Configured Tunnel End Point Option for DHCPv6

draft-ietf-dhc-dhcpv6-ctep-opt-01.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

For the newly deployed IPv6 networks to interoperate with vastly deployed IPv4 networks, various transition mechanisms had been proposed. One such mechanism is configured tunnels. This document provides a mechanism by which the DHCPv6 servers can provide information about the various configured tunnel end points to reach the IPv6 nodes which are separated by IPv4 networks.
1. Introduction

In the initial deployment of IPv6, the IPv6 nodes may need to communicate with the other IPv6 nodes via IPv4 networks. Configured tunnels [3] provide a way to encapsulate the IPv6 packets in IPv4 packets and tunnel them in the IPv4 network.

This document defines a new option called Configured Tunnel End Point by which the DHCPv6 [1] server can notify the client with the list of end point of the configured tunnels to the various IPv6 networks separated by the IPv4 networks.

2. Background

Configured Tunnel described in this document is a simple and temporary mechanism which allows isolated IPv6 networks or hosts, attached to a legacy IPv4 network which has no native IPv6 connectivity, to communicate with other such IPv6 networks or hosts with manual configuration. The configured tunnel end-point received from the DHCPv6 server is not used for IPv6 connectivity as long as IPv6 networks or hosts are communicating with other IPv6 networks or hosts via IPv6 network which has native IPv6 connectivity and only available when communicating with other IPv6 networks or hosts via IPv4 networks.

In this scenario, 6to4 [4] can be a possible alternative instead of configured tunnel and does not require IPv4-compatible IPv6 addresses or configured tunnels.

As indicated in [4], the mechanisms are intended as a start-up transition tool used during the period of co-existence of IPv4 and IPv6. It is not intended as a permanent solution.

3. Requirements

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in RFC 2119 [2].

4. Terminology

This document uses terminology specific to IPv6 and DHCPv6 as defined in "Terminology" section of the DHCPv6 specification [1].
5. Configured Tunnel End Point Option

The Configured Tunnel End Point Option gives the information to the clients about the Configured Tunnel End Point [3] to be contacted for reaching the nodes in the various IPv6 networks which are separated by IPv4 networks. The clients are expected to install these routes in their machines.

The format of the Configured Tunnel End Point Option is as shown 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           OPTION_CTEP         |           option-len          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   prefix-len  |                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                 Destination Prefix (16 bytes)                 |
|                                                               |
|                                                               |
|                Configured TEP Address (16 bytes)              |
|                                                               |
|                                                               |
|               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+|
|               |                                               |
|               +---------------------------------------------+
|               | prefix-len |                               |
|               |                       |                               |
|               |                       | prefix-len    |                               |
|               |                       |                       |                               |
|               |                       |                       |                       |   . . . |
|               |                       |                       |                       | +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
option-code: OPTION_CTEP (TBD)

option-len: Total length of the prefix-len, Destination Prefix and Configured Tunnel Address lists in octets; It should be a multiple of 33.

prefix-len: prefix length of the Destination Prefix

Destination Prefix: An IPv6 Prefix;

Configured TEP Address: IPv6 Address of the Configured TEP. This address is a IPv4-compatible IPv6 address.

The clients are expected to install the routes identified by the tuples <Destination Prefix/prefix-len, Configured TEP Address> once they receive this option from the server.

6. Appearance of this option

The Configured Tunnel End Point Option MUST NOT appear in other than the following messages: Solicit, Advertise, Request, Renew, Rebind, Information-Request and Reply.

The option numbers of Configured Tunnel End Point option MAY appear in the Option Request Option [1] in the following messages: Solicit, Request, Renew, Rebind, Information-Request and Reconfigure.

7. Security Considerations

The Configured Tunnel End Point Option may be used by an intruder DHCPv6 server to provide invalid or incorrect configured tunnel end point. This makes the client unable to reach its destination IPv6 node or to reach incorrect destination. The latter one has very severe security issues as IPv6 destination is spoofed here.

To avoid attacks through this option, the DHCPv6 client SHOULD use authenticated DHCP (see section "Authentication of DHCP messages" in the DHCPv6 specification [1]).
8. IANA Considerations

IANA is requested to assign an option code to the following options from the option-code space defined in "DHCPv6 Options" section of the DHCPv6 specification [1].

<table>
<thead>
<tr>
<th>Option Name</th>
<th>Value</th>
<th>Described in</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPTION_CTEP</td>
<td>TBD</td>
<td>Section 4</td>
</tr>
</tbody>
</table>

9. References

9.1 Normative References


9.2 Informative References


Authors’ Addresses

Soomhong Daniel Park
Mobile Platform Laboratory
Samsung Electronics.
Suwon
Korea

Phone: +81-31-200-4508
E-Mail: soohong.park@samsung.com

Vijayabhaskar A K
Hewlett-Packard STSD-I
29, Cunningham Road
Bangalore – 560052
India

Phone: +91-80-2053085
E-Mail: vijayak@india.hp.com

Acknowledgements

Thanks to the DHC Working Group for their time and input into the specification. In particular, thanks to Pekka Savola, Bernie Volz, Ralph Droms, Margaret Wasserman for their valuable comments on this work.
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF’s procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Copyright (C) The Internet Society (2004). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING
Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.