6man Working Group   A. Matsumoto
Internet-Draft   T. Fujisaki
Intended status: Standards Track   J. Kato
Expires: December 30, 2011   NTT
                                                              T. Chown
                                              University of Southampton
                                                         June 28, 2011

Distributing Address Selection Policy using DHCPv6
draft-ietf-6man-addr-select-opt-01.txt

Abstract

   RFC 3484 defines default address selection mechanisms for IPv6 that
   allow nodes to select appropriate address when faced with multiple
   source and/or destination addresses to choose between. The RFC
   allowed for the future definition of methods to administratively
   configure the address selection policy information. This document
   defines a new DHCPv6 option for such configuration, allowing a site
   administrator to distribute address selection policy, and thus
   control the address selection behavior of nodes in their site. While
   RFC 3484 is in the process of being updated, with a revised default
   policy table, that table may not suit every scenario, and thus the
   DHCPv6 option defined in this text may be used to override that
   policy where desired.

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 December 30, 2011.

Copyright Notice

1. Introduction

RFC 3484 [RFC3484] describes default algorithms for selecting an
address when a node has multiple destination and/or source addresses
to choose between by using an address selection policy. In Section 2
of RFC 3484, it is suggested that the default policy table may be
administratively configured to suit the specific needs of a site.
This text defines a new DHCPv6 option for such configuration.

Some problems have been identified with the default address selection
policy detailed in RFC 3484 [RFC5220], and as a result the RFC is in
the process of being updated, as per [I-D.ietf-6man-rfc3484-revise].
While this update provides a better default address selection policy,
it is unlikely that such a default will suit all scenarios, and thus
mechanisms to control the source address selection policy will be
necessary. Requirements for those mechanisms are described in
[RFC5221], while solutions are discussed in
[I-D.ietf-6man-addr-select-sol] and
[I-D.ietf-6man-addr-select-considerations]. Those documents have
helped shape the improvements in [I-D.ietf-6man-rfc3484-revise] as
well as the DHCPv6 option defined here.

1.1. Conventions Used in This Document

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].

1.2. Terminology

This document uses the terminology defined in [RFC2460] and the
DHCPv6 specification defined in [RFC3315]

2. Address Selection Policy Option

The Address Selection Policy Option provides the policy table for
address selection rules as described in RFC 3484 and updated in
[I-D.ietf-6man-rfc3484-revise].

Each end node is expected to configure its policy table, as described
in RFC 3484, using the Address Selection Policy option information as
described in the section below on processing the option.

The format of the Address Selection Policy option is given below:

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |          OPTION_DASP          |          option-len           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |    label     |  precedence   |z|  reserved   |  prefix-len   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |              zone-index (if present (z = 1))                 |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                             |
   |                 Prefix   (Variable Length)                  |
   |                                                             |
   |                                                             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |    label     |  precedence   |z|  reserved   |  prefix-len   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |              zone-index (if present (z = 1))                 |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                             |
   |                 Prefix   (Variable Length)                  |
   |                                                             |
   |                                                             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   .                                                             .
   .                                                             .
   .                                                             .
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |    label     |  precedence   |z|  reserved   |  prefix-len   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |              zone-index (if present (z = 1))                 |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                             |
   |                 Prefix   (Variable Length)                  |
   |                                                             |
   |                                                             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
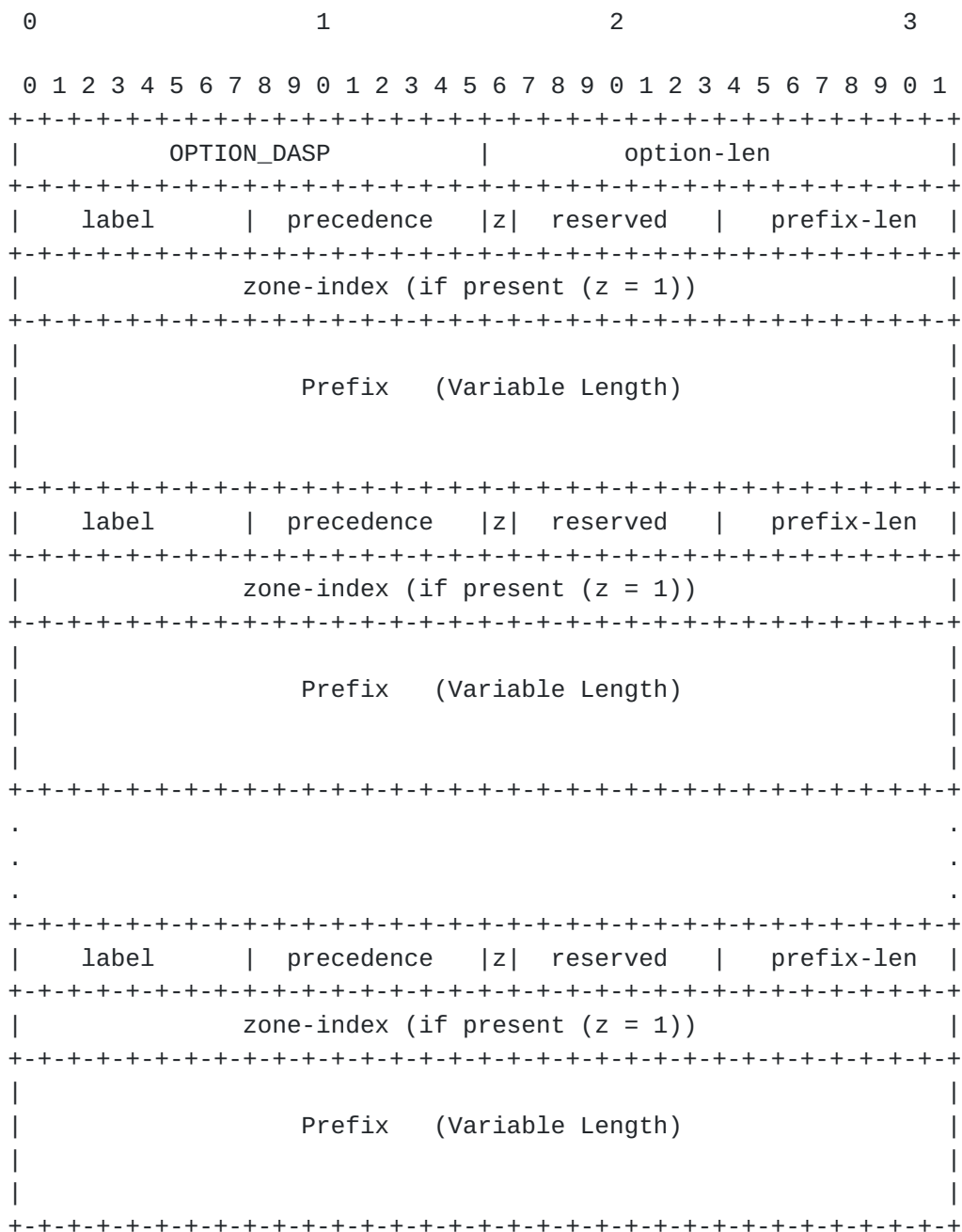
                         [Fig. 1]

   Fields:

   option-code: OPTION_DASP (TBD)

   option-len: The total length of the label fields, precedence fields,
      zone-index fields, prefix-len fields, and prefix fields in
      octets.

   label: An 8-bit unsigned integer; this value is used to make a
      combination of source address prefixes and destination address
      prefixes.

   precedence: An 8-bit unsigned integer; this value is used for
      sorting destination addresses.

   z bit: 'zone-index' bit. If z bit is set to 1, 32 bit zone-index
      value is included right after the "prefix-len" field, and
      "Prefix" value continues after the "zone-index" field. If z bit
      is 0, "Prefix" value continues right after the "prefix-len"
      value.

   reserved: 6-bit reserved field. Initialized to zero by sender, and
      ignored by receiver.

   zone-index: If the z-bit is set to 1, this field is inserted between
      "prefix-len" field and "Prefix" field. The zone-index field is
      an 32-bit unsigned integer and used to specify zones for scoped
      addresses. This bit length is defined in RFC3493 [RFC3493] as
      'scope ID'.

   prefix-len: An 8-bit unsigned integer; the number of leading bits in
      the prefix that are valid. The value ranges from 0 to 128. The
      Prefix field is 0, 4, 8, 12, or 16 octets, depending on the
      length.

