Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 27, 2016

S. Jiang, Ed.
D. Guo
Huawei Technologies Co., Ltd
L. Xue

November 24, 2015

Dynamic GRE Tunnel
draft-jiang-intarea-dynamic-gre-01

Abstract

Generic Routing Encapsulation (GRE) is regarded as a popular encapsulation tunnel technology. When a node tries to encapsulate the user traffic in GRE, it needs the IP address of the destination node which decapsulates the GRE packets. In practice, the GRE tunnel destination IP addresses are mainly configured manually. This configuration mechanism causes efficiency issues for operators. This document proposes an approach to configure the GRE information dynamically.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Generic Routing Encapsulation (GRE, [RFC1701], [RFC2784]) is widely deployed in the operators' networks. When a node tries to encapsulate the user traffic in a GRE tunnel, it needs the IP address of the destination node which decapsulates the GRE packets.

In practice, the GRE tunnel destination IP addresses are mainly configured manually on the nodes. This configuration mechanism causes efficiency issues for operators. As an example, when GRE tunneling is used in the access network, there may a large amount of configuration needed at the access side. Also, the configuration is rigid. It may cause more issues in renumbering scenarios.

This document introduces a use case requiring the deployment of a large amount of GRE tunnels, which motivates a dynamic approach. This document proposes a solution to enable the dynamic discovery of the GRE decapsulation device using Dynamic Host Configuration Protocol (DHCP).

2. Requirements Language and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] when they appear in ALL CAPS. When these words are not in ALL CAPS (such as "should" or "Should"), they have their usual English meanings, and are not to be interpreted as [RFC2119] key words.

Access Controller (AC) The network entity that provides Wireless Termination Point (WTP) access to the network infrastructure in the data plane, control plane, management plane, or a combination therein.

Customer Premises Equipment (CPE) The box that a provider may distribute to the customers. When CPE is using DHCP to obtain network address, CPE is acting as "DHCP Client".

Wireless Termination Point (WTP) The physical or logical network entity that contains an RF antenna and wireless physical layer (PHY) to transmit and receive station traffic for wireless access networks.

3. GRE Use Case - WLAN Network

Wireless Local Area Network (WLAN) has emerged as an important access technology for service operators. A typical WLAN network contains a large number of WTPs, centrally managed and controlled by the Access Controller (AC). It is desirable to distribute customer data frames to an endpoint through an Access Router (AR) different from the AC. GRE encapsulation can be used between a WTP and an AR as one of the optional tunneling technologies shown in [I-D.ietf-opsawg-capwap-alt-tunnel]

An illustration of a WLAN network is shown in Figure 1. In order for a WTP to encapsulate the user traffic in a GRE tunnel, it needs to know the Access Router (AR) IP address. This IP address is usually configured on WTPs manually. An AC may dynamically configure the WTP with the AR address via extended CAPWAP message elements (see [I-D.ietf-opsawg-capwap-alt-tunnel]).

```
                 CAPWAP   +--------+
                ++========+   AC   |
               //         +--------+
              //
      +-----+//   DATA Tunnel (GRE)     +--------------+
      | WTP |===========================| Access Router|
      +-----+                           +--------------+
```

Figure 1: GRE Use Case - WLAN Network 1

However, this approach does not apply to a WLAN network where the CAPWAP protocol is not deployed, as the network shown in Figure 2. In fact, it is quite common for operators to have their own private control plane between the WTP and the AC rather than CAPWAP.

```
         Private Control  +--------+
                ++========+   AC   |
               //         +--------+
              //
      +-----+//   DATA Tunnel (GRE)     +--------------+
      | WTP |===========================| Access Router|
      +-----+                           +--------------+
```

Figure 2: GRE Use Case - WLAN Network 2

Moreover, there are also WLAN deployments without AC, as in the fat WTPs scenario (see Figure 3). A general approach to resolve this problem is desirable.

```
      +-----+     DATA Tunnel (GRE)     +--------------+
      | WTP |===========================| Access Router|
      +-----+                           +--------------+
```

Figure 3: GRE Use Case - WLAN Network 3

4. Dynamic GRE Tunnel Overview

The DHCP options defined in Section 5 enable an automated way to inform the GRE encapsulator with the GRE destination IP address. Additionally, some other GRE tunnel information may be provided. In this way, a GRE tunnel can be setup dynamically.

