Independent Submission
Internet Draft
Intended Category: Informational
Expires: April 11, 2016
October 9, 2015

N. Leymann
C. Heidemann
Deutsche Telekom AG
M. Zhang
B. Sarikaya
Huawei
M. Cullen
Painless Security

GRE Tunnel Bonding
draft-zhang-gre-tunnel-bonding-01.txt

Abstract

There is an emerging demand for solutions that provide redundancy and load-sharing across wired and cellular links from a single service provider, so that a single subscriber is provided with hybrid access to multiple heterogeneous connections at the same time.

In this document, GRE (Generic Routing Encapsulation) Tunnel Bonding is specified as an enabling approach for Hybrid Access to a wired and a wireless network in customer premises, e.g. homes. In GRE Tunnel Bonding, two GRE tunnels, one per network connection, are set up and bonded together to form a single GRE tunnel for a subscriber. Compared with each composing connection, the bonding connection promises increased access capacity and improved reliability. The solution described in this document is currently implemented by Huawei and deployed by Deutsche Telekom AG.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright and License Notice

Table of Contents

1. Introduction

Service providers used to provide subscribers with separate access to their fixed broadband networks and mobile networks. It has become desirable to bond these heterogeneous networks together to offer access service to subscribers that offer increased access capacity and improved reliability. In this document, "Hybrid Access" is used to refer to such bonding access services. The Broadband Forum first proposes the concept of Hybrid Access and develops a set of

requirements in [WT-348].

In this document, Hybrid Access focuses on the use case that DSL (Digital Subscriber Line) connection and LTE (Long Term Evolution) connection are bonded together to form a bonding connection. When the traffic volume exceeds the bandwidth of the DSL connection, the excess amount can be offloaded to the LTE connection. Hybrid Customer Premises Equipment (HCPE) is the equipment at the customer side initiating the DSL and LTE connections. Hybrid Access Gateway (HAG) is the network function that resides in the provider's networks to terminate the bonded connections. Note that if there were more than two connections that needed to be bonded, the GRE Tunnel Bonding mechanism could support that scenario, as well. However, support for more than two connections is out the scope of this document.

This document bases the solution on GRE (Generic Routing Encapsulation [RFC2890]) since GRE is widely supported in both fixed and mobile networks. One GRE tunnel is set up for each heterogeneous connection (DSL and LTE) between the HCPE and HAG. Those GRE tunnels are further bonded together to form a logical GRE tunnel for the subscriber. HCPE conceals the composing GRE tunnels from the end nodes, and end nodes simply treat the logical GRE tunnel as a single IP link. This provides an overlay: the users' IP packets (inner IP) are encapsulated in GRE which is in turn carried over IP (outer IP).

2. Acronyms and Terminology

GRE: Generic Routing Encapsulation [RFC2890]

DSL: Digital Subscriber Line is a family of technologies that are used to transmit digital data over telephone lines

LTE: Long Term Evolution. A standard for wireless communication of high-speed data for mobile phones and data terminals. Commonly marketed as 4G LTE.

Hybrid Access: The bonding of multiple access connections based on heterogeneous technologies (e.g., DSL and LTE).

HCPE: Hybrid Customer Premises Equipment (CPE). A CPE enhanced to support the simultaneous use of both fixed broadband and 3GPP access connections.

HAG: Hybrid Access Gateway. A logical function in the operator network implementing a bonding mechanism for subscriber access services.

CIR: Committed Information Rate [RFC2698]

RTT: Round Trip Time

AAA: Authentication, Authorization and Accounting [RFC6733]

SOAP: Simple Object Access Protocol. It is a protocol specification for exchanging structured information in the implementation of web services in computer networks.

FQDN: A Fully Qualified Domain Name (FQDN) is a domain name that includes all higher level domains relevant to the entity named. [RFC1594]

DSCP: The six-bit codepoint (DSCP) of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers [RFC2724].

BRAS: Broadband Remote Access Server. It routes traffic to and from broadband remote access devices such as Digital Subscriber Line Access Multiplexers (DSLAM) on an Internet service provider's (ISP) network.

PGW: Packet Data Network Gateway. In the Long Term Evolution (LTE) architecture for the Evolved Packet Core (EPC), the PGW acts as an anchor for user plane mobility.

PDP: Packet Data Protocol. A packet transfer protocol used in wireless GPRS (General Packet Radio Service)/HSDPA (High Speed Downlink Packet Access) networks.

PPPoE: Point-to-Point Protocol over Ethernet is a network protocol for encapsulating PPP frames inside Ethernet frames.

DNS: Domain Name System is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network.

DHCP: Dynamic Host Configuration Protocol. A standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.

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 RFC 2119 [RFC2119].

3. Use Case

```
             +-+                            +-+
             | +---- Bonding Connection ---+ |
             | |                            | |
             | | +-+                        | |
  subscriber |C| |E+---- LTE Connection ---+H| Internet
             | | +-+                        | |
             | | +-+                        | |
             | | |D+---- DSL Connection ---+ |
             +-+ +-+                        +-+
             \_____/
              HCPE                          HAG
```

C: The endpoint of the bonding connection at the HCPE.
E: The endpoint of the LTE connection resides in HCPE.
D: The endpoint of the DSL connection resides in HCPE
H: The endpoint of the bonding connection at HAG. It is also used as the endpoint for each heterogeneous connection.

Figure 3.1: Offloading from DSL to LTE, increased access capacity

For a Service Provider who runs heterogeneous networks, such as fixed and mobile, subscribers wish to use those networks simultaneously for increased access capacity rather than just using a single network. As shown by the reference model in Figure 3.1, the subscriber expects the whole bandwidth of the bonding connection equals the sum of the bandwidth of the DSL connection and the LTE connection between HCPE and HAG. In other words, when the traffic volume exceeds the bandwidth of the DSL connection, the excess amount may be offloaded to the LTE connection.

Most load balancing solutions spread load based on per-flow load-balancing among multiple paths. However, the solution described here is about per-packet offloading rather than per-flow load-balancing. For per-flow load-balancing, the maximum bandwidth that may be used by a flow is equal to the bandwidth of the connection selected. However, per-packet load-balancing allows a single flow to use the bandwidth of both connections. A GRE Tunnel Bonding mechanism could also support per-flow traffic classification and distribution, though that is out of scope for this document.

4. Overview

In this document, the widely supported GRE is chosen as the tunneling technique. With the newly defined control protocol, GRE tunnels are setup on top of the DSL and LTE connections which are ended at D and H or E and H. These tunnels are bonded together to form a single logical bonding GRE tunnel whose endpoint IP addresses are C and H. Subscribers uses this logical tunnel without knowing the composing

GRE tunnels.

