

Network Working Group
Internet Draft
Intended status: Standards Track
Expires: January 14, 2011

Dayong Guo
Sheng Jiang
Huawei Technologies Co., Ltd
Brian Carpenter
University of Auckland
July 12, 2010

Software Concentrator Discovery Using DHCP

draft-guo-software-sc-discovery-04.txt

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on January 14, 2011.

Copyright Notice

Copyright (c) 2010 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 (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Abstract

Several types of Carrier Grade NATs have been proposed to simplify IPv4/IPv6 transition of the edge network by integrating tunnels and NAT. A very common scenario is that many users set up softwires to a software concentrator for public or private access services. In order to establish softwires successfully, a new mechanism is required to enable users in the edge network to discover the information of the concentrator. This document describes how a host or Customer Premises Equipment discovers the remote software concentrator or CGN in a hub and spoke network using DHCP. Based on two new Software Concentrator Discovery DHCP Options, proposed in the document, a user can obtain the information of the software concentrator or CGN and then set up a tunnel to it.

Table of Contents

1. Introduction.....	3
2. Terminology.....	4
3. DHCP Solution Overview for Software Concentrator Discovery....	4
4. DHCPv4 Software Concentrator Discovery (SCD) Option.....	5
4.1. Suboptions in DHCPv4 SCD Option.....	6
4.1.1. Protocol Type Suboption.....	7
4.1.2. GRE Key Suboption.....	7
5. DHCPv6 Software Concentrator Discovery (SCD) Option.....	7
5.1. Suboptions in DHCPv6 SCD Option.....	8
5.1.1. Protocol Type Suboption.....	9
5.1.2. Prefix Suboption.....	10
5.1.3. GRE Key Suboption.....	10
6. Illustration Examples.....	11
6.1. Example 1: Incremental CGN scenario.....	11
6.2. Example 2: two CGN in DS lite scenario.....	11
7. Security Considerations.....	11
8. IANA Considerations.....	12
8.1. Tunnel Types.....	12
8.2. DHCPv4 SCD Suboption Types.....	12
8.3. DHCPv6 SCD Suboption Types.....	13
9. Acknowledgments.....	13
10. Change Log [RFC Editor please remove].....	13
11. References.....	13
11.1. Normative References.....	13
11.2. Informative References.....	14

1. Introduction

Transition is an important factor for user experience in IPv4 and IPv6 coexistence phase. The transition of the edge network is the most complicated because it is near lots of users and uses multiple network technologies. Recently, several types of Carrier-Grade-NATs (CGNs) have been proposed to simplify IPv4/IPv6 transition of the edge network by integrating tunnels and NAT. Incremental CGN [I-D.ietf-v6ops-incremental-cgn] and 6rd [I-D.ietf-software-ipv6-6rd] and describes how dispersed IPv6 users bridge with the IPv6 Internet by tunnel spanning ipv4 infrastructure. The dual-stack lite technology [I-D.ietf-software-dual-stack-lite] is intended for maintaining connectivity to legacy IPv4 devices and networks using IPv4-over-IPv6 softwires while a service provider deploys an IPv6-only network. A very common scenario is that many users set up softwires or tunnels to a software concentrator for public or private access services.

The aforementioned scenarios have been abstracted as hub and spoke networks in the IETF Software working group, and several encapsulation techniques have been defined [RFC4925] [RFC5512]. [RFC5571] discloses a mechanism in mesh network by BGP extension for users to discover the information of a tunnel end point. However, the nodes in an edge network do not have BGP capability generally. Manual configuration is not suitable because the address and other attribute of the concentrator may change. A new mechanism is required to enable users in edge network to discover the information of the concentrator automatically.

In order to establish a software successfully, users must know the information of a software concentrator or CGN, such as address, tunnel type. Additionally, the discovery process may also support multiple protocol type in tunnel, load-sharing and recovery from a single point of failure.