Figure 4 illustrates the procedure to set up a dynamic GRE tunnel in the network (only in IPv4 network scenario).

```
    /    \      IPv4-x.x.x.x                   IPv4-y.y.y.y     /    \
  /      \       +-------+       +-------+      +-------+      /      \
  |       |      |       |       |       |      |       |      |       |
  | Host  +------+  CPE  +-------+  DHCP +------+  AR   +------+Internet
  \       /      |       |       | Server|      |       |      \       /
   \     /       +-------+       +-------+      +-------+       \     /
                 DHCP Client     DHCP Server
     |              |               |               |
     |              |  DHCPREQUEST  |               |
     |         (1)  + ------------->|               |
     |              |               |               |
     |              |    DHCPACK    |               |
     |              + <-------------|               |
     |              | with y.y.y.y and              |
                    |information (optional)         |
     |              |                               |
     |              *-------------------------------*
     |<-User Packet->+<---User Packet-in-GRE-Encap.->|
     |         (2)  *----with  x.x.x.x -------------*
     |              |                        /             \
     |              |                        | Tunnel Client |
     |              |                        \ List Config.  /
     |              |                               |
     |              *-------------------------------*
     |         (3)  |<-------Keepalive Packet------>|
     |              *-------------------------------*
```

Figure 4: Dynamic GRE Tunnel

The steps to set up a GRE tunnel between the CPE and the AR are as follows:

1. The CPE, as one endpoint of GRE tunnel, sends the DHCPREQUEST message to the DHCP server to acquire the AR access. The GRE DHCP Option should be included in Parameter List Option, as defined in Section 6.2. When the DHCP server receives this request, it replies to the CPE the DHCPACK message, containing the AR address and the tunnel information if needed.

2. The CPE can encapsulate the upstream packets from the hosts within GRE tunnel packets. Generally, upstream packets are either data packets or control packets. When the AR gets an encapsulated GRE tunnel packet, the AR checks whether there is an existing GRE tunnel with the CPE. If this is a new endpoint without GRE record, the AR should add this CPE into the tunnel client list. This would be mainly used for the correspondent downstream packets.

3. A keepalive mechanism may be required for a GRE tunnel between the CPE and the AR. If there is neither keepalive packet nor data packet, when a keepalive timer expires, the AR or the CPE will tear down the tunnel and release resources.

5. DHCP Options Definition

This section defines the new DHCPv4 and DHCPv6 options that support the Dynamic stateless GRE tunnel.

5.1. DHCPv4 GRE Discovery Option

The DHCPv4 GRE Discovery option provides to a GRE encapsulator a list of one or more IPv4 addresses of a GRE decapsulator. According to [RFC2131], the DHCPv4 GRE Discovery Option is structured as shown in Figure 5.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Option Code   | Option Len    |  AR IPv4 Address              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  AR IPv4 Address              |   AR IPv4 Address (optional)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 5: DHCPv4 GRE Discovery Option

option-code   OPTION_V4_GRE_DISCOVERY (TBA1).

option-len   4 + 4*n (in octets).

AR IPv4 Address AR IPv4 address, an endpoint of GRE tunnel. More than one AR IPv4 addresses may be provided for redundancy reasons. The default priority of the listed AR IPv4 addresses may be from highest to lowest.

5.2. DHCPv4 GRE Information Option

The DHCPv4 GRE Information option provides a list of the GRE information as defined in and [RFC2784][RFC2890]. The GRE information may include the key. According to [RFC2131], the DHCPv4 GRE Information Option is structured as shown in Figure 6.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Option Code   | Option Len    |       GRE Key                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     GRE Key (cont.)           |       Reserved                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 6: DHCPv4 GRE Information Option

option-code   OPTION_V4_GRE_INFO (TBA2).

option-len   6 (in octets).

GRE Key   The Key field contains a four octet number which is inserted by the GRE encapsulator according to [RFC2890].

Reserved   This field is reserved for future use. These bits MUST be sent as zero and MUST be ignored on receipt.

5.3. DHCPv6 GRE Discovery Option

The DHCPv6 GRE Discovery option provides to a GRE encapsulator a list of one or more IPv6 addresses of a GRE decapsulator. According to [RFC7227], the DHCPv6 GRE Discovery Option is structured as shown in Figure 7.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Option Code                |       Option Len              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
.                AR IPv6 Address                                .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
.                AR IPv6 Address (Optional)                     .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 7: DHCPv6 GRE Discovery Option

option-code   OPTION_V6_GRE_DISCOVERY (TBA3).

option-len   16 + 16*n (in octets).

AR IPv4 Address AR IPv64 address(es), an endpoint of GRE tunnel. More than one AR IPv6 addresses may be provided for redundancy reasons. The default priority of the listed AR IPv6 addresses may be from highest to lowest.

5.4. DHCPv6 GRE Information Option

The DHCPv6 GRE Information option provides a list of the GRE information as defined in and [RFC2784][RFC2890]. The GRE information may include the key.

According to [RFC7227], the DHCPv6 GRE Information Option is structured as shown in Figure 8.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Option Code           |       Option Len              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               GRE Key                                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Reserved                                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 8: DHCPv6 GRE Information Option

option-code OPTION_V6_GRE_INFO (TBA4).

option-len 8 (in octets).

GRE Key The Key field contains a four octet number which is inserted by the GRE encapsulator according to [RFC2890].

