Workgroup: opsawg
Internet-Draft:
draft-ietf-opsawg-add-encrypted-dns-12
Updates: 4014 (if approved)
Published: 26 March 2023
Intended Status: Standards Track
Expires: 27 September 2023
Authors: M. Boucadair T. Reddy A. DeKok
Orange Nokia FreeRADIUS

RADIUS Extensions for DHCP Configured Services

Abstract

This document specifies two new Remote Authentication Dial-In User Service (RADIUS) attributes that carry DHCP options. The specification is generic and can be applicable to any service that relies upon DHCP. Both DHCPv4 and DHCPv6 configured services are covered.

Also, this document updates RFC 4014 by relaxing a constraint on permitted RADIUS Attributes in the RADIUS Attributes DHCP suboption.

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 https://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 27 September 2023.

Copyright Notice

Copyright (c) 2023 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 (https://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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction
2. Terminology
3. DHCP Options RADIUS Attributes
  3.1. DHCPv6-Options Attribute
  3.2. DHCPv4-Options Attribute
4. Passing DHCP Options RADIUS Attributes by DHCP Relay Agents to DHCP Servers
  4.1. Context
  4.2. Updates to RFC 4014
    4.2.1. Section 3 of RFC 4014
    4.2.2. Section 4 of RFC 4014
5. An Example: Applicability to Encrypted DNS Provisioning
6. Security Considerations
7. Table of Attributes
8. IANA Considerations
  8.1. New RADIUS Attributes
  8.2. New RADIUS Attribute Permitted in DHCPv6 RADIUS Option
  8.3. RADIUS Attributes Permitted in RADIUS Attributes DHCP Sub-option
  8.4. DHCP Options Permitted in the RADIUS DHCP*-Options Attribute
    8.4.1. DHCPv6
    8.4.2. DHCPv4
    8.4.3. Guidelines for the Designated Experts
9. Acknowledgements
10. References
  10.1. Normative References
  10.2. Informative References
Authors' Addresses

1. Introduction

In the context of broadband services, Internet Service Providers (ISPs) usually provide DNS resolvers to their customers. To that aim, ISPs deploy dedicated mechanisms (e.g., DHCP [RFC2132] [RFC8415], IPv6 Router Advertisement [RFC4861]) to advertise a list of DNS recursive servers to their customers. Typically, the information used to populate DHCP messages and/or IPv6 Router Advertisements relies upon specific Remote Authentication Dial-In User Service (RADIUS) [RFC2865] attributes, such as the DNS-Server-IPv6-Address Attribute specified in [RFC6911].

With the advent of encrypted DNS (e.g., DNS-over-HTTPS (DoH) [RFC8484], DNS-over-TLS (DoT) [RFC7858], or DNS-over-QUIC (DoQ) [RFC9250]), additional means are required to provision hosts with network-designated encrypted DNS. To fill that void, [I-D.ietf-add-dnr] leverages existing protocols such as DHCP to provide hosts with the required information to connect to an encrypted DNS resolver. However, there are no RADIUS attributes that can be used to populate the discovery messages discussed in [I-D.ietf-add-dnr]. The same concern is likely to be encountered for future services that are configured using DHCP.

This document specifies two new RADIUS attributes: DHCPv6-Options (Section 3.1) and DHCPv4-Options (Section 3.2) Attributes. These attributes can include DHCP options that are listed under the IANA registries that are created in Sections 8.4.1 and 8.4.2. These two attributes are specified in order to accommodate both IPv4 and IPv6 deployment contexts while taking into account the constraints in Section 3.4 of [RFC6158].

The mechanism specified in this document is a generic mechanism and might be employed in network scenarios where the DHCP server and the RADIUS client are located in the same device. The new attributes can also be used in deployments that rely upon the mechanisms defined in [RFC4014] or [RFC7037], which allow a DHCP relay agent that is collocated with a RADIUS client to pass attributes obtained from a RADIUS server to a DHCP server. However, an update to [RFC4014] is required so that a DHCP relay agent can pass the DHCPv4-Options Attribute obtained from a RADIUS server to a DHCP server (Section 4).

