

Network Working Group
Internet Draft
Intended status: Standards Track
Expires: April 18, 2010

Dayong Guo
Sheng Jiang
Huawei Technologies Co., Ltd
October 19, 2009

Auto GRE Tunnel for Hub and Spoke Software

[draft-guo-software-auto-gre-00.txt](#)

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [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 18, 2010.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Internet-Draft [draft-guo-softwire-auto-gre-00.txt](#)

October 2009

Abstract

This document proposes an auto-configured GRE tunnel mechanism in hub and spoke network. This mechanism automatically configures GRE tunnel encapsulation parameters to end user devices using DHCP protocol. It can also simplify and drive IPv6 transition.

Table of Contents

1.	Introduction.....	3
2.	Terminology.....	4
3.	Auto GRE Tunnel.....	4
3.1.	Preliminary Phase.....	4
3.1.1.	SC discovery on SI.....	4
3.1.2.	Pre-configuration on SC.....	4
3.2.	Tunnel Establishment.....	4
3.3.	Tunnel Maintenance.....	5
3.4.	Tunnel Teardown.....	5
4.	Application Example of Auto GRE Tunnel.....	6
4.1.	Auto GRE Tunnel deploys in IPv6 network.....	6
5.	Security Considerations.....	7
6.	IANA Considerations.....	7
7.	References.....	7
7.1.	Normative References.....	7
7.2.	Informative References.....	8
	Author's Addresses.....	9

Internet-Draft [draft-guo-software-auto-gre-00.txt](#)

October 2009

1. Introduction

The Softwires Working Group has standardized Layer Two Tunneling Protocol version 2 (L2TPv2) as the phase 1 protocol to be deployed in the Software "Hub and Spoke" solution space [[RFC5571](#)]. L2TPv2 supports "IPvX/PPP/L2TPv2/UDP/IPvY" encapsulations and fulfills requirements in [[RFC4925](#)]. Especially L2TPv2 has good capacity to traverse NAT, since L2TPv2 runs over UDP.

However, as a multi-layers encapsulation protocol, L2TPv2 has to carry multiple protocol headers per data packet. It is complicated and costly, mostly used for Virtual Private Network (VPN). Most Customer Premises Equipment (CPE) is too simple to be L2TPv2 initiator.

In most scenarios, providers do not need such a complicated transition method that meets all requirements in [[RFC4925](#)]. For example, NAT does NOT exist in many scenarios. A simple Auto GRE (Generic Routing Encapsulation) Tunnel, proposed in this document, can meet most requirements in [[RFC4925](#)] except for the NAT traverse requirements.

GRE [[RFC2784](#)] is widely deployed in the ISP networks. Up to now, GRE tunnels are stateless and configured manually. The proposed Auto GRE mechanism does not modify encapsulation format of GRE, but adds signaling, using Dynamic Host Configuration Protocol (DHCP) [[RFC2131](#)] or DHCP for IPv6 [[RFC3315](#)], so that the software can be automatically set up or torn down.

Carrier Grade NATs (CGNs) in IPv4/IPv6 transition are such scenarios that do not require NAT traversal. CGN solutions have recently been proposed to simplify IPv4/IPv6 transition in the edge network. [Incremental CGN] and [DS-lite CGN] describes a few dispersive IPvX users bridge IPvX Internet by software spanning IPvY infrastructure. Both scenarios require users set up tunnels to CGN. Obviously, there is no NAT between CPE and CGN in both DS-lite and Incremental CGN

scenarios.

Additionally, the auto-configure mechanism described in the document can also support auto IP-in-IP tunnel. The advantage of GRE is more manageable and extensible than IP-in-IP. Auto IP-in-IP tunnel is out of the focus of this document.

[2](#). Terminology

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](#) [[RFC2119](#)].

[3](#). Auto GRE Tunnel

Auto GRE tunnel mechanism enables a Softwire Initiator (SI) exchanges tunnel control signals with its correspondent Softwire Concentrator (SC). DHCP is commonly used when an administrator requires more control to hosts. DHCP or DHCPv6 is adopted as the signaling protocol. This document does NOT project to invent a new signaling protocol but makes full use of DHCP and GRE combinations.