Since ISPs may use different software technologies, an ISP-independent CPE should support as many as possible potential software technologies and be able to auto discovery which software technologies is in use. Even within a single ISP, different software technologies may also use to differentiate customers, e.g., support of secured encapsulation for some customers and plain IP-in-IP encapsulation for others.

For scalability and stability purposes, customers may be assigned different/multiple software concentrators through the discovery mechanism.

The Dynamic Host Configuration Protocol (DHCP [RFC2131], [RFC3315]) is widely used in edge networks to enable auto-configuration. This document extends DHCP to support discovery of a software concentrator or CGN. This mechanism is general for 6rd, incremental CGN, DS-Lite and Port-range Router [I-D.boucadair-port-rang]. It can also be extended to support the discovery of other concentrators with tunnels.

In the absence of DHCP, PPP or Router Advertisements could be used to find a software concentrator or CGN automatically, but this document does not discuss these methods in detail.

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. DHCP Solution Overview for Software Concentrator Discovery

In order to support software concentrator or CGN discovery, two new DHCP options are defined respectively for DHCPv4 and DHCPv6. They have the identical structure apart from address length.

When a DHCP server answers a client request message, software concentrator information can be carried in a DHCP reply message. Thus a client is configured the address and other attributes of a software concentrator or CGN and can automatically set up a tunnel.

DHCP server decides to attach SCD option based on policy. One choice is to respond only if the client requests the SCD option; another is to append it to every reply no matter the client requests the SCD option or not.

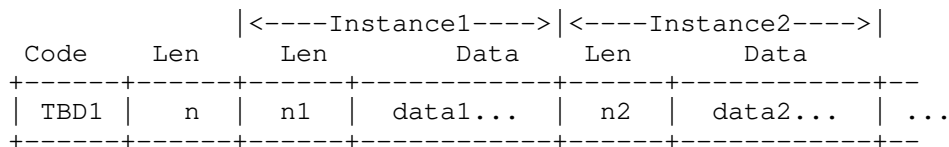
For load sharing or single-point failure recovery purposes, a DHCPv4 reply message may carry multiple instances in a single DHCPv4 SCD option; a DHCPv6 reply message may carry more than one DHCPv6 SCP options.

Section 4 defines a new DHCPv4 Software Concentrator Discovery (SCD) option while Section 5 defines DHCPv6 SCD option. Section 4.1 defines sub-options that apply to DHCPv4 SCD option while Section 5.1 defines sub-options that apply to DHCPv6 SCD option.

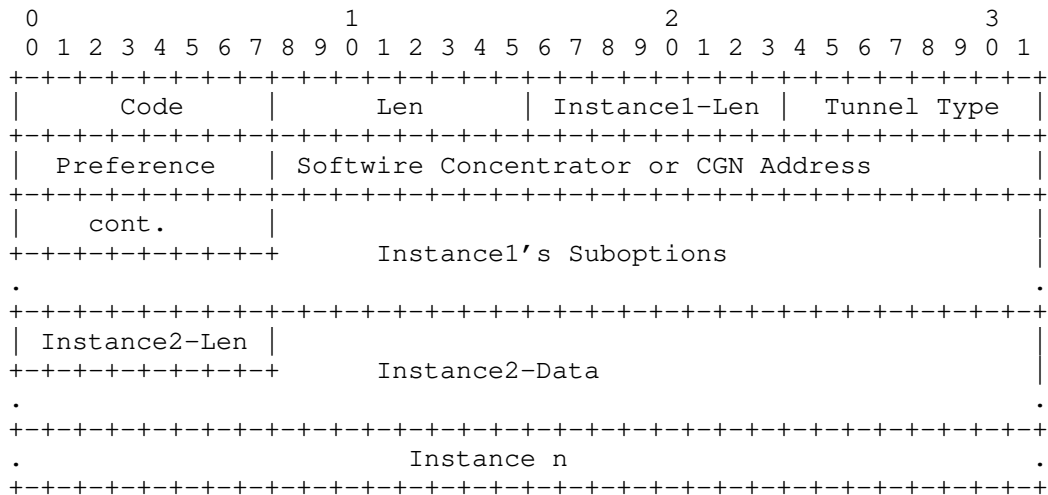
4. DHCPv4 Software Concentrator Discovery (SCD) Option

The DHCPv4 Software Concentrator Discovery (SCD) Option is mainly used when an IPv6 host or CPE in an IPv4 ISP network wants to obtain an IPv4 address of an IPv6 access point or an incremental CGN. The Option is carried in DHCPv4.