4.1. Control Plane

A clean-slate control protocol is designed to manage the GRE tunnels that are setup per heterogeneous connection between HCPE and HAG. The goal is to design a compact control plane for Hybrid Access only instead of reusing existing control planes.

In order to measure the performance of connections, control packets need to co-route the same path with data packets. Therefore, a GRE Channel is opened for the purpose of data plane forwarding of control plane packets. The GRE header (shown in Figure 6.1) as specified in [RFC2890] is being used. The GRE Protocol Type (tbd1) is used to identify this GRE Channel. A family of control messages are encapsulated with GRE header and carried over this channel. Attributes, formatted in Type-Length-Value style, are further defined and included in each control message.

With the newly defined control plane, the GRE tunnels between HCPE and HAG can be established, managed and released without the involvement of human operators.

4.2. Data Plane

Using the control plane defined in Section 4.1, GRE tunnels can be automatically setup per heterogeneous connection between the HCPE and the HAG. For the use case described in Section 3, one GRE tunnel is terminated at the DSL WAN interfaces, e.g., DSL GRE tunnel, and another GRE tunnel is terminated at the LTE WAN interfaces, e.g., LTE GRE tunnel. Each tunnel may carry user's IP packets as payload, which forms a typical IP-in-IP overlay. These tunnels are bonded together to offer a single access point to subscribers.

The GRE header [RFC2890] is used to encapsulate data packets. The Protocol Type is 0x0800, which indicates the inner header is an IP header. For per-packet offloading use case, the Key field is set to a unique value for the entire bonding. The Sequence Number field is used to maintain the sequence of packets transported in all GRE tunnels as a single flow between the HCPE and the HAG.

4.3. Traffic Classification and Distribution

For the offloading use case, the coloring mechanism specified in [RFC2698] is being used to classify subscriber's IP packets, both upstream and downstream, into the DSL GRE tunnel or the LTE GRE tunnel. Packets colored as green will be distributed into the DSL GRE tunnel and packets colored as yellow will be distributed into the LTE

GRE tunnel. For the scenario that requires more than two GRE tunnels, multiple levels of token buckets might be realized. However, that is out of the scope for this document.

The Committed Information Rate (CIR) of the coloring mechanism is set to the total DSL WAN bandwidth minus the bypassing DSL bandwidth (See Section 4.4.). The total DSL WAN bandwidth MAY be configured, MAY be obtained from the management system (AAA server, SOAP server, etc.), or MAY be detected and reported in real-time using ANCP [RFC6320].

4.4. Traffic Recombination

The recombination function at the receiver provides in-order delivery of subscribers' traffic. As specified in [RFC2890], the receiver maintains a small reordering buffer and orders the data packets in this buffer by the Sequence Number field of the GRE header. For the offloading use case, all bonded GRE tunnels use the same Key value. All packets carried on these bonded GRE tunnels go into a single reordering buffer.

4.5. Bypassing

Service Providers provide some services that should not be delivered over a bonded connection. For example, Service Providers do not expect real-time IPTV to be carried by the LTE GRE tunnel. It is required that these services bypass GRE Tunnel Bonding and use the raw DSL bandwidth. In this way, they are not subject to the traffic classification and distribution specified above. There are two kinds of bypassing:

o Full bypassing: The raw DSL connection used for bypassing is not controlled by the HAG. It may or may not go through HAG.

o Partial bypassing: HAG controls the raw DSL connection used for bypassing. The raw DSL connection goes through the HAG.

For either type of bypassing, the HAG announces the service types that need to bypass the bonded GRE tunnels using the Filter List Package attribute as specified in Section 5.6.2. The HCPE and the HAG need to set aside the DSL bandwidth for bypassing. The available DSL bandwidth for GRE Tunnel Bonding is equal to the total DSL bandwidth minus the bypassing bandwidth.

4.6. Measurement

Since control packets are routed using the same paths as the data packets, the real performance of the data paths (e.g., the GRE tunnels) can be measured. The GRE Tunnel Hello messages specified in

Section 5.3 are used to carry the timestamp information and the Round Trip Time (RTT) value can therefore be calculated based on the timestamp.

Besides the end-to-end delay of the GRE tunnels, the HCPE and the HAG need also measure the capacity of the tunnels. For example, for full bypassing, the HCPE is REQUIRED to measure the downstream bypassing bandwidth in real time, and report it to the HAG (See Section 5.6.1.).

4.7. Policy Control Considerations

Operators and customers may input policies into the GRE Tunnel Bonding. These policies will be interpreted into parameters or actions that impact the traffic classification, distribution, combination, measurement and bypassing.

Operators and customers may offer the service types that need to bypass the bonded GRE tunnels. These service types will be delivered from the HAG to the HCPE, and the HCPE will use the raw DSL interface to transmit traffic for these service types.

Since the GRE tunnels are setup on top of heterogeneous DSL and LTE connections, if the difference of the transmission delays of these connections exceeds a given threshold for a certain period, the HCPE and the HAG should be able to stop the offloading behavior and fallback to a traditional transmission mode, where the LTE GRE tunnel is disabled while all traffic is transmitted over the DSL GRE tunnel. Operators are allowed to define this threshold and period.

Operators may determine the maximum allowed size (See MAX_PERFLOW_BUFFER in [RFC2890]) of the buffer for reordering. They may also define the maximum time (See OUTOFORDER_TIMER in [RFC2890]) that a packet can stay in the buffer for reordering. These parameters impact the traffic recombination.

Operators may specify the interval for sending Hello messages and the retry times for the HCPE or the HAG to send out Hello messages before the failure of a connection.

5. Control Protocol Specification (Control Plane)

Control messages are used to establish, maintain, measure and tear down GRE tunnels between the HCPE and the HAG. Also, the control plane undertakes the responsibility to bond tunnels and convey traffic policies.

For the purpose of measurement, control messages need to be delivered

as GRE encapsulated packets and co-routed with data plane packets. The new GRE Protocol Type (tbd1) is allocated for this purpose and the standard GRE header as per [RFC2890] is used. The format of the GRE header is 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|C| |K|S| Reserved0       | Ver |         Protocol Type         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Key (optional)                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

C (Bit 0)
   Checksum Present. Set to zero (0).

K (Bit 2)
   Key Present. Set to one (1).

S (Bit 3)
   Sequence Number Present. Set to zero (0).

Protocol Type (2 octets)
   Set to tbd1.

Key
   The Key field is used as a demultiplexer for the GRE tunnels at the HAG. This value of the Key is generated by the HAG and informed to the HCPE. (See Section 5.2.9.)

