DHC Working Group
Internet Draft
Document: draft-ietf-dhc-v6-relay-radius-02.txt
Expires: August 2, 2006

Wing Cheong Lau
The Chinese University
of Hong Kong

Feb 03, 2006

DHCPv6 Relay agent RADIUS Attribute Option

Status of this Memo

Abstract

This document introduces the capabilities of the DHCPv4 Relay Agent Information Option in RFC 3046 and the corresponding RADIUS-Attributes Sub-option to DHCPv6. In particular, the document describes a new DHCPv6 option called the Relay agent RADIUS Attributes Option (RRAO) which extends the set of DHCPv6 options as defined in RFC 3315 and 3376. Following its DHCPv4 counterpart, the new option is inserted by the DHCPv6 relay agent when forwarding client-originated DHCPv6 packets to a DHCPv6 server. Servers recognizing the RRAO may use the information to implement IP address or other parameter assignment policies. The DHCP Server echoes the option back verbatim to the relay agent in server-to-client replies, and the relay agent strips the option before forwarding the reply to the client.

Conventions used in this document

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 RFC 2119 [2].

The use of the standard keywords MUST, SHOULD, MUST NOT and SHOULD NOT within this specification are with respect to RADIUS clients and servers that implement the optional features of this specification, do not create any normative requirements outside of that scope and do not modify the base RADIUS specifications, such as RFC2865 [6] or RFC2866 [11].

Throughout this document, "DHCP" refers to DHCP for IPv6 unless explicitly stated otherwise.

Table of Contents

1. Introduction

In some access network environment, a Network Access Server (NAS) enabling authenticated network access may also act as a DHCPv6 relay agent to forward requests and responses between the access client and a DHCPv6 server within the network. The DHCPv6 server may be used for assigning various configuration parameters for the client[9,10]. The NAS, using RADIUS as an authentication authority, will receive attributes from a RADIUS server that may be used by the DHCP server in the selection of configuration parameters to be delivered to the device requesting access. The Relay agent RADIUS Attributes Option (RRAO) enables the NAS, which doubles as a DHCPv6 relay agent, to

pass along attributes for the user of a device received during RADIUS authentication to a DHCP server [3].

The IEEE 802.1X [9] access authentication mechanism is an example through which a NAS can authenticate the identity of the user of a device before providing network access using RADIUS as the Authentication Service specified in [6]. In IEEE 802.1X authenticated access, an access client must first exchange some authentication credentials with the NAS. The NAS then supplies these credentials to a RADIUS server, which eventually sends either an Access-Accept or an Access-Reject in response to an Access-Request. The NAS, based on the reply of the RADIUS server, then allows or denies network access to the requesting device. Figure 1 summarizes the message exchange among the participants in such access authentication environment.

```
+-------------------+
|      Device       |
|    requesting     |
|  network access   |
+-------------------+
    |         ^
    |         |
   (1) Request for access
    |         |
    |        (4) Success/Failure
    v         |
+--------------------+
|        NAS         |
|  which also acts   |
|       as a         |
|DHCPv6 relay agent)|
+--------------------+
      |     ^
      |     |
     (2) Request for authentication
      |     |
      |    (3) Access-Accept/Reject
      v     |
+------------------+
|     RADIUS       |
|     Server       |
+------------------+
```

Figure 1

In the application described in this document, the NAS also acts as a

DHCPv6 relay agent. It adds a DHCPv6 Relay agent RADIUS Attributes option (RRAO) to DHCP messages. At the successful conclusion of network access authentication, a RADIUS Access-Accept provides attributes for service authorizations to the NAS. The NAS stores these attributes locally. When the NAS subsequently forwards DHCP messages from the device requesting network access, the NAS adds these attributes in a DHCPv6 RRAO.

The 3GPP2 access authentication mechanism is another example through which a PDSN (which doubles as the NAS) can authenticate the identity of the user of a device before providing network access using RADIUS as the Authentication Service specified in [10]. In 3GPP2 authenticated access, an MS must first exchange some authentication credentials with the PDSN. The PDSN then supplies these credentials to a RADIUS server, which eventually sends either an Access-Accept or an Access-Reject in response to an Access-Request. The PDSN, based on the reply of the RADIUS server, then allows or denies network access to the requesting device.

