Softwire   S. Jiang
Internet-Draft   Huawei Technologies Co., Ltd
Intended status: Standards Track   Y. Fu
Expires: June 25, 2016   CNNIC
                                                             B. Liu
                                           Huawei Technologies Co., Ltd
                                                           P. Deacon
                                                    IEA Software, Inc.
                                                  December 23, 2015

RADIUS Attribute for MAP
draft-ietf-softwire-map-radius-05

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.

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 June 25, 2016.

Copyright Notice

Table of Contents

1. Introduction

Recently providers start to deploy IPv6 and consider how to transit
to IPv6. Mapping of Address and Port (MAP)[I-D.ietf-softwire-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. 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.ietf-softwire-map-dhcp] to discover MAP Border
Relay (in tunnel model only) and to configure relevant MAP rules.

In many networks, user configuration information may be stored 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
initiated by hosts.

Since the MAP configuration information is stored in AAA servers and
user configuration is mainly transmitted 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
attributes designed in this document are especially for the MAP
encapsulation mode, while providing enough information to form the
correspondent DHCPv6 MAP option [I-D.ietf-softwire-map-dhcp].

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].

The terms MAP CE and MAP Border Relay are defined in
[I-D.ietf-softwire-map].

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.

```
     MAP CE                        BNG                      AAA Server
       |                            |                            |
       |------DHCPv6 Solicit----->|                            |
       |(Option Request w/ MAP option)                          |
       |                          |--Access-Request(MAP Attr)-->|
       |                          |                            |
       |                          |<--Access-Accept(MAP Attr)---|
       |<---DHCPv6 Advertisement--|                            |
       |                          |                            |
       |------DHCPv6  Request---->|                            |
       |        (MAP Option)      |                            |
       |<---- -DHCPv6 Reply-------|                            |
       |        (MAP option)      |                            |
       |                          |                            |
              DHCPv6                        RADIUS
```
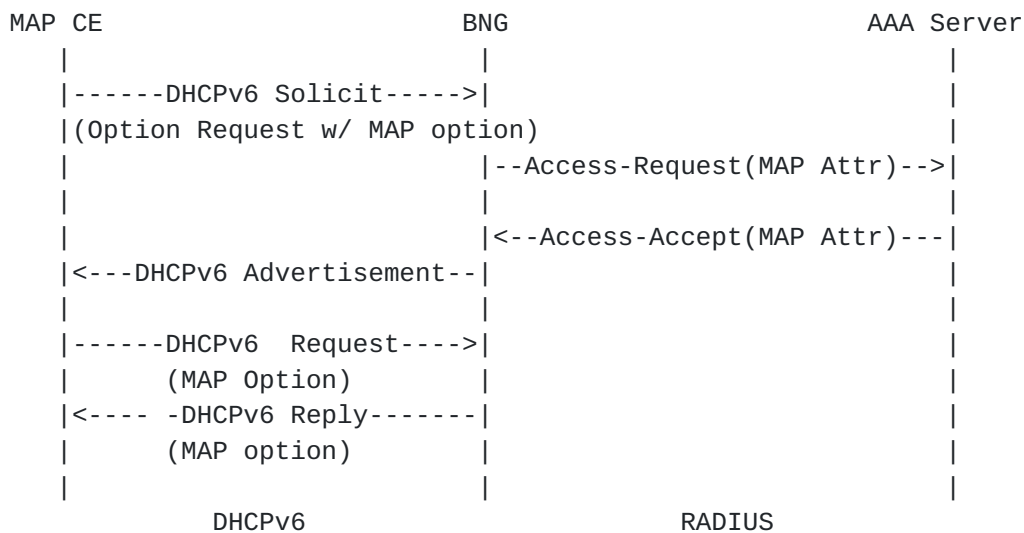
Figure 1: the cooperation between DHCPv6 and RADIUS combining with
                     RADIUS authentication

