

Softwire WG
Internet-Draft
Intended status: Standards Track
Expires: July 27, 2012

T. Mrugalski, Ed.
ISC
M. Boucadair
X. Deng
France Telecom
O. Troan
Cisco
C. Bao
Tsinghua University
January 24, 2012

DHCPv6 Options for Mapping of Address and Port
draft-mdt-softwire-map-dhcp-option-02

Abstract

Generic mechanism for mapping between an IPv4 prefix, address or parts of thereof, and transport layer ports and an IPv6 prefix or address is specified in [[I-D.mdt-softwire-mapping-address-and-port](#)]. This is a companion document that specifies provisioning mechanism of MAP rules. It defines DHCPv6 options which are meant to be used between Customer Edge (CE) devices and DHCPv6 server to obtain necessary parameters to configure MAP rules. Since specification of MAP architecture is still expected to evolve, DHCPv6 options may have to evolve too to fit the revised MAP specification.

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 27, 2012.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the

Internet-Draft

MAP DHCPv6 Options

January 2012

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.

Table of Contents

1.	Introduction	3
2.	Conventions	3
3.	Provisioning mechanism	3
4.	DHCPv6 Options Format	4
4.1.	Options Cardinality	5
4.2.	MAP Flags Option	5
4.3.	MAP Rule Option	6
4.4.	Port Parameters Option	8
4.5.	MAP Options Examples	9
4.5.1.	BMR Option Example	9
4.5.2.	FMR Option Example	9
4.5.3.	DMR Option Example	9
5.	DHCPv6 Server Behavior	9
6.	DHCPv6 Client Behavior	10
7.	IANA Considerations	11
8.	Security Considerations	11
9.	Contributors	11
10.	Acknowledgements	11
11.	References	12
11.1.	Normative References	12
11.2.	Informative References	12
	Authors' Addresses	13

1. Introduction

Mapping of Address and Port (MAP) defined in [\[I-D.mdt-softwire-mapping-address-and-port\]](#) is a mechanism for providing IPv4 connectivity service to end users over a service provider's IPv6 network. It defines both MAP Border Relay (BR) router that is located at the edge of a MAP domain and MAP Customer Edge (CE) that typically deployed at customers' location. In a residential broadband deployment, CE is sometimes referred to as a Residential Gateway (RG) or Customer Premises Equipment (CPE). A MAP CE may also be referred to simply as a "CE" within the context of MAP.

A typical CE adopting MAP rules will serve a residential site with one WAN side interface and one or more LAN side interfaces. To operate properly, it requires one or more MAP rules and additional informations. In larger networks it is infeasible to configure such parameters manually. Therefore provisioning mechanism is required. Such mechanism is defined in this document. It leverages existing DHCPv6 [\[RFC3315\]](#) protocol to deliver necessary parameters to CE.

This document defines several DHCPv6 options that allow delivery of required information to configure CE. Configuration of the BR is outside of scope of this document. Definitions of used parameters are provided in [\[I-D.mdt-softwire-mapping-address-and-port\]](#).

Since specification of MAP architecture is still expected to evolve, DHCPv6 options may have to evolve too to fit the revised MAP specification.

Described proposal is not a dynamic port allocation mechanism.

Reader interested in deployment considerations is encouraged to read [\[map-d\]](#).

[2.](#) Conventions

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 [RFC 2119](#) [[RFC2119](#)].

[3.](#) Provisioning mechanism

A typical MAP CE usually acts as a DHCPv6 client and requests options that are being provided by a DHCPv6 server located somewhere in ISP network. This server provides typical information to configured

nodes: namely IPv6 address (in IA_NA option) and delegates a prefix (in IA_PD option). Server also provides additional parameters that are MAP specific. In particular, it provides the following information:

- o One or more MAP rules. MAP mapping rules are defined in Section 4 of [[I-D.mdt-software-mapping-address-and-port](#)]. There are several mapping rule types defined: Basic Mapping Rule (BMR), Forwarding Mapping Rule (FMR) and Default Mapping Rule (DMR). Depending on rule type, number of exact useful parameters may be different. Rule parameters may contain Rule IPv6 prefix (including prefix length), Rule IPv4 prefix (including prefix length), and additional values that define Rule Port Parameters. One MAP CE can receive one or more MAP mapping rules from the DHCPv6 server. Exactly one of those rules MUST be the default MAP mapping rule for the initiated CE of its own, possibly accompanied with additional mapping rules within the MAP domain if necessary.
- o Transport mode indicates encapsulation or translation mode for MAP approach. It should be conducted on interface-by-interface basis.