DHCP options that are included in the new RADIUS attributes can be controlled by a deployment specific policy. Discussing such a policy is out of scope.

This document adheres to [RFC8044] for defining the new attributes.

A sample deployment usage of the DHCPv6-Options and DHCPv4-Options RADIUS attributes is described in Section 5.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This document makes use of the terms defined in [RFC2865], [RFC8415], and [RFC8499]. The following additional terms are used:

DHCP:
refers to both DHCPv4 [RFC2132] and DHCPv6 [RFC8415].

Encrypted DNS: refers to a scheme where DNS exchanges are transported over an encrypted channel. Examples of encrypted DNS are DoT, DoH, and DoQ.

Encrypted DNS resolver: refers to a resolver (Section 6 of [RFC8499]) that supports encrypted DNS.

DHCP*-Options: refers to DHCPv4-Options and DHCPv6-Options Attributes (Section 3).

3. DHCP Options RADIUS Attributes

This section specifies two new RADIUS attributes for RADIUS clients and servers to exchange DHCP-encoded data. This data is then used to feed the DHCP procedure between a DHCP client and a DHCP server.

Both DHCPv4-Options and DHCPv6-Options Attributes use the "Long Extended Type" format (Section 2.2 of [RFC6929]). The description of the fields is provided in Sections 3.1 and 3.2.

These attributes use the "Long Extended Type" format in order to permit the transport of attributes encapsulating more than 253 octets of data. DHCP options that can be included in the DHCP*-Options RADIUS attributes are limited by the maximum packet size of 4096 bytes (Section 3 of [RFC2865]). In order to accommodate deployments with large DHCP options, RADIUS implementations are RECOMMENDED to support a packet size up to 65535 bytes. Such a recommendation can be met if RADIUS implementations support a mechanism that relaxes the 4096 bytes limit (e.g., [RFC7499] or [RFC7930]).

The value fields of DHCP*-Options Attributes are encoded in clear and not encrypted as, for example, Tunnel-Password Attribute [RFC2868].

RADIUS implementations may support a configuration parameter to control the DHCP options that can be included in a DHCP*-Options RADIUS attribute. Likewise, DHCP server implementations may support a configuration parameter to control the permitted DHCP options in a DHCP*-Options RADIUS attribute. Absent explicit configuration, RADIUS implementations and DHCP server implementations SHOULD ignore non-permitted DHCP options received in a DHCP*-Options RADIUS attribute.

RADIUS supplied data is specific configuration data that is returned as a function of authentication and authorization checks. As such, absent any explicit configuration on the DHCP server, RADIUS

supplied data by means of DHCP*-Options Attributes take precedence over any local configuration.

These attributes are defined with globally unique names. The naming of the attributes follows the guidelines in Section 2.7.1 of [RFC6929]. Invalid attributes are handled as per Section 2.8 of [RFC6929].

3.1. DHCPv6-Options Attribute

This attribute is of type "string" as defined in Section 3.5 of [RFC8044].

The DHCPv6-Options Attribute MAY appear in a RADIUS Access-Accept packet. It MAY also appear in a RADIUS Access-Request packet as a hint to the RADIUS server to indicate a preference. However, the server is not required to honor such a preference.

The DHCPv6-Options Attribute MAY appear in a RADIUS CoA-Request packet.

The DHCPv6-Options Attribute MAY appear in a RADIUS Accounting-Request packet.

The DHCPv6-Options Attribute MUST NOT appear in any other RADIUS packet.

The DHCPv6-Options Attribute is structured as follows:

Type

245

Length

This field indicates the total length, in octets, of all fields of this attribute, including the Type, Length, Extended-Type, and "Value".

Extended-Type

TBA1 (see Section 8.1).

