

Network Working Group  
Internet Draft  
Intended status: Standards Track  
Expires: August 18, 2014

Sheng Jiang (Editor)  
Yu Fu  
Bing Liu  
Huawei Technologies Co., Ltd  
February 14, 2014

## RADIUS Attribute for 4rd

[draft-jiang-softwire-4rd-radius-04.txt](#)

### 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 18, 2014.

### Copyright Notice

Copyright (c) 2014 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.

## Abstract

IPv4 Residual Deployment via IPv6 (4rd) is a stateless mechanism for running IPv4 over IPv6-only infrastructure. It provides both IPv4 and IPv6 connectivity services simultaneously during the IPv4/IPv6 co-existing period. The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) 4rd options has been defined to configure 4rd Customer Edge (CE). However, in many networks, the configuration information may be stored in Authentication Authorization and Accounting (AAA) servers while user configuration is mainly from Broadband Network Gateway (BNG) through DHCPv6 protocol. This document defines a Remote Authentication Dial In User Service (RADIUS) attribute that carries 4rd configuration information from AAA server to BNG. The 4rd RADIUS attribute are designed following the simplify principle. It provides just enough information to form the correspondent DHCPv6 4rd option.

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction</a>	<a href="#">3</a>
<a href="#">2.</a>	<a href="#">Terminology</a>	<a href="#">3</a>
<a href="#">3.</a>	<a href="#">4rd Configuration process with RADIUS</a>	<a href="#">3</a>
<a href="#">4.</a>	<a href="#">Attributes</a>	<a href="#">6</a>
<a href="#">4.1.</a>	<a href="#">4rd-Configuration Attribute</a>	<a href="#">6</a>
<a href="#">4.2.</a>	<a href="#">4rd Non-mapping-rule Parameter option</a>	<a href="#">7</a>
<a href="#">4.3.</a>	<a href="#">4rd Rule Options</a>	<a href="#">7</a>
<a href="#">4.4.</a>	<a href="#">4rd Rule Sub Options</a>	<a href="#">8</a>
<a href="#">4.4.1.</a>	<a href="#">Rule-IPv6-Prefix Sub Option</a>	<a href="#">8</a>
<a href="#">4.4.2.</a>	<a href="#">Rule-IPv6-Suffix Sub Option</a>	<a href="#">9</a>
<a href="#">4.4.3.</a>	<a href="#">Rule-IPv4-Prefix Sub Option</a>	<a href="#">10</a>
<a href="#">4.4.4.</a>	<a href="#">Misc Sub Option</a>	<a href="#">11</a>
<a href="#">4.5.</a>	<a href="#">Table of attributes</a>	<a href="#">11</a>
<a href="#">5.</a>	<a href="#">Diameter Considerations</a>	<a href="#">12</a>
<a href="#">6.</a>	<a href="#">Security Considerations</a>	<a href="#">12</a>
<a href="#">7.</a>	<a href="#">IANA Considerations</a>	<a href="#">12</a>
<a href="#">8.</a>	<a href="#">Acknowledgments</a>	<a href="#">13</a>
<a href="#">9.</a>	<a href="#">References</a>	<a href="#">13</a>
<a href="#">9.1.</a>	<a href="#">Normative References</a>	<a href="#">13</a>

## [1](#). Introduction

Recently providers start to deploy IPv6 and consider how to transit to IPv6. IPv4 Residual Deployment via IPv6 (4rd) [[I-D.ietf-software-4rd](#)] is a stateless mechanism for running IPv4 over IPv6-only infrastructure. It provides both IPv4 and IPv6 connectivity services simultaneously during the IPv4/IPv6 co-existing period. 4rd has adopted Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [[RFC3315](#)] as auto-configuring protocol. The 4rd Customer Edge (CE) uses the DHCPv6 extension options [[I-D.ietf-software-4rd](#)] to discover 4rd Border Relay and to configure relevant 4rd rules.

In many networks, user configuration information may be managed by AAA (Authentication, Authorization, and Accounting) servers. Current AAA servers communicate using the Remote Authentication Dial In User Service (RADIUS) [[RFC2865](#)] protocol. In a fixed line broadband network, the Broadband Network Gateways (BNGs) act as the access gateway of users. The BNGs are assumed to embed a DHCPv6 server function that allows them to locally handle any DHCPv6 requests issued by hosts.