[4.](#) DHCPv6 Options Format

DHCPv6 protocol is used for CE provisioning. Several new options are defined for conveying MAP-specific parameters. Their format and usage is defined in the following sections.

Discussion: As the exact parameters required to configure MAP rules and MAP in general are expected to change, this section is expected

to be updated or even rewritten completely.

Discussion: Proposed layout assumes that several simple options are used. Such approach simplifies implementation as it is much easier for implementors to reuse existing code handling such options. This design choice comes at a cost, however. Clients must perform checks if provided set of options is complete. Alternatively, it would be possible to define one complex option that contains all mandatory parameters.

Discussion: It should be noted that initial concept of 4rd provisioning was presented in DHC working group meeting. It used one complex option to convey all required parameters. Strong suggestion from DHC WG was to use several simpler options. Options (possibly nested) are preferred over conditional option formatting. See DHCP option guidelines document [[I-D.ietf-dhc-option-guidelines](#)]).

[4.1.](#) Options Cardinality

MAP rule is defined in [[I-D.mdt-software-mapping-address-and-port](#)], Section 4.

Discussion: If you want additional parameter added to the OPTION_MAP_RULE option (or any other option), please update [[I-D.mdt-software-mapping-address-and-port](#)] first.

Server that supports MAP configuration and is configured to provision requesting CE MUST include exactly one OPTION_MAP option in a REPLY message for each MAP domain. It is envisaged that in typical network, there will be only one MAP domain deployed.

OPTION_MAP option MUST include one or more OPTION_MAP_RULE options.

[4.2.](#) MAP Flags Option

This option specifies MAP flags and is used to group all rules for specified MAP domain. Currently the only defined flag is T that describes transport mode. Other flags that affect all mapping rules or the whole MAP domain may be specified here at a later date.

Each OPTION_MAP option MUST contain one or more MAP Rule Options.

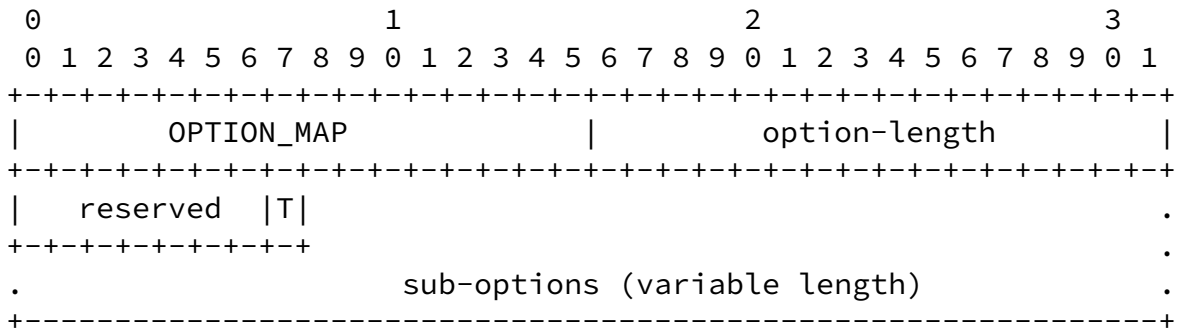


Figure 1: MAP Flags Option

- o option-code: OPTION_MAP (TBD1)
- o option-length: 1
- o reserved: This 7-bits long reserved field is not used and MUST be set to 0 by server. Its value MUST be ignored by clients.
- o T: 1 bit field that specifies transport mode: translation (0) or encapsulation (1).
- o suboptions: sub-options specific to this MAP domain. MUST contain one or more MAP_RULE options.

It was suggested to also provision information whether MAP network is

working in hub and spoke or full mesh mode. That is not necessary, as this information can be derived from provisioned MAP rules. In the hub and spoke mode, all traffic should be forwarded using DMR. Hub and spoke mode is achieved with a BMR IPv4 rule prefix length of 32 and no further FMR.

