

Network Working Group
Internet Draft
Intended status: Standards Track
Expires: July 14, 2012

Sheng Jiang (Editor)
Yu Fu
Huawei Technologies Co., Ltd
Peter Deacon
IEA Software, Inc.
January 12, 2012

RADIUS Attribute for MAP

[draft-jiang-softwire-map-radius-00.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 July 14, 2012.

Copyright Notice

Copyright (c) 2012 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

Mapping of Address and Port (MAP) 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) MAP options has been defined to configure MAP 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 MAP configuration information from AAA server to BNG. The MAP RADIUS attribute are designed following the simplify principle. It provides just enough information to form the correspondent DHCPv6 MAP option.

Table of Contents

| | | |
|------------------------|---|--------------------|
| 1. | Introduction | 3 |
| 2. | Terminology | 3 |
| 3. | MAP Configuration process with RADIUS | 3 |
| 4. | Attributes | 5 |
| 4.1. | IPv6-MAP-Configuration Attribute | 5 |
| 4.2. | MAP Rule Option | 6 |
| 4.3. | Necessary Sub Options | 7 |
| 4.3.1. | Rule-IPv6-Prefix Sub Option | 7 |
| 4.3.2. | Rule-IPv4-Prefix Sub Option | 8 |
| 4.4. | Optional Sub Options | 8 |
| 4.4.1. | Rule ID Sub Option | 8 |
| 4.4.2. | Encapsulation/Translation Flag Sub Option | 9 |
| 4.4.3. | Exclude Port Sub Option | 9 |
| 4.4.4. | Port Calculation Option | 10 |
| 4.5. | Table of attributes | 11 |
| 5. | Diameter Considerations | 11 |
| 6. | Security Considerations | 11 |
| 7. | IANA Considerations | 12 |
| 8. | Acknowledgments | 12 |
| 9. | References | 12 |
| 9.1. | Normative References | 12 |
| 9.2. | Informative References | 13 |

1. Introduction

Recently providers start to deploy IPv6 and consider how to transit to IPv6. Mapping of Address and Port (MAP) [[I-D.mdt-software-mapping-address-and-port](#)] 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. MAP has adopted Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [[RFC3315](#)] as auto-configuring protocol. The MAP Customer Edge (CE) uses the DHCPv6 extension options [[I-D.mdt-software-map-dhcp-option](#)] to discover MAP Border Relay (in tunnel model only) and to configure relevant MAP 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 MAP 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 MAP RADIUS attribute are designed following the simplify principle, while providing enough information to form the correspondent DHCPv6 MAP option. [[I-D.mdt-software-map-dhcp-option](#)].

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 MAP CE and MAP Border Relay are defined in [[I-D.mdt-software-mapping-address-and-port](#)].

