DHC Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 29, 2013

L. Yeh
Freelancer Technologies
M. Boucadair
France Telecom

February 25, 2013

RADIUS Option for DHCPv6 Relay Agent on the Broadband Access Servers
draft-ietf-dhc-dhcpv6-radius-opt-09

Abstract

The DHCPv6 RADIUS option provides a mechanism to exchange authorization and identification information between the DHCPv6 relay agent and the DHCPv6 server. This mechanism is meant for the centralized DHCPv6 server to select the right configuration for the requesting DHCPv6 client based on the authorization information received from the RADIUS server, which is not co-located with the DHCPv6 server. The Network Access Server (NAS) acts as DHCPv6 relay agent and RADIUS client simultaneously in this document.

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 August 29, 2013.

Copyright Notice

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], IPv6 prefix [RFC3633], etc. 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 the service provision in Broadband access network. [RFC3162], [RFC4818], [RFC6519] and [I-D.ietf-radext-ipv6-access] specified attributes that support the service provision for IPv6-only and IPv6-transition access. 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.

These mechanisms work well in the deployment scenarios where the NAS acts as the distributed DHCPv6 server. In that case the NAS directly responds the DHCPv6 messages as per the indication conveyed by the attributes in the Access-Accept message from the RADIUS server. These mechanisms might also work well in the scenario where the centralized DHCPv6 server is co-located with the RADIUS server, where they can share the same database of the users. But when the NAS acts as the relay agent and RADIUS client simultaneously, and the centralized DHCPv6 server is not located in the same place as the RADIUS server, a new communication mechanism is needed for the 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 keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in BCP 14, [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.

