Network Working Group   Sheng Jiang (Editor)
Internet Draft   Yu Fu
Intended status: Standards Track   Bing Liu
Expires: January 14, 2013   Huawei Technologies Co., Ltd
July 16, 2012

RADIUS Attribute for 4rd

draft-jiang-softwire-4rd-radius-01.txt

Status of this Memo

Copyright Notice

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

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

1. Introduction

Recently providers start to deploy IPv6 and consider how to transit to IPv6. IPv4 Residual Deployment via IPv6 (4rd) [I-D.ietf-softwire-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-softwire-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-softwire-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-softwire-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.

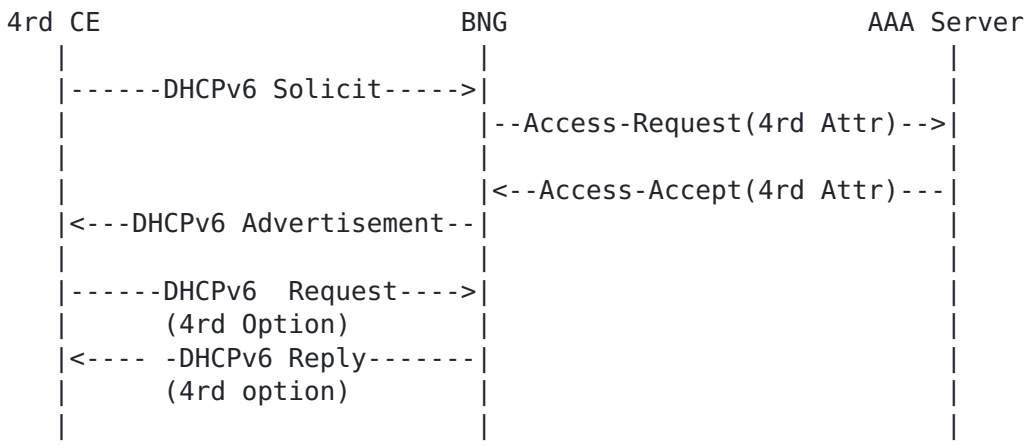


Figure 1: the cooperation between DHCPv6 and RADIUS

BNGs act as a client of RADIUS and as a DHCPv6 server for DHCPv6 protocol. First, a BNG receives a DHCPv6 Solicit message from the 4rd CE. It initiates the BNG to request correspondent user authentication relevant from an AAA server using RADIUS protocol. A 4rd configuration request may also be sent in the same message. If the user authentication is approved by the AAA server, an Access-Accept message is acknowledged with the IPv6-4rd-Configuration Attribute, defined in the next Section. After the BNG responds to the user with an Advertisement message, the user requests for a 4rd Option. Then, the BNG can reply the user using the DHCPv6 protocol.

In the abovementioned scenario, the Access-Request packet contains a Service-Type attribute with the value Authorize Only (17), thus according to [RFC5080] the Access-Request packet MUST contain a State attribute.

Figure 2 describes another scenario, in which the authentication operation is not coupled with DHCPv6. In the authentication stage, which may be initiated by other user behavior, such as PPP dial-up, the BNG obtains the 4rd configuration information from the AAA server through the RADIUS protocol. When the user requests the 4rd Option, the BNG replies with a 4rd option in DHCPv6 Reply message.