Value

This field contains a list of DHCPv6 options (Section 21 of [RFC8415]). Multiple instances of the same DHCPv6 option MAY be included. If an option appears multiple times, each instance is considered separate and the data areas of the options MUST NOT be concatenated or otherwise combined. Consistent with Section 17 of

[RFC7227], this document does not impose any option order when multiple options are present.

Permitted DHCPv6 options in the DHCPv6-Options Attribute are maintained by IANA in the registry created in Section 8.4.1.

The DHCPv6-Options Attribute is associated with the following identifier: 245.TBA1.

3.2. DHCPv4-Options Attribute

This attribute is of type "string" as defined in Section 3.5 of [RFC8044].

The DHCPv4-Options Attribute MAY appear in a RADIUS Access-Accept packet. It MAY also appear in a RADIUS Access-Request packet as a hint to the RADIUS server to indicate a preference. However, the server is not required to honor such a preference.

The DHCPv4-Options Attribute MAY appear in a RADIUS CoA-Request packet.

The DHCPv4-Options Attribute MAY appear in a RADIUS Accounting-Request packet.

The DHCPv4-Options Attribute MUST NOT appear in any other RADIUS packet.

The DHCPv4-Options Attribute is structured as follows:

Type

245

Length

This field indicates the total length, in octets, of all fields of this attribute, including the Type, Length, Extended-Type, and "Value".

Extended-Type

TBA2 (see Section 8.1).

Value

This field contains a list of DHCPv4 options. Multiple instances of the same DHCPv4 option MAY be included, especially for

concatenation-requiring options that exceed the maximum DHCPv4 option size of 255 octets. The mechanism specified in [RFC3396] MUST be used for splitting and concatenating the instances of a concatenation-requiring option.

Permitted DHCPv4 options in the DHCPv4-Options Attribute are maintained by IANA in the registry created in Section 8.4.2.

The DHCPv4-Options Attribute is associated with the following identifier: 245.TBA2.

4. Passing DHCP Options RADIUS Attributes by DHCP Relay Agents to DHCP Servers

4.1. Context

The RADIUS Attributes suboption [RFC4014] enables a DHCPv4 relay agent to pass identification and authorization attributes received during RADIUS authentication to a DHCPv4 server. However, [RFC4014] defines a frozen set of RADIUS attributes that can be included in such a suboption. This limitation is suboptimal in contexts where new services are deployed (e.g., support of encrypted DNS [I-D.ietf-add-dnr]).

Section 4.2 updates [RFC4014] by relaxing that constraint and allowing to tag additional RADIUS attributes as permitted in the RADIUS Attributes DHCP suboption. Section 8.3 creates a new IANA registry to maintain the set of permitted attributes in the RADIUS Attributes DHCP suboption.

4.2. Updates to RFC 4014

4.2.1. Section 3 of RFC 4014

This document updates Section 3 of [RFC4014] as follows:

OLD:

To avoid dependencies between the address allocation and other state information between the RADIUS server and the DHCP server, the DHCP relay agent SHOULD include only the attributes in the table below in an instance of the RADIUS Attributes suboption. The table, based on the analysis in RFC 3580 [8], lists attributes that MAY be included:

#	Attribute
1	User-Name (RFC 2865 [3])
6	Service-Type (RFC 2865)
26	Vendor-Specific (RFC 2865)
27	Session-Timeout (RFC 2865)
88	Framed-Pool (RFC 2869)
100	Framed-IPv6-Pool (RFC 3162 [7])

NEW:

To avoid dependencies between the address allocation and other state information between the RADIUS server and the DHCP server, the DHCP relay agent SHOULD include only the attributes in the IANA-maintained registry (Section 8.3 of [This-Document]) in an instance of the RADIUS Attributes suboption. The DHCP relay agent may support a configuration parameter to control the attributes in a RADIUS Attributes suboption.

4.2.2. Section 4 of RFC 4014

This document updates Section 4 of [RFC4014] as follows:

OLD:

If the relay agent relays RADIUS attributes not included in the table in Section 4, the DHCP server SHOULD ignore them.