A DHCPv4 message can carry only one DHCPv4 SCD Option. Multiple instances can be concatenated in the DHCPv4 SCD Option, as follow:



The DHCPv4 SCD Option is structured as follows:



Code TBD1.

Len n + Len1 + Len2 + ... + Len n.

Instance-Len 6 + length of Instance's sub options in octets.

Tunnel Type Tunnel type which users connect to software concentrators or CGN. A few initial value assignments, like L2TPv2, GRE, ISATAP, 6to4, 6rd, IPSec and other IP in IP, is listed in Section 8 IANA consideration.

Preference This indicates the preference level for a software concentrator or CGN. 0 is the highest. When receiving multiple instances, the user chooses a primary software concentrator among them based on the preference. The others are backup software concentrators. The service provider assigns different preference for each software concentrator to support traffic engineering.

Software Concentrator or CGN Address The outer layer IPv4 address of software concentrator, which is used to establish tunnel.

Sub Options An optional, variable length field which is defined in Section 4.1.

4.1. Suboptions in DHCPv4 SCD Option

The suboptions defined in this section can be applied to DHCPv4 SCD option, defined above. They are used to configure the complementary tunnel information.

The DHCPv4 SCD suboption is structured in TLV style as follows:

```

      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 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
| Suboption Type | Suboption Len |                               |
+-----+-----+-----+-----+-----+-----+-----+-----+
.                               Suboption Value (Variable)                               .
+-----+-----+-----+-----+-----+-----+-----+-----+

```

* DHCPv4 SCD Suboption Type (1 octet): each suboption type defines a certain property about the tunnel. The following are the types defined in this document:

- Protocol Type: suboption type = 0
- GRE Key: suboption type = 1

New suboptions may be defined in the future. Any unknown suboptions MUST be ignored and skipped.

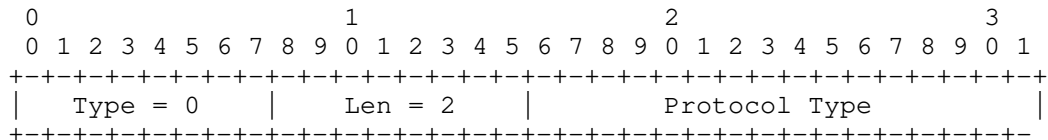
* Suboption Length (1 octet): the total number of octets of the suboption value field.

- * Suboption Value (variable): encodings of the value field depend on the suboption type as enumerated above.

The following sub-sections define the encoding in detail.

4.1.1. Protocol Type Suboption

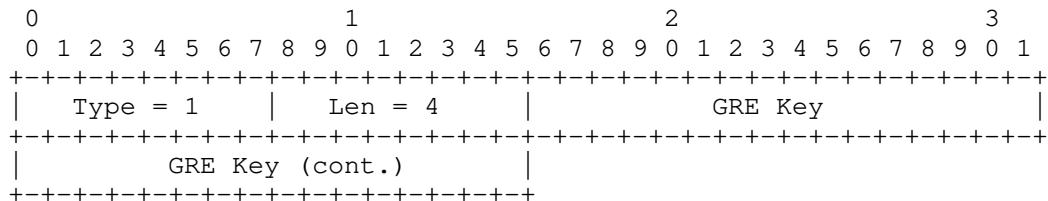
This suboption designates which protocol is encapsulated in tunnel.



The Protocol Type field is defined in [IANA-ET] as ETHER TYPEs. The most used protocols are IPv4 (0x0800) and IPv6 (0x86dd).

