DHC Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 30, 2014

L. Yeh
Freelancer Technologies
M. Boucadair
France Telecom
July 29, 2013

RADIUS Option for DHCPv6 Relay Agent
draft-ietf-dhc-dhcpv6-radius-opt-14

Abstract

The DHCPv6 RADIUS option provides a mechanism to exchange authorization and identification information between DHCPv6 relay agent and DHCPv6 server. This architecture assumes that the Network Access Server(NAS) acts as both DHCPv6 relay agent and RADIUS client. When receiving messages from the DHCPv6 clients, the NAS consults the RADIUS server and adds the RADIUS response when forwarding the DHCPv6 client's messages to the DHCPv6 server. The DHCPv6 server then uses that additional information to generate appropriate response to the DHCPv6 client's requests.

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 January 30, 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

DHCPv6 provides a mechanism that allows the server to assign or delegate both stateful and stateless configuration parameters to the clients. The stateful configuration parameters include IPv6 address [RFC3315] and IPv6 prefix [RFC3633]. The stateless configuration parameters [RFC3736] include, for example, DNS [RFC3646], or a FQDN of AFTR [RFC6334]. In the scenarios described in this document, the DHCPv6 server is deployed in the central part of an ISP network.

RADIUS [RFC2865] is widely used as the centralized authentication, authorization and user management mechanism for service provision in Broadband access network. [RFC3162], [RFC4818], [RFC6519] and [RFC6911] specified the attributes that support the service provision for IPv6-only and IPv6-transition access. The RADIUS server authorizes the Network Access Server (NAS) to assign an IPv6 address or prefix from the indicated pool, or to assign an IPv6 address or prefix with an explicitly indicated value, and other configuration parameters as per the attributes for the subscribers.

When the NAS acts as distributed DHCPv6 server and RADIUS client simultaneously, it communicates with RADIUS server after receiving request from DHCPv6 client. Upon receiving the Access-Accept message from the RADIUS server, the NAS then responds to the DHCPv6 client's requests per the associated authorization information indicated by the RADIUS attributes in the Access-Accept message. When NAS acts as DHCPv6 relay agent and RADIUS client simultaneously, and the centralized DHCPv6 server is co-located with the RADIUS server, they may share the same database of the users; but when the centralized DHCPv6 server is not located in the same place as the RADIUS server, a new communication mechanism is needed for the DHCPv6 relay agent to transfer the authorization information indicated by the RADIUS attributes to the DHCPv6 server.

2. Terminology and Language

This document specifies a new DHCPv6 option for the DHCPv6 Relay Agent to transfer the authorization information of RADIUS attributes received in the Access-Accept message from the RADIUS server to the centralized DHCPv6 server. Definitions for terms and acronyms not specified in this document are defined in [RFC2865] and [RFC3315].

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. Network Scenarios

Figure 1 and Figure 2 show the typical network scenarios where the communication mechanism introduced in this document is necessary. In these scenarios, the centralized DHCPv6 server is not co-located with the RADIUS server, but both of them are in the same administrative domain. The NAS acts as the DHCPv6 relay agent and the RADIUS client simultaneously. Figure 1 shows the sequence of DHCPv6 and RADIUS messages for IP over Ethernet (IPoE) access model, when the access loop adopts the direct Ethernet encapsulation. Figure 2 shows the sequence of DHCPv6 and RADIUS messages for PPP over Ethernet (PPPoE) access model.

The mechanism introduced in this document is a generic mechanism, and might also be employed in other network scenarios where the DHCPv6 relay agent and the RADIUS client locate in the same device.