3. MAP Configuration process with RADIUS

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

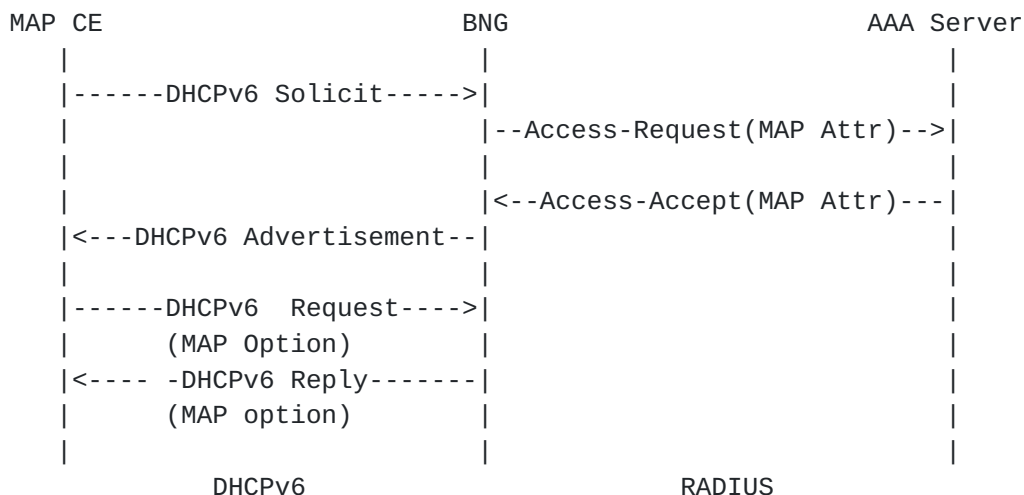


Figure 1: the cooperation between DHCPv6 and RADIUS

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 MAP CE. It initiates the BNG to request correspondent user authentication relevant from an AAA server using RADIUS protocol. A MAP 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-MAP-Configuration Attribute, defined in the next Section. After the BNG responds to the user with an Advertisement message, the user requests for a MAP 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 MAP configuration information from the AAA server through the RADIUS protocol. When the user requests the MAP Option, the BNG replies with a MAP option in DHCPv6 Reply message.

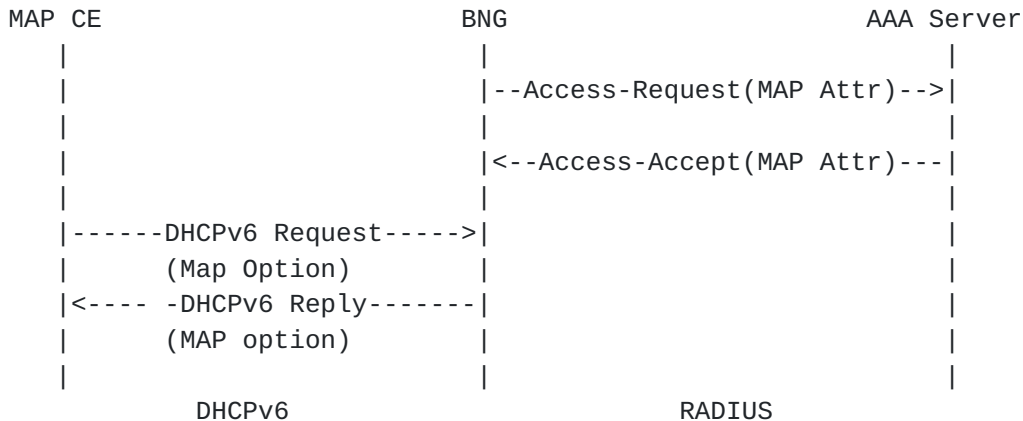


Figure 2: the cooperation between DHCPv6 and RADIUS

After receiving the IPv6-MAP-Configuration Attribute in the initial Access-Accept, the BNG MUST store the received MAP configuration parameters locally. When the MAP 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 MAP configuration parameters. The BNG retrieves the previously stored MAP 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-MAP-Configuration Attribute in its Access-Request. If the BNG does not receive the IPv6-MAP-Configuration Attribute in the Access-Accept it MAY fallback to a pre-configured default MAP configuration, if any.

4. Attributes

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

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

4.1. IPv6-MAP-Configuration Attribute

The IPv6-MAP-Configuration Attribute is structured as follows:




```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Type   |   Length   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|
+           Rule Option(s)
|
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Type

TBD

Length

2 + the length of the Rule option(s)

Sub Option

a variable field that may contains one or more Rule option(s), defined in [Section 4.2](#).

4.2. MAP Rule Option

Depending on deployment scenario, one or more MAP Rules may be included in one IPv6-MAP-Configuration Attribute.

```

      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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Type   |   Length   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|
+           Sub Options
|
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Type

0

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](#).

4.3. Necessary Sub Options

Rule-IPv6-Prefix Sub Option and Rule-IPv4-Prefix Sub Option are necessary for every MAP Rule option. They should appear for once and only once.

4.3.1. 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

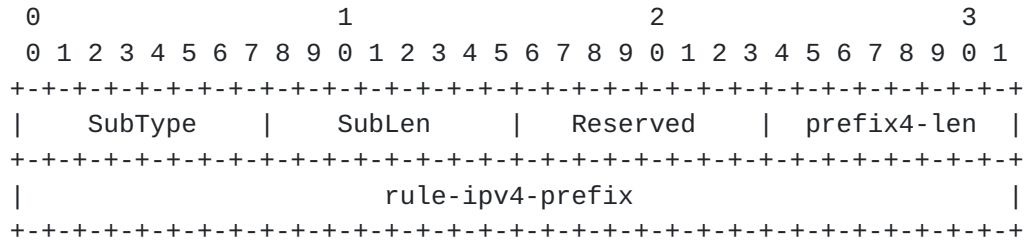
length of the IPv6 prefix, specified in the rule-ipv6-prefix field, expressed in bits

rule-ipv6-prefix

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

"For the encapsulation mode the Rule IPv6 prefix can be the full IPv6 address of the BR." [[I-D.mdt-software-mapping-address-and-port](#)]