4.3. MAP Rule Option

MAP Rule Option option represents a single MAP Rule. Depending on deployment mode, each CE may require one or more MAP Rules to operate properly.

Server includes one or more MAP Rule Options in MAP Flags option.

Server MAY send more than one MAP Rule Option, if it is configured to

do so. Clients MUST NOT send MAP Rule Option.

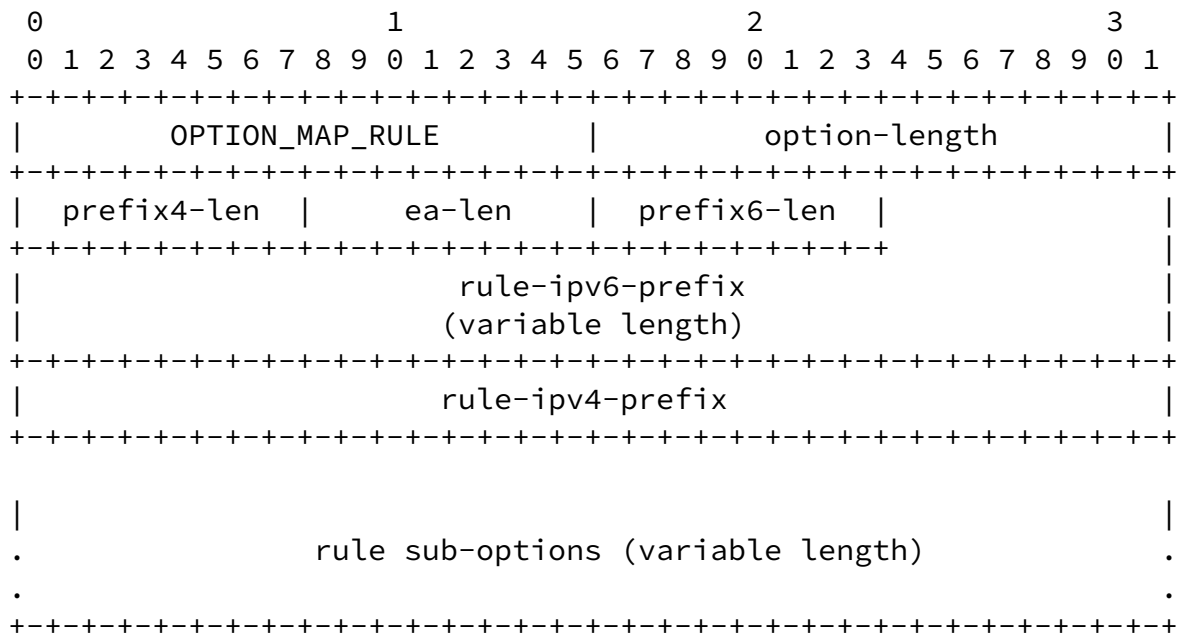


Figure 2: MAP Rule Option

Explicit parameters are:

- o option-code: OPTION_MAP_RULE (TBD2)
- o option-length: length of the option, excluding option-code and option-length fields, including length of all sub-options.
- o prefix4-len: 8 bits long field expressing length of the IPv4 prefix, specified in the rule-ipv4-prefix field, expressed in bits.

- o ea-len: 8-bits long field that specifies Embedded-Address (EA) - length, expressed in bits. This field is meaningful only for FMR. For other rules types, it MUST be set to zero by the server and its content MUST be ignored by the clients.
- o prefix6-len: 8 bits long length of the IPv6 prefix, specified in the rule-ipv6-prefix field, expressed in bits.
- o rule-ipv6-prefix: a variable size field that specifies Rule IPv6 prefix. Length of the field is defined by prefix6-len field and

is rounded up to the nearest octet boundary (if case when prefix6-len is not divisible by 8). In such case additional padding bits must be zeroed.

- o rule-ipv4-prefix: a 32-bits long field that specifies an IPv4 prefix that appears in a MAP rule.
- o rule sub-options: a variable field that may contains zero or more options that specify additional parameters for this rule. Those options follow standard DHCPv6 option format, as defined in [\[RFC3315\], Section 22.1](#). Currently there is only one option defined that may appear in rule sub-options field. This option is OPTION_MAP_PORTPARAMS, defined in section [Section 4.4](#). Other options may be defined at a later date.