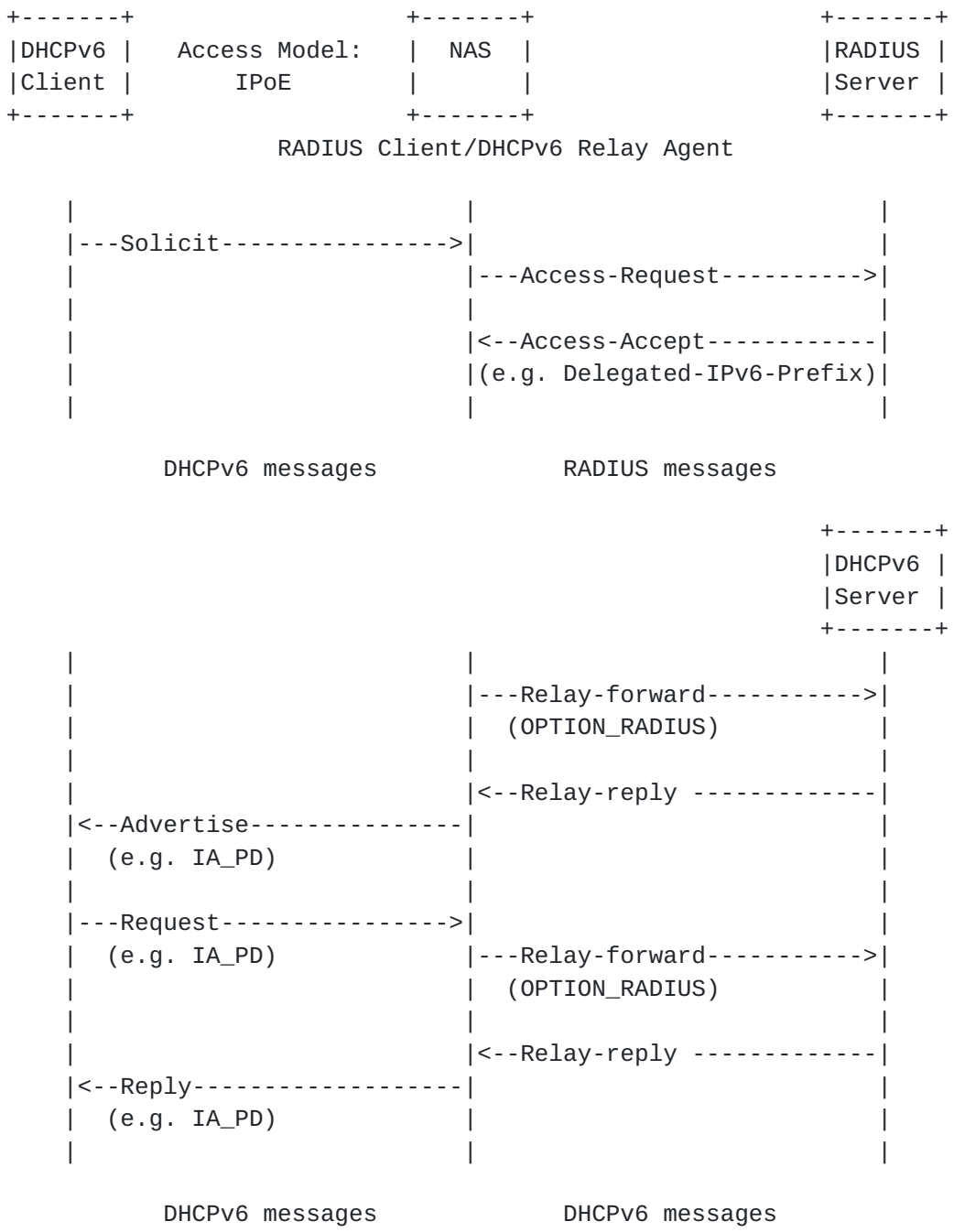


Figure 1: Network scenario and message sequence when employing DHCPv6 RADIUS option in IPoE access