The general format of the entire control message is 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0| |1|0|   Reserved0     | Ver |     Protocol Type = tbd1      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Key (optional)                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|MsgType| Rsvd1 |                                               |
+-+-+-+-+-+-+-+-+           Attributes                          +
~                                                               ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

MsgType (4 bits)
   Message Type. The control message family contains the following 6 types of control messages:

```
                 Control Message Family          Type
                ==========================    =========
                 GRE Tunnel Setup Request        1
                 GRE Tunnel Setup Accept         2
                 GRE Tunnel Setup Deny           3
                 GRE Tunnel Hello                4
                 GRE Tunnel Tear Down            5
                 GRE Tunnel Notify               6
                 Reserved                        0,7-15
```

Rsvd1 (4 bits)
Reserved1. These bits MUST be set to zero.

Attributes
The Attributes field includes the attributes that need to be carried in the control message. Each Attribute has the following format.

```
   +-+-+-+-+-+-+-+-+
   |Attribute Type |                  (1 byte)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Attribute Length             |  (2 bytes)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Attribute Value              ~  (variable)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Attribute Type (1 octet)
The Attribute Type specifies the type of the attribute.

Attribute Length (2 octets)
Attribute Length indicates the length of the Attribute Value.

Attribute Value (variable)
The Attribute Value includes the value of the attribute.

All control messages are sent in network byte order (high order octets first). Since the Protocol Type carried in the GRE header for the control message is tbd1, the receiver will determine to consume it locally rather than further forwarding.

5.1. GRE Tunnel Setup Request

HCPE uses the GRE Tunnel Setup Request message to request that the HAG establish the GRE tunnels. It is sent out from HCPE's LTE and DSL WAN interfaces separately. Attributes that need to be included in this message are defined in the following subsections.

5.1.1. Client Identification Name

Operator uses the Client Identification Name (CIN) to identify the HCPE. The HCPE sends the CIN to the HAG for authentication and authorization as specified in [TS23.401]. It is REQUIRED that the GRE Tunnel Setup Request message sent out from the LTE WAN interface contains the CIN attribute while the GRE Tunnel Setup Request message sent out from the DSL WAN interface does not contain this attribute.

The CIN attribute has the following format:

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                   (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |   (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  Client Identification Name       (40 bytes)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+...+-+
```

Attribute Type
CIN, set to 3.

Attribute Length
Set to 40.

Client Identification Name
This is a 40-byte ANSI string value set by the operator. It is used as the identification of the HCPE in the operator's network.

5.1.2. Session ID

This Session ID is generated by the HAG when the LTE GRE Tunnel Setup Request message is received. The HAG announces the Session ID to the HCPE in the LTE GRE Tunnel Setup Accept message. For those WAN interfaces that need to be bonded together, the HCPE MUST use the same Session ID. The HCPE MUST carry the Session ID attribute in each DSL GRE Tunnel Setup Request message. For the first time that the LTE GRE Tunnel Setup Request message is sent to the HAG, the Session ID attribute need not be included. However, if the LTE GRE Tunnel fails and HCPE tries to revive it, the LTE GRE Tunnel Setup Request message MUST include the Session ID attribute.

The Session ID attribute has the following format:

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                   (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |   (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  Session ID                       (4 bytes)   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+...+-+
```

Attribute Type
Session ID, set to 4.

Attribute Length
Set to 4.

Session ID
This is a 4-byte ANSI string value generated by the HAG. It is used as the identification of bonded GRE Tunnels.

5.1.3. DSL Synchronization Rate

The HCPE uses the DSL Synchronization Rate to notify the HAG about the downstream bandwidth of the DSL link. The DSL GRE Tunnel Setup Request message MUST include the DSL Synchronization Rate attribute. The LTE GRE Tunnel Setup Request message SHOULD NOT include this attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                   (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |   (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  DSL Synchronization Rate         (4 bytes)   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+...+-+
```

Attribute Type
DSL Synchronization Rate, set to 7.

Attribute Length
Set to 4.

DSL Synchronization Rate
This is an unsigned integer measured in kbps.

5.2. GRE Tunnel Setup Accept

The HAG uses the GRE Tunnel Setup Accept message as the response to the GRE Tunnel Setup Request message. This message indicates acceptance of the tunnel establishment and carries parameters of the

GRE tunnels. Attributes that need be to included in this message are defined below.

5.2.1. H IPv4 Address

The HAG uses the H IPv4 Address attribute to inform the HCPE of the H IPv4 address. HCPE uses the H IPv4 address as the endpoint IPv4 address of the GRE tunnels. The LTE GRE Tunnel Setup Accept message MUST include the H IPv4 Address attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                   (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |   (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  H IPv4 Address                   (4 bytes)   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...+-+
```

Attribute Type
   H IPv4 Address, set to 1.

Attribute Length
   Set to 4.

H IPv4 Address
   Set to the pre-configured IPv4 address which is used as the endpoint IP address of GRE tunnels by the HAG.

5.2.2. H IPv6 Address

HAG uses the H IPv6 Address attribute to inform the HCPE of the H IPv6 address. The HCPE uses the H IPv6 address as the endpoint IPv6 address of the GRE tunnels. The LTE GRE Tunnel Setup Accept message MUST include the H IPv6 Address attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                   (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |   (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  H IPv6 Address                   (16 bytes)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...+-+
```

Attribute Type
   H IPv6 Address, set to 1.

Attribute Length
   Set to 16.

H IPv6 Address
Set to the pre-configured IPv6 address which is used as the endpoint IP address of GRE tunnels by HAG.

5.2.3. Session ID

The LTE GRE Tunnel Setup Accept message MUST include Session ID attribute as defined in Section 5.1.2.

5.2.4. RTT Difference Threshold

The HAG uses the RTT Difference Threshold attribute to inform the HCPE of the acceptable threshold of RTT difference between the DSL link and the LTE link. If the measured RTT difference exceeds this threshold, the HCPE SHOULD stop offloading traffic to the LTE GRE tunnel. The LTE GRE Tunnel Setup Accept message MUST include the RTT Difference Threshold attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                   (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |   (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  RTT Difference Threshold         (4 bytes)   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+...+-+
```

Attribute Type
RTT Difference Threshold, set to 9.

Attribute Length
Set to 4.

RTT Difference Threshold
An unsigned integer measured in milliseconds. This value can be chosen in the range 0 through 1000.

5.2.5. Bypass Bandwidth Check Interval

The HAG uses the Bypass Bandwidth Check Interval attribute to inform the HCPE of how frequently the bypass bandwidth should be checked. The HCPE should check the bypass bandwidth of the DSL WAN interface in each time period indicated by this interval. The LTE GRE Tunnel Setup Accept message MUST include the Bypass Bandwidth Check Interval attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                   (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |   (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  Bypass Bandwidth Check Interval  (4 bytes)   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+...+-+
```

Attribute Type
Bypass Bandwidth Check Interval, set to 10.

