Softwire
Internet-Draft
Intended status: Standards Track
Expires: January 8, 2017

S. Jiang, Ed.
Huawei Technologies Co., Ltd
Y. Fu, Ed.
CNNIC
B. Liu
Huawei Technologies Co., Ltd
P. Deacon
IEA Software, Inc.
C. Xie
China Telecom
T. Li
Tsinghua University
July 7, 2016

RADIUS Attribute for Softwire
draft-ietf-softwire-map-radius-07

Abstract

IPv4-over-IPv6 transition mechanisms provide both IPv4 and IPv6 connectivity services simultaneously during the IPv4/IPv6 co-existing period. The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) options have been defined to configure Customer Edge (CE) in MAP-E, MAP-T, and Lightweight 4over6. 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 CE configuration information from AAA server to BNG.

Table of Contents

1. Introduction

Recently providers start to deploy IPv6 and consider how to transit to IPv6. Many transition mechanisms have been proposed for running IPv4 over IPv6-only infrastructure, including MAP-E, MAP-T, and Lightweight 4over6. Mapping of Address and Port with Encapsulation(MAP-E)[RFC7597], Mapping of Address and Port with using Translation(MAP-T)[RFC7599] are stateless mechanisms for running IPv4 over IPv6-only infrastructure. Lightweight 4over6[RFC7596] is a hub-and-spoke IPv4-over-IPv6 tunneling mechanism, with complete independence of IPv4 and IPv6 addressing. They provide both IPv4 and IPv6 connectivity services simultaneously during the IPv4/IPv6 co-existing period. MAP-E, MAP-T and Lightweight 4over6 have adopted Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [RFC3315] as auto-configuring protocol. The Customer Edge (CE) uses DHCPv6 options to discover the Border Relay (BR) and get S46 configurations.

In many networks, user configuration information may be stored in 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 S46 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 RADIUS attributes designed in this document are especially for the MAP-E[RFC7597], MAP-T[RFC7599] and Lightweight 4over6[RFC7596], providing enough information to form the correspondent DHCPv6 configuration options[RFC7598].

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].

3. Configuration process with RADIUS

The below Figure 1 illustrates how the RADIUS protocol and DHCPv6 cooperate to provide CE with MAP configuration information. The BNG acts as a RADIUS client and as a DHCPv6 server.

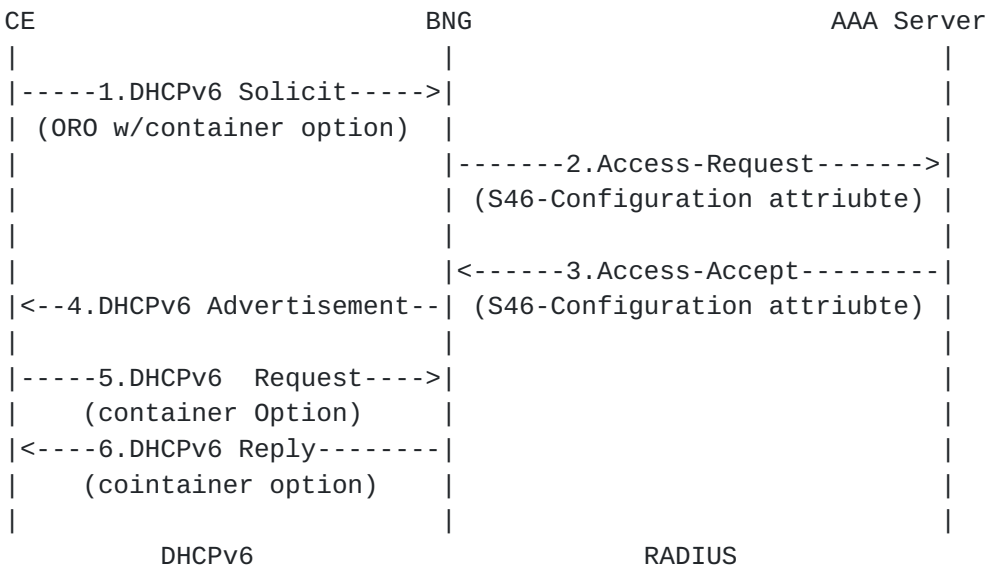


Figure 1: the cooperation between DHCPv6 and RADIUS combining with RADIUS authentication

