Network Working Group
Internet-Draft
Expires: November 5, 2005

S. Daniel Park
SAMSUNG Electronics
May 7, 2005

DHCP Option for Configuring IPv6-over-IPv4 Tunnels
draft-daniel-dhc-ipv6in4-opt-06.txt

Status of this Memo

Copyright Notice

Abstract

This document provides a mechanism by which the DHCPv4 servers can provide information about the IPv6-over-IPv4 tunnel endpoint. The IPv4/IPv6 dual stack nodes can use this information to set up a tunnel to the tunnel endpoint to obtain IPv6 connectivity without requiring manual intervention at any of the tunnel endpoints at tunnel establishment time.

Table of Contents

1. Introduction 3
1.1 Terminology 3
2. Requirements 4
3. IPv6-over-IPv4 Tunnel End Point Option 4
4. DHCP Client Behavior 4
5. Multiple Tunnel End Point Considerations 6
6. Security Considerations 6
7. Extended Usage 7
8. IANA Considerations 7
9. Acknowledgements 7
10. Impmenentation Experiences 8
11. References 8
11.1 Normative References 8
11.2 Informative References 8
Author's Address 9
Intellectual Property and Copyright Statements 10

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 tunnel between a client and a tunnel router.

This document defines a new option by which the DHCPv4 [RFC2131] server can notify the client with the list of endpoints of the possible IPv6-over-IPv4 tunnel defined in [RFC2893] in an automated manner. Through this mechanism, dual stack users attached to IPv4 only networks can connect its IPv6 connectivity to the endpoints as a tunnel router.

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 [RFC3053] 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.

1.1 Terminology

The following terms pertaining to tunnel are used in this document as defined in [RFC2893]

- IPv6-over-IPv4 Tunnel:

  The technique of encapsulating IPv6 packets within IPv4 so that they can be carried across IPv4 routing infrastructures. IPv6-over-IPv4 tunnel where the IPv4 tunnel endpoint address is determined by configuration information learned from the DHCP Server on the encapsulating node.

- Tunnel endpoint address:

  Destination address of IPv4 encapsulating IPv6 packets. It is an IPv4 address in the TEP Option originated from the DHCP Server.

2. 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].

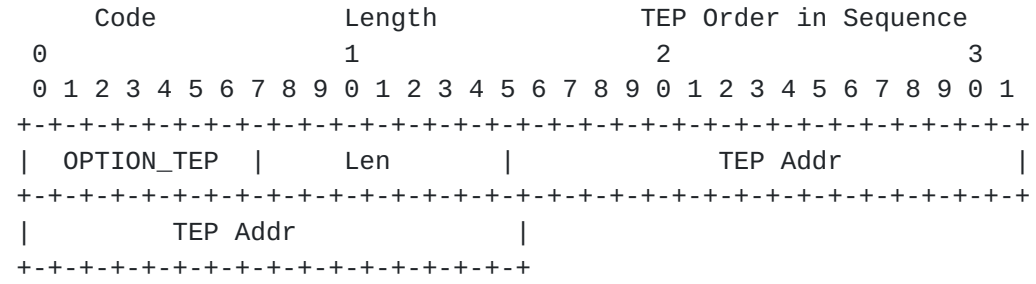
3. IPv6-over-IPv4 Tunnel End Point Option

This option specifies the IPv6-over-IPv4 tunnel endpoint 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 endpoint for the IPv6-over-IPv4 tunnel.

The format of the IPv6-over-IPv4 Tunnel End Point Option is shown as below;

The code for this option is TBD. The length of this option is 4 (in case of single endpoint).



In the above diagram, TEP Addr is 32-bit integers corresponding to DHCP options which specify the IP address of a different IPv6-over-IPv4 tunnel endpoint.

All IPv6 traffic generated on the dual node SHOULD be encapsulated within IPv4 and forwarded to the endpoint assigned into the TEP Addr field of TEP option.

4. DHCP Client Behavior

The DHCP client will use this option to create a tunnel endpoint address for IPv6-over-IPv4 tunnel. The client may receive tunnel services in this option that it does not support or has not been

configured to access. Likewise, a client may receive an option that tunnel services for which no corresponding DHCP option was supplied. Clients will interpret this option in a system-specific manner whose specification is outside the scope of this document.

As described in [RFC2893], the dual node received TEP option MUST store the tunnel endpoint address and this address is used as destination address for the encapsulating IPv4 header.

Although the dual node obtains available tunnel endpoint address from the DHCP server, it can not receive any IPv6 packets from the tunnel router via IPv6-over-IPv4 tunnel because the tunnel router does not recognize which node is likely to configure its tunnel attached to the tunnel router. As described in [I-D.nielsen-v6ops-zeroconf-goals] the tunnel protocol proposed in this document MUST allow for one tunnel endpoint to verify the reachability of other tunnel endpoint towards which it intends to send packets. After verifying the reachability between them, IPv6 Router Advertisement messages including address configuration information are reached to the dual node correctly, and the dual node configures its unique IPv6 address by itself in a stateless address autoconfiguration manner [RFC2461]. The dual node thus is able to forward its IPv6 traffics to the tunnel router learned from the TEP option of DHCP.

One example of the reachability function is shown in Section 10 while specific considerations is beyond scope of this document.