   Prefix: A variable-length field containing an IP address or the
      prefix of an IP address. An IPv4-mapped address [RFC4291] must
      be used to represent an IPv4 address as a prefix value.

3. Appearance of this Option

   The Address Selection Policy option MUST NOT appear in any messages
   other than the following ones: Solicit, Advertise, Request, Renew,
   Rebind, Information-Request, and Reply.

4. Processing the Address Selection Policy Option

   This section describes how to process received Address Selection
   Policy Options at the DHCPv6 client.

   This option's concept is to serve as a hint for a node about how to
   behave in the network. So, basically, it should be up to the node's
   administrator how to make use of or even ignore the received policy
   information.

   However, we need to define the default behavior of the receiving node
   in order to reduce operational complexity.

4.1. Handling the local policy table

   RFC3484 defines the default policy for the policy table. Also, a
   user is usually able to configure the policy table to satisfy his
   requirement.

   The client node SHOULD provide the following choices:

   a) It receives distributed policy table, and replaces the existing
      policy tables with that.
   b) It preserves the default policy table, or manually configured
      policy.

4.2. Processing multiple received policy tables

   The policy table is node-global information by its nature. So, the
   node cannot use multiple received policy tables at the same time.

   It should be noted that adopting a received policy table as the node-
   global information can cause security problems, such as DOS attack,
   and leak of privacy information.

   Moreover, it also should be noted that, when a node is single-homed
   and has only one upstream line, adopting a received policy table does
   not degrade the security level.

   Under the above assumptions, we specify how to handle multiple
   received policy tables below.

   A node MAY use OPTION_DASP in any of the following two cases:

   1: The address selection option is delivered across a secure, trusted
      channel.
   2: The address selection option is not secured, but the node is
      single-homed.

   In other cases the node MUST NOT use OPTION_DASP unless the node is
   specifically configured to do so.

5. Implementation Considerations

   o The value 'label' is passed as an unsigned integer, but there is
      no special meaning for the value, that is whether it is a large or
      small number. It is used to select a preferred source address
      prefix corresponding to a destination address prefix by matching
      the same label value within the DHCP message. DHCPv6 clients need
      to convert this label to a representation specified by each
      implementation (e.g., string).

   o Currently, the label and precedence values are defined as 8-bit
      unsigned integers. In almost all cases, this value will be
      enough.

   o The maximum number of address selection rules that may be conveyed
      in one DHCPv6 message depends on the prefix length of each rule
      and the maximum DHCPv6 message size defined in RFC 3315. It is
      possible to carry over 3,000 rules in one DHCPv6 message (maximum
      UDP message size), but the usual number would be much smaller,
      e.g. the default policy table defined in RFC 3484 contains 5
      rules.

   o Since the number of selection rules could be large, an
      administrator configuring the policy to be distributed should
      consider the resulting DHCPv6 message size.

6. Security Considerations

   A rogue DHCPv6 server could issue bogus address selection policies to
   a client. This might lead to incorrect address selection by the
   client, and the affected packets might be blocked at an outgoing ISP
   because of ingress filtering. Alternatively, an IPv6 transition
   mechanism might be preferred over native IPv6, even if it is
   available.

   To guard against such attacks, both DCHP clients and servers SHOULD
   use DHCP authentication, as described in section 21 of RFC 3315,

"Authentication of DHCP messages."

7. IANA Considerations

IANA is requested to assign option codes to OPTION_DASP from the
option-code space as defined in section "DHCPv6 Options" of RFC 3315.

8. References

8.1. Normative References

[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.