Since the 4rd configuration information is stored in AAA servers and user configuration is mainly through DHCPv6 protocol between BNGs and hosts/CEs, new RADIUS attributes are needed to propagate the information from AAA servers to BNGs. The 4rd RADIUS attribute are designed following the simplify principle, while providing enough information to form the correspondent DHCPv6 4rd option. [[I-D.ietf-software-4rd](#)].

## [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](#) [[RFC2119](#)].

The terms 4rd CE and 4rd Border Relay are defined in [\[I-D.ietf-software-4rd\]](#).

### 3. 4rd Configuration process with RADIUS

The below Figure 1 illustrates how the RADIUS protocol and DHCPv6 cooperate to provide 4rd CE with 4rd configuration information.

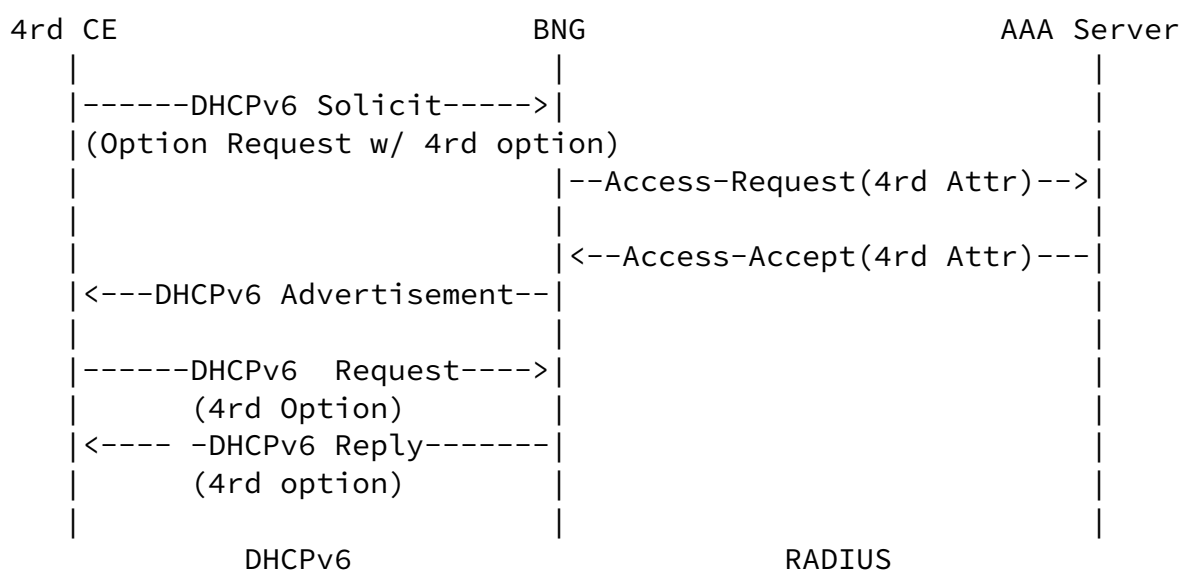


Figure 1: the cooperation between DHCPv6 and RADIUS combining with RADIUS authentication

BNGs act as a client of RADIUS and as a DHCPv6 server. First, the 4rd CE MAY initiate a DHCPv6 Solicit message that includes an Option Request option (6) [\[RFC3315\]](#) with the 4rd option [\[draft-ietf-software-4rd\]](#) from the 4rd CE. When BNG receives the SOLICIT, it SHOULD initiate an RADIUS Access-Request message, in which the User-Name attribute (1) SHOULD be filled by the 4rd CE MAC address, to the RADIUS server and the User-password attribute (2) SHOULD be filled by the shared 4rd password that has been preconfigured on the DHCPv6 server, requesting authentication as defined in [\[RFC2865\]](#) with 4rd-Configuration attribute, defined in the next Section. If the authentication request is approved by the AAA server, an Access-Accept message MUST contain the 4rd-Configuration Attribute. After receiving the Access-Accept message with 4rd-

Configuration Attribute, the BNG SHOULD respond to the user with an Advertisement message. Then the user can request a 4rd Option, the BNG SHOULD reply the user with a message containing the 4rd option. The recommended format of the MAC address is as defined in Calling-Station-Id ([Section 3.20 in \[RFC3580\]](#)) without the SSID (Service Set Identifier) portion.