The BNG acts as a RADIUS client and as a DHCPv6 server. First, the
MAP CE MAY initiate a DHCPv6 Solicit message that includes an Option
Request option (6) [RFC3315] with the MAP option
[I-D.ietf-softwire-map-dhcp] from the MAP CE. But note that the ORO
(Option Request option) with the MAP option could be optional if the
network was planned as MAP-enabled as default. When BNG receives the
SOLICIT, it SHOULD initiates radius Access-Request message, in which
the User-Name attribute (1) SHOULD be filled by the MAP CE MAC
address or interface-id or both, to the RADIUS server and the User-
password attribute (2) SHOULD be filled by the shared MAP password
that has been preconfigured on the DHCPv6 server, requesting
authentication as defined in [RFC2865] with MAP-Configuration
attribute, which will be defined in the next Section. If the
authentication request is approved by the AAA server, an Access-
Accept message MUST be acknowledged with the IPv6-MAP-Configuration
Attribute. After receiving the Access-Accept message with MAP-
Configuration Attribute, the BNG SHOULD respond the user an
Advertisement message. Then the user can requests for a MAP Option,
and the BNG SHOULD reply the user with the message containing the MAP
option. The recommended format of the MAC address is defined as
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 MAP is done independently after the authentication process. As
similar to above scenario, the ORO with the MAP option in the initial
DHCPv6 request could be optional if the network was planned as MAP-
enabled as default.

```
     MAP CE                         BNG                    AAA Server
       |                             |                          |
       |------DHCPv6  Request---->|                          |
       |(Option Request w/ MAP option)                        |
       |                           |--Access-Request(MAP Attr)-->|
       |                             |                          |
       |                           |<--Access-Accept(MAP Attr)---|
       |                             |                          |
       |<-----DHCPv6 Reply--------|                          |
       |        (MAP option)       |                          |
       |                             |                          |
              DHCPv6                         RADIUS
```
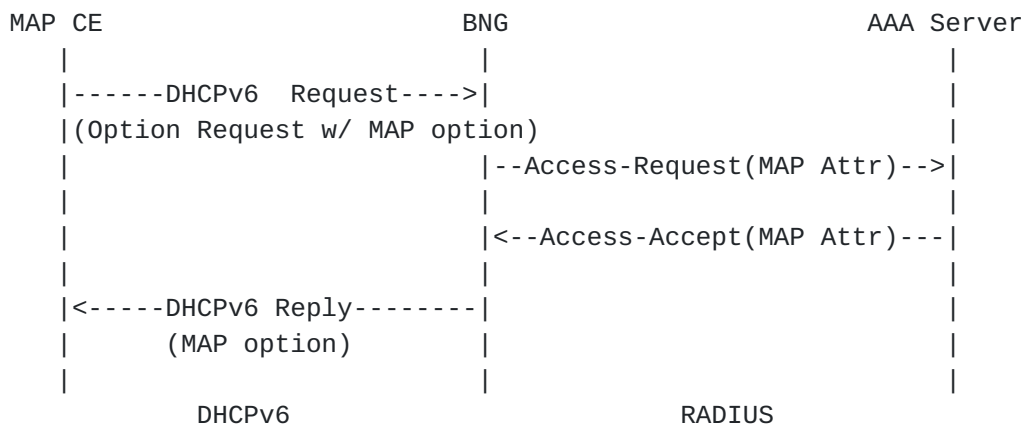
Figure 2: the cooperation between DHCPv6 and RADIUS decoupled with
                    RADIUS authentication

In the above mentioned 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 MAP-Configuration Attribute in the initial
Access-Accept, the BNG SHOULD 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
could retrieve the previously stored MAP configuration parameters and
use them in its reply.

If the BNG does not receive the MAP-Configuration Attribute in the
Access-Accept it MAY fallback to a pre-configured default MAP
configuration, if any. If the BNG does not have any pre-configured
default MAP configuration or if the BNG receives an Access-Reject,
the tunnel cannot be established.

As specified in [RFC3315], section 18.1.4, "Creation and Transmission
of Rebind Messages ", if the DHCPv6 server to which the DHCPv6 Renew
message was sent at time T1 has not responded by time T2, the MAP CE
(DHCPv6 client) SHOULD enters the Rebind state and attempt to contact
any available server. In this situation, the secondary BNG receiving
the DHCPv6 message MUST initiate a new Access-Request towards the AAA

server. The secondary BNG MAY include the MAP-Configuration
Attribute in its Access-Request.