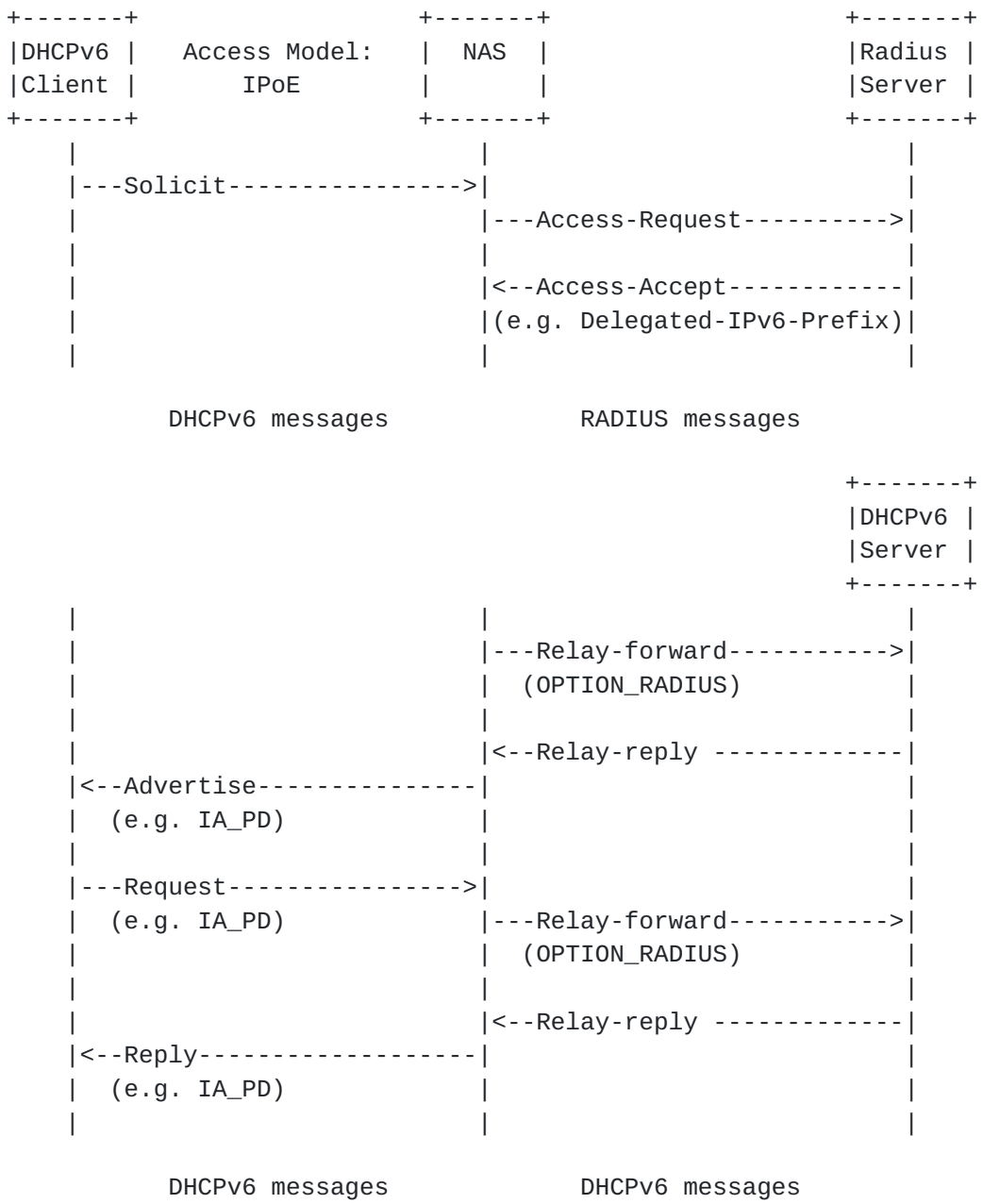


Figure 1: Network scenario and message sequence when employing DHCPv6 RADIUS option in IPoE access

