Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 27, 2015

L. Xue
D. Guo
Huawei

October 24, 2014

Dynamic Stateless GRE Tunnel
draft-xue-dhc-dynamic-gre-03

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 address may be manually configured. This configuration may introduce efficiency issues for operators. This work proposes an approach to configure the GRE information dynamically.

Requirements Language

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]

Table of Contents

1. Introduction

Generic Routing Encapsulation (GRE, see [RFC1701] and [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 can decapsulate the GRE packets. In practice, the manual configuration happens on the nodes. This may introduce efficiency issues for operators. As an example, if GRE tunneling is used in the access network, there may a large amount of configuration needed at the access side. This specification introduces a use case requiring the deployment of a large amount of GRE tunnels, which motivates a dynamic approach. The specification proposes a solution to enable the dynamic discovery of the GRE decapsulation device through use of a Dynamic Host Configuration Protocol (DHCP) option.

2. Terminology

The following terms are used in this document:

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 deployed on WTPs manually, which may introduce efficiency issues for operators. An AC may dynamically configure the WTP with the AR address via extended CAPWAP message elements (see [I-D.ietf-opsawg-capwap-alt-tunnel]). 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. 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.

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

Figure 1: GRE Use Case - WLAN Network 1

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

Figure 2: GRE Use Case - WLAN Network 2

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

Figure 3: GRE Use Case - WLAN Network 3

4. DHCP Options Definition

4.1. GRE Discovery DHCPv4 Option

The GRE Discovery DHCPv4 option provides to a GRE encapsulator a list of one or more IPv4 addresses of a GRE decapsulator. According to [RFC2131], the GRE Discovery DHCPv4 Option is structured as shown in Figure 4.

```
     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              |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4: GRE Discovery DHCPv4 Option

Code: TBD

Len: 4

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.

4.2. GRE Information DHCPv4 Option

The GRE Information DHCPv4 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 GRE Information DHCPv4 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    |       GRE Key                 |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |     GRE Key (cont.)            |       Reserved                |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 5: GRE Information DHCPv4 Option

Code: TBD

Len: 6

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.

4.3. GRE Discovery DHCPv6 Option

The GRE Discovery DHCPv6 option provides to a GRE encapsulator a list of one or more IPv6 addresses of a GRE decapsulator. According to [RFC7227], the GRE Discovery DHCPv6 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              |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 .                AR IPv6 Address                                 .
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 .                AR IPv6 Address (Optional)                      .
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 6: DHCPv6 GRE Discovery Option

Code: TBD

Len: >=16

AR IPv6 Address: AR IPv6 address, 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 the lowest.

4.4. GRE Information DHCPv6 Option

The GRE Information DHCPv6 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 GRE Information DHCPv6 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              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               GRE Key                                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Reserved                                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 7: GRE Information DHCPv6 Option

Code: TBD

Len: 8

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. Dynamic GRE Tunnel

The DHCP options defined in Section 4 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 8 illustrates the procedure to set up a dynamic GRE tunnel in the network.

```
    /    \      IPv4-x.x.x.x                  IPv4-y.y.y.y     /    \
   /      \      +--------+       +--------+      +--------+      /      \
   |       |     |       |       |       |      |       |      |       |
   | Host  +-----+  CPE  +--------+  DHCP +-------+  AR   +-------+Internet
   \       /     |       |       | Server|      |       |      \       /
    \     /      +--------+       +--------+      +--------+       \     /
                 DHCP Client     DHCP Server
      |              |               |               |
      |              |DHCPv4 Request |               |
      |       (1)    + ------------->|               |
      |              |               |               |
      |              | DHCPv4 Reply  |               |
      |              + <-------------|               |
      |              | with y.y.y.y and information  |
                     |                   (optional)  |
      |              |                               |
      |              *-------------------------------*
      |--------------+----User Packet-in-GRE-Encap.->|
      |       (2)    *----with  x.x.x.x -------------*
      |              |                    /               \
      |              |                    | Tunnel Client |
      |              |                    \ List Config.  /
      |              |                               |
      |             *-------------------------------*
      |       (3)    |<-------Keepalive Packet------>|
      |              *-------------------------------*
```

Figure 8: 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 DHCP request message to the DHCP server to acquire the AR access. The GRE Discovery DHCP Option should be included, with AR IPv4 address set to zero. When the DHCP server receives this request, it replies to the CPE the DHCP Reply message, containing the AR address and the tunnel information if needed.

2. The CPE can encapsulate the upstream packets from the hosts within GRE packets. Generally, upstream packets are either data packets or control packets. When the AR gets an encapsulated GRE 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.

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.

6. IANA Considerations

TBD

7. References

7.1. Normative References

[RFC1701] Hanks, S., Li, T., Farinacci, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 1701, October 1994.

[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.

[RFC2784] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.

[RFC2890] Dommety, G., "Key and Sequence Number Extensions to GRE", RFC 2890, September 2000.

[RFC7227] Hankins, D., Mrugalski, T., Siodelski, M., Jiang, S., and S. Krishnan, "Guidelines for Creating New DHCPv6 Options", BCP 187, RFC 7227, May 2014.

7.2. Informative References

[I-D.ietf-opsawg-capwap-alt-tunnel]
Zhang, R., Cao, Z., Deng, H., Pazhyannur, R., Gundavelli, S., and L. Xue, "Alternate Tunnel Encapsulation for Data Frames in CAPWAP", draft-ietf-opsawg-capwap-alt-tunnel-03 (work in progress), September 2014.

Authors' Addresses

Li Xue
Huawei
No. 156 Beiqing Rd. Z-park, Shi-Chuang-Ke-Ji-Shi-Fan-Yuan
Beijing, Haidian District 100095
China

Email: xueli@huawei.com

Dayong Guo
Huawei
No. 156 Beiqing Rd. Z-park, Shi-Chuang-Ke-Ji-Shi-Fan-Yuan
Beijing, Haidian District 100095
China

Email: guoseu@huawei.com