Figure 2 describes another scenario, in which the authorization operation is not coupled with authentication. Authorization relevant to 4RD is done independently after the authentication process.

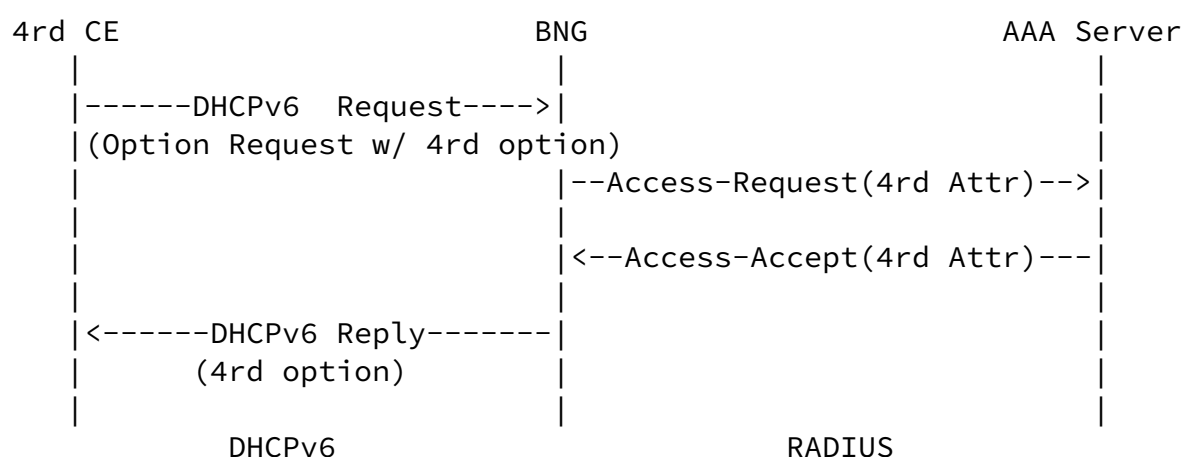


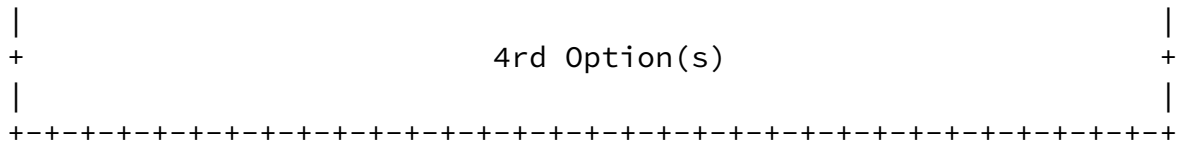
Figure 2: the cooperation between DHCPv6 and RADIUS decoupled with RADIUS authentication

In the abovementioned scenario, 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 obtained from the previous authentication process.

In both above-mentioned scenarios, Message-authenticator (type 80) [\[RFC2869\]](#) SHOULD be used to protect both Access-Request and Access-Accept messages.

After receiving the 4rd-Configuration Attribute in the initial





Type

TBD

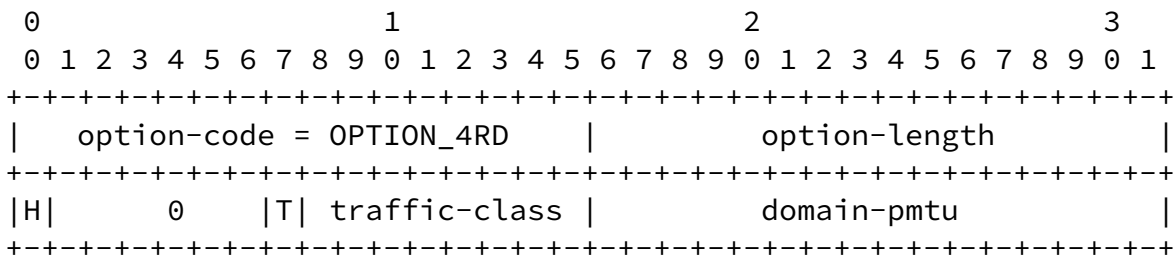
Length

6 + the length of the Rule option(s)

Sub Option

a variable field that may contains a 4rd non-mapping-rule parameter option andone or more Rule option(s), defined in [Section 4.2](#) and 4.3.