1. First, CE MAY initiate a DHCPv6 Solicit message that includes an Option Request option(6) [RFC3315] with the S46 Container options as defined in[RFC7598]. OPTION_S46_CONT_MAPE should be included for MAP-E[RFC7597], OPTION_S46_CONT_MAPT for MAP-T[RFC7599], and OPTION_S46_CONT_LW for Lightweight 4over6[RFC7596]. But note that the ORO (Option Request option) with the S46 Container options could be optional if the network was planned as S46-enabled as default.

2. When BNG receives the SOLICIT, it SHOULD initiate the radius Access-Request message, in which the User-Name attribute (1) SHOULD be filled by the CE MAC address or interface-id or both, to the RADIUS server and the User-password attribute (2) SHOULD be filled by the shared password that has been preconfigured on the DHCPv6 server, requesting authentication as defined in [RFC2865] with the corresponding Softwire46-Configuration Attribute, which will be defined in the next Section.

3. If the authentication request is approved by the AAA server, an Access-Accept message MUST be acknowledged with the corresponding Softwire46-Configuration Attribute.

4. After receiving the Access-Accept message with the corresponding Attribute, the BNG SHOULD respond the user an Advertisement message.

5. After receiving the Advertise message, the user can request for the corresponding S46 Container option, by including the S46 Container option in the Request Message.

6. After receiving the client's Request messsage, containing the corresponding S46 Container option the BNG SHOULD reply the user with the message containing the S46 Container 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.

For Lightweight 4over6 [RFC7596], the subscriber's binding state should be synchronized between AAA server and the lwAFTR. If the bindings are pre-configured statically in both AAA server and lwAFTR, the AAA server does not need to configure lwAFTR anymore. Otherwise, if the bindings are locally creately in AAA server on-demand, it should inform the lwAFTR with the subscriber's binding state, to synchronise the binding information of the lwB4 with the lwAFTR. In the Lightweight 4over6 scenario, the lwB4 could also be configured through DHCPv4-over-DHCPv6 [RFC7341] as well as PCP [RFC6887], in which the lwB4 act a PCP client and the BNG act as both a Radius client and a PCP server.

The authorization operation could also be done independently after the authentication process. In such scenario, after the authentication operation, the client MAY initiate a DHCPv6 Request message that includes the corresponding S46 Container options. As similar to above scenario, the ORO with the corresponding S46 Container option in the initial DHCPv6 request could be optional if the network was planned as S46-enabled as default. When BNG receives the DHCPv6 Request, it SHOULD initiate the radius Access-Request message, which MUST contain a Service-Type attribute (6) with the value Authorize Only (17), the corresponding Softwire46-Configuration Attribute, and a State attribute obtained from the previous authentication process according to [RFC5080]. If the authorization request is approved by the AAA server, an Access-Accept message MUST be acknowledged with the corresponding Softwire46-Configuration Attribute. The BNG SHOULD then send the DHCPv6 Reply message containing the S46 Container option.

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

If the BNG does not receive the corresponding MAP-Configuration Attribute in the Access-Accept it MAY fallback to a pre-configured default S46 configuration, if any. If the BNG does not have any pre-configured default S46 configuration or if the BNG receives an Access-Reject, then S46 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 CE (DHCPv6 client) SHOULD enter 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.