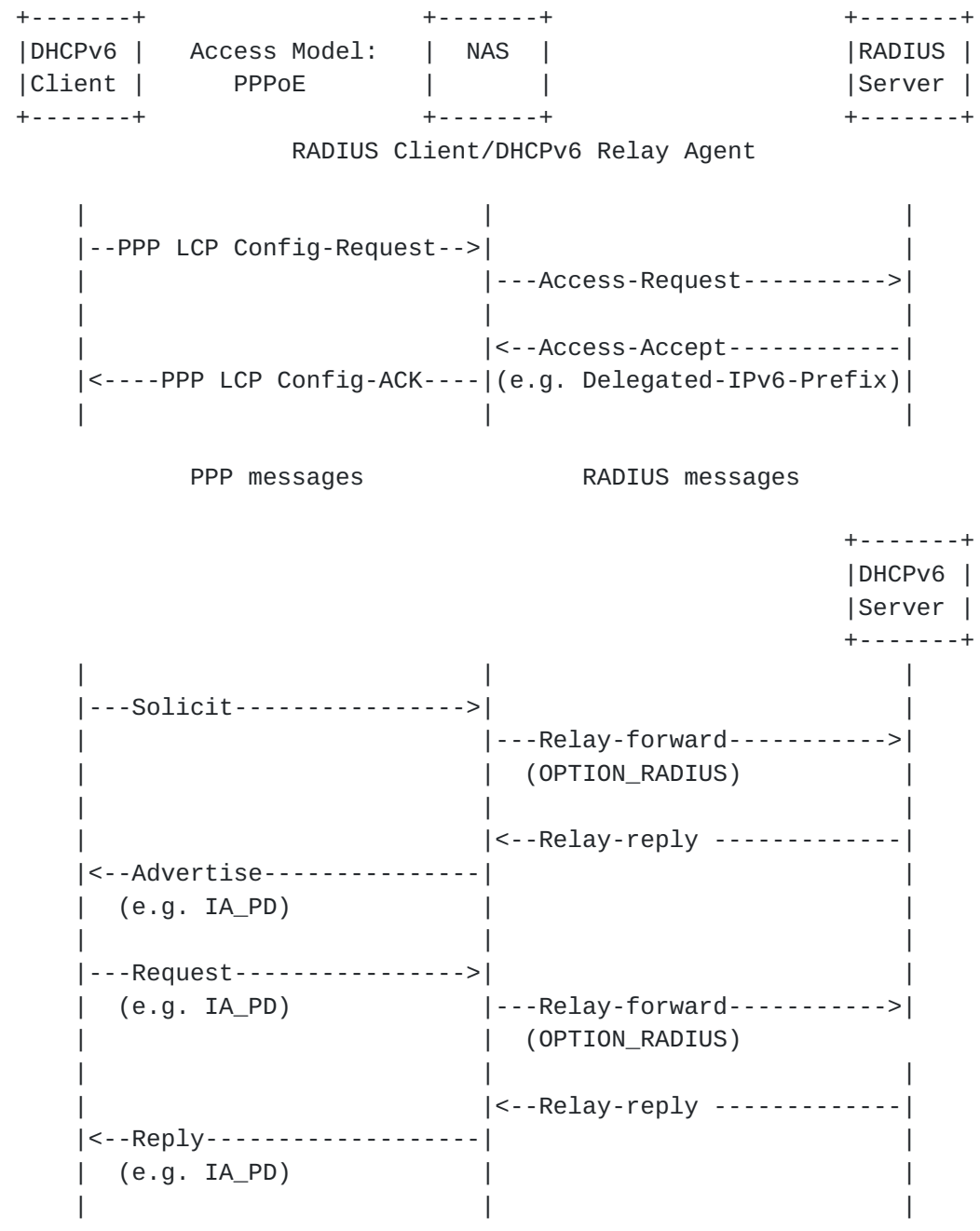


Figure 2: Network scenario and message sequence when employing DHCPv6 RADIUS option in PPPoE access

If the authentication or the authorization through RADIUS fails, the associated message sequences will stop. The NAS acting as the DHCPv6 relay agent will not forward the message received from the client to the DHCPv6 server. If the authentication or the authorization through RADIUS passes, the NAS MUST store the information indicated

