Softwire WG	T. Mrugalski, Ed.
Internet-Draft	ISC
Intended status: Standards Track	M. Boucadair
Expires: April 26, 2012	France Telecom
	O. Troan
	Cisco
	October 24, 2011

DHCPv6 Options for Mapping of Address and Port
draft-mdt-softwire-map-dhcp-option-00.txt

Abstract

Generic mechanism for mapping between an IPv4 prefix, address or parts of thereof, and transport layer between ports and an IPv6 prefix or address is specified in [map-design]. 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

Copyright Notice

Table of Contents

1. Introduction

Mapping of Address and Port (MAP) defined in [map-design] is a mechanism for providing IPv4 connectivity service to end users over a service provider's IPv6 network. It defines MAP Border Relay (BR) router that is located that the edge of a MAP domain. MAP Customer Edge (CE) is also defined as a device typically deployed at customers' location. In a residential broadband deployment, this type of device 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 MAP CE adopting MAP rules will serve a residential site with one WAN side interface, 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 [map-design].
Since specification of MAP architecture is still expected to evolve, DHCPv6 options may have to evolve too to fit the revised MAP specification.

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. It would adopt three kinds of parameters independently:

*MAP mapping rules are defined in [map-design], including Rule IPv6 prefix/length, Rule IPv4 prefix and BR IPv6 prefix. One MAP CE can receive one or more MAP mapping rules from the DHCPv6 server, the first of which should be the default MAP mapping rule for the initiated CE of its own, followed by other mapping rules within the MAP domain if necessary.

*Transport mode indicates encapsulation or translation mode for MAP approach. It should be conducted on interface-by-interface basis

*Discussion: Qiong also proposed to add deployment mode here. Jacni Qin recommends against it. Deployment mode is to notify whether CE is in Hub and spoke mode or mesh. In Hub and spoke mode, only the first default MAP mapping rule is needed in the following MAP procedure. While in mesh mode, all MAP mapping rules are included to achieve CE-CE traffic optimization.

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. MAP Options Cardinality

MAP rule is defined in [map-design], Section 4.
Discussion: If you want additional parameter added to the OPTION_MAP_RULE option, please update [map-design] first.
In each REPLY message, server that supports MAP configuration MUST include exactly one OPTION_MAP_FLAGS option.
MAP_FLAGS option MUST include one or more OPTION_MAP_RULE options.
For proper operation, additional parameters obtained via other options are necessary. In particular, L parameter is equal to a length of a prefix delegated to CE, conveyed in OPTION_IA_PD and IAPREFIX, as defined in [RFC3633].

4.2. MAP Flags Option

. This option specifies MAP flags. Currently the only defined flag is T - transport mode. 0 designates translation and 1 designates encapsulation.
Each MAP_FLAGS option MUST contain one or more MAP Rule Options.

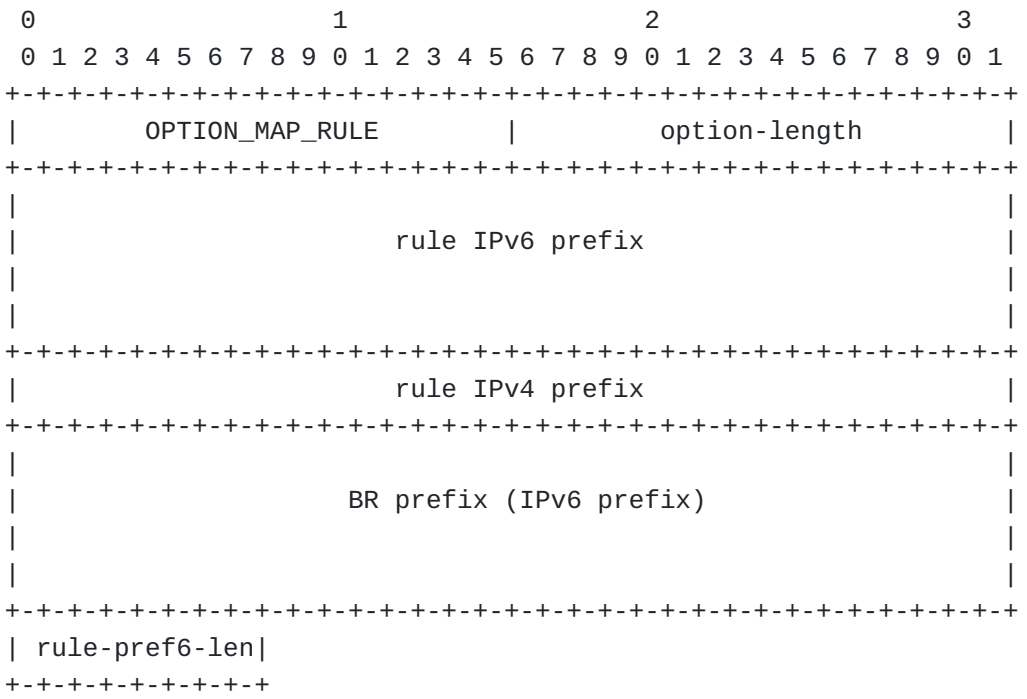
TODO: Add format here later

option-code: OPTION_MAP_FLAGS (TBD)