Attribute Length
Set to 4.

Bypass Bandwidth Check Interval
An unsigned integer measured in seconds. This value can be chosen in the range 0 through 300.

5.2.6. Active Hello Interval

The HAG uses the Active Hello Interval attribute to inform the HCPE of the pre-configured interval for sending out GRE Tunnel Hellos. The HCPE should send out GRE Tunnel Hellos via both the DSL and LTE WAN interfaces in each time period as indicated by this interval. The LTE GRE Tunnel Setup Accept message MUST include the Active Hello Interval attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                   (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |   (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  Active Hello Interval            (4 bytes)   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+...+-+
```

Attribute Type
Active Hello Interval, set to 14.

Attribute Length
Set to 4.

Active Hello Interval
An unsigned integer measured in seconds. This value can be chosen in the range 0 through 100.

5.2.7. Hello Retry Times

The HAG uses the Hello Retry Times attribute to inform the HCPE of

the retry times for sending GRE Tunnel Hellos. If the HCPE does not receive any acknowledgement from the HAG for the number of GRE Tunnel Hello attempts specified in this attribute, the HCPE will declare a failure of the GRE Tunnel. The LTE GRE Tunnel Setup Accept message MUST include the Hello Retry Times attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                   (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |   (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  Hello Retry Times                (4 bytes)    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+...+-+
```

Attribute Type
   Hello Retry Times, set to 15.

Attribute Length
   Set to 4.

Hello Retry Times
   An unsigned integer, which takes values in the range 3 through 10.

5.2.8. Idle Timeout

The HAG uses the Idle Timeout attribute to inform the HCPE of the pre-configured timeout value to terminate the DSL GRE tunnel. When an LTE GRE Tunnel failure is detected, all traffic will be sent over the DSL GRE tunnel. If the failure of the LTE GRE tunnel lasts longer than the Idle Timeout, subsequent traffic will be sent over raw DSL rather than over a tunnel, and the DSL GRE tunnel SHOULD be terminated. The LTE Tunnel Setup Accept message MUST include the Idle Timeout attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                   (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |   (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  Idle Timeout                     (4 bytes)    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+...+-+
```

Attribute Type
   Idle Timeout, set to 16.

Attribute Length
   Set to 4.

Idle Timeout
An unsigned integer measured in seconds. It takes values in the range 0 through 172,800 with the granularity of 60. The default value is 1,440 (24 hours). The value 0 indicates the idle timer never expires.

5.2.9. Bonding Key Value

The HAG uses the Bonding Key Value attribute to inform the HCPE of the number which is to be used as the Key of the GRE header for each tunneled control message. The Bonding Key Value is generated by the HAG and used for the purpose of demultiplexing. The HAG is REQUIRED to distinguish the GRE tunnels from the Bonding Key Value. Different tunnels MUST use different Bonding Key Values. The HAG SHOULD identify the GRE tunnels by their source IP addresses which are carried in the outer IP header. Since the CIN attribute is carried in the GRE Tunnel Setup Request sent on the LTE GRE tunnel only, the HAG can figure out the source IP address used for the LTE GRE tunnel from the message carrying the CIN attribute. Similarly, the HAG can figure out the source IP address used for the DSL GRE tunnel from the message carrying the DSL Synchronization Rate attribute.

The method used to generate this number is up to implementations. The Pseudo Random Number Generator defined in ANSI X9.31 Appendix A.2.4 is RECOMMENDED. Both the LTE GRE Tunnel Setup Accept message and the DSL GRE Tunnel Setup Accept message MUST include the Bonding Key Value attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                   (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |   (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  Bonding Key Value                (4 bytes)    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...+-+
```

Attribute Type
Bonding Key Value, set to 20.

Attribute Length
Set to 4.

Bonding Key Value
A 32-bit number generated by the HAG. It is REQUIRED that different tunnels are allocated different Key values. The HAG MAY set aside a few bits (e.g., the highest 4 bits) in the Key field as the demultiplexer for the tunnels while other bits are filled in with a value generated by a random number generator.

5.2.10. Configured DSL Upstream Bandwidth

The HAG obtains the upstream bandwidth of the DSL link from the management system and uses the Configured DSL Upstream Bandwidth attribute to inform the HCPE. The HCPE uses the received upstream bandwidth as the Committed Information Rate for the DSL link [RFC2698]. The DSL GRE Tunnel Setup Accept message MUST include the Configured DSL Upstream Bandwidth attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                   (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |   (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
| Configured DSL Upstream Bandwidth (4 bytes)   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+...+-+
```

Attribute Type
   Configured DSL Upstream Bandwidth, set to 22.

Attribute Length
   Set to 4.

Configured DSL Upstream Bandwidth
   An unsigned integer measured in kbps.

5.2.11. Configured DSL Downstream Bandwidth

The HAG obtains the downstream bandwidth of the DSL link from the management system and uses the Configured DSL Downstream Bandwidth attribute to inform the HCPE. The HCPE uses the received downstream bandwidth as the base in calculating the bypassing bandwidth. The DSL GRE Tunnel Setup Accept message MUST include the Configured DSL Downstream Bandwidth attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                   (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |   (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|Configured DSL Downstream Bandwidth(4 bytes)   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+...+-+
```

Attribute Type
   Configured DSL Downstream Bandwidth, set to 23.

Attribute Length
   Set to 4.

Configured DSL Downstream Bandwidth
An unsigned integer measured in kbps.

5.2.12. RTT Difference Threshold Violation

The HAG uses the RTT Difference Threshold Violation attribute to inform the HCPE of the number of times in a row that the RTT Difference Threshold (See Section 5.2.4.) may be violated before the HCPE MUST stop using the LTE GRE Tunnel. If the RTT Difference Threshold is continuously violated for more than the indicated number of measurements, the HCPE MUST stop using the LTE GRE tunnel. The LTE GRE Tunnel Setup Accept message MUST include the RTT Difference Threshold Violation attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                   (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |   (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  RTT Diff Threshold Violation     (4 bytes)    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...+-+
```

Attribute Type
RTT Difference Threshold Violation, set to 24.

Attribute Length
Set to 4.

RTT Difference Threshold Violation
An unsigned integer which takes values in the range 1 through 25. A typical value is 3.

5.2.13. RTT Difference Threshold Compliance

The HAG uses the RTT Difference Threshold Compliance attribute to inform the HCPE of the number of times in a row the RTT Difference Threshold (See Section 5.2.4.) must be compliant before use of the LTE GRE tunnel can be resumed. If the RTT Difference Threshold is continuously detected to be compliant across more than this number of measurments, the HCPE MAY resume using the LTE GRE tunnel. The LTE GRE Tunnel Setup Accept message MUST include the RTT Difference Threshold Compliance attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                   (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |   (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  RTT Diff Threshold Compliance    (4 bytes)   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+...+-+
```

Attribute Type
RTT Diff Threshold Compliance, set to 25.