The SI in Auto GRE may be a CPE, a host or an edge router. The SC may be a tunnel concentrator or CGN.

The Process is described in the following sub-sections.

[3.1](#). Preliminary Phase

[3.1.1](#). SC discovery on SI

Before tunneling to SC, SI MUST get the address and other parameters of a SC. The information may be configured manually on the SI.

However, manual configuration are difficult to operate when the information of the SC changes. [[Discovery](#)] proposes an auto SC discovery method by extending DHCP or Point-to-Point Protocol (PPP)[[RFC1661](#)].

[3.1.2.](#) Pre-configuration on SC

To support auto-configure GRE tunnel, the SC MUST configure a GRE tunnel interface and listen to GRE packet being sent to the interface. A DHCP snooping is REQUIRED in SC in order to trigger configuration and updating state of the tunnel.

[3.2.](#) Tunnel Establishment

To set up softwires to the SC, a SI should send a DHCP request message with GRE encapsulation to request an inner address of the tunnel and other relevant network parameters. The destination IP of outer layer header in GRE encapsulation comes from description of [Section 2.1.1](#) SC discovery. The outer source IP uses the IP address of the SI.

When SC receives the DHCP request message with GRE encapsulation, it SHOULD look up the outer source IP of the packet in its tunnel client list. If it is a new client, the SC adds source IP into the tunnel client list, decapsulates GRE header and deals with the DHCP request. The SC sends the DHCP reply message, which allocates the inner address, with GRE encapsulation too. The source and destination address in IP header of DHCP reply should comply with DHCP or DHCPv6. The source and destination of the GRE encapsulation MUST originate from the destination and source IP of outer GRE encapsulation of the DHCP request message.

The tunnel client list records the information of all tunnel clients. Each entry of the list describes information of a tunnel, includes the mapping of the inner address of tunnel and the outer IP of client, the lifetime of the tunnel. The lifetime of the tunnel SHOULD synchronize with the lifetime of SI inner address. For inbound traffic, SC checks the tunnel client list according to destination address of the packet and decides which tunnel the traffic should be forwarded to.

While SI receives the DHCP reply message with GRE encapsulation, SI configures itself with the allocated address and other network parameters in the DHCP message.

[3.3.](#) Tunnel Maintenance

DHCP address lifetime or lease is used for the SC to maintain tunnel

state. A SI SHOULD periodically renew the lifetime of the address to keep tunnel alive. The SI renew period SHOULD be shorter than the lifetime. When the lifetime of SI inner address is renewed, the lifetime of the tunnel in the tunnel client list SHOULD be synchronized. Once the lifetime of tunnel expires, the SC tears down the tunnel and releases resource. The lifetime SHOULD be set to appropriate time so that SC deletes inactivity tunnel as well as avoids too frequently renew procedures.