NEW:

If the relay agent relays RADIUS attributes not included in the IANA-maintained registry (Section 8.3 of [This-Document]), and absent explicit configuration, the DHCP server SHOULD ignore them.

5. An Example: Applicability to Encrypted DNS Provisioning

Typical deployment scenarios are similar to those described, for instance, in Section 2 of [RFC6911]. For illustration purposes, Figure 1 shows an example where a Customer Premises Equipment (CPE) is provided with an encrypted DNS resolver. This example assumes that the Network Access Server (NAS) embeds both RADIUS client and DHCPv6 server capabilities.

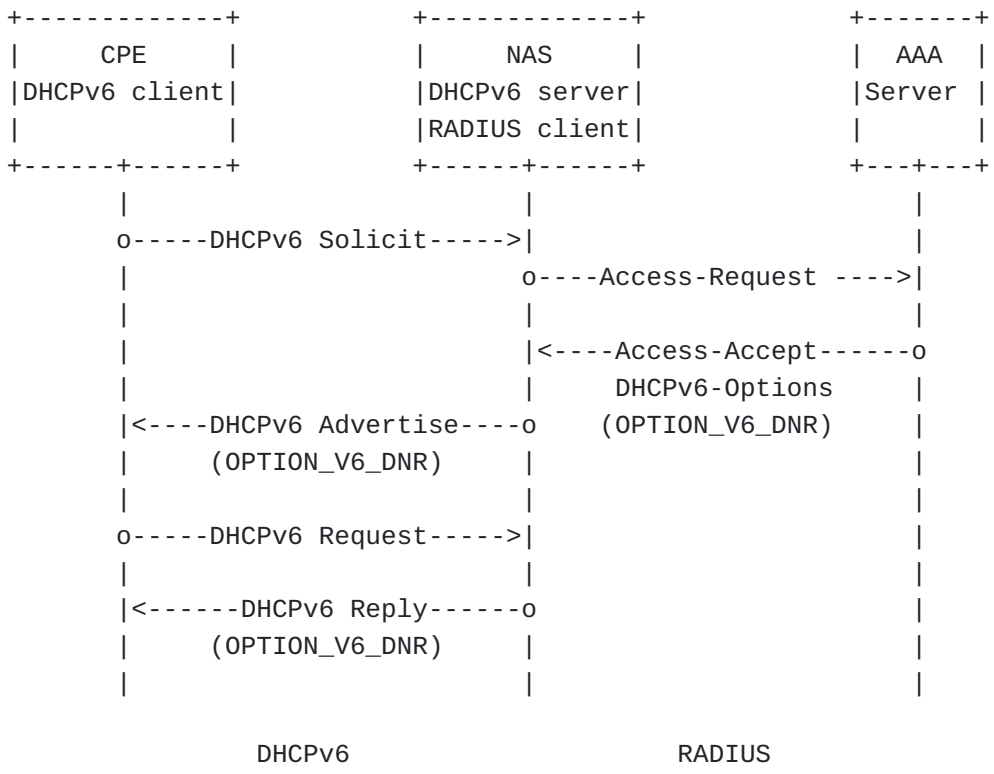

Figure 1: An Example of RADIUS IPv6 Encrypted DNS Exchange

Upon receipt of the DHCPv6 Solicit message from a CPE, the NAS sends a RADIUS Access-Request message to the Authentication, Authorization, and Accounting (AAA) server. Once the AAA server receives the request, it replies with an Access-Accept message (possibly after having sent a RADIUS Access-Challenge message and assuming the CPE is entitled to connect to the network) that carries a list of parameters to be used for this session, and which include the encrypted DNS information. Such an information is encoded as OPTION_V6_DNR (144) instances ([I-D.ietf-add-dnr]) in the DHCPv6-Options RADIUS attribute. These instances are then used by the NAS to complete the DHCPv6 procedure that the CPE initiated to retrieve information about the encrypted DNS service to use. The Discovery of Network-designated Resolvers (DNR) procedure defined in [I-D.ietf-add-dnr] is then followed between the DHCPv6 client and the DHCPv6 server.

