned above, Message-Authenticator (type 80) according to [RFC2869] SHOULD be used to protect both Access-Request and Access-Accept Messages.

In case that the PCP server name is re-configured, the RADIUS server must send a RADIUS CoA message [RFC5176] that carries the RADIUS PCP server name attribute to the NAS, which once accepts and sends back a RADIUS CoA ACK message, the new PCP server name replaces the original one and is then re-propulated by the DHCPv6 server.

A similar message flow also applies to the IPv4 scenario when DHCPv4 is used to provide connectivity to the user (Figure 3).

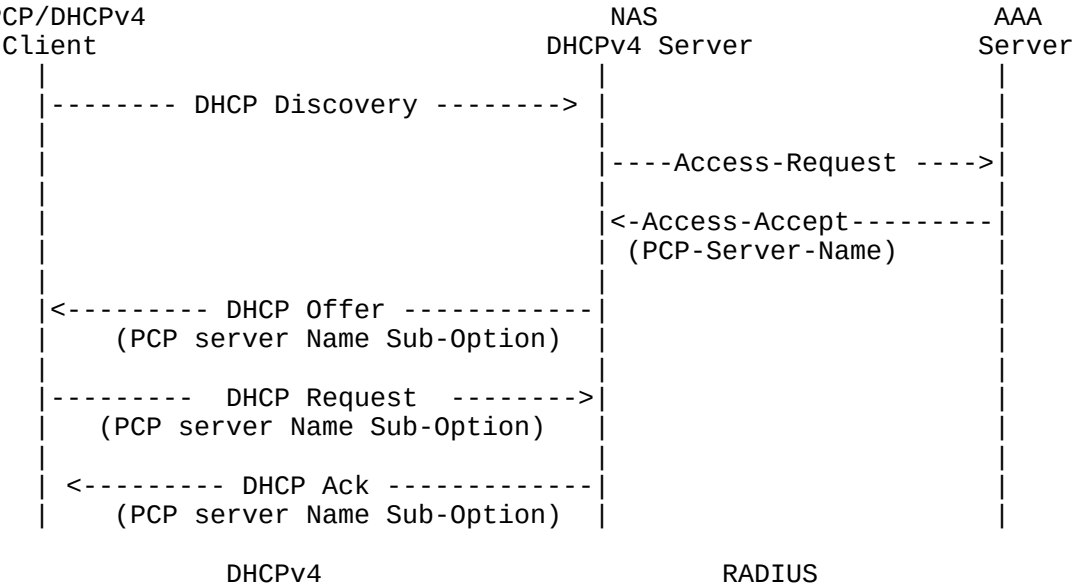


Figure 3: RADIUS and DHCPv4 Message Flow for an IP Session

After receiving the PCP server name in the initial Access-Accept the NAS MUST store the received PCP Server Name locally. When the PCP Client sends a DHCPv4 message to request an extension of the lifetimes for the assigned address or prefix, the NAS does not have to initiate a new Access-Request towards the AAA server to request the PCP server name. The NAS retrieves the previously stored PCP Server name and uses it in its reply.

If the DHCPv4 server to which the DHCP Renew message was sent at time T1 has not responded, the DHCPv4 client initiates a Rebind/Reply exchange with any available server. In this scenario the NAS MUST initiate a new Access-Request towards the AAA server, after the co-located DHCPv4 server receives the DHCP message. The NAS MAY include the PCP Server Name attribute in its Access-Request.

If the NAS does not receive the PCP server name attribute in the Access-Accept it MAY fallback to a pre-configured default tunnel name, if any. If the NAS does not have any pre-configured default tunnel name or if the NAS receives an Access-Reject, the PCP client can not be configured by the NAS.

The handling when the PCP server name is re-configured on the RADIUS server is similar to that in IPv6 case, i.e., the new PCP server name is conveyed to the NAS in a RADIUS CoA message, which if accepted, the new PCP server name replaces the original one and is then re-propulated by the DHCPv4 server.

The scenario with PPP Session and IPv4 only connectivity does not require DHCPv4: 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 IPCP option would be required.

4. PCP-Server-Name RADIUS Attribute

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

The PCP-Server-Name attribute contains a name that refers to a PCP server the client requests to establish a connection to for PCP related service. The NAS shall use the name(s) returned in the RADIUS PCP-Server-Name attribute instance(s) to populate the PCP Server Name DHCP Sub-Option in IPv4 addressing context, or the PCP Server Name DHCPv6 Option in IPv6 addressing context, as determined by the DHCP server [I-D.ietf-pcp-dhcp]. The same or distinct PCP Server Names MAY be configured; it is out of scope of this document to elaborate on this point. Nevertheless, the PCP-Server-Name attribute conveys an indication for the deployment context.