3.4. Tunnel Teardown

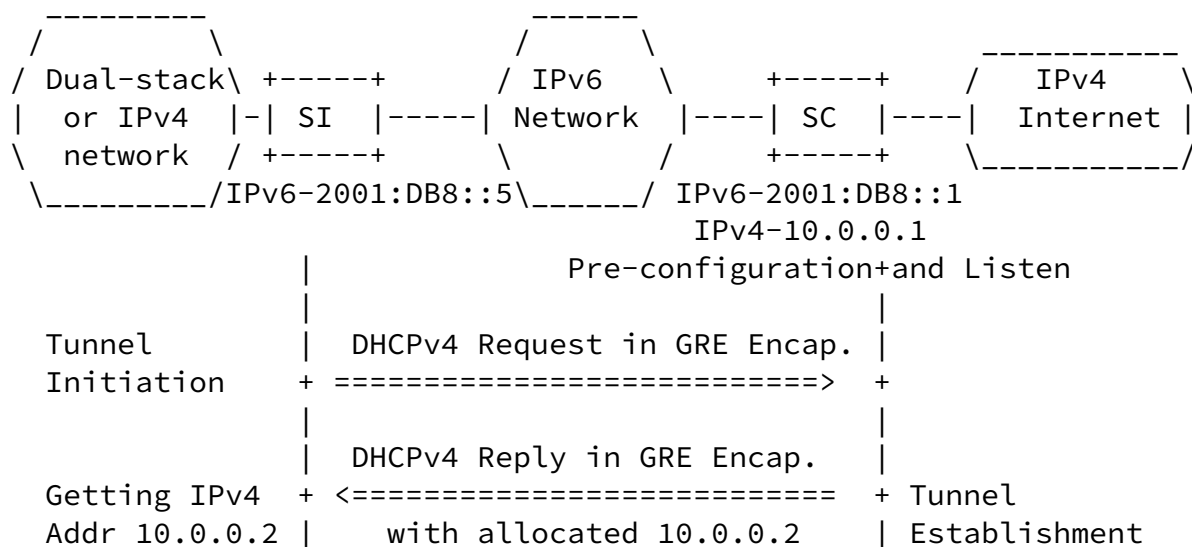
Tunnels are naturally torn down when the SI inner address expires, as is described in [Section 2.3](#).

If the SI wants to actively tear down the GRE tunnel, it will send a DHCP Release Message with GRE encapsulation and then delete the tunnel. While SC receives the DHCP release message encapsulated in GRE tunnel, it tears down the related Auto GRE tunnel.

4. Application Example of Auto GRE Tunnel

4.1. Auto GRE Tunnel deploys in IPv6 network

Figure 1 illustrates how Auto GRE tunnel deploys in DS lite case. The CPE and CGN in DS lite are respectively the SI and SC in software.



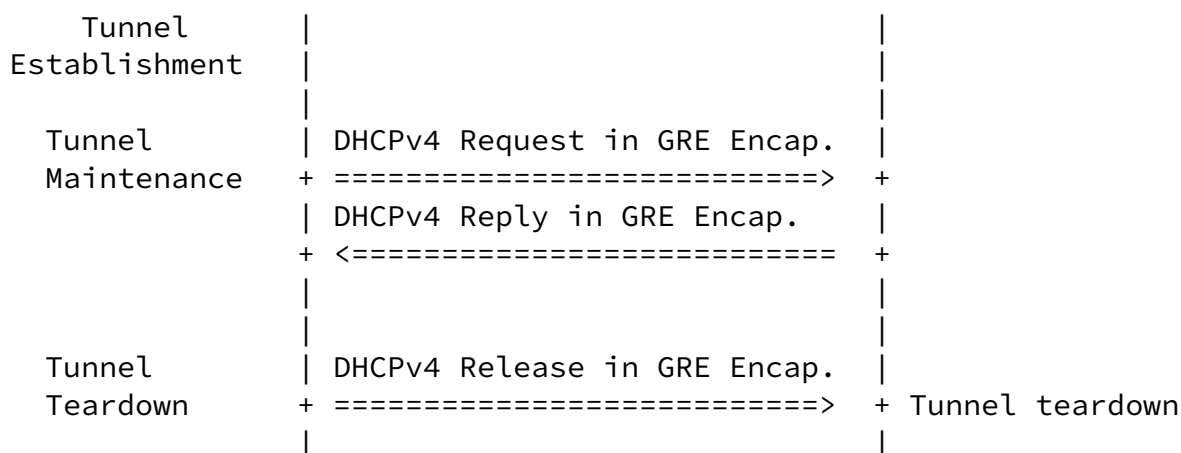


Figure 1 Auto-configuring GRE tunnel in DS lite case

Before initiating tunnel establishment, the SI may get information of SC by the method mentioned in [Section 2.2.1](#). The SC is listening to GRE setup requests of all clients.

When the SI starts to set up Auto GRE tunnel, it sends a DHCPv4 Request message with GRE encapsulation to the SC's IPv6 address 2001:DB8::1. The source IP of GRE header is 2001:DB8::5.