4.2. 4rd Non-mapping-rule Parameter option



Type

1

Length

4

H bit

Hub&spoke topology (= 1 if Yes)

T bit

Traffic-class flag (= 1 if a Tunnel traffic class is provided)

traffic-class

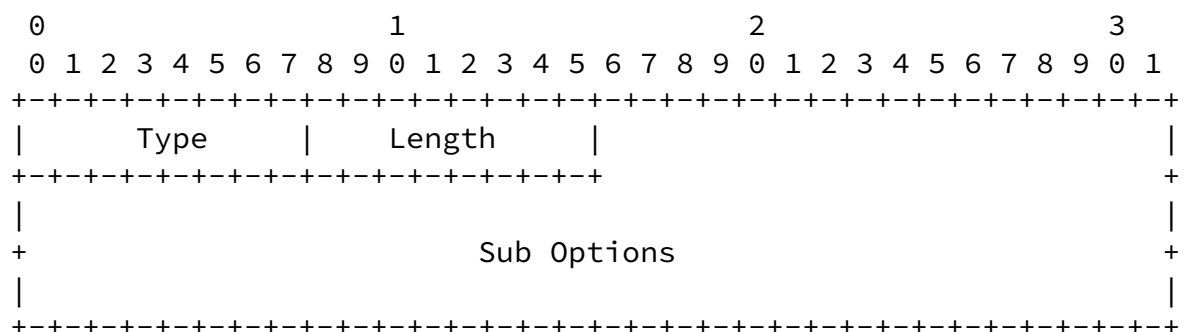
Tunnel-traffic class

domain-pmtu

Domain PMTU (at least 1280)

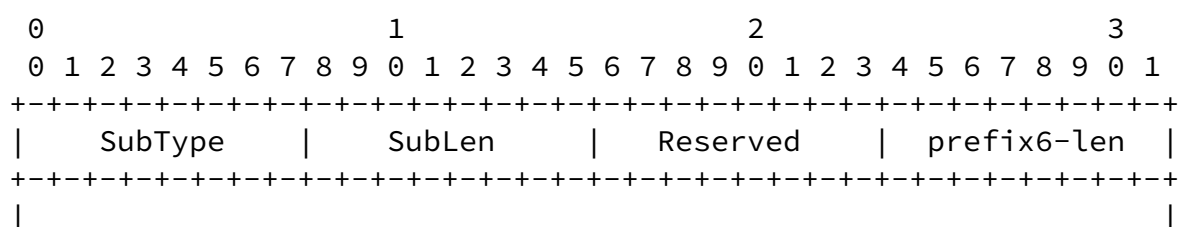
### 4.3. 4rd Rule Options

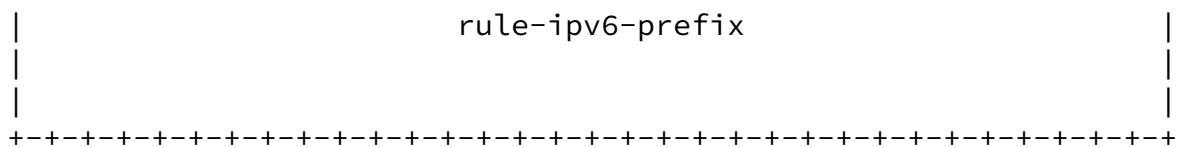
Depending on deployment scenario, at least one BR Mapping Rule one and one or more CE Mapping Rules MUST be included in one 4rd-Configuration Attribute.



Type







SubType

0 (SubType number, for the Rule-IPv6-Prefix6 sub option)

SubLen

20 (the length of the Rule-IPv6-Prefix6 sub option)

Reserved

Reserved for future usage. It should be set to all zero.