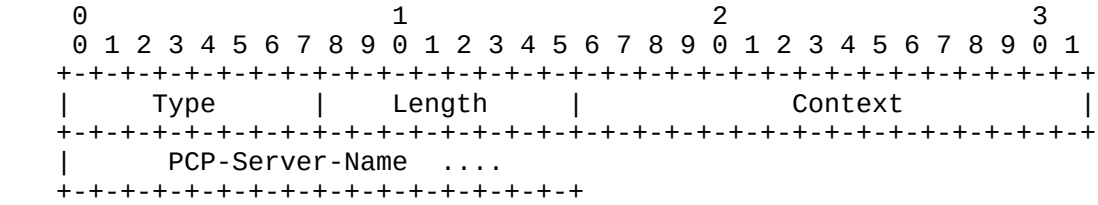
The PCP-Server-Name attribute MAY appear in an Access-Accept packet. This attribute MAY be used in Access-Request packets as a hint to the RADIUS server; for example if the NAS is pre-configured with a default PCP server name, this name MAY be inserted in the attribute. The RADIUS server MAY ignore the hint sent by the NAS and it MAY assign a different PCP Server name. If the NAS includes the PCP Server Name attribute, but the AAA server does not recognize it, this attribute MUST be ignored by the AAA Server. If the NAS does not receive PCP Server Name attribute in the Access-Accept it MAY fallback to a pre-configured default PCP server name, if any. If the NAS is pre-provisioned with a default PCP server name and the PCP server name received in Access-Accept is different from the configured default, then the PCP server name received in the Access-Accept message MUST be used for the session.

The PCP server Name RADIUS attribute MAY be present in Accounting-Request records where the Acct-Status-Type is set to Start, Stop or Interim-Update.

The PCP server name RADIUS attribute MAY be present in an CoA-Request packet, when the PCP server name is re-configured.

The PCP Server Name RADIUS attribute MAY appear more than once in a message.

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



The description of the fields is as follows:

Type:

TBA1 for PCP-Server-Name.

Length:

This field indicates the total length in octets of this attribute including the Type, the Length fields.

Context:

This field indicates the IP connectivity context:

0: Dual-Stack. The same option is provided for both DHCPv4 and DHCPv6 requesting hosts.
1: This option is provided for DHCPv4 requesting hosts.
2: This option is provided for DHCPv6 requesting hosts.

PCP-Server-Name:

Includes a PCP Server Name. As defined in , PCP Server Name is a UTF-8 [RFC3629] string that can be passed to getaddrinfo(), such as a DNS name, address literals, etc. The name MUST NOT contain spaces or nulls.

This attribute is type of complex [RFC6158].

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+	0+	0	0	0+	TBA1	PCP-Server-Name
0-1	0-1	0	0	0-1	6	Service-Type
0-1	0-1	0-1	0-1	0-1	80	Message-Authenticator

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. Acknowledgments

The authors would like to thank Mario Ullio, Alan Dekok, Sheng Jiang and Tassos Chatzithomaoglou for their valuable comments and assistance.

9. References

9.1. Normative References

[I-D.ietf-pcp-dhcp]
Boucadair, M., Penno, R., and D. Wing, "DHCP Options for the Port Control Protocol (PCP)", draft-ietf-pcp-dhcp-07 (work in progress), March 2013.

[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.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

[RFC5080] Nelson, D. and A. DeKok, "Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes", RFC 5080, December 2007.

[RFC6158] DeKok, A. and G. Weber, "RADIUS Design Guidelines", BCP 158, RFC 6158, March 2011.

[RFC6519] Maglione, R. and A. Durand, "RADIUS Extensions for Dual-Stack Lite", RFC 6519, February 2012.

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

9.2. Informative References

[RFC2869] Rigney, C., Willats, W., and P. Calhoun, "RADIUS Extensions", RFC 2869, June 2000.

[RFC5176] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 5176, January 2008.

[RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", RFC 6333, August 2011.

[RFC6911] Dec, W., Sarikaya, B., Zorn, G., Miles, D., and B. Lourdelet, "RADIUS Attributes for IPv6 Access Networks", RFC 6911, April 2013.

Authors' Addresses

Roberta Maglione
Cisco Systems
181 Bay Street
Toronto, ON M5J 2T3
Canada

Email: 'robmgl@cisco.com'

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

Phone: +1 408 330 4754
Email: dean.cheng@huawei.com

Mohamed Boucadair
France Telecom
Rennes 35000
France

Email: mohamed.boucadair@orange.com