4. Attributes

This section defines MAP-Rule Attribute which is used in the MAP
scenario. The attribute design follows [RFC6158] and refers
to[RFC6929].

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. MAP-Configuration Attribute

The MAP-Configuration Attribute is structured 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               +
|                                                               |
+                       MAP Rule Option(s)                      +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   Type
     TBD
   Length
     2 + the length of the Rule option(s)
   MAP Rule Option (s)
     A variable field that may contains one or more Rule option(s),
    defined in Section 4.2
```
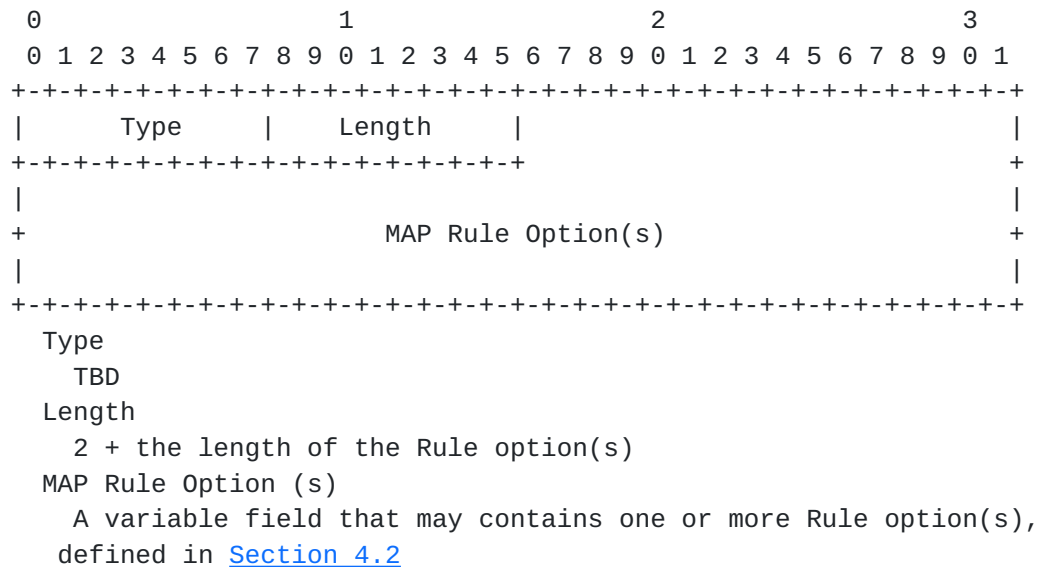
4.2. MAP Rule Options

Depending on deployment scenario, one Basic Mapping Rule and zero or
more Forwarding Mapping Rules MUST be included in one 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                           +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
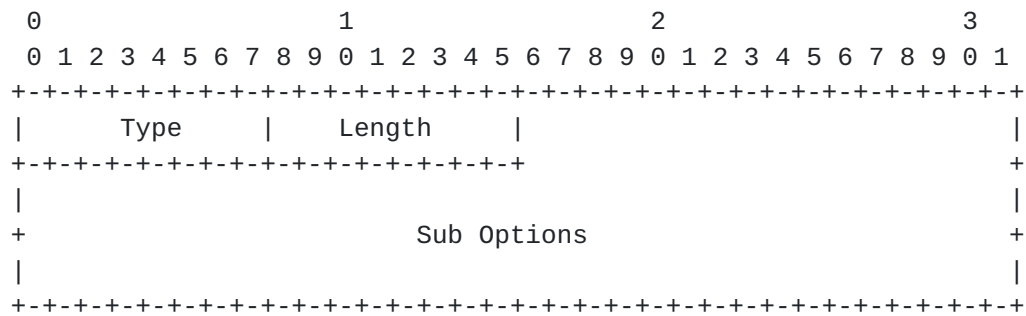
       Type
         1 Basic Mapping Rule (Not Forwarding Mapping Rule)
         2 Forwarding Mapping Rule (Not Basic Mapping Rule)
         3 Basic & Forwarding Mapping Rule
       Length
         2 + the length of the sub options
       Sub Option
         A variable field that contains necessary sub options defined in
         Section 4.3 and zero or several optional sub options, defined
         in Section 4.4

4.3. Sub Options for MAP Rule Option

4.3.1. Rule-IPv6-Prefix Sub Option

   The Rule-IPv6-Prefix Sub Option is necessary for every MAP Rule
   option. It should appear for once and only once.

   The IPv6 Prefix sub option is followed the framed IPv6 prefix
   designed in [RFC3162].
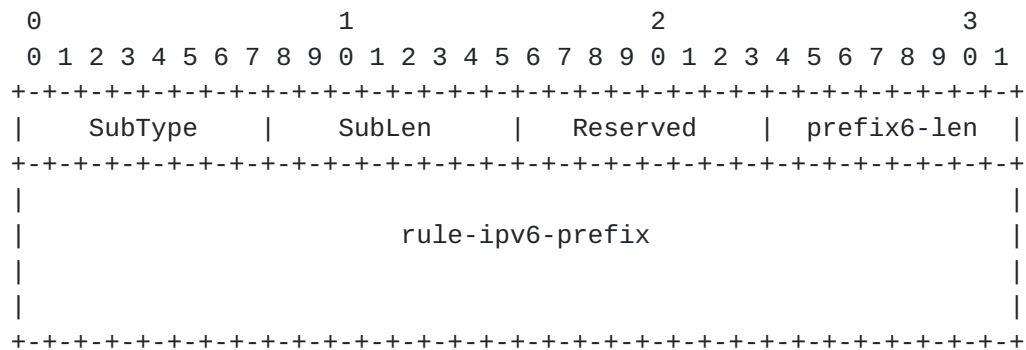
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    SubType    |    SubLen     |   Reserved    |  prefix6-len  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                        rule-ipv6-prefix                       |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     SubType
        1 (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
```