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 [RFC2893].

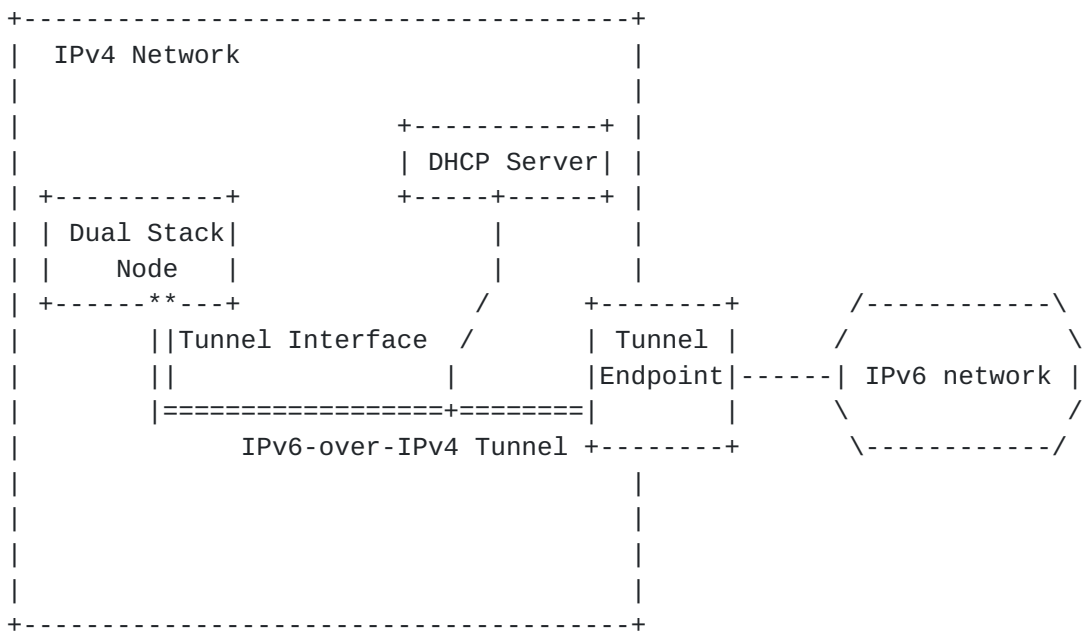


Fig. 1, Simple network model for TEP option use case

5. Multiple Tunnel End Point Considerations

For the simple IPv6-over-IPv4 tunnel, one tunnel endpoint is generally used and it assumes that all the networks will be reached through the same endpoint. In this case, one TEP Addr field in the TEP option is used for configured tunnel service.

The list of endpoints 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 [I-D.ietf-ipv6-host-load-sharing]. Instead there can be specific default routes for the different destination.

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

6. Security Considerations

A rouge DHCP server can issue invalid or incorrect IPv6-over-IPv4 tunnel endpoint. 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 endpoint 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 endpoints, 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 [RFC3118] can be also used for secure exchange between users and tunnel endpoints.

7. 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 [RFC3053], 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 TEP option.

To increase secure exchange between users and tunnel endpoints (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.

8. IANA Considerations

IANA is requested to an assign value for the IPv6-over-IPv4 Tunnel End Point option code in accordance with [RFC2939].

Option Name	Value	Described in
OPTION_TEP	TBD	Section 3.
OPTION_TBCO	TBD	Section 7. (if necessary)

9. Acknowledgements

Special thanks to Pekka Savola, Vijayabhaskar A K, Eric Nordmark, Ralph Droms, Bernie Volz 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.

Specially, authors would like to acknowledge the implementation contributions by Minho Lee of Samsung Electronics.

10. Impmenentation Experiences

We have implemented TEP option using the Internet Systems Consortium DHCP source code (DHCP-3.0.1-rc13 version) on both DHCP server and client, particularly client is an IPv4/IPv6 dual stack based on Linux operating system.

For the simple implementation, TCP/UDP port assigned both endpoints by operator in advance was used to verify the reachability in this document.

11. References

11.1 Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC2939] Droms, R., "Procedures and IANA Guidelines for Definition of New DHCP Options and Message Types", BCP 43, RFC 2939, September 2000.

[RFC3118] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001.

11.2 Informative References

[I-D.ietf-ipv6-host-load-sharing]
Hinden, R., "IPv6 Host to Router Load Sharing", draft-ietf-ipv6-host-load-sharing-03 (work in progress), October 2004.

[I-D.nielsen-v6ops-zeroconf-goals]
Morelli, M., "Goals for Zero-Configuration Tunneling", draft-nielsen-v6ops-zeroconf-goals-01 (work in progress), September 2004.

[RFC2461] Narten, T., Nordmark, E. and W. Simpson, "Neighbor

Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[RFC2893] Gilligan, R. and E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers", RFC 2893, August 2000.

[RFC3053] Durand, A., Fasano, P., Guardini, I. and D. Lento, "IPv6 Tunnel Broker", RFC 3053, January 2001.

Author's Address

Soohong Daniel Park
SAMSUNG Electronics
416 Maetan-3dong, Yeongtong-gu
Suwon-si, Gyeonggi-do 443-742
KOREA

Phone: +82 31 200 4508
EMail: soohong.park@samsung.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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