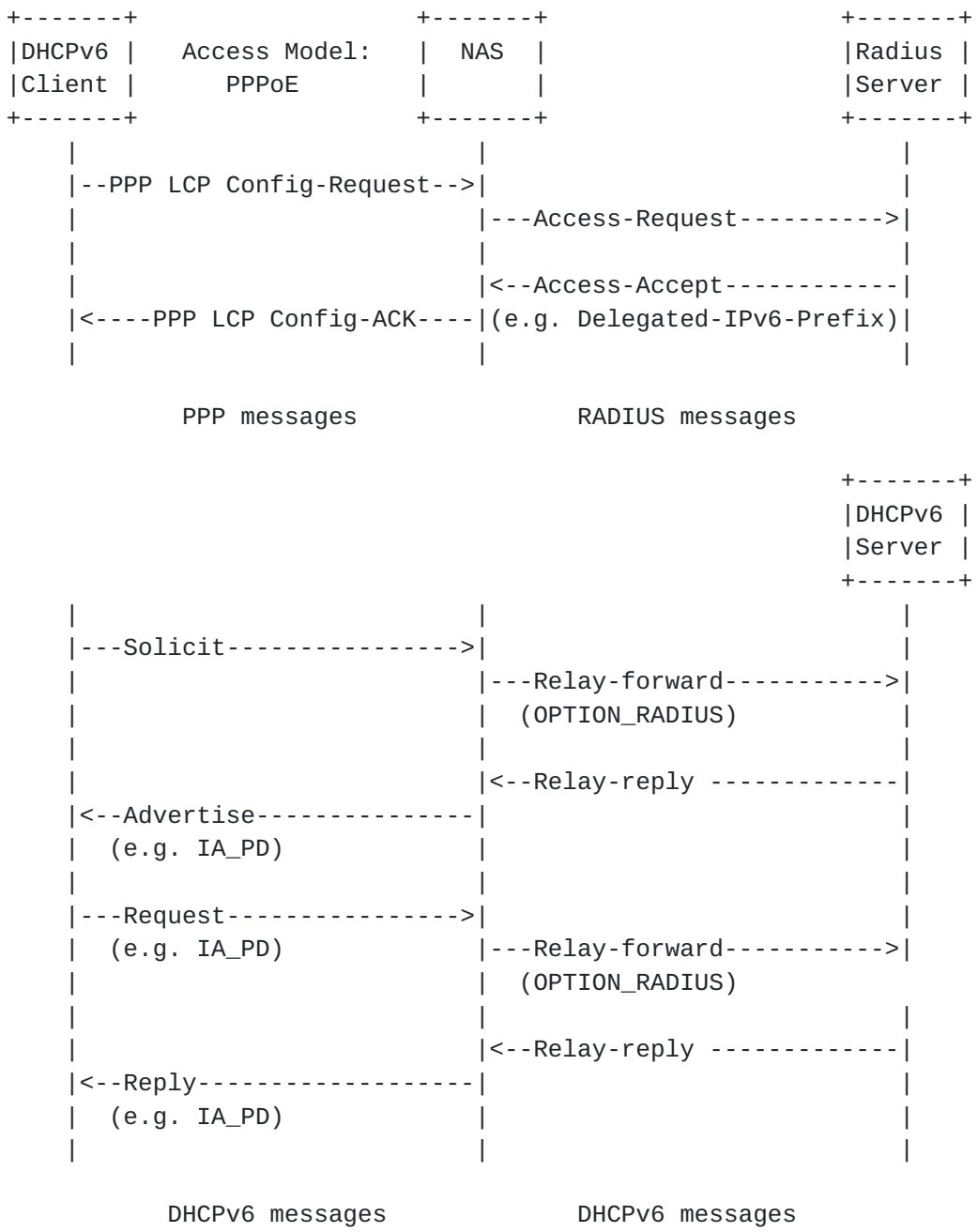


Figure 2: Network scenario and message sequence when employing DHCPv6 RADIUS option in PPPoE access

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

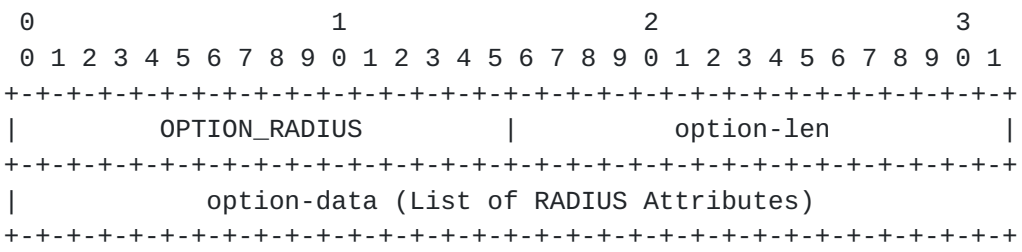
these information during the RADIUS session is out of the scope of this document.

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; but after receiving REBIND (6) message from the DHCPv6 client, the NAS SHOULD initiate a new Access-Request/Access-Accept message exchange with the RADIUS server.

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. Only the attributes listed in the IANA Registry of 'RADIUS Attributes Permitted in the DHCPv6 RADIUS option' SHOULD be included in the OPTION_RADIUS.

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 the DHCPv6 RADIUS option'. New RADIUS attributes MAY be added to this list after the IETF Expert Review [RFC5226].

Type Code	Attribute	Reference
26	Vendor-Specific	[RFC2865]
123	Delegated-IPv6-Prefix	[RFC4818]
144	DS-Lite-Tunnel-Name	[RFC6519]
[TBD]	Framed-IPv6-Address	[I-D.ietf-radext-ipv6-access]
[TBD]	Stateful-IPv6-Address-Pool	[I-D.ietf-radext-ipv6-access]
[TBD]	Delegated-IPv6-Prefix-Pool	[I-D.ietf-radext-ipv6-access]
[TBD]	DNS-Server-IPv6-Address	[I-D.ietf-radext-ipv6-access]

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

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.

5. Relay Agent Behavior

The DHCPv6 relay agent MAY include OPTION_RADIUS in the RELAY-FORW (12) message. When the value in the attributes of Stateful-IPv6-Address-Pool, Delegated-IPv6-Prefix-Pool, Delegated-IPv6-Prefix (123) or Framed-IPv6-Address in the Access-Accept message replied from RADIUS server are valid, the relay agent that supports OPTION_RADIUS SHOULD include these RADIUS attributes into the container option, OPTION_RADIUS.

6. Server Behavior

Upon receipt of the RELAY-FORW (12) message with OPTION_RADIUS from a relay agent, the DHCPv6 server 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. 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].

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, in the network scenarios described in the section 3, NAS could always be regarded as a trusted network component in the real deployment.

9. IANA Considerations

This document requests to assign a new DHCPv6 option code for OPTION_RADIUS, and to create a new registry on the same assignment page, which can be entitled as 'RADIUS Attributes Permitted in the DHCPv6 RADIUS option'. 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. New RADIUS attributes MAY be added to this list after the IETF Expert Review [RFC5226]. The IETF expert review SHOULD include careful consideration of the security implications of allowing the relay agent to include the RADIUS attribute being considered for 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

[I-D.ietf-radext-ipv6-access]
Dec, W., Sarikaya, B., Zorn, G., Miles, D., and B.

Lourdelet, "RADIUS attributes for IPv6 Access Networks", draft-ietf-radext-ipv6-access-15 (work in progress), January 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.

[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.

[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.

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