4.3. MAP Rule Option

This 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.

Discussion: Do we need to distinguish or reference rules? (i.e. Is some kind of ID field required?)
Server MAY send more than one MAP Rule Option, if it is configured to do so. Clients MUST NOT send MAP Rule Option.



*option-code: OPTION_MAP_RULE (TBD)

*option-length: 37 in octets

*rule-pref6-len: length for the rule IPv6 prefix in bits

*rule IPv6 prefix: an IPv6 prefix that appears in a MAP rule.

*rule IPv4 prefix: an IPv4 prefix that appears in a MAP rule.

*BR prefix: the IPv6 prefix of BR that appears in a MAP rule

4.4. MAP Options Example

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

```
<MAP_FLAGS>
    <MAP_RULE1/>
    <MAP_RULE2/>
    ...
    <MAP_RULEN/>
</MAP_FLAGS>
```

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 transmist 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_FLAGS 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 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 specfication MUST include OPTION_MAP_RULE and OPTION_MAP_FLAGS 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 as all parameters are delivered over DHCPv6.
Client SHOULD request OPTION_MAP_RULE and OPTION_MAP_FLAGS 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

This specification does not require any IANA actions.

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 [map-design] 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. IANA Considerations

IANA is requested to allocate DHCPv6 option codes referencing this document, delineating OPTION_MAP_RULE, OPTION_MAP_BR_PREFIX6, OPTION_MAP_PREFIX6, OPTION_MAP_PREFIX4 and OPTION_MAP_FLAGS option names.

10. Contributors

The members of the MAP design team are:

1. Mohamed Boucadair
2. Gang Chen
3. Wojciech Dec
4. Xiaohong Deng
5. Jouni Korhonen
6. Xing Li
7. Maoke
8. Satoru Matsushima

9. Tomasz Mrugalski

10. Jacni Qin

11. Tina Tsou

12. Ole Troan

13. Dan Wing

14. Leaf Yeh

15. Jan Zorz

11. Acknowledgements

Authors would like to thank Xiaohong Deng, Congxiao Bao, Jacni Qin, Qiong Sun for their comments and suggestions.

12. References

12.1. Normative References

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[map-design]	Troan, O., "Mapping of Address and Port (MAP)", draft-ietf-softwire-mapping-address-and-port 00, 10 2011.
[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.

12.2. Informative References

[I-D.ietf-dhc-option-guidelines]	Hankins, D, "Guidelines for Creating New DHCP Options", Internet-Draft draft-ietf-dhc-option-guidelines-07, October 2011.
[I-D.mrugalski-dhc-dhcpv6-4rd]	Mrugalski, T, "DHCPv6 Options for IPv4 Residual Deployment (4rd)", Internet-Draft draft-mrugalski-dhc-dhcpv6-4rd-00, July 2011.
[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", Internet-Draft draft-boucadair-dhcpv6-shared-address-option-01, December 2009.

[I-D.ietf-dhc-secure-dhcpv6]	Jiang, S and S Shen, "Secure DHCPv6 Using CGAs", Internet-Draft draft-ietf-dhc-secure-dhcpv6-03, June 2011.
[I-D.murakami-softwire-4rd]	Murakami, T, Troan, O and S Matsushima, "IPv4 Residual Deployment on IPv6 infrastructure - protocol specification", Internet-Draft draft-murakami-softwire-4rd-01, September 2011.

Authors' Addresses

Tomasz Mrugalski editor Mrugalski Internet Systems Consortium, Inc. 950 Charter Street Redwood City, CA 94063 USA Phone: +1 650 423 1345 EMail: tomasz.mrugalski@gmail.com

Mohamed Boucadair Boucadair France Telecom Rennes, 35000 France EMail: mohamed.boucadair@gmail.com

Ole Troan Troan Cisco Systems, Inc. Telemarksvingen 20 Oslo, N-0655 Norway EMail: ot@cisco.com