There are also number of implicit parameters that may be derived from content of MAP and other options. In particular, End-User IPv6 Prefix (or Delegated prefix, specified in IA_PD option, see [\[RFC3633\]](#)) and assigned IPv6 address (specified in IA_NA option, see [\[RFC3315\]](#)) are needed. Even though these values are not provided explicitly, they are required for proper MAP rule configuration.

Following implicit parameters may be calculated:

- o rule type: Depending on rule content, it can be Basic Mapping Rule (BMR), Forwarding Mapping Rule (FMR) or Default Mapping Rule (DMR). See Sections [4.2](#), [4.3](#) and [4.4](#) in [\[I-D.mdt-software-mapping-address-and-port\]](#) for detailed description of those rules. A CE node can determine, which received rule is the basic rule based on the longest match between End-User IPv6 prefix (received in IAPREFIX option in IA_PD) and the Rule IPv6 prefix (received in Map Rule Option). A Default rule can be determined by the fact that it has Rule IPv4 prefix of 0.0.0.0/0.
- o Embedded Address bits (EA-bits) length can be derived as a length of the delegated prefix (specified in prefix-length field in IAPREFIX option) decreased by MAP Domain IPv6 prefix length (specified in prefix6-len of the DMR).

It is expected that in a typical simple scenarios, there will be a single BMR with a single DMR (that will also work as FMR). For detailed discussion about MAP deployment considerations, see [\[map-d\]](#).

Note that the DMR is a simplified version of BMR. While it reuses

the same DHCPv6 option format, DMR uses only Rule IPv6 prefix, Rule

IPv6 Prefix Length and IPv4 address that denotes BR IPv4 address. All other parameters are ignored for Default Mapping Rule. Client MUST ignore those parameters for DMR and server MUST set those parameters to zero.

4.4. Port Parameters Option

Port Parameters Option specifies optional Rule Port Parameters that MAY be provided as part of the Mapping Rule. It MAY appear as sub-option in OPTION_MAP_RULE option. It MUST NOT appear directly in a message.

See [[I-D.mdt-software-mapping-address-and-port](#)], Section 4.1 for detailed description of Port mapping algorithm.

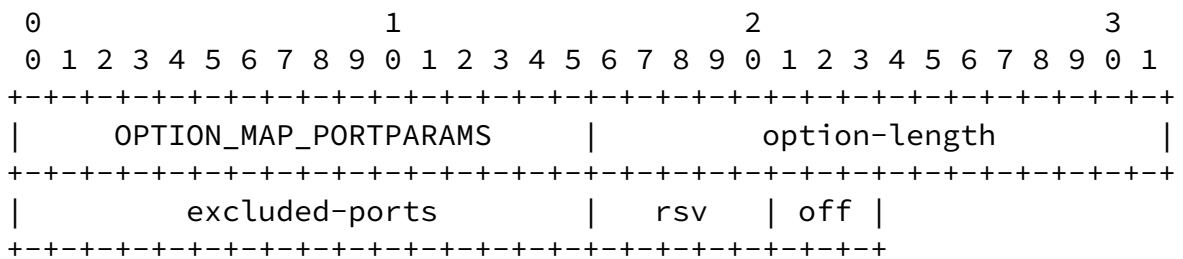


Figure 3: MAP Port Parameters Option

- o option-code: OPTION_MAP_PORTPARAMS (TBD3)
- o option-length: 3
- o excluded-ports: defines upper bound for range of excluded ports. The lower range is 0. For example a value 1023 means that excluded range is 0-1023 ports. Value of 0 (range 0-0) means that no ports are excluded.
- o rsvd: This 5-bits long field is currently not used and MUST be set to 0 by server. Its value MUST be ignored by clients.
- o off: 3 bits long field that specifies offset bits. It is referred to as 'a' value and specifies length of a A field, as presented in Fig. 1 in [[I-D.mdt-software-mapping-address-and-port](#)], [Section 4.1.1](#).

TODO: Ole pointed out that excluded-ports are related to the offset. with a = 6, j > 0 you exclude 0-1023; with a = 4, j > 0 you exclude 0-4095; with a = 0, no ports excluded and number of systems ports per user given by PSID/PSID length the flag would allow j = 0.