4.3.2. Rule-IPv4-Prefix Sub Option



SubType

1 (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

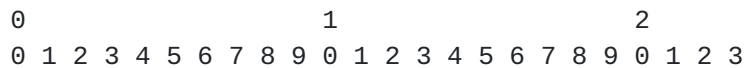
rule-ipv4-prefix

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

4.4. Optional Sub Options

This section presents several optional sub options. They may appear once in each Rule Option. Different from [[I-D.mdt-software-map-dhcp-option](#)], 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 ID Sub Option




```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|  SubType   |  SubLen   |  rule-id   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

SubType

2 (SubType number, for the rule-id sub option)

SubLen

3 (the length of the rule-id sub option)

rule-id

identifier that uniquely identifies this rule.

4.4.2. Encapsulation/Translation Flag Sub Option

```

0                               1                               2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|  SubType   |  SubLen   |  E/T Flag  |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

SubType

3 (SubType number, for the rule-id sub option)

SubLen

3 (the length of the rule-id sub option)

E/T Flag

indicate the MAP transport mode: encapsulation or translation.
all 0 for encapsulation, all 1 for translation.

If this sub option is not present, the following default values are to be assumed: encapsulation mode.

4.4.3. Exclude Port Sub Option

```

0                               1                               2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|  SubType   |  SubLen   |  exclude-port |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```


SubType

4 (SubType number, for the exclude-port sub option)

SubLen

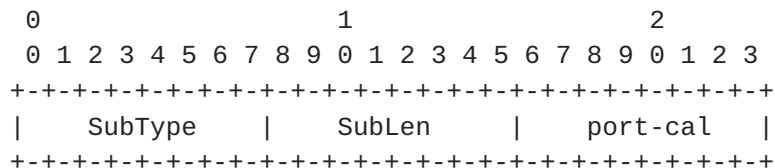
3 (the length of the exclude-port sub option)

excluded-ports: defines upper bound for range of excluded ports. The lower range is 0. For example, for value 2047, excluded range is 0-2047 ports. Value of 0 (range 0-0) means that no ports are excluded.

If this sub option is not present, the following default values are to be assumed: Excluded ports: 0-1023 (excluded-ports field value is 1023).

4.4.4. Port Calculation Option

Port Calculation Sub Option includes parameters that will be used to calculate IPv4/IPv6 address and port mapping.



SubType

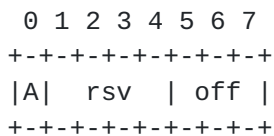
5 (SubType number, for the port-cal sub option)

SubLen

3 (the length of the port-cal sub option)

Port-cal field

Port-cal field include 3 parts as below:



A: Specifies if the offset is for a (0) or m (1).

svd: This 4-bits long field is currently not used and MUST be set to 0 by server. Its value MUST be ignored by clients.

off: specifies offset bits. Currently defined values are 4 and 6.

If this sub option is not present, the following default values are to be assumed:

- a). A: offset is for a (A field value is 0)
- b). Offset bits: 6 (off field value is 6)

If administrator wants to provision only one of those two parameters, remaining fields SHOULD be set to their default value.

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 | Request 0-1 | TBD1 | IPv6-MAP- 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:

- o IPv6-MAP-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.mdt-software-mapping-address-and-port]
O. Troan, "Mapping of Address and Port (MAP)", [draft-mdt-software-mapping-address-and-port](#), working in progress.

[I-D.mdt-software-map-dhcp-option]
T. Mrugalski, "DHCPv6 Options for Mapping of Address and Port", [draft-mdt-software-map-dhcp-option](#), 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

Peter Deacon
IEA Software, Inc.
P.O. Box 1170
Veradale, WA 99037
USA
EMail: peterd@iea-software.com