Figure 2 summarizes the message exchange among the participants in 3GPP2 network access authentication.

```
+------------------+
|Mobile Station(MS)|
|    requesting    |
|  network access  |
+------------------+
    |         ^
    |         |
   (1) Request for access
    |         |
    |        (4) Success/Failure
    v         |
+-------------------+
|    3GPP2 PDSN     |
|  (Acts as NAS     |
|    and DHCPv6     |
|server/relay agent)|
+-------------------+
      |     ^
      |     |
     (2) Request for authentication
      |     |
      |    (3) Access-Accept/Reject
      v     |
+-----------------+
|     RADIUS      |
|     Server      |
+-----------------+
```

Figure 2

Without the DHCPv6 RRAO described in this document, the NAS and the DHCPv6 server would need to co-locate within the PDSN (which is the case in [10]) in order to allow the DHCPv6 server to make use of the information carried by the RADIUS Access-Accept message while generating DHCPv6 replies. However, forcing the DHCPv6 server to co-locate with the PDSN is undesirable as it imposes unnecessary constraints on network topology and configuration. Furthermore, since [10] already requires the PDSN to behave as a DHCPv6 relay-agent for some types of queries, e.g. for dynamic configuration of the DNS server or SIP proxy for the MS, requiring the PDSN to be double as a DHCPv6 server will cause unnecessary implementation and processing complexity.

By using the RRAO described in this document, the PDSN no longer needs to take the dual role with respect to DHCPv6. It only needs to be DHCPv6 Relay Agent (and a NAS). At the successful conclusion of network access authentication, a RADIUS Access-Accept provides attributes for service authorizations to the NAS. The NAS stores these attributes locally. When the NAS subsequently forwards DHCP messages from the device requesting network access, the NAS adds these attributes in a RADIUS Attributes Sub-option for the Relay Agent Information option.

This document uses IEEE 802.1X and 3GPP2 access authentication as two examples to motivate the use of the RRAO by a NAS. The RRAO described in this document is not limited to use in conjunction with IEEE 802.1X or 3GPP2. It can be used to carry RADIUS attributes obtained by the relay agent for any reason but is constrained by RADIUS semantics.

The scope of applicability of this specification is such that the NAS (which acts as a DHCPv6 relay agent), any other participating DHCPv6 relay agent, the DHCPv6 server and DHCPv6 client should be within the same administrative domain while the RADIUS service involved may span multiple administrative domains. See the Section 4 for details of security considerations when this specification is deployed with RADIUS service operating across multiple administrative domains. Global interoperability of this specification, across arbitrary administrative domains, is not supported.

2. Terminology

2.1 DHCP Terminology

The following terms are used as defined in RFC3315 and RFC3736: DHCP relay agent, DHCP server, DHCP client, Stateless DHCP.

2.2 RADIUS Terminology

The following terms are used in conjunction with RADIUS:

RADIUS server: A RADIUS server is responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user.

Attribute: A Type-Length-Value tuple encapsulating data elements as defined in RFC 2865 [6].

NAS: A Network Access Server (NAS) provides access to the network and operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response which is returned.

3. Relay agent RADIUS Attributes Option for DHCPv6

To support the capability of the NAS/ DHCP relay agent as described in Section 1, we introduce the DHCPv6 equivalent of the DHCPv4 Relay Agent Information Option and the RADIUS Attributes Sub-option as defined in RFC3046 [12] and [13] respectively. In particular, this document describes a new DHCPv6 option called the Relay agent RADIUS Attribute Option (RRAO) which extends the set of DHCPv6 options as defined in RFC 3315 [3] and 3736 [4]. Following its DHCPv4 counterpart as defined in RFC 3046 and [13], the new option is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers recognizing the RRAO may use the information to implement IP address or other parameter assignment policies. The DHCP Server echoes the option back verbatim to the relay agent in server-to-client replies, and the relay agent strips the option before forwarding the reply to the client.

