

Network Working Group  
Internet-Draft  
Expires: April 22, 2006

S. Daniel Park  
SAMSUNG Electronics  
A. Vijayabhaskar  
HP  
October 22, 2005

**Configured Tunnel End Point Option for DHCPv6**  
**draft-ietf-dhc-dhcpv6-ctep-opt-02.txt**

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

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>.

This Internet-Draft will expire on April 22, 2006.

Copyright Notice

Copyright (C) The Internet Society (2005). 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 tunnel discovery mechanism by which the DHCPv6 servers can provide information about the available 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 [[RFC4213](#)] 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 [[RFC3315](#)] 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 [[RFC3056](#)] can be a possible alternative instead of configured tunnel.

As indicated in [[RFC3056](#)], 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 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](#)].

## **4. Terminology**

This document uses terminology specific to IPv6 and DHCPv6 as defined in "Terminology" section of the DHCPv6 specification [[RFC3315](#)].

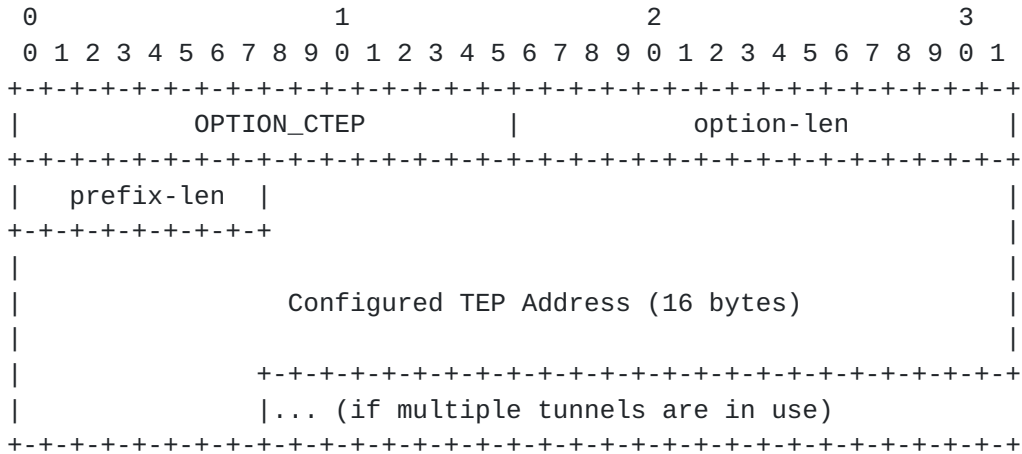
## **5. Configured Tunnel End Point Option**

The Configured Tunnel End Point Option gives the information to the clients about the Configured Tunnel End Point [[RFC4213](#)] 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:



option-code: OPTION\_CTEP (TBD)

option-len: Total length of the prefix-len, Configured Tunnel Address lists in octets; It should be a multiple of 17.

prefix-len: prefix length of this Configured TEP Address in bits.

Configured TEP Address: IPv6 Address of the Configured TEP.

The clients are expected to install the routes identified by the tuples (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 [RFC3315] in the following messages: Solicit, Request, Renew, Rebind, Information-Request and Reconfigure.



## **7. multiple Tunnel End Point Considerations**

For the simple tunnel discovery, one tunnel endpoint is generally used and it assumes that all the networks will be reached through the same endpoint. In this case, one Configured TEP field in the TEP option is used for configured tunnel service.

The list of endpoints can be installed if the IPv6 host load-sharing is honored, but there may not be a need for installing multiple configured tunnel endpoints unless administrator wants two for redundancy purposes. It is beyond scope of this document.

## **8. Security Considerations**

The Configured Tunnel End Point Option may be used by an intruder DHCPv6 server to provide invalid or incorrect configured tunnel endpoint. 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 [[RFC3315](#)]).

## **9. 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 [[RFC3315](#)].

Option Name	Value	Described in
OPTION_CTEP	TBD	<a href="#">Section 4</a>

## **10. References**

### **10.1 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.

### **10.2 Informative References**

- [RFC3056] Carpenter, B. and K. Moore, "Connection of IPv6 Domains





via IPv4 Clouds", [RFC 3056](#), February 2001.

[RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", [RFC 4213](#), October 2005.

#### Authors' Addresses

SooHong Daniel Park  
SAMSUNG Electronics  
416 Maetan-3dong, Yeongtong-gu  
Suwon-si, Gyeonggi-do 442-742  
KOREA

Phone: +82 31 200 4635  
EMail: soohong.park@samsung.com

Vijayabhaskar A K  
Hewlett-Packard  
29, Cunningham Road  
Bangalore 560052  
INDIA

Phone: +91 80 205308582  
EMail: vijayak@india.hp.com



## Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights 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; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat 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 implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).

## Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

## Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

## Acknowledgment

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