4.1.2. GRE Key Suboption

When the tunnel type is GRE, this suboption may be contained.



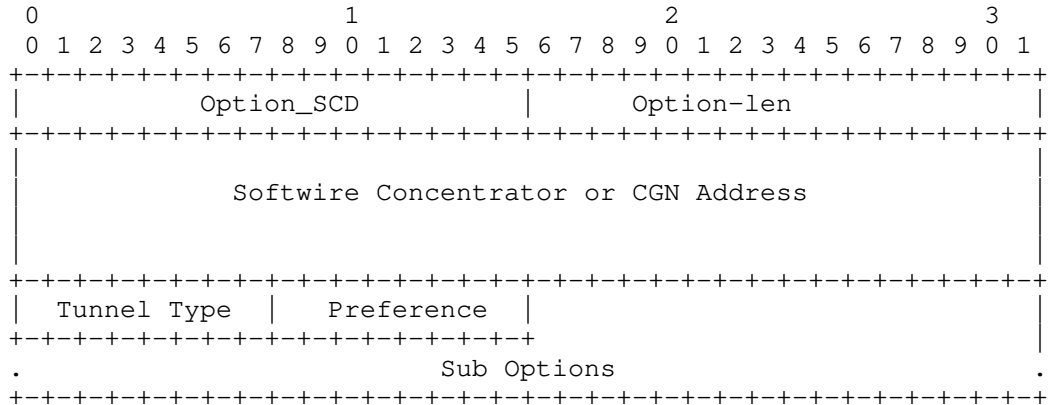
GRE Key: 4-octet field [RFC2890] that is generated by the Software Concentrator or CGN. If the client receives the GRE Key suboption, the key MUST be inserted into the GRE encapsulation header of the payload packets sent by the client to the Software Concentrator or CGN. It is used for identifying extra context information about the received payload. The payload packets without the correspondent GRE key or with an unmatched GRE Key will be silently dropped.

5. DHCPv6 Software Concentrator Discovery (SCD) Option

The DHCPv6 Software Concentrator Discovery (SCD) Option is mainly used when an IPv4 host or CPE in an IPv6 ISP network wants to learn an IPv6 address of an IPv4 access point or a DS-lite CGN. The Option is carried in DHCPv6.

A DHCPv6 Reply message can carry more than one SCD Options.

The DHCPv6 SCD Option is structured as follows:



Option-code Option_SCD (TBD2).

Option-len 18 + length of sub options in octets.

Software Concentrator or CGN Address The outer layer IPv6 address of software concentrator, which is used to establish tunnel.

Tunnel Type Tunnel type which users connect to software concentrators or CGN. A few initial value assignments, like L2TPv2, GRE, IPSec and IP in IP, is listed in Section 8 IANA consideration.

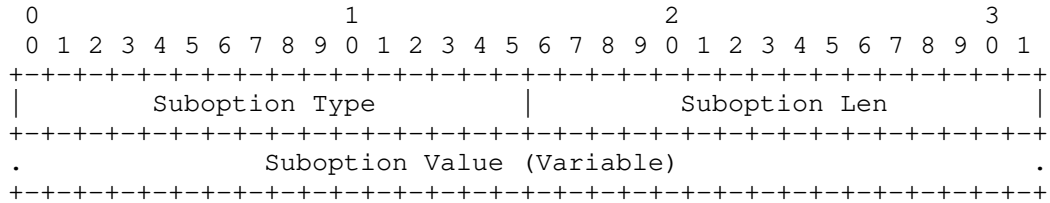
Preference This indicates the preference level for a software concentrator or CGN. 0 is the highest. When receiving multiple options, user chooses a primary software concentrator among them based on the preference. The others are backup software concentrators. The service provider assigns different preference of each software concentrator to support traffic engineering.

Sub Options An optional, variable length field is defined in Section 5.1.

5.1. Suboptions in DHCPv6 SCD Option

The suboptions defined in this section can be applied to DHCPv6 SCD option, defined above. They are used to configure the complementary tunnel information.