The format of the RRAO follows that of the DHCP Options as defined in Section 22.1 of RFC 3315 [3] as follows:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      OPTION_RRAO              |           option-len          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         RADIUS Attributes                     |
|                     (variable no. of octets)                  |
.                                                               .
```

```
.                                                               .
.                                                               .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

option-code   OPTION_RRAO (TBD). This is the DHCP option code for the Relay agent RADIUS Attribute Option

option-len   An unsigned integer giving the length of the RADIUS Attributes field in octets.

RADIUS Attributes
This consists of a sequence of RADIUS Attributes encoded according to the encoding rules in RFC 2865.

3.1 Relay Agent Operation

The adding of the DHCP RRAO SHOULD be configurable, and SHOULD be disabled by default.

Relay agents are NOT required to monitor or modify client-originated DHCP packets addressed to a server unicast address.

3.1.1 Relaying a Message from a Client

When a relay agent receives a valid DHCP message to be relayed from a client, it constructs a new Relay-forward message per Section 20.1.1 of RFC 3315 [3] and then adds to the Relay-forward message the RRAO, along with other option(s), e.g. the Interface-Id option, if it is configured to do so. The relay agent MUST be aware of the recommendations on packet sizes and the use of fragmentation in Section 5 of RFC 2460 [8].

The RRAO MUST only contain the attributes provided in the RADIUS Access/Accept message. The DHCP relay agent MUST NOT add more than one RRAO in a message.

The relay agent MUST include the User-Name and IPv6 Framed-Pool attributes in the RRAO if available, and MAY include other attributes.

In order 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 RRAO. The following table lists attributes that MAY be included:

Attribute

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

3.1.2 Relaying a Message from a Relay Agent

When a relay agent receives a valid Relay-forward message from another relay agent closer to the client, regardless of whether the message already includes a Relay Agent Information option or not, the relay agent shall construct a new Relay-forward message per Section 20.1.2 of RFC 3315 [3] and then add to this newly created Relay-forward message the RRAO, along with other option(s), as described in Section 3.1.1, if it is configured to do so. The relay agent MUST be aware of the recommendations on packet sizes and the use of fragmentation in Section 5 of RFC 2460 [8].

3.1.3 Relaying a Replay-reply Message

The RRAO echoed by a server MUST be removed by the relay agent which added it when forwarding a server-to-client response back to the client.

3.2 Server Operation

DHCP servers unaware of the RRAO will ignore the option upon receive and will not echo it back on responses. This is the specified server behavior for unknown options.

DHCP servers claiming to support the RRAO MUST discard the message and increment an error count if a Relay Agent Information option was added by a DHCP client but not by a relay agent. (This situation can be identified by the nesting of a RRAO inside the content of the Relay Message option created by the first-hop relay agent.) We put the responsibility of such checking to the DHCP server instead of the relay agents in order to simplify the operations of the latter. Furthermore, it is unreasonable to require a relay agent not supporting/ understanding the RRAO to perform such checking.

When the DHCP server receives a message from a relay agent containing a RRAO, it extracts the contents of the option and MAY use that information as a hint in selecting configuration parameters for the client. If the relay agent forwards RADIUS attributes not included in the table in Section 3.1.1, the DHCP server SHOULD ignore them. If

the DHCP server uses attributes not specified in the table, it might result in side effects not anticipated in the existing RADIUS specifications.

DHCP servers claiming to support the RRAO MUST echo the entire contents of the RRAO in all of its relay-replies. The nesting of the echoed RRAO(s) within the possibly nested relay-reply message MUST be according to the nesting order of those options within the original the Relay-forward message. DHCP servers must be aware of the recommendations on packet sizes and the use of fragmentation in Section 5 of RFC 2460 [8].

3.3 DHCP Client Behavior

Relay agent options are exchanged only between relay agents and DHCP server, so DHCP clients are never aware of their use.