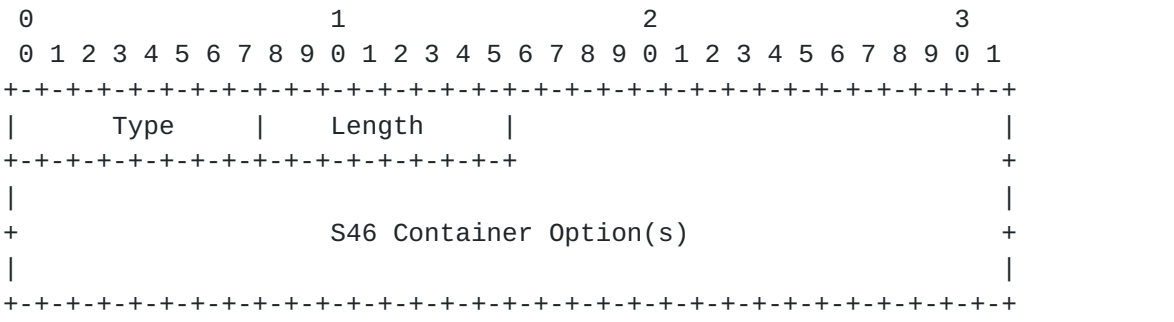
4. Attributes

This section defines S46 Attributes which are used in the MAP scenario. The attribute design follows [RFC6158] and refers to[RFC6929].

The S46 attributes are designed following the simplify principle. Different sub options are required for each type of S46 Container option.

4.1. Softwire46-Configuration Attribute

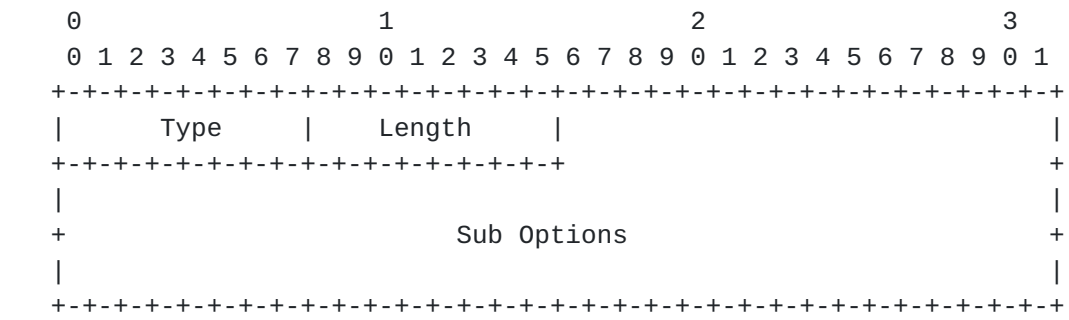
The Softwire46-Configuration Attribute is structured as follows:



Type
TBD
Length
2 + the length of the S46 Container option(s)
S46 Container Option (s)
A variable field that may contains one or more S46 Container option(s), defined in Section 4.2

4.2. S46 Container Options

Depending on the deployment scenario, a client might request for more than one transition mechanism at a time, at least one S46 Container option MUST be included in one MAP-Configuration Attribute.

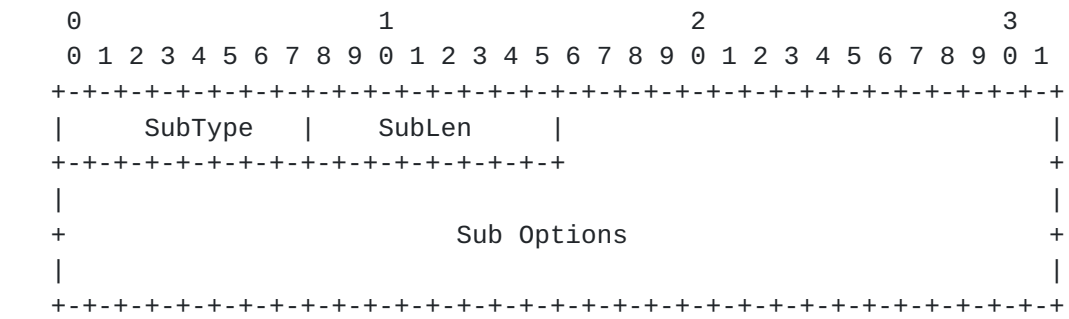


Type
1 MAP-E Container Option
2 MAP-T Container Option
3 Lightweight 4over6 Container Option
Length
2 + the length of the sub options
Sub Option
A variable field that contains necessary sub options defined in Section 4.3 and zero or several optional sub options, defined in Section 4.4