Map Port Parameters Option is optional. If it is not present, the following default values are assumed:

1. Excluded ports: 0-4095 (excluded-ports field value is 4095)

2. Offset bits: 4 (off field value is 4)

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

[4.5.](#) MAP Options Examples

DHCPv6 server provisioning a single MAP Rule to a CE (DHCPv6 client) will convey the following MAP options in its messages:

[4.5.1.](#) BMR Option Example

TODO: Reflect example in [section 4.2](#) of MAP draft

Figure 4: BMR Option Example

[4.5.2.](#) FMR Option Example

TODO: Reflect example in [section 4.3](#) of MAP draft

Figure 5: FMR Option Example

[4.5.3.](#) DMR Option Example

TODO: Reflect example in [section 4.4](#) of MAP draft

Figure 6: DMR Option Examples

[5.](#) DHCPv6 Server Behavior

[RFC 3315 Section 17.2.2](#) [[RFC3315](#)] describes how a DHCPv6 client and server negotiate configuration values using the ORO. As a convenience to the reader, we mention here that a server will not reply with a MAP Rule Option if the client has not explicitly enumerated it on its Option Request Option.

Server conformant to this specification MUST allow configuration of one or more MAP Rule Options.

Server MUST transmit all configured instances of the Mapping Rule Options with all sub-options, if client requested it using OPTION_MAP_RULE in its Option Request Option (ORO). Server MUST

transmit MAP Flags Option if client requested OPTION_MAP in its ORO.

Rules assignment is a stateless process from the server's perspective. Server does not need to maintain a state of rules provisioned to clients, track lifetimes, expire outdated rules etc. Server SHOULDs assign the same set of rules to all CEs in one MAP Domain, unless there are several classes of CEs defined, e.g. regular and premium users. In such case, each class of CEs is expected to get the same set of rules. Server is not expected to track MAP rules on a per CE basis. Exact assignment of specific rules to a specific CEs is outside of scope of this document.

6. DHCPv6 Client Behavior

Although other use cases are allowed, in a typical use case CE will act as DHCPv6 client and will request MAP configuration to be assigned by the DHCPv6 server located in the ISP network. A client that supports MAP CE functionality and conforms to this specification MUST include OPTION_MAP_RULE and OPTION_MAP in its ORO.

For proper operation, MAP CE client MUST also request IPv6 address (OPTION_IA_NA, defined in [[RFC3315](#)]) and prefix delegation (OPTION_IA_PD, defined in [[RFC3633](#)]). MAP CE client SHOULD NOT initiate DHCPv4 configuration for the purpose of MAP configuration as all parameters are delivered over DHCPv6.

Client supporting MAP functionality SHOULD request OPTION_MAP_RULE and OPTION_MAP options in SOLICIT, REQUEST, RENEW, REBIND and INFORMATION-REQUEST messages.

If client receives more than one OPTION_MAP_RULE option, it MUST use all received instances. It MUST NOT use only the first one, while discarding remaining ones.

Note that system implementing MAP CE functionality may have multiple network interfaces, and these interfaces may be configured differently; some may be connected to networks that call for MAP, and some may be connected to networks that are using normal dual stack or other means. The MAP CE system should approach this specification on an interface-by-interface basis. For example, if the CE system is

attached to multiple networks that provide the MAP Mapping Rule Option, then the CE system MUST configure a MAP connection (i.e. a translation or encapsulation) for each interface separately as each MAP provides IPv4 connectivity for each distinct interface. Means to bind a MAP configuration to a given interface in a multiple interfaces device are out of scope of this document.

7. IANA Considerations

IANA is kindly requested to allocate DHCPv6 option code TBD1 to the OPTION_MAP, TBD2 to OPTION_MAP_RULE and TBD3 to OPTION_MAP_PORTPARAMS. All three values should be added to the DHCPv6 option code space defined in [Section 24.3 of \[RFC3315\]](#).

8. Security Considerations

Implementation of this document does not present any new security issues, but as with all DHCPv6-derived configuration state, it is completely possible that the configuration is being delivered by a third party (Man In The Middle). As such, there is no basis to trust that the access over the MAP can be trusted, and it should not therefore bypass any security mechanisms such as IP firewalls.

Readers concerned with security of MAP provisioning over DHCPv6 are encouraged to familiarize with [\[I-D.ietf-dhc-secure-dhcpv6\]](#).