4.3.2. Rule-IPv4-Prefix Sub Option

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    SubType    |    SubLen     |   Reserved    |  prefix4-len  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        rule-ipv4-prefix                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

     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 MAP rule
```
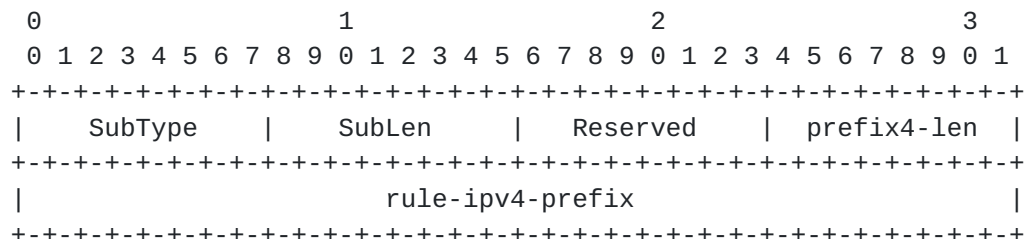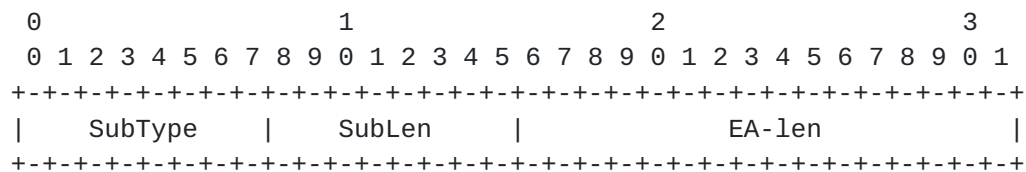
4.3.3. EA Length Sub Option

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    SubType     |    SubLen     |             EA-len            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

      SubType
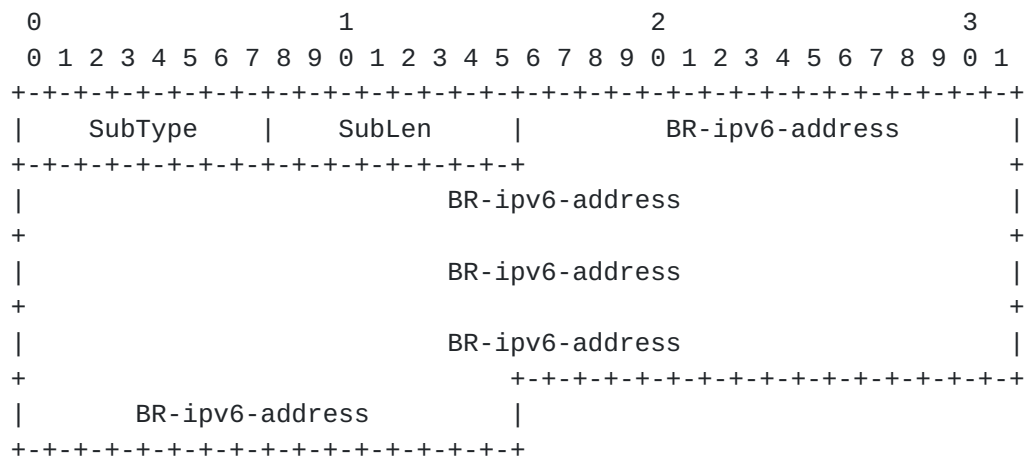   3 (SubType number, for the EA Length sub option)
      SubLen
         4 (the length of the EA Length sub option)
      EA-len
         16 bits long field that specifies the Embedded-Address (EA)
         bit length. Allowed values range from 0 to 48

4.3.4. BR-IPv6-Address Sub Option

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    SubType     |    SubLen     |          BR-ipv6-address      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               +
|                          BR-ipv6-address                      |
+                                                               +
|                          BR-ipv6-address                      |
+                                                               +
|                          BR-ipv6-address                      |
+                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      BR-ipv6-address          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

      SubType
         4 (SubType number, for the BR-ipv6-address sub option)
      SubLen
         20 (the length of the BR-ipv6-address sub option)
      BR-ipv6-address
         a 128-bits field that specifies the IPv6 address for the BR.

4.3.5. PSID Sub Option