4.3. Sub Options for S46 Container Option

4.3.1. S46-Rule Sub Option

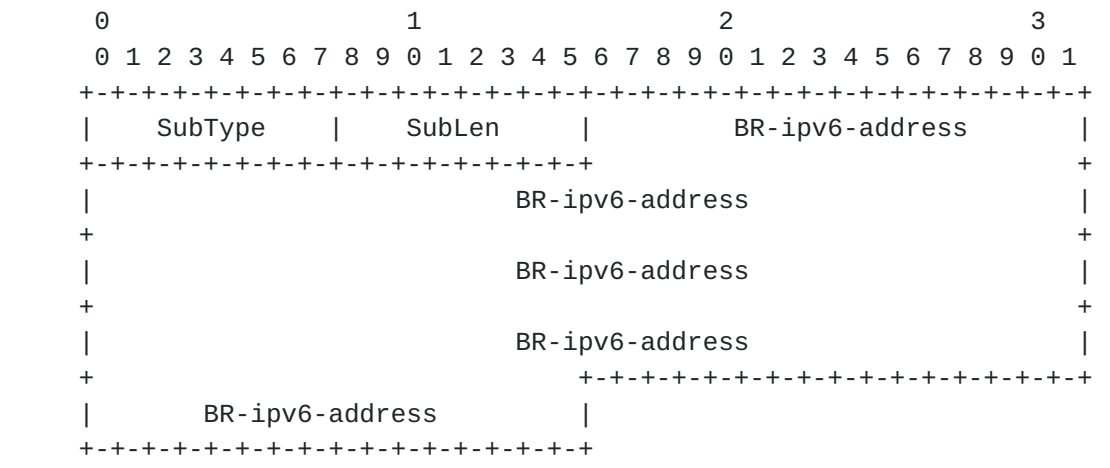
Depending on deployment scenario, one Basic Mapping Rule and zero or more Forwarding Mapping Rules MUST be included in one MAP-E or MAP-T Container Option.



SubType
1 Basic Mapping Rule (Not Forwarding Mapping Rule)
2 Forwarding Mapping Rule (Not Basic Mapping Rule)
3 Basic & Forwarding Mapping Rule
SubLen
2 + the length of the sub options
Sub Option
A variable field that contains sub options defined in Section 4.4

4.3.2. S46-BR Sub Option

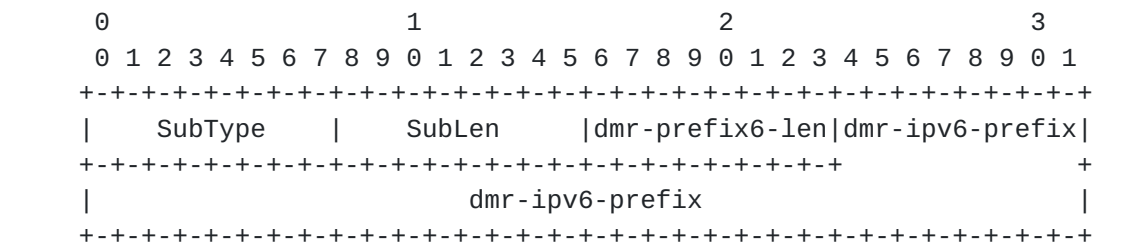
There MUST be atleast one S46-BR Sub Option included in each MAP-E Container Option or Lightweight 4over6 Container Option.