Once a SC receives the packet, it answers an IPv4 address in DHCPv4 reply message with GRE encapsulation. At the same time, the SC creates and configures a new GRE tunnel. Because the SC allocate IP

address 10.0.0.2 to the SI, a mapping "inner address of tunnel: 10.0.0.2, outer IP of client: 2001:DB8::5" is added into the tunnel client list on the SC.

After SI received the DHCPv4 packet with GRE encapsulation, it completes inner address configuration based on parameters in the DHCPv4 message. Finally the application IPv4 traffic can pass through the GRE tunnel.

The SI should periodically intercommunicate DHCPv4 Request/Reply message with GRE encapsulation to keep tunnel alive. The SI may either sends a DHCPv4 release message in GRE tunnel to inform CGN tears down or wait until lifetime expires.

5. Security Considerations

[RFC5619] has listed security analysis and requirements in hub and

spoke network. It is watchful for SC to resist Denial of Service. DHCP security mechanisms [RFC3118, [RFC3315](#), SecDHC] can be used when necessary.

[6.](#) IANA Considerations

There are no IANA considerations in this document.

[7.](#) References

7.1. Normative References

- [RFC1661] W. Simpson, "The Point-to-Point Protocol (PPP)", [RFC 1661](#), July 1994
- [RFC2131] R. Droms, "Dynamic Host Configuration Protocol", [RFC 2131](#), March 1997.
- [RFC2784] D. Farinacci, T. Li, S. Hanks, D. Meyer and P. Traina, "Generic Routing Encapsulation (GRE)", [RFC 2784](#), March 2000.
- [RFC3118] R. Droms and W. Arbaugh, "Authentication for DHCP Messages", [RFC 3118](#), June 2001.
- [RFC3315] R. Droms, Ed., J. Bound, B. Volz, T. Lemon, C. Perkins and M. Carney, "Dynamic Host Configure Protocol for IPv6", [RFC3315](#), July 2003.

- [RFC5571] B. Storer, C. Pignataro, Ed., M. Dos Santos, B. Stevant, Ed., L. Toutain and J. Tremblay, "Software Hub & Spoke Deployment Framework with L2TPv2", [RFC 5571](#), June 2009.
- [RFC5619] S. Yamamoto, C. Williams, H. Yokota and F. Parent, "Software Security Analysis and Requirements", [RFC 5619](#), August 2009.

7.2. Informative References

- [RFC4925] X. Li, S. Dawkins, D. Ward and A. Durand, "Software Problem Statement", [RFC 4925](#), July 2007.

- [Ds-lite CGN] A. Durand, R. Droms, B. Haberman, and J. Woodyatt, "Dual-stack lite broadband deployments post IPv4 exhaustion", [draft-ietf-softwire-dual-stack-lite-01](#), work in progress, July 2009.
- [Incremental CGN] S. Jiang, D. Guo and B. Carpenter, "An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition" [draft-jiang-v6ops-incremental-cgn-03](#), work in progress, September 2009.
- [Discovery] D. Guo and S. Jiang "DHCP Option for CGN or Tunnel Concentrator Discovery", [draft-guo-dhc-tunnel-discovery-02](#), work in progress, October 2009.
- [SecDHC] S. Jiang and S. Shen, "Secure DHCPv6 Using CGAs", [draft-jiang-dhc-secure-dhcpv6-02.txt](#), work in progress, July 2009.

Author's Addresses

Dayong Guo
Huawei Technologies Co., Ltd
KuiKe Building, No.9 Xinxu Rd.,
Shang-Di Information Industry Base, Hai-Dian District, Beijing 100085
P.R. China
Phone: 86-10-82836077

Email: guoseu@huawei.com

Sheng Jiang

Huawei Technologies Co., Ltd

KuiKe Building, No.9 Xinxu Rd.,

Shang-Di Information Industry Base, Hai-Dian District, Beijing 100085

P.R. China

Phone: 86-10-82836081

Email: shengjiang@huawei.com