[RFC3484]   Draves, R., "Default Address Selection for Internet
            Protocol version 6 (IPv6)", RFC 3484, February 2003.

8.2. Informative References

[I-D.ietf-6man-addr-select-considerations]
            Chown, T., "Considerations for IPv6 Address Selection
            Policy Changes",
            draft-ietf-6man-addr-select-considerations-03 (work in
            progress), March 2011.

[I-D.ietf-6man-addr-select-sol]
            Matsumoto, A., Fujisaki, T., and R. Hiromi, "Solution
            approaches for address-selection problems",
            draft-ietf-6man-addr-select-sol-03 (work in progress),
            March 2010.

[I-D.ietf-6man-rfc3484-revise]
            Matsumoto, A., Kato, J., and T. Fujisaki, "Update to RFC
            3484 Default Address Selection for IPv6",
            draft-ietf-6man-rfc3484-revise-03 (work in progress),
            June 2011.

[RFC2460]   Deering, S. and R. Hinden, "Internet Protocol, Version 6
            (IPv6) Specification", RFC 2460, December 1998.

[RFC3493]   Gilligan, R., Thomson, S., Bound, J., McCann, J., and W.
            Stevens, "Basic Socket Interface Extensions for IPv6",

RFC 3493, February 2003.

   [RFC4291]   Hinden, R. and S. Deering, "IP Version 6 Addressing
               Architecture", RFC 4291, February 2006.

   [RFC4941]   Narten, T., Draves, R., and S. Krishnan, "Privacy
               Extensions for Stateless Address Autoconfiguration in
               IPv6", RFC 4941, September 2007.

   [RFC5220]   Matsumoto, A., Fujisaki, T., Hiromi, R., and K. Kanayama,
               "Problem Statement for Default Address Selection in Multi-
               Prefix Environments: Operational Issues of RFC 3484
               Default Rules", RFC 5220, July 2008.

   [RFC5221]   Matsumoto, A., Fujisaki, T., Hiromi, R., and K. Kanayama,
               "Requirements for Address Selection Mechanisms", RFC 5221,
               July 2008.

Appendix A. Past Discussion

o The 'zone index' value is used to specify a particular zone for
   scoped addresses. This can be used effectively to control address
   selection in the site scope (e.g., to tell a node to use a
   specified source address corresponding to a site-scoped multicast
   address). However, in some cases such as a link-local scope
   address, the value specifying one zone is only meaningful locally
   within that node. There might be some cases where the
   administrator knows which clients are on the network and wants
   specific interfaces to be used though. However, in general case,
   it is hard to use this value.

o Since we got a comment that some implementations use 32-bit
   integers for zone index value, we extended the bit length of the
   'zone index' field. However, as described above, there might be
   few cases to specify 'zone index' in policy distribution, we
   defined this field as optional, controlled by a flag.

o There may be some demands to control the use of special address
   types such as the temporary addresses described in RFC4941
   [RFC4941], address assigned by DHCPv6 and so on. (e.g., informing
   not to use a temporary address when it communicate within the an
   organization's network). It is possible to indicate the type of
   addresses using reserved field value.

Authors' Addresses

   Arifumi Matsumoto
   NTT SI Lab
   3-9-11 Midori-Cho
   Musashino-shi, Tokyo 180-8585
   Japan

   Phone: +81 422 59 3334
   Email: arifumi@nttv6.net

   Tomohiro Fujisaki
   NTT PF Lab
   3-9-11 Midori-Cho
   Musashino-shi, Tokyo 180-8585
   Japan

   Phone: +81 422 59 7351
   Email: fujisaki@nttv6.net

   Jun-ya Kato
   NTT SI Lab
   3-9-11 Midori-Cho
   Musashino-shi, Tokyo 180-8585
   Japan

   Phone: +81 422 59 2939
   Email: kato@syce.net

   Tim Chown
   University of Southampton
   Southampton, Hampshire SO17 1BJ
   United Kingdom

   Email: tjc@ecs.soton.ac.uk