Attribute Length
Set to 4.

RTT Diff Threshold Compliance
An unsigned integer which takes values in the range 1 through 25.
A typical value is 3.

5.2.14. Idle Hello Interval

The HAG uses the Idle Hello Interval attribute to inform the HCPE of the pre-configured interval for sending out GRE Tunnel Hellos when the subscriber is detected to be idle. The HCPE SHOULD begin to send out GRE Tunnel Hellos via both the DSL and LTE WAN interfaces in each time period as indicated by this interval, if the bonding tunnels have seen no traffic longer than the "No Traffic Monitored Interval" (See Section 5.2.15.). The LTE GRE Tunnel Setup Accept message MUST include the Idle Hello Interval attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                    (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |    (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  Idle Hello Interval               (4 bytes)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+...+-+
```

Attribute Type
Idle Hello Interval, set to 31.

Attribute Length
Set to 4.

Idle Hello Interval
An unsigned integer measured in seconds. This value can be chosen from the range 100 through 86,400 (24 hours) with the granularity of 100. The default value is 1800 (30 minutes).

5.2.15. No Traffic Monitored Interval

The HAG uses the No Traffic Monitored Interval attribute to inform the HCPE of the pre-configured interval for switching the GRE Tunnel Hello mode. If traffic is detected on the bonding GRE tunnels before this informed interval expires, the HCPE SHOULD switch to the Active Hello Interval. The LTE GRE Tunnel Setup Accept message MUST include the No Traffic Monitored Interval attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                    (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |    (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  No Traffic Monitored Interval      (4 bytes)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...+-+
```

Attribute Type
   No Traffic Monitored Interval, set to 32.

Attribute Length
   Set to 4.

No Traffic Monitored Interval
   An unsigned integer measured in seconds. This value is in the range 30 through 86,400 (24 hours). The default value is 60.

5.3. GRE Tunnel Setup Deny

HAG MUST sends the GRE Tunnel Setup Deny message to HCPE if the GRE tunnel setup request from this HCPE is denied. The HCPE MUST terminate the GRE tunnel setup process as soon as it receives the GRE Tunnel Setup Deny message.

5.3.1. Error Code

The HAG uses the Error Code attribute to inform the HCPE of the error code. The error code depicts the reason why the GRE tunnel setup request is denied. Both the LTE GRE Tunnel Setup Deny message and the DSL GRE Tunnel Setup Deny message MUST include the Error Code attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                    (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |    (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  Error Code                        (4 bytes)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+...+-+
```

Attribute Type
Error Code, set to 17.

Attribute Length
Set to 4.

Error Code
An unsigned integer. The list of the codes are listed as follows.

1: The HAG was not reachable over LTE during the GRE tunnel setup request.
2: The HAG was not reachable via DSL during the GRE tunnel setup request.
3: The LTE GRE tunnel to the HAG failed.
4: The DSL GRE tunnel to the HAG failed.
5: The given DSL User ID is not allowed to use the GRE tunnel bonding service.
6: The given User Alias (TOID)/User ID (GUID) is not allowed to use the GRE tunnel bonding service.
7: The LTE and DSL User IDs do not match.
8: The HAG denied the GRE tunnel setup request because a bonding session with the same User ID already exists.
9: The HAG denied the GRE tunnel setup request because the user's CIN is not permitted.
10: The HAG terminated a GRE tunnel bonding session for maintenance reasons.
11: There was a communication error between the HAG and the management system during the LTE tunnel setup request.
12: There was a communication error between the HAG and management system during the DSL tunnel setup request.

5.4. GRE Tunnel Hello

After the GRE tunnel is established, the HCPE begins to periodically send out GRE Tunnel Hello messages, which the HAG acknowledges by returning GRE Tunnel Hello messages back to the HCPE. This continues until the tunnel is terminated.

5.4.1. Timestamp

The HAG uses the Timestamp attribute to inform the HCPE of the timestamp value that is used for RTT calculation. Both the LTE GRE Tunnel Hello message and DSL GRE Tunnel Hello message MUST include the Timestamp attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                    (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |    (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  Timestamp                         (8 bytes)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+...+-+
```

Attribute Type
   Timestamp, set to 5.

Attribute Length
   Set to 8.

Timestamp
   The high-order 4 octets indicate an unsigned integer in units of one second; the low-order 4 octets indicate an unsigned integer in unit of one millisecond.

5.4.2. IPv6 Prefix Assigned by HAG

The HAG uses the IPv6 Prefix Assigned by the HAG attribute to inform the HCPE of the assigned IPv6 prefix. This IPv6 prefix is to be captured by the Lawful Interception. Both the LTE GRE Tunnel Hello message and the DSL GRE Tunnel Hello message MUST include the IPv6 Prefix Assigned by HAG attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                    (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |    (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  IPv6 Prefix Assigned by HAG       (16 bytes)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+...+-+
```

Attribute Type
   IPv6 Prefix Assigned by HAG, set to 13.

Attribute Length
   Set to 17.

IPv6 Prefix Assigned by HAG
   The highest-order 16 octets encode an IPv6 address. The lowest-

order one octet encodes the prefix length. These two values are put together to represent an IPv6 prefix.

5.5. GRE Tunnel Tear Down

The HAG can terminate a GRE tunnel by sending the GRE Tunnel Tear Down message to the HCPE. The Error Code attribute as defined in Section 5.3.1 MUST be included in this message.

5.6. GRE Tunnel Notify

The HCPE and the HAG use the GRE Tunnel Notify message to notify each other about their status, the information for the bonding tunnels, the actions that need to be taken, etc.

Usually, the receiver just sends the received attributes back as the acknowledgement for each GRE Tunnel Notify message. There is an exception for the Filter List Package. Since the size of the Filter List Package attribute can be very large, a special attribute is specified in Section 5.6.12 as the acknowledgement.

Attributes that need be to included in the GRE Tunnel Notify message are defined below.

5.6.1. Bypass Traffic Rate

There are a few types of traffic that need to transmitted over the raw DSL WAN interface rather than the bonding GRE tunnels. The HCPE has to set aside bypass bandwidth on the DSL WAN interface for these traffic types. Therefore, the available bandwidth of the DSL GRE tunnel is the entire DSL WAN interface bandwidth minus the occupied bypass bandwidth.

The HCPE uses the Bypass Traffic Rate attribute to inform the HAG of the downstream bypass bandwidth for the DSL WAN interface. The Bypass Traffic Rate attribute will be included in the DSL GRE Tunnel Notify message. The HAG calculates the available downstream bandwidth for the DSL GRE tunnel as the Configured DSL Downstream Bandwidth minus this informed bypass bandwidth. The available DSL bandwidth will be used as the Committed Information Rate (CIR) of the coloring system [RFC2698].