SubType
4 (SubType number, for the S46-BR sub option)
SubLen
18 (the length of the S46-BR sub option)
BR-ipv6-address
a 128-bits field that specifies the IPv6 address for the BR.

4.3.3. S46-DMR Sub Option

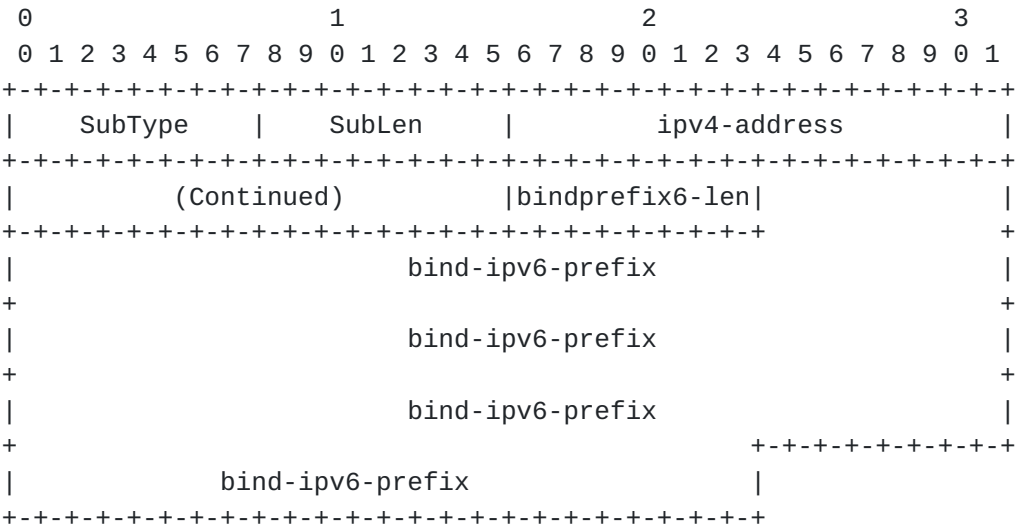
There MUST be exactly one S46-DMR Sub Option included in one MAP-T Container Option.



SubType
5 (SubType number, for the S46-DMR sub option)
SubLen
8 (the length of the Rule-IPv4-Prefix6 sub option)
dmr-prefix6-len
length of the IPv6 prefix, specified in the dmr-ipv6-prefix field, expressed in bits
dmr-ipv6-prefix
a 32-bits field that specifies an IPv6 prefix that appears in the Default Mapping Rule

4.3.4. S46-V4V6Bind Sub Option

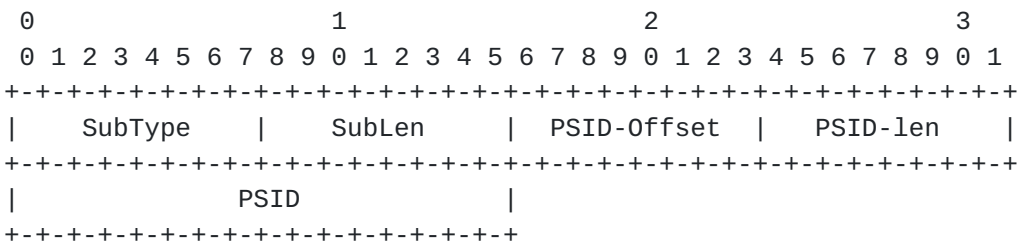
There MUST be atmost one S46-RULE Sub Option included in each Lightweight 4over6 Container Option.



SubType
6 (SubType number, for the S46-V4V6Bind sub option)
SubLen
23 (the length of the S46-V4V6Bind sub option)
ipv4-address
a 32-bits field that specifies an IPv4 address that appears in the V4V6Bind Option
bindprefix6-len
length of the IPv6 prefix, specified in the bind-ipv6-prefix field, expressed in bits
bind-ipv6-prefix
a 128-bits field that specifies an IPv6 prefix that appears in the V4V6Bind Option

4.3.5. S46-PORTPARAMS Sub Option

The S46-PORTPARAMS sub option specifies optional port set information that MAY be provided to CEs. The S46-PORTPARAMS sub option canbe included optionally by each type of S46 Container Option.