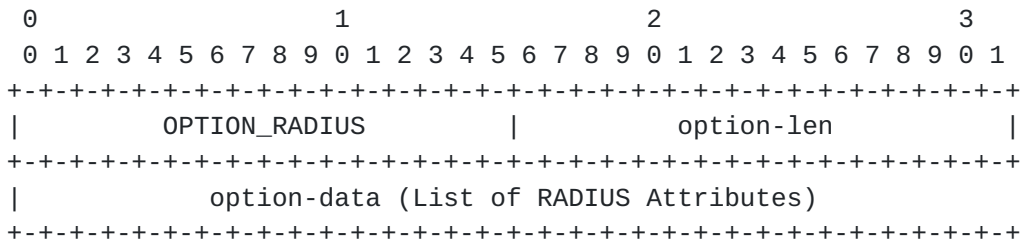
in the RADIUS attributes received in the Access-Accept message from the RADIUS server during the whole session. How the NAS manages these information during the RADIUS session is out of the scope of this document.

After receiving RENEW (5) message from the DHCPv6 client, the NAS SHOULD NOT initiate a new Access-Request/Access-Accept message exchange with the RADIUS server. After receiving REBIND (6) message from the DHCPv6 client, the NAS MUST initiate a new Access-Request/ Access-Accept message exchange with the RADIUS server, unless RADIUS capability is disabled on the NAS.

4. DHCPv6 RADIUS option

The OPTION_RADIUS is a DHCPv6 option used by the DHCPv6 relay agent to carry the authorization information of RADIUS attributes received in the Access-Accept message from the RADIUS server.

The format of the OPTION_RADIUS option is defined as follows:



option-code TBD
option-len Length of the option-data in octets
option-data List of one or more RADIUS attributes

The option-data of OPTION_RADIUS is a list of one or more RADIUS attributes received in the Access-Accept message from the RADIUS server. The format of RADIUS attributes is defined in section 5 of [RFC2865] as well as sections 2.1 and 2.2 of [RFC6929]. If multiple attributes with the same type (including the Long Extended type defined in sections 2.2 of [RFC6929]) are present, the order of attributes with the same type MUST be the same as that received from the RADIUS server. The OPTION_RADIUS can only contain the RADIUS attributes listed in the IANA Registry of 'RADIUS attributes permitted in DHCPv6 RADIUS option'.

According to the network scenarios described in section 3, the OPTION_RADIUS should appear in the RELAY-FORW (12) message relaying SOLICIT (1), REQUEST (3) and REBIND (6) from the DHCPv6 client, and may appear in the RELAY-FORW (12) relaying any other message from the

DHCPv6 client.

4.1. RADIUS attributes permitted in DHCPv6 RADIUS option

The RADIUS attributes listed in the below table are recommended as the first batch of attributes in the IANA Registry of 'RADIUS attributes permitted in DHCPv6 RADIUS option'. New RADIUS attributes can be added to this list after Expert Review [RFC5226].

Type Code	Attribute	Reference
26	Vendor-Specific	[RFC2865]
123	Delegated-IPv6-Prefix	[RFC4818]
144	DS-Lite-Tunnel-Name	[RFC6519]
168	Framed-IPv6-Address	[RFC6911]
169	DNS-Server-IPv6-Address	[RFC6911]
171	Delegated-IPv6-Prefix-Pool	[RFC6911]
172	Stateful-IPv6-Address-Pool	[RFC6911]

Note: The RADIUS attribute's 'Length' defined in section 5 of [RFC2865] includes the length of 'Type' and 'Length' fields.

5. DHCPv6 Relay Agent Behavior

If the Relay Agent is configured to send OPTION_RADIUS, and the Access-Accept message from the RADIUS server contained RADIUS attributes permitted for use in OPTION_RADIUS, the Relay Agent MUST include OPTION_RADIUS in the RELAY-FORW (12) message. The DHCPv6 relay agent includes the permitted RADIUS attributes into OPTION_RADIUS one by one; if multiple attributes with the same type are present, the order of attributes with the same type MUST be the same as that received from the RADIUS server.