```
+-+-+-+-+-+-+-+-+-+
|Attribute Type |                    (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |    (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  Bypass Traffic Rate               (4 bytes)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...+-+
```

Attribute Type
   Bypass Traffic Rate, set to 6.

Attribute Length
   Set to 4.

Bypass Traffic Rate
   An unsigned integer measured in kbps.

5.6.2. Filter List Package

The HAG uses the Filter List Package attribute to inform the HCPE of the service types that need to bypass the bonding GRE tunnels. Each Filter List Package carries a collection of Filter List TLVs and each such Filter List TLV specifies a filter item. At the HCPE, a list of filter items is maintained. Also, the HCPE needs to maintain an exception list of filter items. For example, the packets carrying the control messages defined in this document should be excluded from the filter list.

Incoming packets that match a filter item in the filter list while not matching any item in the exception list MUST be transmitted over the raw DSL rather than the bonding GRE tunnels. Both the LTE GRE Tunnel Notify message and GRE Tunnel Notify message MAY include the Filter List Package attribute. The DSL GRE Tunnel Notify message is preferred.

```
+-+-+-+-+-+-+-+-+-+
|Attribute Type |                    (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |    (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  Filter List TLVs                  (variable) ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...+-+
```

Attribute Type
   Filter List Package, set to 8.

Attribute Length
   The total length of the Filter List TLVs. The maximum length is

969 bytes.

Filter List TLVs

Each Filter List TLV has the following format.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Commit_Count                                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Packet_Sum               |         Packet_ID             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Type                  |          Length               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Enable                |     Description Length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                 Description Value (0~4 bytes)                 ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                        Value (0~32 bytes)                     ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Commit_Count

An unsigned integer which identifies the version of the Filter List Package. HCPE will refresh its filter list when a new Commit_Count is received.

Packet_Sum

If the Filter List Package attribute might make the control message larger than the MTU, fragmentation is used. The Packet_Sum indicates the total number of Filter List Packages.

Packet_ID

The fragmentation index of this Filter List Package.

Type

The Type of the Filter List TLV. Currently used types are described as follows.

Filter List TLVs	Type
FQDN [RFC1594]	1
DSCP [RFC2724]	2
Destination Port	3
Destination IP	4
Destination IP&Port	5
Source Port	6
Source IP	7
Source IP&Port	8

Source Mac	9
Protocol	10
Source IP Range	11
Destination IP Range	12
Source IP Range&Port	13
Destination IP Range&Port	14
Reserved	

Length
The length of the Filter List TLV. Commit_Count, Packet Sum, Packet ID, Type and Length are excluded.

Enable
Whether the filter item defined in this Filter List TLV is enabled. One means enabled and zero means disabled. Other possible values are reserved.

Description Length
The length of the Description Value.

Description Value
A variable ASCII string that describes the Filter List TLV (e.g., "FQDN").

Value
A variable ASCII string that specifies the value of the Filter List TLV (e.g. "www.yahoo.com"). As an example, Type = 1 and Value = "www.yahoo.com" means that packets whose FQDN field equals "www.yahoo.com" match the filter item.

The lengths of the auxiliary Description Value and Value fields are restricted to a maximum of 4 bytes and 32 bytes respectively, which aims to limit the size of the Filter List TLV sent on the GRE tunnel.

5.6.3. Switching to DSL Tunnel

If the RTT difference is continuously detected to violate the RTT Difference Threshold (See Section 5.2.4.) more than the times specified in the RTT Difference Threshold Violation (See Section 5.2.12.), the HCPE uses the Switching to DSL Tunnel attribute to inform the HAG to use the DSL GRE tunnel only. When the HAG receives this attribute, it MUST begin to transmit downstream traffic to this HCPE solely over the DSL GRE tunnel. The DSL GRE Tunnel Notify message MAY include the Switching to DSL Tunnel attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                    (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length              |    (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Attribute Type
   Switching to DSL Tunnel, set to 11.

Attribute Length
   Set to 0.

5.6.4. Overflowing to LTE Tunnel

If the RTT difference is continuously detected to not violated the RTT Difference Threshold attribute (See Section 5.2.4.) more than the number of times specified in the RTT Difference Compliance attribute (See Section 5.2.13), the HCPE uses the Overflowing to LTE Tunnel attribute to inform HAG that LTE GRE tunnel can be used again. The DSL GRE Tunnel Notify message MAY include the Overflowing to LTE Tunnel attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                    (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length              |    (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Attribute Type
   Overflowing to LTE Tunnel, set to 12.

Attribute Length
   Set to 0.

5.6.5. DSL Link Failure

When the HCPE detects the DSL WAN interface status is down, it MUST tear down the DSL GRE tunnel. It informs HAG about the failure using the DSL Link Failure attribute. The HAG MUST tear down the DSL GRE tunnel upon the DSL Link Failure attribute is received. The DSL Link Failure attribute SHOULD be carried in the LTE GRE Tunnel Notify message.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                    (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length              |    (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Attribute Type
DSL Link Failure, set to 18.

Attribute Length
Set to 0.

5.6.6. LTE Link Failure

When the HCPE detects the LTE WAN interface status is down, it MUST tear down the LTE GRE tunnel. It informs the HAG about the failure using the LTE Link Failure attribute. HAG MUST tear down the LTE GRE tunnel upon the LTE Link Failure attribute is received. The LTE Link Failure attribute SHOULD be carried in the DSL GRE Tunnel Notify message.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                    (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |    (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Attribute Type
LTE Link Failure, set to 19.

Attribute Length
Set to 0.

5.6.7. IPv6 Prefix Assigned to Host

If the HCPE changes the IPv6 prefix assigned to the host, it uses the IPv6 Prefix Assigned to Host attribute to inform the HAG. Both the LTE GRE Tunnel Notify message and the DSL GRE Tunnel Notify message MAY include the IPv6 Prefix Assigned to Host attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                    (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |    (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  IPv6 Prefix Assigned to Host      (16 bytes) |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...+-+
```

Attribute Type
IPv6 Prefix Assigned to Host, set to 21.