Should any encrypted DNS-related information (e.g., Authentication Domain Name (ADN), IPv6 address) change, the RADIUS server sends a RADIUS Change-of-Authorization (CoA) message [RFC5176] that carries the DHCPv6-Options Attribute with the updated OPTION_V6_DNR information to the NAS. Once that message is received and validated by the NAS, it replies with a RADIUS CoA ACK message. The NAS replaces the old encrypted DNS resolver information with the new one and sends a DHCPv6 Reconfigure message which leads the DHCPv6 client to initiate a Renew/Reply message exchange with the DHCPv6 server.

In deployments where the NAS behaves as a DHCPv6 relay agent, the procedure discussed in Section 3 of [RFC7037] can be followed. To that aim, Section 8.2 updates the "RADIUS Attributes Permitted in DHCPv6 RADIUS Option" registry ([DHCP-RADIUS]). CoA-Requests can be used following the procedure specified in [RFC6977].

Figure 2 shows another example where a CPE is provided with an encrypted DNS resolver, but the CPE uses DHCPv4 to retrieve its encrypted DNS resolver.

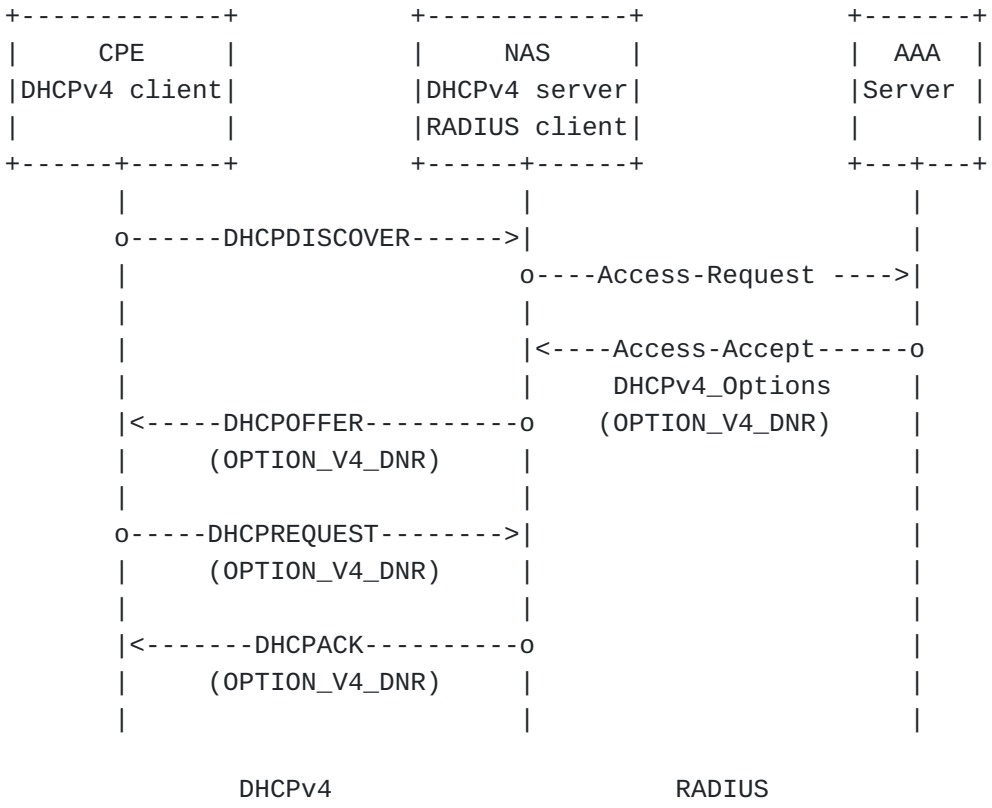

Figure 2: An Example of RADIUS IPv4 Encrypted DNS Exchange

Other deployment scenarios can be envisaged, such as returning customized service parameters (e.g., different DoH URI Templates) as a function of the service/policies/preferences that are set by a network administrator. How an administrator indicates its service/policies/preferences to an AAA server is out of scope.

