DHCP Option for Configuring IPv6-over-IPv4 Tunnels
<draft-daniel-dhc-ipv6in4-opt-03.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

This document provides a mechanism by which the DHCPv4 servers can provide information about the configured IPv6-over-IPv4 tunnel end-point. The IPv4/IPv6 dual-stack nodes can use this information to set up a configured tunnel to the tunnel end-point to obtain IPv6 connectivity.
1. Introduction

In the initial deployment of IPv6, the IPv6 nodes may need to communicate with the other IPv6 nodes via IPv4 tunnel service. The connectivity can be obtained by setting up an IPv6-over-IPv4 configured tunnel between a client and a tunnel router.

This document defines a new option by which the DHCPv4 [RFC-2131] server can notify the client with the list of end-points of the possible configured tunnels.

Particularly, this mechanism is useful where the ISP is providing the IPv6 services but is doing it using tunneling over IPv4 to avoid upgrading all their infrastructure to support IPv6 on day one.

Regarding IPv6-over-IPv4 tunnel, the tunnel broker [RFC-3053] architecture has been widely deployed in the dual networks to obtain IPv6 connectivity via tunnel service because of easy configuration on the users. After configuring IPv6-over-IPv4 tunnel between the users and the selected tunnel server, tunnel broker allows user to get access to the 6bone or any other IPv6 network the tunnel server is connected to. In case of no tunnel broker, the proposed mechanism in this document can allow users to obtain the IPv6 connectivity efficiently.

2. 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 [RFC-2119].

3. Configured Tunnel End Point Option

This option specifies the configured tunnel end-point that client should use when discovering the IPv4 address of the ISP’s tunnel router somehow via the Dynamic Host Configuration Protocol.

Once the IPv4 address has been learned, it is configured as the tunnel end-point for the configured IPv6-over-IPv4 tunnel.

The format of the Configured Tunnel End Point Option is shown as below;

The code for this option is TBD. The length of this option is 4.

<table>
<thead>
<tr>
<th>Code</th>
<th>Length</th>
<th>CTEP Order in Sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In the above diagram, CTEP Addr is 32-bit integers corresponding to DHCP options which specify the IP address of different configured tunnel end-point.

As described in [RFC-2893], the dual node received CTEP option MUST store the tunnel end-point address and this address is used as destination address for the encapsulating IPv4 header.

The determination of which packets to tunnel is usually made by routing information on the encapsulator. This is usually done via a routing table, which directs packets based on their destination address using the prefix mask and match technique. For more information, refer to section 4. Configured Tunneling in [RFC-2893].

4. Multiple Tunnel End Point Considerations
For the simple configured tunnel, one tunnel end-point is generally used and it assumes that all the networks will be reached through the same end-point. In this case, one CTEP Addr field in the CTEP option is used for configured tunnel service.

The list of end-points can be installed as the default routes and the routes will be tried in a round robin fashion if the IPv6 host load-sharing is honored [IPv6LOAD]. Instead there can be specific default routes for the different destination.

Generally, there may not be a need for installing multiple configured tunnel end-points unless administrator wants two for redundancy purposes. It is out of scope of this draft.

5. Security Considerations

A rouge DHCP server can issue invalid or incorrect configured tunnel end-point. This may cause denial of service due to unreachability or makes the client to reach incorrect destination.

The latter has very severe security issues as the tunnel end-point is on-the-path towards all the IPv6 destinations, and can trivially act as a man-in-the-middle attacker.

To increase secure exchange between users and tunnel end-points, the tunnel broker or any tunnel agent can be used for configuring IPv6-over-IPv4 tunnels including authentication, security association and so on, but it is not scope of this document.

The authenticated DHCP [RFC-3118] can be also used for secure exchange between users and tunnel end-points (routers).

6. Extended Usage

As stated in Introduction, the tunnel broker is a nice tool for allowing user to get the IPv6 connectivity through IPv6-over-IPv4 tunnel. To configure tunnel between users and tunnel servers, users have to access to the tunnel broker by web registration and then tunnel broker set up tunnel between users and a selected tunnel server. Prior to filling up the form on the tunnel broker, users have to know the IPv4 address of the tunnel broker (as described in [6], it may be IPv6 addressable but not mandatory). Regarding this operation, this option proposed in this document can allow users to
obtain an available tunnel broker address (or addresses) without any
manual operations.

For this operation, a new option (called Tunnel Broker Configuration
Option: option name is OPTION_TBCO and value is TBD) can be simply
made by DHCPv4 option extension which may be the same format as CTEP
option.

To increase secure exchange between users and tunnel end-points
(tunnel servers or dual routers) this extended usage can be applied
for configuring IPv6-over-IPv4 tunnel instead of direct tunnel
configuration between them. Specific method for secure exchange is
beyond scope of this document.

7. IANA Considerations

IANA is requested to assign a value for the Configured Tunnel End
Point option code in accordance with RFC 2939 [RFC-2939].

<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 3.</td>
</tr>
</tbody>
</table>

8. References

8.1 Normative References

2131, Bucknell University, March 1997.

[RFC-2119] Bradner, S., "Key words for use in RFCs to Indicate

[RFC-2939] Droms, R., "Procedures and IANA Guidelines for Definition
of New DHCP Options and Message Types", RFC 2939,
September 2000.

[RFC-3118] Droms, R., "Authentication for DHCP Messages", RFC 3118,

8.2 Informative Reference

[RFC-2893] Nordmark, E. and Gilligan, R.E., "Basic Transition
Mechanisms for IPv6 Hosts and Routers", RFC 2893, August
2000.


9. Authors’ Addresses

Soohong Daniel Park  
Mobile Platform Laboratory  
Samsung Electronics.  
Suwon  
Korea  

Phone: +81 31 200 4508  
Email: soohong.park@samsung.com

Pyungsoo Kim  
Mobile Platform Laboratory  
Samsung Electronics.  
Suwon  
Korea  

Phone: +81 31 200 4635  
Email: kims@samsung.com

10. Acknowledgements

Special thanks to Pekka Savola, Vijayabhaskar A K, Eric Nordmark and Alain Durand for their many valuable revisions and comments. In particular, Pekka Savola kindly clarified the multiple tunnel end point considerations with his good experience as well.
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
TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

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