The DHCPv6 SCD suboption is structured in TLV style as follows:



* DHCPv4 SCD Suboption Type (2 octet): each suboption type defines a certain property about the tunnel. The following are the types defined in this document:

- Protocol Type: suboption type = 0
- Prefix: suboption type = 1
- GRE Key: suboption type = 2

New suboptions may be defined in the future. Any unknown suboptions MUST be ignored and skipped.

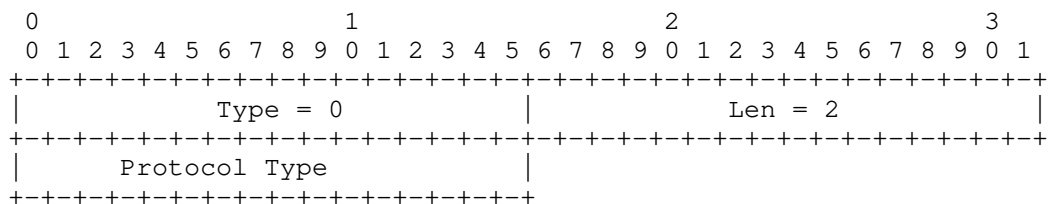
* Suboption Length (2 octet): the total number of octets of the suboption value field.

* Suboption Value (variable): encodings of the value field depend on the suboption type as enumerated above.

The following sub-sections define the encoding in detail.

5.1.1. Protocol Type Suboption

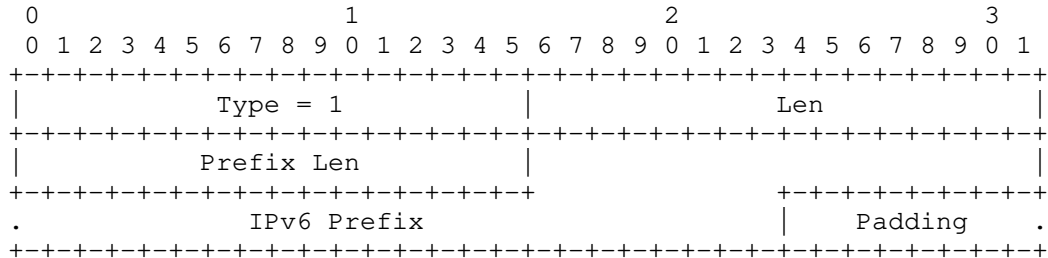
This suboption designates which protocol is encapsulated in tunnel.



The Protocol Type field is defined in [IANA-ET] as ETHER TYPEs. The most used protocols are IPv4 (0x0800) and IPv6 (0x86dd).

5.1.2. Prefix Suboption

This suboption designates IPv6 prefix which is used to construct internal address of the tunnel.



Len: total length of the prefix and padding fields in octets.

Prefix Len: Length for this prefix in bits.

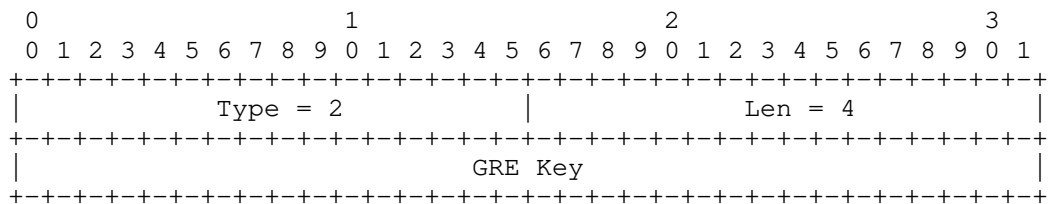
IPv6 Prefix: IPv6 prefix allocated to the client to construct internal address of the tunnel.

Padding: additional 0~7 bits MUST be padded at the end of IPv6 Prefix field when the value in Prefix Len field is not a multiple of 8-bit. The padding bits SHOULD be set as 0.