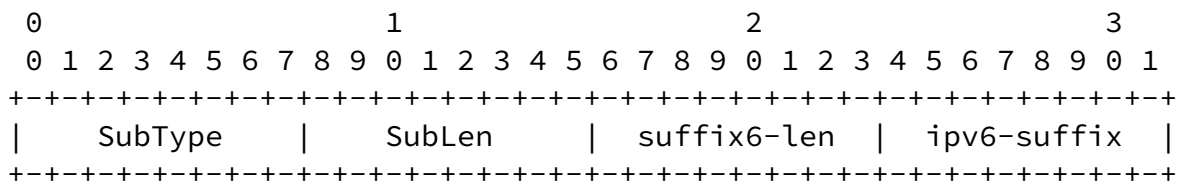
prefix6-len

length of the IPv6 prefix, specified in the rule-ipv6-prefix field, expressed in bits

rule-ipv6-prefix

a 128-bits field that specifies an IPv6 prefix that appears in a 4rd rule

4.4.2. Rule-IPv6-Suffix Sub Option



SubType

1 (SubType number, for the Rule-IPv6-Suffix6 sub option)

SubLen

4 (the length of the Rule-IPv6-Suffix6 sub option)

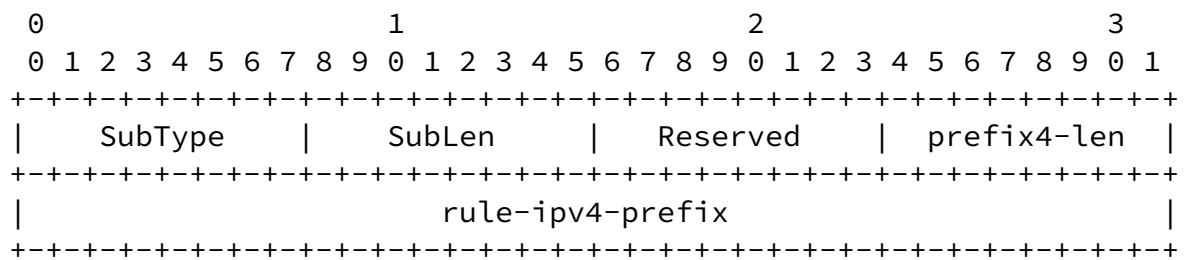
```
prefix6-len
```

length of the IPv6 suffix, specified in the rule-ipv6-suffix field, expressed in bits. In attendance, the value should be 1~4 only.

rule-ipv6-suffix

a 8-bits field that specifies an IPv6 suffix that appears in a 4rd rule

#### 4.4.3. Rule-IPv4-Prefix Sub Option



SubType

2 (SubType number, for the Rule-IPv4-Prefix6 sub option)

SubLen

8 (the length of the Rule-IPv4-Prefix6 sub option)

Reserved

Reserved for future usage. It should be set to all zero.

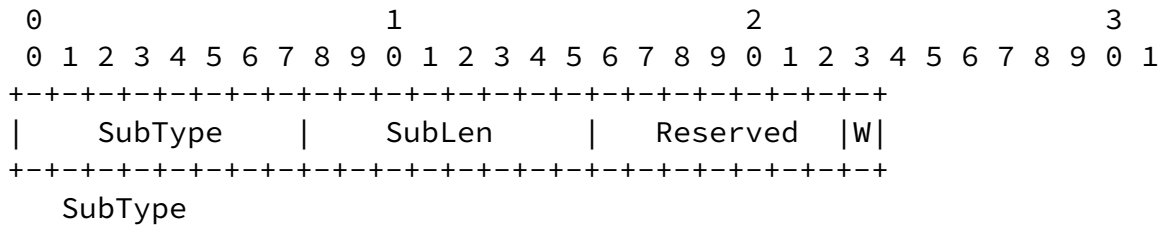
Prefix4-len

length of the IPv6 prefix, specified in the rule-ipv6-prefix field, expressed in bits

rule-ipv4-prefix

a 32-bits field that specifies an IPv4 prefix that appears in a 4rd rule

#### 4.4.4. Misc Sub Option



3 (SubType number, for the Rule-IPv4-Prefix6 sub option)

SubLen

1 (the length of the Rule-IPv4-Prefix6 sub option)

Reserved

Reserved for future usage. It should be set to all zero.