```
   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
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |    SubType    |    SubLen     |               PSID            |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   SubType
      5 (SubType number, for the PSID Sub Option sub option)
   SubLen
      4 (the length of the PSID Sub Option sub option)
   PSID (Port-set ID)
      Explicit 16-bit (unsigned word) PSID value. The PSID value
      algorithmically identifies a set of ports assigned to a CE. The
      first k-bits on the left of this 2-octets field is the PSID
      value. The remaining (16-k) bits on the right are padding zeros.

4.3.6. PSID Length Sub Option

```
   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
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |    SubType    |    SubLen     |             PSID-len          |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   SubType
      6 (SubType number, for the PSID Length sub option)
   SubLen
      4 (the length of the PSID Length sub option)
   PSID-len
      Bit length value of the number of significant bits in the PSID
      field. (also known as 'k'). When set to 0, the PSID field is to
      be ignored. After the first 'a' bits, there are k bits in the
      port number representing valid of PSID. Subsequently, the
      address sharing ratio would be 2^k.

4.3.7. PSID Offset Sub Option

```
  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
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |    SubType     |    SubLen      |         PSID Offset         |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

    SubType
       7 (SubType number, for the PSID Offset sub option)
    SubLen
       4 (the length of the PSID Offset sub option)
    PSID Offset
       4 bits long field that specifies the numeric value for the MAP
       algorithm's excluded port range/offset bits (A-bits), as per
       section 5.1.1 in [I-D.ietf-softwire-map]. Default must be set
       to 4.

4.4. 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	MAP-Configuration
0-1	0-1	0	0	0-1	1	User-Name
0-1	0	0	0	0	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. 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 MAP-Configuration TBD1

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

7. Security Considerations

   In MAP 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 [RFC2607], [RFC2865], and[RFC2869]. Use of IPsec [RFC4301] for
   providing security when RADIUS is carried in IPv6 is discussed in
   [RFC3162].

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

   Security considerations for MAP specific between MAP CE and BNG are
   discussed in [I-D.ietf-softwire-map]. Furthermore, generic DHCPv6
   security mechanisms can be applied DHCPv6 intercommunication between
   MAP CE and BNG.