The semantics of the value field is determined by the tunnel type. For example, a client can obtain IPv6 Prefix of ISATAP tunnel by this suboption in DHCPv6 SDC Option.

5.1.3. GRE Key Suboption

When the tunnel type is GRE, this suboption may be contained.



GRE Key: 4-octet field [RFC2890] that is generated by the Software Concentrator or CGN. If the client receives the GRE Key suboption, the key MUST be inserted into the GRE encapsulation header of the payload packets sent by the client to the Software Concentrator or CGN. It is used for identifying extra context

information about the received payload. The payload packets without the correspondent GRE key or with an unmatched GRE Key will be silently dropped.

6. Illustration Examples

6.1. Example 1: Incremental CGN scenario

As an example, an incremental CGN with IP address 192.0.2.1 and L2TPv2 tunnel support is deployed in an IPv4 ISP network. The CGN information is stored in a DHCPv4 server. When a dual stack user in the network wants to connect IPv6 Internet, it will send a DHCPv4 request message to the DHCP server to obtain the CGN information. The DHCP server replies with a SCD option. The parameters in the SCD option are "CGN address = 192.0.2.1, tunnel type = 1, preference = 80". After the user receives the option, it can set up an L2TPv2 tunnel with the CGN.

6.2. Example 2: two CGN in DS lite scenario

In another example scenario, there are two DS lite CGNs deployed in order to provide redundancy and load balancing. DS lite CGN1 is 2001:db8:a::1, the other CGN2 is 2001:db8:b::1. Both of them support IPv4 in IPv6 tunnel. The preference of each CGN is decided by the network management policy. A user may get two SCD options, one describes CGN1 "CGN address = 2001:db8:a::1, tunnel type = 3, preference = 80" and the other describes CGN2 "CGN address = 2001:db8:b::1, tunnel type = 3, preference = 255". The user should establish an IPv4 in IPv6 tunnel with the CGN1, which has higher preference. When the CGN1 is down, the user may re-establish tunnel to the CGN2.

For the load balancing purpose, another user may receive the options, in which CGN2 has the higher preference value. The user may set CGN2 as its primary CGN.

7. Security Considerations

There are two forms of attack using bogus SCD options should be noticeable:

1. A wiretap attack, in which a bogus concentrator observes the traffic before pretending to be the real client and sending the traffic to the real concentrator.
2. A DoS attack, in which a bogus concentrator is used in some way to create a loop or simply to act as a source of DoS packets.

The mechanisms based on DHCPv6 are all vulnerable by man-in-middle attacks. Proper use of DHCPv6 auto-configuration facilities [RFC3315], such as AUTH option or Secure DHCPv6 [I-D.ietf-dhc-secure-dhcpv6] can prevent these threats, provided that a configuration token is known to both the client and the server.

8. IANA Considerations

IANA is requested to allocate one DHCPv4 SCD Option code TBD1 and one DHCPv6 Option code TBD2.

This document defines three new namespaces:

- Tunnel Types
- DHCPv4 SCD Suboption Types
- DHCPv6 SCD Suboption Types

8.1. Tunnel Types

Section 4 & 5 defines the following Tunnel Types, which should be assigned by IANA for use within DHCPv4 & DHCPv6 SCD Option. IANA set up a registry for "Tunnel Types for DHCP SCD Option". This is a registry of one-octet values (0-255), to be assigned on a first-come, first-served basis. The initial assignments are as follows:

Tunnel Name	Type
-----	-----
Reserved	0
L2TPv2	1
GRE	2
IP-in-IP	3
ISATAP	4
6to4	5
6rd	6
IPsec	7

8.2. DHCPv4 SCD Suboption Types

Section 4.1 defines the following SCD Suboption Types, which should be assigned by IANA for use within DHCPv4 SCD Option. IANA set up a registry for "DHCPv4 SCD Suboption Types". This is a registry of one-octet values (0-255), to be assigned on a first-come, first-served basis. The initial assignments are as follows:

Tunnel Name	Type
-----	-----
Protocol Type	0
GRE Key	1

8.3. DHCPv6 SCD Suboption Types

Section 5.1 defines the following SCD Suboption Types, which should be assigned by IANA for use within DHCPv6 SCD Option. IANA set up a registry for "DHCPv6 SCD Suboption Types". This is a registry of one-octet values (0-255), to be assigned on a first-come, first-served basis. The initial assignments are as follows:

Tunnel Name	Type
-----	-----
Protocol Type	0
Prefix	1
GRE Key	2

9. Acknowledgments

The authors would like to thank Wei Cao, Huawei, Bernie Volz, Cisco for valuable comments.

10. Change Log [RFC Editor please remove]

draft-guo-software-sc-discovery-00, original version, 2009-06-23.

draft-guo-software-sc-discovery-01, revised for protocol type, 2009-07-13.

draft-guo-software-sc-discovery-02, revised after comments at IETF75 and comments on the maillist, 2009-10-26.

draft-guo-software-sc-discovery-03, minor update, 2010-03-05.

draft-guo-software-sc-discovery-04, revised after comments at IETF77 and comments on the maillist, 2010-07-12.

11. References

11.1. Normative References

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

- [RFC2131] R. Droms, "Dynamic Host Configuration Protocol", RFC 2131, March 1997.
- [RFC2890] G. Dommety, "Key and Sequence Number Extensions to GRE", RFC 2890, September 2000.
- [RFC3315] R. Droms, et al., "Dynamic Host Configure Protocol for IPv6", RFC3315, July 2003.
- [RFC5512] P. Mohapatra, E. and Rosen, "The BGP Encapsulation Subsequent Address Family Identifier (SAFI) and the BGP Tunnel Encapsulation Attribute", RFC 5512, April 2009.
- [RFC5571] B. Storer, et al., "Softwire Hub & Spoke Deployment Framework with L2TPv2", RFC 5571, June 2009.

11.2. Informative References

- [RFC4925] X. Li, S. Dawkins, D. Ward, and A. Durand, "Softwire Problem Statement", RFC 4925, July 2007.
- [I-D.ietf-software-dual-stack-lite]
A. Durand, R. Droms, B. Haberman, and J. Woodyatt, "Dual-stack lite broadband deployments post IPv4 exhaustion", draft-ietf-software-dual-stack-lite, work in progress, March 2010.
- [I-D.ietf-v6ops-incremental-cgn]
S. Jiang, D. Guo, and B. Carpenter, "An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition" draft-ietf-v6ops-incremental-cgn, work in progress, June 2010.
- [I-D.ietf-dhc-secure-dhcpv6]
S. Jiang and S. Shen, "Secure DHCPv6 Using CGAs", draft-ietf-dhc-secure-dhcpv6, work in progress, June 2010.
- [I-D.ietf-software-ipv6-6rd]
Townesley W., et al., "IPv6 via IPv4 Service Provider Networks (6rd)", draft-ietf-software-ipv6-6rd, (work in progress), March 2010.
- [I-D.boucadair-port-rang]
B. Storer, et al., "IPv4 Connectivity Access in the Context of IPv4 Address Exhaustion", draft-boucadair-port-range-02.txt, work in progress, July 2009.

[IANA-ET] "Ether Types", <http://www.iana.org/assignments/ethernet-numbers>.

Author's Addresses

Dayong Guo
Huawei Technologies Co., Ltd
Huawei Building, No.3 Xixi Rd.,
Shang-Di Information Industry Base, Hai-Dian District, Beijing 100085
P.R. China
Email: guoseu@huawei.com

Sheng Jiang
Huawei Technologies Co., Ltd
Huawei Building, No.3 Xixi Rd.,
Shang-Di Information Industry Base, Hai-Dian District, Beijing 100085
P.R. China
Email: shengjiang@huawei.com

Brian Carpenter
Department of Computer Science
University of Auckland
PB 92019
Auckland, 1142
New Zealand
Email: brian.e.carpenter@gmail.com