Reserved This field is reserved for future use. These bits MUST be sent as zero and MUST be ignored on receipt.

6. DHCP/DHCPv6 server and client behaviors

This section defines the DHCP/DHCPv6 server and client behaviors during the procedure of configure GRE options.

6.1. DHCP Server Behavior

Section 3.5 of [RFC2131] describes how a DHCP client and server negotiate configuration values using the Parameter List (55) option [RFC2132]. By default, a server will not reply with a GRE option if the client has not explicitly enumerated one in its Parameter List option.

6.2. DHCP Client Behavior

A WTP/CPE acting as DHCP client will request DHCP GRE configuration parameters from the DHCP server located in the IPv4 network. Such a client MUST request the DHCP GRE option(s) that it is configured for in Parameter List option in its DHCPDISCOVER, DHCPREQUEST, or DHCPINFORM messages.

The client SHOULD use the received GRE destination address and information to establish GRE tunnels.

6.3. DHCPv6 Server Behavior

Section 17.2.2 of [RFC3315] describes how a DHCPv6 client and server negotiate configuration values using the Option Request (6) Option[RFC3315]. By default, a server will not reply with a GRE option if the client has not explicitly enumerated one in its ORO.

6.4. DHCPv6 Client Behavior

A WTP/CPE acting as DHCPv6 client will request DHCPv6 GRE configuration parameters from the DHCPv6 server located in the IPv6 network. Such a client MUST request the GRE option(s) that it is configured for in its ORO in SOLICIT, REQUEST, RENEW, REBIND or INFORMATION-REQUEST messages.

The client SHOULD use the received GRE destination address and information to establish GRE tunnels.

7. Security Considerations

Section 23 of [RFC3315] discusses DHCPv6-related security issues. As with all DHCPv6-derived configuration state, it is possible that configuration is actually being delivered by a third party (Man In The Middle). As such, there is no basis on which access over the stateless GRE tunnel can be trusted. Therefore, the stateless GRE tunnel should not bypass any security mechanisms such as IP firewalls or user authentication.

8. IANA Considerations

This document defines two new DHCPv4 [RFC2131] options. The IANA is requested to assign values for these four options from the DHCPv4 Option Codes table of the DHCPv4 Parameters registry maintained in http://www.iana.org/assignments/bootp-dhcp-parameters. The four options are:

The GRE Discovery Option (TBA1), described in Section 5.1.

The GRE Information Option (TBA2), described in Section 5.2.

This document defines three new DHCPv6 [RFC3315] options. The IANA is requested to assign values for these three options from the DHCPv6 Option Codes table of the DHCPv6 Parameters registry maintained in http://www.iana.org/assignments/dhcpv6-parameters. The three options are:

The GRE Discovery Option (TBA3), described in Section 5.3.

The GRE Information Option (TBA4), described in described in Section 5.4.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, March 1997, <http://www.rfc-editor.org/info/rfc2131>.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, DOI 10.17487/RFC2132, March 1997, <http://www.rfc-editor.org/info/rfc2132>.

[RFC2784] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, DOI 10.17487/RFC2784, March 2000, <http://www.rfc-editor.org/info/rfc2784>.

[RFC2890] Dommety, G., "Key and Sequence Number Extensions to GRE", RFC 2890, DOI 10.17487/RFC2890, September 2000, <http://www.rfc-editor.org/info/rfc2890>.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <http://www.rfc-editor.org/info/rfc3315>.

[RFC7227] Hankins, D., Mrugalski, T., Siodelski, M., Jiang, S., and S. Krishnan, "Guidelines for Creating New DHCPv6 Options", BCP 187, RFC 7227, DOI 10.17487/RFC7227, May 2014, <http://www.rfc-editor.org/info/rfc7227>.

9.2. Informative References

[I-D.ietf-opsawg-capwap-alt-tunnel]
Zhang, R., Cao, Z., Hui, D., Pazhyannur, R., Gundavelli, S., Xue, L., and J. You, "Alternate Tunnel Encapsulation for Data Frames in CAPWAP", draft-ietf-opsawg-capwap-alt-tunnel-06 (work in progress), October 2015.

[RFC1701] Hanks, S., Li, T., Farinacci, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 1701, DOI 10.17487/RFC1701, October 1994, <http://www.rfc-editor.org/info/rfc1701>.

Authors' Addresses

Sheng Jiang (editor)
Huawei Technologies Co., Ltd
Q14, Huawei Campus, No.156 Beiqing Road
Hai-Dian District, Beijing, 100095
CN

Email: jiangsheng@huawei.com

Dayong Guo
Huawei Technologies Co., Ltd
Q14, Huawei Campus, No.156 Beiqing Road, Hai-Dian District
Beijing, 100095
China

Email: guoseu@huawei.com

Li Xue

Email: xueli_jas@163.com