4. Security Considerations

The DHCP RRAO depends on a trusted relationship between the DHCP relay agent and the server. If a client message is relayed through multiple relay agents, each of the relay agents must have established independent, pairwise trust relationships. While the introduction of fraudulent RRAO may be prevented by a perimeter defense that blocks these options unless the relay agent is trusted, a deeper defense using IPsec [5] SHOULD be deployed as well. Refer to Section 21.1 of RFC 3315 [3] for detail IPsec configurations required to protect communications between the DHCP relay agent(s) and server.

There are several data in a DHCP message that convey information that may identify an individual host on the network. Depending on the type of data included, the RRAO may also convey information that identifies a specific host or a specific user on the network. In practice, this information is not exposed outside the internal service-provider network, where DHCP messages are usually confined. Administrators who configure data that is going to be used in the RRAO should be careful to use data that are appropriate for the types of networks they administer. If DHCP messages travel outside the service-provider's own network, or if the RRAO values may become visible to other users, that may raise privacy concerns for the access provider or service provider.

The RADIUS protocol [6] was designed for intra-domain use, where the NAS, proxy, and home server exist within a single administrative domain, and proxies may be considered a trusted component. However, under roaming situation, the NAS, proxies, and home server will typically be managed by different administrative entities. As a

result, inter-domain RADIUS operations are inherently required for roaming applications, and proxies cannot necessarily be trusted. Refer to Section 7 of RFC 2609 for a detailed security threat analysis, limitations and precautions of operating RADIUS in an inter-domain environment. In general, robust and secure operations of RADIUS across multiple administrative domains require pre-established agreement, mutual trust, and secure communications channel amongst all the participating domains.

5. IANA Considerations

IANA is requested to assign a new option code, in the registry of DHCP option codes, for the DHCP Relay agent RADIUS Attributes Option.

6. Acknowledgments

Many thanks to R. Droms, M. Patrick, J. Schnizlein, M. Stapp, R. Johnson and T. Palaniappan as this document is based on their work on the DHCPv4 relay agent information option RFC3046 [12] and the related sub-options [13,14]. The document follows closely the original structure and borrows text from [12,13,14]. The author would also like to thank R. Droms, B. Volz, T. Lemon, K. Chowdhury, P. Barany, T. Hardie, R. Hsu, M. Lioy, A.C. Mahendran, R. Rezaiifar, S. Veerepalli and J. Wang for their helpful discussions.

7. Intellectual Property Statement

this document. Please address the information to the IETF Executive Director.

8. Full copyright statement

Author's Address

Wing Cheong Lau
Department of Information Engineering
The Chinese University of Hong Kong
Shatin, N.T.
Hong Kong
Email: wclau@ie.cuhk.edu.hk , lau@ieee.org

References

Normative References

[1]Bradner, S., "Intellectual Property Rights in IETF Technology", BCP 79, RFC 3979, March 2005.

[2]Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[3]Droms, R., Ed., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

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

[5]Kent, S. and Atkinson R., "Security Architecture for the Internet Protocol", RFC 2401, Nov. 1998.

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

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

[8]Deering, S and Hinden, R., "Internet Protocol Version 6 (IPv6) Specification", RFC 2460, Dec. 1998.

Informative References

[9]Institute of Electrical and Electronics Engineers, "Local and Metropolitan Area Networks: Port based Network Access Control", IEEE Standard 802.1X, March 2001.

[10]3GPP2 X.S0011-002-D v.0.4, "cdma2000 Wireless IP Network Standard:Simple IP and Mobile IP services," Work in progress.

[11]Rigney, C. "RADIUS Accounting", RFC 2866, June 2000.

[12]M.Patrick, "DHCP Relay Agent Information Option", RFC3046, Jan 2001.

[13]Droms, R., Schnizlein J., "RADIUS Attributes Sub-option for the DHCP Relay Agent Information Option", draft-ietf-dhc-agentopt-radius-08.txt, August 18, 2004.

[14]Stapp, M., Johnson, R., and Palaniappan, T., "Vendor-Specific Information Sub-option for the DHCP Relay Agent Option", draft-ietf-dhc-vendor-suboption-00.txt, Work-in-progress, Aug. 2004.

[15]Aboba B. and Vollbrecht J., "Proxy Chaining and Policy Implementation in Roaming", RFC 2607, June 1999.