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

8. Acknowledgements

   The authors would like to thank the valuable comments made by Peter
   Lothberg, Wojciech Dec, Suresh Krishnan and Ross Chandler for this
   document.

   This document was produced using the xml2rfc tool [RFC2629].

9. References

9.1. 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,
            <http://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,
            <http://www.rfc-editor.org/info/rfc2865>.

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

[RFC3315]   Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins,
            C., and M. Carney, "Dynamic Host Configuration Protocol
            for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July
            2003, <http://www.rfc-editor.org/info/rfc3315>.

[RFC3580]   Congdon, P., Aboba, B., Smith, A., Zorn, G., and J. Roese,
            "IEEE 802.1X Remote Authentication Dial In User Service
            (RADIUS) Usage Guidelines", RFC 3580,
            DOI 10.17487/RFC3580, September 2003,
            <http://www.rfc-editor.org/info/rfc3580>.

[RFC5080]   Nelson, D. and A. DeKok, "Common Remote Authentication
            Dial In User Service (RADIUS) Implementation Issues and
            Suggested Fixes", RFC 5080, DOI 10.17487/RFC5080, December
            2007, <http://www.rfc-editor.org/info/rfc5080>.

[RFC6158]   DeKok, A., Ed. and G. Weber, "RADIUS Design Guidelines",
            BCP 158, RFC 6158, DOI 10.17487/RFC6158, March 2011,
            <http://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,
            <http://www.rfc-editor.org/info/rfc6929>.

9.2. Informative References

[I-D.ietf-softwire-map]
          Troan, O., Dec, W., Li, X., Bao, C., Matsushima, S.,
          Murakami, T., and T. Taylor, "Mapping of Address and Port
          with Encapsulation (MAP)", draft-ietf-softwire-map-13
          (work in progress), March 2015.

[I-D.ietf-softwire-map-dhcp]
          Mrugalski, T., Troan, O., Farrer, I., Perreault, S., Dec,
          W., Bao, C., Yeh, L., and X. Deng, "DHCPv6 Options for
          configuration of Softwire Address and Port Mapped
          Clients", draft-ietf-softwire-map-dhcp-12 (work in
          progress), March 2015.

[RFC2607] Aboba, B. and J. Vollbrecht, "Proxy Chaining and Policy
          Implementation in Roaming", RFC 2607,
          DOI 10.17487/RFC2607, June 1999,
          <http://www.rfc-editor.org/info/rfc2607>.

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629,
          DOI 10.17487/RFC2629, June 1999,
          <http://www.rfc-editor.org/info/rfc2629>.

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

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the
          Internet Protocol", RFC 4301, DOI 10.17487/RFC4301,
          December 2005, <http://www.rfc-editor.org/info/rfc4301>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an
          IANA Considerations Section in RFCs", BCP 26, RFC 5226,
          DOI 10.17487/RFC5226, May 2008,
          <http://www.rfc-editor.org/info/rfc5226>.

[RFC6733] Fajardo, V., Ed., Arkko, J., Loughney, J., and G. Zorn,
          Ed., "Diameter Base Protocol", RFC 6733,
          DOI 10.17487/RFC6733, October 2012,
          <http://www.rfc-editor.org/info/rfc6733>.

Authors' Addresses

      Sheng Jiang
      Huawei Technologies Co., Ltd
      Q14, Huawei Campus, No.156 Beiqing Road
      Hai-Dian District, Beijing, 100095
      P.R. China

      Email: jiangsheng@huawei.com

      Yu Fu
      CNNIC
      No.4 South 4th Street, Zhongguancun
      Hai-Dian District, Beijing, 100190
      P.R. China

      Email: fuyu@cnnic.cn

      Bing Liu
      Huawei Technologies Co., Ltd
      Q14, Huawei Campus, No.156 Beiqing Road
      Hai-Dian District, Beijing, 100095
      P.R. China

      Email: leo.liubing@huawei.com

      Peter Deacon
      IEA Software, Inc.
      P.O. Box 1170
      Veradale, WA 99037
      USA

      Email: peterd@iea-software.com