Section XX of [\[I-D.mdt-softwire-mapping-address-and-port\]](#) discusses security issues of the MAP mechanism.

[Section 23 of \[RFC3315\]](#) discusses DHCPv6-related security issues.

Section 6 of [\[I-D.murakami-softwire-4rd\]](#) discusses 4rd related security issues that are partially applicable to MAP mechanism.

9. Contributors

The current members of the MAP design team are: Congxiao Bao, Mohamed

Boucadair, Gang Chen, Maoke Chen, Wojciech Dec, Xiaohong Deng, Jouni Korhonen, Xing Li, Satoru Matsushima, Tomasz Mrugalski, Tetsuya Murakami, Jacni Qin, Necj Scoberne, Qiong Sun, Tina Tsou, Dan Wing, Leaf Yeh and Jan Zorz.

Former MAP design team members are: Remi Despres.

10. Acknowledgements

Authors would like to thank Jacni Qin, Qiong Sun and Remi Despres for their comments and suggestions.

11. References

Mrugalski, et al. Expires July 27, 2012 [Page 11]

Internet-Draft MAP DHCPv6 Options January 2012

11.1. Normative References

- [I-D.mdt-software-mapping-address-and-port]
Troan, O., "Mapping of Address and Port (MAP)",
[draft-mdt-software-mapping-address-and-port-02](#) (work in progress), November 2011.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [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.
- [RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", [RFC 3633](#), December 2003.

11.2. Informative References

- [I-D.boucadair-dhcpv6-shared-address-option]
Boucadair, M., Levis, P., Grimault, J., Savolainen, T., and G. Bajko, "Dynamic Host Configuration Protocol (DHCPv6) Options for Shared IP Addresses Solutions",
[draft-boucadair-dhcpv6-shared-address-option-01](#) (work in progress)

progress), December 2009.

[I-D.ietf-dhc-option-guidelines]

Hankins, D., "Guidelines for Creating New DHCP Options", [draft-ietf-dhc-option-guidelines-07](#) (work in progress), October 2011.

[I-D.ietf-dhc-secure-dhcpv6]

Jiang, S. and S. Shen, "Secure DHCPv6 Using CGAs", [draft-ietf-dhc-secure-dhcpv6-04](#) (work in progress), December 2011.

[I-D.mrugalski-dhc-dhcpv6-4rd]

Mrugalski, T., "DHCPv6 Options for IPv4 Residual Deployment (4rd)", [draft-mrugalski-dhc-dhcpv6-4rd-00](#) (work in progress), July 2011.

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

Murakami, T., Troan, O., and S. Matsushima, "IPv4 Residual Deployment on IPv6 infrastructure - protocol specification", [draft-murakami-softwire-4rd-01](#) (work in progress), September 2011.

Mrugalski, et al.

Expires July 27, 2012

[Page 12]

Internet-Draft

MAP DHCPv6 Options

January 2012

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 5226](#), May 2008.

[map-d] Chen, M., Sun, Q., and G. Chen, "Mapping of Address and Port (MAP) - Deployment Considerations", [draft-mdt-softwire-map-deployment](#) 00, 12 2012.

Authors' Addresses

Tomasz Mrugalski (editor)
Internet Systems Consortium, Inc.
950 Charter Street
Redwood City, CA 94063
USA

Phone: +1 650 423 1345

Email: tomasz.mrugalski@gmail.com

URI: <http://isc.org/>

Mohamed Boucadair

France Telecom

Rennes 35000

France

Email: mohamed.boucadair@gmail.com

URI: <http://www.francetelecom.com/>

Xiaohong Deng

France Telecom

Haidian district

Beijing 100190

China

Email: xiaohong.deng@orange.com

URI: <http://www.francetelecom.com/>

Mrugalski, et al.

Expires July 27, 2012

[Page 13]

Internet-Draft

MAP DHCPv6 Options

January 2012

Ole Troan

Cisco Systems, Inc.

Telemarksvingen 20

Oslo N-0655

Norway

Email: ot@cisco.com

URI: <http://cisco.com>

Congxiao Bao

CERNET Center/Tsinghua University
Room 225, Main Building, Tsinghua University
Beijing 100084
CN

Phone: +86 10-62785983
Email: congxiao@cernet.edu.cn