SubType
7 (SubType number, for the S46-PORTPARAMS Sub Option sub option)
SubLen
6 (the length of the S46-PORTPARAMS Sub Option sub option)
PSID Offset
8 bits long field that specifies the numeric value for the S46 algorithm's excluded
port range/ offset bits (a bits), as per Section 5.1 of RFC 7597.
Allowed values are between 0 and 15. Default values for this field are specific to the
Softwire mechanism being implemented and are defined in the relevant specification document.
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.
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.

4.4. Sub Options for S46-RULE Sub Option

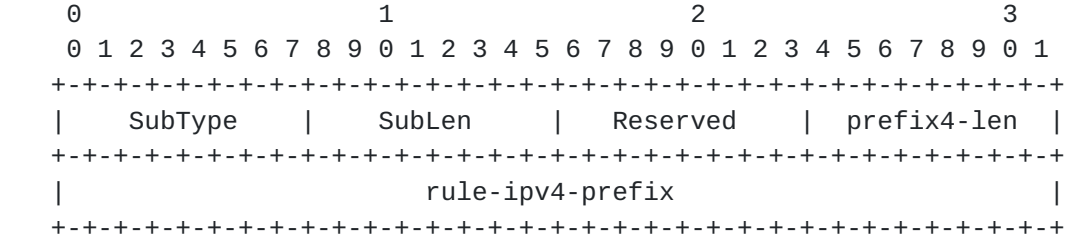
4.4.1. Rule-IPv6-Prefix Sub Option

The Rule-IPv6-Prefix Sub Option is necessary for every S46-RULE sub option. It should appear for once and only once.

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

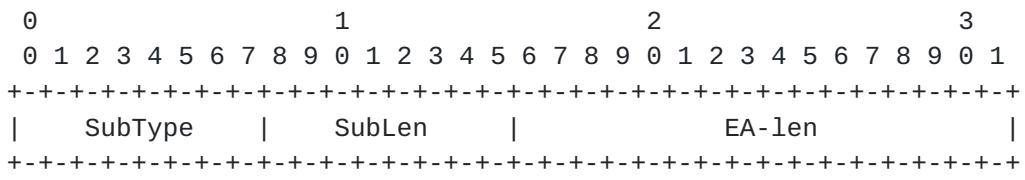
SubType
8 (SubType number, for the Rule-IPv6-Prefix6 sub option)
SubLen
20 (the length of the Rule-IPv6-Prefix6 sub option)
Reserved
Reserved for future usage. It should be set to all zero
prefix6-len
length of the IPv6 prefix, specified in the rule-ipv6-prefix field, expressed in bits
rule-ipv6-prefix
a 128-bits field that specifies an IPv6 prefix that appears in a MAP rule

4.4.2. Rule-IPv4-Prefix Sub Option



SubType
9 (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

4.4.3. EA Length Sub Option



SubType
10 (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

4.5. Softwire46 Sub Options Encapsulation

The table below shows which encapsulated Sub Options are mandatory, optional, or not permitted for each defined S46 Container Option.

Sub Option	MAP-E	MAP-T	Lightweight 4over6
S46-Rule	M	M	N/P
S46-BR	M	N/P	M
S46-DMR	N/P	M	N/P
S46-V4V6Bind	N/P	N/P	O
S46-PORTPARAMS	O	O	O

M - Maandabdatory, O - Optional, N/P - Not Permitted

4.6. 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	Softwire46-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

S46 Configuration using Diameter [RFC6733] is specified in [RFC7678].

6. IANA Considerations

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

o Softwire46-Configuration Attribute TBD1

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

7. Security Considerations

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 password that has been preconfigured on the DHCPv6 server to get unauthorized configuration information.