6. DHCPv6 Server Behavior

Upon receipt of the RELAY-FORW (12) message with OPTION_RADIUS from a relay agent, the DHCPv6 server that supports OPTION_RADIUS SHOULD extract and interpret the RADIUS attributes in the OPTION_RADIUS, and use that information in selecting configuration parameters for the requesting client. If the DHCPv6 server does not support OPTION_RADIUS, the DHCPv6 server MUST silently discard this option.

7. DHCPv6 Client Behavior

OPTION_RADIUS is only exchanged between the relay agents and the servers. DHCPv6 clients are not aware of the usage of OPTION_RADIUS.

DHCPv6 client MUST NOT send OPTION_RADIUS, and MUST ignore OPTION_RADIUS if received.

8. Security Considerations

Known security vulnerabilities of the DHCPv6 and RADIUS protocol may apply to its options. Security issues related with DHCPv6 are described in section 23 of [RFC3315]. Security issues related with RADIUS are described in section 8 of [RFC2865], section 5 of [RFC3162], section 11 of [RFC6929].

The mechanism described in this document may introduce new attack vector against the DHCPv6 server in case the DHCPv6 relay agent is compromised. By forging the RADIUS attributes contained in the OPTION_RADIUS of the RELAY-FORW (12) messages, the attacker may influence the parameter assignment on the DHCPv6 server for the DHCPv6 clients. However, as those network scenarios described in the section 3, NAS always belongs to the same administrative domain of the DHCPv6 server in the real deployment.

Network administrators should be aware that although RADIUS messages are encrypted, DHCPv6 messages are always not encrypted. It is possible that some RADIUS vendor-specific attributes might contain the sensitive or confidential information. Network administrators are strongly advised to prevent including such information into DHCPv6 messages.

If the use of vendor-specific attributes with confidential content is required, administrators are advised to use IPsec with encryption to protect the confidentiality of the RADIUS attributes. Relay agents and servers implementing this specification MUST support the use of IPsec ESP with encryption in transport mode according to section 3.1.1 of [RFC4303] and section 21.1 of [RFC3315].

9. IANA Considerations

This document requests to assign a new DHCPv6 option code for OPTION_RADIUS defined in section 4, and to create a new registry on the same assignment page, which is entitled as 'RADIUS attributes permitted in DHCPv6 RADIUS option' defined in section 4.1. The new registry will enumerate the RADIUS Attributes Types (http://www.iana.org/assignments/radius-types/radius-types.xml) that are permitted to be included in the DHCPv6 RADIUS option. The allocation policy of this 'RADIUS attributes permitted in DHCPv6 RADIUS option' registry is Expert Review [RFC5226]. Designated expert should carefully consider the security implications of

allowing the relay agent to include new RADIUS attribute for the addition to this registry.

10. Acknowledgements

Thanks to Tomek Mrugalski, Bernie Volz, Gaurav Halwasia and Roberta Maglione for their thorough review comments in the mailing list of DHC working group, to Ted Lemon for his continuous encouragement and technical guidance.

11. References

11.1. Normative References

[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.

[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.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC4818] Salowey, J. and R. Droms, "RADIUS Delegated-IPv6-Prefix Attribute", RFC 4818, April 2007.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

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

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

[RFC6929] DeKok, A. and A. Lior, "Remote Authentication Dial In User Service (RADIUS) Protocol Extensions", RFC 6929, April 2013.

11.2. Informative References

[RFC3162] Aboba, B., Zorn, G., and D. Mitton, "RADIUS and IPv6", RFC 3162, August 2001.

[RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.

[RFC3646] Droms, R., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, December 2003.

[RFC3736] Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, April 2004.

[RFC6334] Hankins, D. and T. Mrugalski, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite", RFC 6334, August 2011.

Authors' Addresses

Leaf Y. Yeh
Freelancer Technologies
P. R. China

Email: leaf.yeh.sdo@gmail.com

Mohamed Boucadair
France Telecom
France

Email: mohamed.boucadair@orange.com