6. Security Considerations

RADIUS-related security considerations are discussed in [RFC2865].

DHCPv6-related security issues are discussed in Section 22 of [RFC8415], while DHCPv4-related security issues are discussed in Section 7 of [RFC2131]. Security considerations specific to the DHCP options that are carried in RADIUS are discussed in relevant

documents that specify these options. For example, security considerations (including traffic theft) are discussed in Section 7 of [I-D.ietf-add-dnr].

RADIUS servers have conventionally tolerated the input of arbitrary data via the "string" data type (Section 3.5 of [RFC8044]). This practice allows RADIUS servers to support newer standards without software upgrades, by allowing administrators to manually create complex attribute content and, then, to pass that content to a RADIUS server as opaque strings. While this practice is useful, it is RECOMMENDED that RADIUS servers that implement the present specification are updated to understand the format and encoding of DHCP options. Administrators can, thus, enter the DHCP options as options instead of manually-encoded opaque strings. This recommendation increases security and interoperability by ensuring that the options are encoded correctly. It also increases usability for administrators.

The considerations discussed in Section 7 of [RFC4014] and Section 8 of [RFC7037] should be taken into account in deployments where DHCP relay agents pass the DHCP*-Options Attributes to DHCP servers. Additional considerations specific to the use of Reconfigure messages are discussed in Section 9 of [RFC6977].

7. Table of Attributes

The following table provides a guide as what type of RADIUS packets that may contain these attributes, and in what quantity.

Access-Request	Access-Accept	Access-Reject	Challenge	Acct. Request	#	Attribute
0+	0+	0	0	0+	245.TBA1	DHCPv6-Options
0+	0+	0	0	0+	245.TBA2	DHCPv4-Options

CoA-Request	CoA-ACK	CoA-NACK	#	Attribute
0+	0	0	245.TBA1	DHCPv6-Options
0+	0	0	245.TBA2	DHCPv4-Options

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.

8. IANA Considerations

8.1. New RADIUS Attributes

IANA is requested to assign two new RADIUS attribute types from the IANA registry "Radius Attribute Types" [RADIUS-Types]:

Value	Description	Data Type	Reference
245.TBA1	DHCPv6-Options	string	This-Document
245.TBA2	DHCPv4-Options	string	This-Document

Table 1: New RADIUS Attributes

8.2. New RADIUS Attribute Permitted in DHCPv6 RADIUS Option

IANA is requested to add the following entry to the "RADIUS Attributes Permitted in DHCPv6 RADIUS Option" subregistry in the "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)" registry [DHCP-RADIUS]:

Type Code	Attribute	Reference
245.TBA1	DHCPv6-Options	This-Document

Table 2: New RADIUS Attribute Permitted in DHCPv6 RADIUS Option

8.3. RADIUS Attributes Permitted in RADIUS Attributes DHCP Sub-option

IANA is requested to create a new sub-registry entitled "RADIUS Attributes Permitted in RADIUS Attributes Sub-option" in the "Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) Parameters" registry [BOOTP].

The allocation policy of this new sub-registry is Expert Review (Section 4.5 of [RFC8126]). Designated experts should carefully consider the security implications of allowing the relay agent to include new RADIUS attributes to this registry. Additional considerations are provided in Section 8.4.3.

The initial content of this sub-registry is listed in Table 3. The reference may include the document that registers or specifies the Attribute.