W bit

WKP authorized, = 1 if set

#### 4.5. 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	#	Attribute
0-1	0-1	0	0	0-1	TBD1	4rd-Configuration
0-1	0-1	0	0	0-1	1	User-Name
0-1	0	0	0	0-1	2	User-Password
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.   |

- 1 Exactly one instance of this attribute MUST be present in packet.

## [5.](#) Diameter Considerations

This attribute is usable within either RADIUS or Diameter [[RFC6733](#)]. Since the Attributes defined in this document will be allocated from the standard RADIUS type space, no special handling is required by Diameter entities.

## [6.](#) Security Considerations

In 6rd scenarios, both CE and BNG are within a provider network, which can be considered as a closed network and a lower security threat environment. A similar consideration can be applied to the RADIUS message exchange between BNG and the AAA server.

Known security vulnerabilities of the RADIUS protocol are discussed in [RFC 2607](#) [[RFC2607](#)], [RFC 2865](#) [[RFC2865](#)], and [RFC 2869](#) [[RFC2869](#)]. Use of IPsec [[RFC4301](#)] for providing security when RADIUS is carried in IPv6 is discussed in [RFC 3162](#) [[RFC3162](#)].

A malicious user may use MAC address spoofing and/or dictionary attack on the shared 4rd password that has been preconfigured on the DHCPv6 server to get unauthorized 4rd configuration information.

Security considerations for 4RD specific between 4RD CE and BNG are discussed in [[I-D.ietf-softwire-4rd](#)]. Furthermore, generic DHCPv6 security mechanisms can be applied DHCPv6 intercommunication between 4RD CE and BNG.

Security considerations for the Diameter protocol are discussed in [[RFC6733](#)].

## [7.](#) IANA Considerations

This document requires the assignment of two new RADIUS Attributes Types in the "Radius Types" registry (currently located at <http://www.iana.org/assignments/radius-types> for the following attributes:

- o 4rd-Configuration      TBD1

IANA should allocate the numbers from the standard RADIUS Attributes space using the "IETF Review" policy [[RFC5226](#)].

## [8](#). Acknowledgments

The authors would like to thank for valuable comments.

## [9](#). References

### [9.1](#). 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.
- [RFC3162] Aboba, B., Zorn, G., and D. Mitton, "RADIUS and IPv6", [RFC 3162](#), August 2001.
- [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.
- [[RFC4301](#)] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", [RFC 4301](#), December 2005.
- [RFC5080] Nelson, D. and DeKok A., "Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes", [RFC 5080](#), December 2007.
- [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [RFC 5226](#), May 2008.
- [RFC6158] DeKok, A. and G. Weber, "RADIUS Design Guidelines", [RFC 6158](#), March 2011.
- [RFC6733] V. Fajardo, Ed., J. Arkko, J. Loughney, G. Zorn, Ed., "Diameter Base Protocol", [RFC 6733](#), October 2012.

[I-D.ietf-softwire-4rd]

R. Despres, et al., "IPv4 Residual Deployment via IPv6 - a unified Stateless Solution (4rd)", [draft-ietf-softwire-4rd](#), working in progress.

## [9.2](#). Informative References

[RFC2607] Aboba, B. and J. Vollbrecht, "Proxy Chaining and Policy Implementation in Roaming", [RFC 2607](#), June 1999.

Jiang, et al.

Expires August 18, 2014

[Page 13]

---

Internet-Draft    [draft-jiang-softwire-4rd-radius-04](#)

February 2014

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

## Author's Addresses

Sheng Jiang (Editor)  
Huawei Technologies Co., Ltd  
Q14 Huawei Campus, 156 BeiQi Road,  
ZhongGuan Cun, Hai-Dian District, Beijing 100085  
P.R. China  
EMail: jiangsheng@huawei.com

Yu Fu  
Huawei Technologies Co., Ltd  
Q14 Huawei Campus, 156 BeiQi Road,  
ZhongGuan Cun, Hai-Dian District, Beijing 100085  
P.R. China  
EMail: eleven.fuyu@huawei.com

Bing Liu  
Huawei Technologies Co., Ltd  
Q14 Huawei Campus, 156 BeiQi Road,  
ZhongGuan Cun, Hai-Dian District, Beijing 100085  
P.R. China  
EMail: leo.liubing@huawei.com