Attribute Length
Set to 17.

IPv6 Prefix Assigned to Host
The highest-order 16 octets encode an IPv6 address. The lowest-order one octet encodes the prefix length. These two values are put together to represent an IPv6 prefix.

5.6.8. Diagnostic Start: Bonding Tunnel

The HCPE uses the Diagnostic Start: Bonding Tunnel attribute to inform the HAG to switch to diagnostic mode to test the performance of the entire bonding tunnel. The Diagnostic Start: Bonding Tunnel attribute SHOULD be carried in the DSL GRE Tunnel Notify message.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                    (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length               |    (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Attribute Type
Diagnostic Start: Bonding Tunnel, set to 26.

Attribute Length
Set to 0.

5.6.9. Diagnostic Start: DSL Tunnel

The HCPE uses the Diagnostic Start: DSL Tunnel attribute to inform the HAG to switch to diagnostic mode to test the performance of the DSL GRE tunnel. The Diagnostic Start: DSL Tunnel attribute SHOULD be carried in the DSL GRE Tunnel Notify message.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                    (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length               |    (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Attribute Type
Diagnostic Start: DSL Tunnel, set to 27.

Attribute Length
Set to 0.

5.6.10. Diagnostic Start: LTE Tunnel

The HCPE uses the Diagnostic Start: LTE Tunnel attribute to inform the HAG to switch to diagnostic mode to test the performance of the entire bonding tunnel. The Diagnostic Start: LTE Tunnel attribute

SHOULD be carried in the DSL GRE Tunnel Notify message.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                    (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length              |    (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Attribute Type
   Diagnostic Start: LTE Tunnel, set to 18.

Attribute Length
   Set to 0.

5.6.11. Diagnostic End

The HCPE uses the Diagnostic End attribute to inform th HAG to stop operating in diagnostic mode. The Diagnostic End attribute SHOULD be carried in the DSL GRE Tunnel Notify message.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                    (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length              |    (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Attribute Type
   Diagnostic End, set to 29.

Attribute Length
   Set to 0.

5.6.12. Filter List Package ACK

The HCPE uses the Filter List Package ACK attribute to acknowledge the Filter List Package sent by the HAG. Both the LTE GRE Tunnel Notify message and the DSL GRE Tunnel Notify message MAY include the Filter List Package ACK attribute.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                    (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length              |    (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...-+
|  Filter List Package ACK           (5 bytes)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+...+-+
```

Attribute Type

      Filter List Package ACK, set to 30.

   Attribute Length
      Set to 5.

   Filter List Package ACK
      The highest-order 4 octets are the Commit_Count as defined in Section 5.6.2. The lowest-order 1 octet encodes the following error codes:

      0: The Filter List Package is acknowledged.
      1: The Filter List Package is not acknowledged. The HCPE is a new subscriber and has not ever received a Filter List Package. In this case, the HAG SHOULD tear down the bonding tunnels and force the HCPE to re-establish the GRE Tunnels.
      2: The Filter List Package is not acknowledged. The HCPE has already got a valid Filter List Package. The filter list on the HCPE will continue to be used while HAG need do nothing.

5.6.13. Switching to Active Hello State

If traffic is being sent/received over the bonding GRE tunnels before the "No Traffic Monitored Interval" expires (See Section 5.2.15.), the HCPE sends to the HAG a GRE Tunnel Notify message containing the Switching to Active Hello State attribute.

The HAG will switch to active hello state and send the HCPE a GRE Tunnel Notify message carrying the Switching to Active Hello State attribute as the ACK.

When the HCPE receives the ACK, it will switch to active hello state, start RTT detection and start sending GRE Tunnel Hello messages with the Active Hello Interval (See Section 5.2.6.).

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                    (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |    (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   Attribute Type
      Switching to Active Hello State, set to 33.

   Attribute Length
      Set to 0.

5.6.14. Switching to Idle Hello State

The HCPE initiates switching to idle hello state when the bonding of GRE Tunnels is successfully established and the LTE GRE Tunnel Setup Accept message carrying the Idle Hello Interval attribute (See Section 5.2.14.) is received. The HCPE sends the HAG a GRE Tunnel Notify message containing the Switching to Idle Hello State attribute.

The HAG will switch to idle hello state, clear RTT state and send the HCPE a GRE Tunnel Notify message carrying the Switching to Idle Hello State attribute as the ACK.

When the HCPE receives the ACK, it will switch to idle hello state, stop RTT detection, clear RTT state as well and start sending GRE Tunnel Hello messages with the Idle Hello Interval (See Section 5.2.14).

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                    (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |    (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Attribute Type
   Switching to Idle Hello State, set to 34.

Attribute Length
   Set to 0.

5.6.15. Tunnel Verification

The HAG uses the Tunnel Verification attribute to inform the HCPE to verify whether an existing LTE GRE tunnel is still functioning. The Tunnel Verification attribute SHOULD be carried in the LTE GRE Tunnel Notify message. It provides a means to detect the tunnel faster than the GRE Tunnel Hello, especially when the LTE GRE tunnel is in the Idle Hello state and it takes much longer time to detect this tunnel.

When the HAG receives an LTE GRE Tunnel Setup Request and finds the requested tunnel is conflicting with an existing tunnel, the HAG initiates the Tunnel Verification. The HAG drops all conflicting LTE GRE Tunnel Setup Request messages and sends GRE Tunnel Notify messages carrying the Tunnel Verification attribute until the verification ends. The HCPE MUST respond to the HAG with the same Tunnel Verification attribute as the ACK if the tunnel is still functioning.

If the ACK of the Tunnel Verification attribute is received from the

HCPE, the HAG judges that the existing tunnel is still functioning. An LTE GRE Tunnel Deny message (with Error Code = 8) will be sent to the HCPE. The HCPE SHOULD terminate the GRE tunnel setup request process immediately.

If the HAG does not receive a Tunnel Verification ACK message after 3 attempts (1 initial attempt and 2 retries), it will regard the existing tunnel as failed and the LTE GRE Tunnel Setup Request will be accepted.

```
+-+-+-+-+-+-+-+-+
|Attribute Type |                   (1 byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute Length             |    (2 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Attribute Type
   Tunnel Verification, set to 35.

Attribute Length
   Set to 0.