Type Code	Attribute	Reference
1	User-Name	[RFC2865]
6	Service-Type	[RFC2865]
26	Vendor-Specific	[RFC2865]
27	Session-Timeout	[RFC2865]
88	Framed-Pool	[RFC2869]
100	Framed-IPv6-Pool	[RFC3162]
245.TBA2	DHCPv4-Options	This-Document

Table 3: RADIUS Attributes Permitted in RADIUS Attributes DHCP Suboption

8.4. DHCP Options Permitted in the RADIUS DHCP*-Options Attribute

8.4.1. DHCPv6

IANA is requested to create a new sub-registry entitled "DHCPv6 Options Permitted in the RADIUS DHCPv6-Options Attribute" in the "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)" registry [DHCP-RADIUS].

The registration policy for this new sub-registry is Expert Review (Section 4.5 of [RFC8126]). See more details in Section 8.4.3.

The initial content of this sub-registry is listed in Table 4. The Value and Description fields echo those of [DHCPv6]. The reference may include the document that registers the option or the document that specifies the option.

Value	Description	Reference
144	OPTION_V6_DNR	This-Document

Table 4: Initial DHCPv6 Options Permitted in the RADIUS DHCPv6-Options Attribute

8.4.2. DHCPv4

IANA is requested to create a new sub-registry entitled "DHCP Options Permitted in the RADIUS DHCPv4-Options Attribute" in the "Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) Parameters" registry [BOOTP].

The registration policy for this new sub-registry is Expert Review (Section 4.5 of [RFC8126]). See more details in Section 8.4.3.

The initial content of this sub-registry is listed in Table 5. The Tag and Name fields echo those of [BOOTP]. The reference may include the document that registers the option or the document that specifies the option.

Tag	Name	Reference
162	OPTION_V4_DNR	This-Document

Table 5: Initial DHCPv4 Options Permitted in the RADIUS DHCPv4-Options Attribute

8.4.3. Guidelines for the Designated Experts

It is suggested that multiple designated experts be appointed for registry change requests.

Criteria that should be applied by the designated experts include determining whether the proposed registration duplicates existing entries and whether the registration description is clear and fits the purpose of this registry.

Registration requests are to be sent to radius-dhcp-review@ietf.org and are evaluated within a three-week review period on the advice of one or more designated experts. Within the review period, the designated experts will either approve or deny the registration request, communicating this decision to the review list and IANA. Denials should include an explanation and, if applicable, suggestions as to how to make the request successful.

9. Acknowledgements

Thanks to Christian Jacquenet, Neil Cook, Joe Clarke, Qin Wu, Dirk von-Hugo, Tom Petch, and Chongfeng Xie for the review and suggestions.

Thanks to Ben Schwartz and Bernie Volz for the comments.

Thanks to Rob Wilton for the careful AD review.

Thanks to Ralf Weber for the dnsdir reviews, Robert Sparks for genart review, and Tatuya Jinmei for the int-dir review.

Thanks to Eric Vyncke, Paul Wouters, and Warren Kumari for the IESG review.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <https://www.rfc-editor.org/info/rfc2865>.

[RFC3396] Lemon, T. and S. Cheshire, "Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)", RFC 3396, DOI 10.17487/RFC3396, November 2002, <https://www.rfc-editor.org/info/rfc3396>.

[RFC4014] Droms, R. and J. Schnizlein, "Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the

Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option", RFC 4014, DOI 10.17487/RFC4014, February 2005, <https://www.rfc-editor.org/info/rfc4014>.

[RFC6158] DeKok, A., Ed. and G. Weber, "RADIUS Design Guidelines", BCP 158, RFC 6158, DOI 10.17487/RFC6158, March 2011, <https://www.rfc-editor.org/info/rfc6158>.

[RFC6929] DeKok, A. and A. Lior, "Remote Authentication Dial In User Service (RADIUS) Protocol Extensions", RFC 6929, DOI 10.17487/RFC6929, April 2013, <https://www.rfc-editor.org/info/rfc6929>.

[RFC8044] DeKok, A., "Data Types in RADIUS", RFC 8044, DOI 10.17487/RFC8044, January 2017, <https://www.rfc-editor.org/info/rfc8044>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8415]
Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/info/rfc8415>.