Security considerations for MAP specific between MAP CE and BNG are discussed in [RFC7597]. Security considerations for Lightweight

4over6 are discussed in [RFC7596]. Furthermore, generic DHCPv6 security mechanisms can be applied DHCPv6 intercommunication between 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, and Suresh Krishnan for this document. This document was merged with draft-sun-softwire-lw4over6-radext-01, thanks to everyone who contributed to this draft.

This document was produced using the xml2rfc tool [RFC7749].

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>.

[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>.

[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

[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>.

[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>.

[RFC6887] Wing, D., Ed., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", RFC 6887, DOI 10.17487/RFC6887, April 2013, <http://www.rfc-editor.org/info/rfc6887>.

[RFC7341] Sun, Q., Cui, Y., Siodelski, M., Krishnan, S., and I. Farrer, "DHCPv4-over-DHCPv6 (DHCP 4o6) Transport", RFC 7341, DOI 10.17487/RFC7341, August 2014, <http://www.rfc-editor.org/info/rfc7341>.

[RFC7596] Cui, Y., Sun, Q., Boucadair, M., Tsou, T., Lee, Y., and I. Farrer, "Lightweight 4over6: An Extension to the Dual-Stack Lite Architecture", RFC 7596, DOI 10.17487/RFC7596, July 2015, <http://www.rfc-editor.org/info/rfc7596>.

[RFC7597] Troan, O., Ed., Dec, W., Li, X., Bao, C., Matsushima, S., Murakami, T., and T. Taylor, Ed., "Mapping of Address and Port with Encapsulation (MAP-E)", RFC 7597, DOI 10.17487/RFC7597, July 2015, <http://www.rfc-editor.org/info/rfc7597>.

[RFC7598] 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", RFC 7598, DOI 10.17487/RFC7598, July 2015, <http://www.rfc-editor.org/info/rfc7598>.

[RFC7599] Li, X., Bao, C., Dec, W., Ed., Troan, O., Matsushima, S., and T. Murakami, "Mapping of Address and Port using Translation (MAP-T)", RFC 7599, DOI 10.17487/RFC7599, July 2015, <http://www.rfc-editor.org/info/rfc7599>.

[RFC7678] Zhou, C., Taylor, T., Sun, Q., and M. Boucadair, "Attribute-Value Pairs for Provisioning Customer Equipment Supporting IPv4-Over-IPv6 Transitional Solutions", RFC 7678, DOI 10.17487/RFC7678, October 2015, <http://www.rfc-editor.org/info/rfc7678>.

[RFC7749] Reschke, J., "The "xml2rfc" Version 2 Vocabulary", RFC 7749, DOI 10.17487/RFC7749, February 2016, <http://www.rfc-editor.org/info/rfc7749>.

Additional Authors

Qiong Sun
China Telecom
Beijing China
Email: sunqiong@ctbri.com.cn

Qi Sun
Tsinghua University
Department of Computer Science, Tsinghua University
Beijing 100084
P.R.China
Phone: +86-10-6278-5822
Email: sunqibupt@gmail.com

Cathy Zhou
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
Email: cathy.zhou@huawei.com

Tina Tsou
Huawei Technologies(USA)
2330 Central Expressway
Santa Clara, CA 95050
USA
Email: Tina.Tsou.Zouting@huawei.com

ZiLong Liu
Tsinghua University
Beijing 100084
P.R.China
Phone: +86-10-6278-5822
Email: liuzilong8266@126.com

Yong Cui
Tsinghua University
Beijing 100084
P.R.China
Phone: +86-10-62603059
Email: yong@csnet1.cs.tsinghua.edu.cn

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

Chongfeng Xie
China Telecom
Beijing
P.R. China

Email: xiechf@ctbri.com.cn

Tianxiang Li
Tsinghua University
Beijing 100084
P.R.China

Email: peter416733@gmail.com