6. Tunnel Protocol Operation (Data Plane)

GRE tunnels are set up over heterogeneous connections, such as LTE and DSL, between the HCPE and the HAG. Users' IP (inner) packets are encapsulated in GRE packets which in turn are carried over IP (outer). The general structure of the packets is shown as below.

```
+---------------------------------+
|          Media Header           |
+---------------------------------+
|         Outer IP Header         |
+---------------------------------+
|           GRE Header            |
+---------------------------------+
|         Inner IP Packet         |
+---------------------------------+
```

6.1. The GRE Header

The GRE header is first standardized in [RFC2874]. [RFC2890] adds the optional key and sequence number fields which makes the whole GRE header have the following format.

```
     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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |C| |K|S| Reserved0       | Ver |         Protocol Type         |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |      Checksum (optional)      |       Reserved1 (Optional)    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                         Key (optional)                        |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                 Sequence Number (optional)                    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 6.1 The GRE header

The Checksum is not used in the GRE Tunnel Bonding, therefore the C bit is set to zero.

The Key bit is set to one so that the Key field is present. For per-packet traffic distribution, the Key field is used as a 32-bit random number. It is generated by the HAG and notified to HCPE. Different from the Key field used in control packets, each bonding of GRE tunnels gets a single Key value. HCPE MUST carry this number in each GRE header.

The S bit is set to one, and the Sequence Number field is present and used for in-order delivery as per [RFC2890].

6.2. Automatic Setup of GRE Tunnels

The HCPE gets the DSL WAN interface IP address (D) from the Broadband Remote Access Server (BRAS) via Point-to-Point Protocol over Ethernet (PPPoE), and gets the LTE WAN interface IP address (E) through Packet Data Protocol (PDP) from the Packet Data Network Gateway (PGW). The Domain Name System (DNS) resolution of the HAG's domain name is requested via the DSL/LTE WAN interface. The DNS server will reply with the corresponding HAG IP address (H) which MAY be pre-configured by the operator.

After the interface IP addresses have been acquired, the HCPE starts the following GRE Tunnel Bonding procedure. It is REQUIRED that the HCPE first set up the LTE GRE tunnel and then set up the DSL GRE tunnel.

The HCPE sends the GRE Tunnel Setup Request message to the HAG via the LTE WAN interface. The HAG, which receives the GRE Tunnel Setup Request message, will initiate the Authentication and Authorization procedure, as specified in [TS23.401], to check whether the HCPE is trusted by the PGW.

If the Authentication and Authorization succeed, the HAG will reply to the HCPE's LTE WAN interface with the GRE Tunnel Setup Accept message in which a Session ID randomly generated by the HAG is carried. Otherwise, the HAG MUST send to the HCPE's LTE WAN interface the GRE Tunnel Setup Deny message and the HCPE MUST terminate the tunnel set up process once it receives the GRE Tunnel Setup Deny message.

After the LTE GRE tunnel is successfully set up, the HCPE will obtain the C address over the tunnel from the HAG through Dynamic Host Configuration Protocol (DHCP). After that, the HCPE starts to set up the DSL GRE tunnel. It sends a GRE Tunnel Setup Request message with the HAG's address as the destination IP of GRE Tunnel via the DSL WAN interface, carrying the aforementioned session ID received from the HAG. The HAG, which receives the GRE Tunnel Setup Request message, will initiate the Authentication and Authorization procedure in order to check whether the HCPE is trusted by the BRAS.

If the Authentication and Authorization succeed, the HAG will reply to the HCPE's DSL WAN interface with the GRE Tunnel Setup Accept message. In this way, the two tunnels with the same Session ID can be used to carry traffic from the same user. That is to say, the two tunnels are "bonded" together. Otherwise, if the Authentication and Authorization fail, the HAG MUST send to the HCPE's DSL WAN interface the GRE Tunnel Setup Deny message. Meanwhile, it MUST send to the HCPE's LTE WAN interface the GRE Tunnel Tear Down message. The HCPE MUST terminate the tunnel set up process once it receives the GRE Tunnel Setup Deny message and MUST tear down the LTE GRE tunnel that has been set up once it receives the GRE Tunnel Tear Down Message.

7. Security Considerations

Malicious devices controlled by attackers may intercept the control messages sent on the GRE tunnels. Later on, the rogue devices may fake control messages to disrupt the GRE tunnels or attract traffic of the target HCPE.

As a security feature, the Key field of the GRE header of the control messages and the data packets for the per-packet traffic distribution could be generated as a 32-bit clear-text password.

Moreover, GRE over IP Security (IPSec) could be used to enhance the security.

8. IANA Considerations

The application for an EtherType for the new GRE Protocol Type (tbd1) has been processed by the IEEE Registration Authority.

No IANA action is required in this document. RFC Editor: please remove this section before publication.

9. Contributors

Li Xue Individual

Email: xueli_jas@163.com

10. References

10.1. Normative References

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

[RFC2698] Heinanen, J. and R. Guerin, "A Two Rate Three Color Marker", RFC 2698, September 1999.

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

[TS23.401] "3GPP TS23.401, General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", September 2013.

10.2. Informative References

[WT-348] Broadband Forum Work on "Hybrid Access for Broadband Networks" (WT-348), October 21, 2014, <http://datatracker.ietf.org/liaison/1355/>.

[RFC1594] Marine, A., Reynolds, J., and G. Malkin, "FYI on Questions and Answers - Answers to Commonly asked "New Internet User" Questions", RFC 1594, March 1994.

[RFC2724] Handelman, S., Stibler, S., Brownlee, N., and G. Ruth, "RTFM: New Attributes for Traffic Flow Measurement", RFC 2724, October 1999.

[RFC6320] Wadhwa, S., Moisand, J., Haag, T., Voigt, N., and T. Taylor, Ed., "Protocol for Access Node Control Mechanism in Broadband Networks", RFC 6320, October 2011.

[RFC6733] Fajardo, V., Ed., Arkko, J., Loughney, J., and G. Zorn, Ed., "Diameter Base Protocol", RFC 6733, October 2012.

Author's Addresses

Nicolai Leymann
Deutsche Telekom AG
Winterfeldtstrasse 21-27
Berlin 10781
Germany

Phone: +49-170-2275345
Email: n.leymann@telekom.de

Cornelius Heidemann
Deutsche Telekom AG
Heinrich-Hertz-Strasse 3-7
Darmstadt 64295
Germany

Phone: +4961515812721
Email: heidemannc@telekom.de

Mingui Zhang
Huawei Technologies
No.156 Beiqing Rd. Haidian District,
Beijing 100095 P.R. China

EMail: zhangmingui@huawei.com

Behcet Sarikaya
Huawei USA
5340 Legacy Dr. Building 3
Plano, TX 75024

EMail: sarikaya@ieee.org

Margaret Cullen
Painless Security
14 Summer St. Suite 202
Malden, MA 02148 USA

EMail: margaret@painless-security.com