10.2. Informative References

[BOOTP] IANA, "Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) Parameters", <https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml>.

[DHCP-RADIUS] IANA, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", <https://www.iana.org/assignments/dhcpv6-parameters/dhcpv6-parameters.xhtml>.

[DHCPv6] IANA, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6), Option Codes", <https://www.iana.org/

assignments/dhcpv6-parameters/dhcpv6-parameters.xhtml#dhcpv6-parameters-2>.

[I-D.ietf-add-dnr] Boucadair, M., Reddy.K, T., Wing, D., Cook, N., and T. Jensen, "DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)", Work in Progress, Internet-Draft, draft-ietf-add-dnr-14, 13 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-add-dnr-14>.

[RADIUS-Types] IANA, "RADIUS Types", <http://www.iana.org/assignments/radius-types>.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, March 1997, <https://www.rfc-editor.org/info/rfc2131>.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, DOI 10.17487/RFC2132, March 1997, <https://www.rfc-editor.org/info/rfc2132>.

[RFC2868] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M., and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support", RFC 2868, DOI 10.17487/RFC2868, June 2000, <https://www.rfc-editor.org/info/rfc2868>.

[RFC2869] Rigney, C., Willats, W., and P. Calhoun, "RADIUS Extensions", RFC 2869, DOI 10.17487/RFC2869, June 2000, <https://www.rfc-editor.org/info/rfc2869>.

[RFC3162] Aboba, B., Zorn, G., and D. Mitton, "RADIUS and IPv6", RFC 3162, DOI 10.17487/RFC3162, August 2001, <https://www.rfc-editor.org/info/rfc3162>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[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, DOI 10.17487/RFC5176, January 2008, <https://www.rfc-editor.org/info/rfc5176>.

[RFC6911] Dec, W., Ed., Sarikaya, B., Zorn, G., Ed., Miles, D., and B. Lourdelet, "RADIUS Attributes for IPv6 Access Networks", RFC 6911, DOI 10.17487/RFC6911, April 2013, <https://www.rfc-editor.org/info/rfc6911>.

[RFC6977] Boucadair, M. and X. Pougnard, "Triggering DHCPv6 Reconfiguration from Relay Agents", RFC 6977, DOI 10.17487/RFC6977, July 2013, <https://www.rfc-editor.org/info/rfc6977>.

[RFC7037] Yeh, L. and M. Boucadair, "RADIUS Option for the DHCPv6 Relay Agent", RFC 7037, DOI 10.17487/RFC7037, October 2013, <https://www.rfc-editor.org/info/rfc7037>.

[RFC7227] Hankins, D., Mrugalski, T., Siodelski, M., Jiang, S., and S. Krishnan, "Guidelines for Creating New DHCPv6 Options", BCP 187, RFC 7227, DOI 10.17487/RFC7227, May 2014, <https://www.rfc-editor.org/info/rfc7227>.

[RFC7499] Perez-Mendez, A., Ed., Marin-Lopez, R., Pereniguez-Garcia, F., Lopez-Millan, G., Lopez, D., and A. DeKok, "Support of Fragmentation of RADIUS Packets", RFC 7499, DOI 10.17487/RFC7499, April 2015, <https://www.rfc-editor.org/info/rfc7499>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC7930] Hartman, S., "Larger Packets for RADIUS over TCP", RFC 7930, DOI 10.17487/RFC7930, August 2016, <https://www.rfc-editor.org/info/rfc7930>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

[RFC9250] Huitema, C., Dickinson, S., and A. Mankin, "DNS over Dedicated QUIC Connections", RFC 9250, DOI 10.17487/RFC9250, May 2022, <https://www.rfc-editor.org/info/rfc9250>.

Authors' Addresses

Mohamed Boucadair
Orange
35000 Rennes
France

Email: mohamed.boucadair@orange.com

Tirumaleswar Reddy
Nokia
India

Email: kondtir@gmail.com

Alan DeKok
FreeRADIUS

Email: aland@freeradius.org