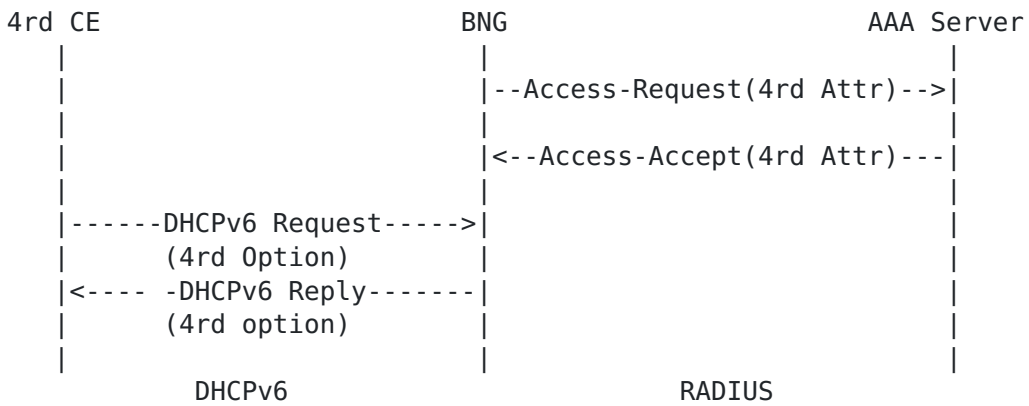


Figure 2: the cooperation between DHCPv6 and RADIUS

After receiving the IPv6-4rd-Configuration Attribute in the initial Access-Accept, the BNG MUST store the received 4rd configuration parameters locally. When the 4rd CE sends a DHCPv6 Request message to request an extension of the lifetimes for the assigned address, the BNG does not have to initiate a new Access-Request towards the AAA server to request the 4rd configuration parameters. The BNG retrieves the previously stored 4rd configuration parameters and use them in its reply.

If the DHCPv6 server to which the DHCPv6 Request message was sent at time T1 has not responded, the DHCPv6 client enters the Rebind state and attempts to contact any server. In this scenario the BNG receiving the DHCPv6 message MUST initiate a new Access-Request towards the AAA server. The BNG MAY include the IPv6-4rd-Configuration Attribute in its Access-Request. If the BNG does not receive the IPv6-4rd-Configuration Attribute in the Access-Accept it MAY fallback to a pre-configured default 4rd configuration, if any.

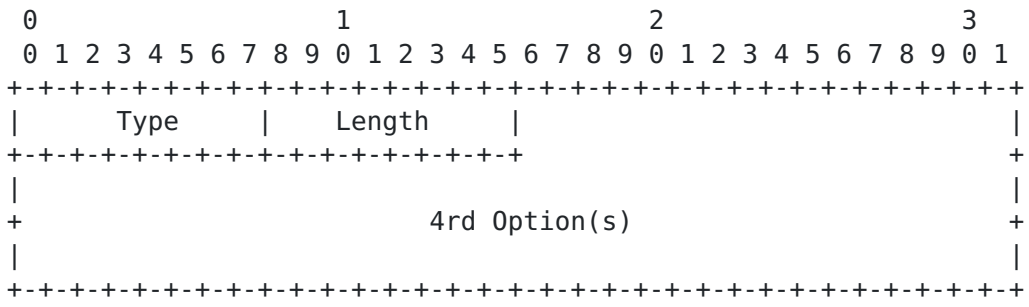
4. Attributes

This section defines IPv6-4rd-Configuration Attribute which is used in the 4rd scenario. The attribute design follows [RFC6158].

The 4rd RADIUS attribute are designed following the simplify principle. The sub options are organized into two categories: the necessary and the optional.

4.1. IPv6-4rd-Configuration Attribute

The IPv6-4rd-Configuration Attribute is structured as follows:



Type

TBD

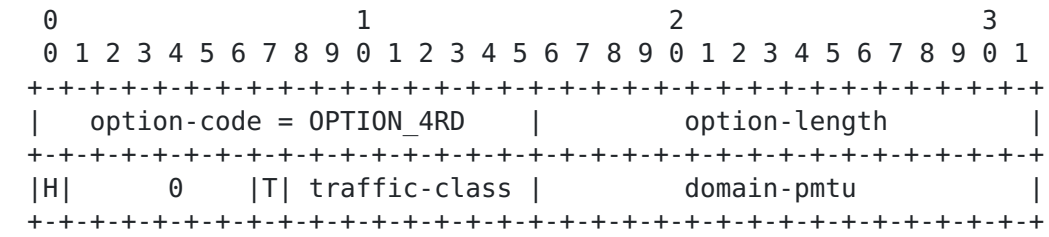
Length

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

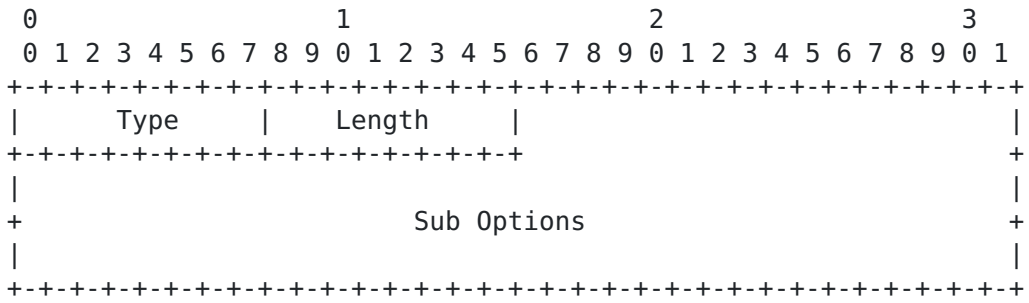
Tunnel-traffic class

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 IPv6-4rd-Configuration Attribute.



Type

2 BR Mapping Rule

3 CE Mapping Rule

Length

2 + the length of the sub options

Sub Option

a variable field that contains necessary sub options defined in Section 4.3 and zero or several optional sub options, defined in Section 4.4.

4.4. 4rd Rule Sub Options

Rule-IPv6-Prefix Sub Option and Rule-IPv4-Prefix Sub Option are necessary for every 4rd Rule option. They should appear for once and only once. Different from [I-D.ietf-softwire-4rd], EA-Len, Embedded-

Address (EA) length, is not present at all, because it can be calculated by the combine of prefix4len, prefix6-len, excluded ports and off bits.

4.4.1. Rule-IPv6-Prefix Sub Option

The IPv6 Prefix sub option is follow the framed IPv6 prefix designed in [RFC3162].

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.

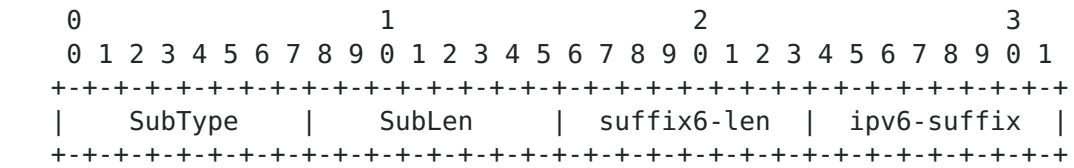
prefix6-len

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)

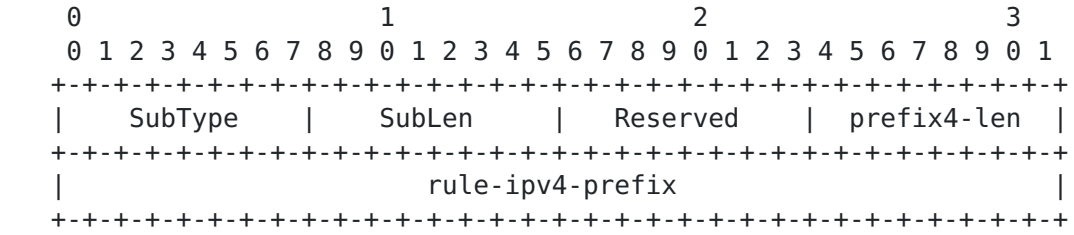
prefix6-len

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.

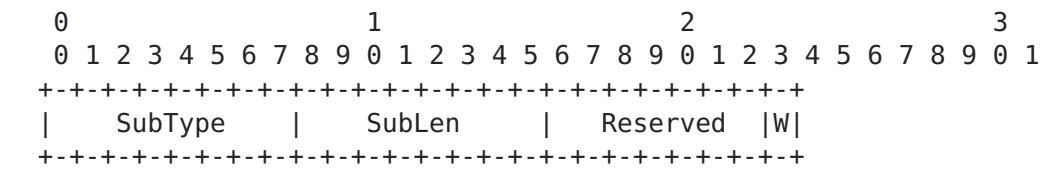
Prefix4-len

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



SubType

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 Request	#	Attribute
0-1	0-1	0	0	0-1	TBD1	IPv6-4rd-Configuration

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 [RFC3588]. 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

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].

Security considerations for the Diameter protocol are discussed in RFC 3588 [RFC3588].

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:

- IPv6-4rd-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.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J., Arkko, "Diameter Base Protocol", RFC 3588, September 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.

[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.

[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