Independent Submission
Request for Comments: 8157
Category: Informational
ISSN: 2070-1721

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

May 2017

Huawei's GRE Tunnel Bonding Protocol

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 bonded access to heterogeneous connections at the same time.

In this document, GRE (Generic Routing Encapsulation) Tunnel Bonding is specified as an enabling approach for bonded 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 subconnection, the bonded connections promise increased access capacity and improved reliability. The solution described in this document is currently implemented by Huawei and deployed by Deutsche Telekom AG. This document will enable other developers to build interoperable implementations.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Service Providers used to provide subscribers with separate access to their fixed networks and mobile networks. It has become desirable to bond these heterogeneous networks together to offer access service to subscribers; this service will provide increased access capacity and improved reliability.

This document focuses on the use case where a DSL (Digital Subscriber Line) connection and an LTE (Long Term Evolution) connection are bonded together. When the traffic volume exceeds the bandwidth of the DSL connection, the excess amount can be offloaded to the LTE connection. A Home Gateway (HG) is a Customer Premises Equipment (CPE) device initiating the DSL and LTE connections. A Hybrid Access Aggregation Point (HAAP) is the network function that resides in the provider’s networks to terminate these bonded connections. Note that if there were more than two connections that need to be bonded, the GRE Tunnel Bonding mechanism could support that scenario as well. However, support for more than two connections is out of scope for this document. Also, the protocol specified in this document is limited to the single-operator scenario only, i.e., the two peering boxes -- the HG and the HAAP -- are operated by a single provider. The adaptation of the GRE Tunnel Bonding Protocol to the multi-provider scenario is left for future work.

This document bases the solution on GRE (Generic Routing Encapsulation [RFC2784] [RFC2890]), since GRE is widely supported in both fixed and mobile networks. Approaches specified in this document might also be used by other tunneling technologies to achieve tunnel bonding. However, such variants are out of scope for this document.

For each heterogeneous connection (DSL and LTE) between the HG and the HAAP, one GRE tunnel is set up. The HG and the HAAP, respectively, serve as the common termination point of the two tunnels at both ends. Those GRE tunnels are further bonded together to form a logical GRE tunnel for the subscriber. The HG conceals the 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).

The GRE Tunnel Bonding Protocol is developed by Huawei and has been deployed in networks operated by Deutsche Telekom AG. This document makes this protocol available to the public, thereby enabling other developers to build interoperable implementations.

2. Acronyms and Terminology

GRE: Generic Routing Encapsulation [RFC2784] [RFC2890].

DSL: Digital Subscriber Line. A family of technologies 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.

HG: Home Gateway. A CPE device that is enhanced to support the simultaneous use of both fixed broadband and 3GPP access connections.

HAAP: Hybrid Access Aggregation Point. A logical function in an operator’s network, terminating bonded connections while offering high-speed Internet.

CIR: Committed Information Rate [RFC2697].

RTT: Round-Trip Time.

AAA: Authentication, Authorization, and Accounting [RFC6733].

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

FQDN: Fully Qualified Domain Name. Generally, a host name with at least one domain label under the top-level domain. For example, "dhcp.example.org" is an FQDN [RFC7031].

DSCP: The 6-bit codepoint (DSCP) of the Differentiated Services field (DS field) in the IPv4 and IPv6 headers [RFC2724].

BRAS: Broadband Remote Access Server. Routes traffic to and from broadband remote access devices such as Digital Subscriber Line Access Multiplexers (DSLAMs) on an Internet Service Provider’s (ISP’s) network.

PGW: Packet Data Network Gateway. In the Long Term Evolution (LTE) architecture for the Evolved Packet Core (EPC), 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 over Ethernet. A network protocol for encapsulating PPP frames inside Ethernet frames.

DNS: Domain Name System. 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
                  +-+ ****************************
                  | | *+-+                    +-+*
                  | | *|E+-- LTE Connection --+ |*
       subscriber |C| *+-+                    |H|*  Internet
                  | | *+-+                    | |*
                  | | *|D+-- DSL Connection --+ |*
                  | | *+-+                    +-+*
                  +-+ ****************************
                  \______/                    \__/
                     HG                       HAAP
```

C: The service endpoint of the bonding service at the HG.
E: The endpoint of the LTE connection resides in the HG.
D: The endpoint of the DSL connection resides in the HG.
H: The endpoint for each heterogeneous connection at the HAAP.

Figure 1: Offloading from DSL to LTE, Increased Access Capacity

If a Service Provider runs heterogeneous networks, such as fixed and mobile, subscribers might be eager to use those networks simultaneously for increased access capacity rather than just using a single network. As shown by the reference model in Figure 1, the subscriber expects a significantly higher access bandwidth from the bonding connection than from the DSL connection. In other words, when the traffic volume exceeds the bandwidth of the DSL connection, the excess amount may be offloaded to the LTE connection.

Compared to per-flow load-balancing mechanisms, which are widely used nowadays, the use case described in this document requires a per-packet offloading approach. For per-flow load balancing, the maximum bandwidth that may be used by a traffic flow is the bandwidth of an individual connection, while for per-packet offloading, a single flow may use the combined bandwidth of the two connections.

4. Overview

In this document, the widely supported GRE is chosen as the tunneling technique. With the newly defined control protocol, GRE tunnels are set up on top of the DSL and LTE connections, which are ended at D and H or at E and H, as shown in Figure 1. These tunnels are bonded together to form a single logical bonding connection between the HG and the HAAP. Subscribers use this logical connection without knowing the GRE tunnels.

4.1. Control Plane

A clean-slate control protocol is designed to manage the GRE tunnels that are set up per heterogeneous connection between the HG and the HAAP. The goal is to design a compact control plane for bonding access 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. As shown in Figure 2 (see Section 5), the GRE header [RFC2784] with the Key extension specified by [RFC2890] is being used. The GRE Protocol Type (0xB7EA) is used to identify this GRE Channel. A family of control messages is encapsulated with a GRE header and carried over this channel. Attributes, formatted in Type-Length-Value (TLV) style, are further defined and included in each control message.

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

4.2. Data Plane

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

As shown in Figure 3 (see Section 6.1), the GRE header [RFC2784] with the Key and Sequence Number extensions specified by [RFC2890] is used to encapsulate data packets. The Protocol Type is either 0x0800 (listed as "0x800" in [RFC2784]) or 0x86DD [RFC7676], which indicates that the inner packet is either an IPv4 packet or an IPv6 packet, respectively. The GRE Key field is set to a unique value for the entire bonding connection. The GRE Sequence Number field is used to maintain the sequence of packets transported in all GRE tunnels as a single flow between the HG and the HAAP.

4.3. Traffic Classification and Distribution

For the offloading use case, the coloring mechanism specified in [RFC2697] is being used to classify subscribers' IP packets, both upstream and downstream, into the DSL GRE tunnel or the LTE GRE tunnel. Packets colored as green or yellow will be distributed into the DSL GRE tunnel, and packets colored as red 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 scenario is out of scope for this document.

The Committed Information Rate (CIR) of the coloring mechanism is set to the total DSL WAN bandwidth minus the bypass DSL bandwidth (see Section 4.5). The total DSL WAN bandwidth MAY be configured, MAY be obtained from the management system (AAA server, SOAP server, etc.), or MAY be detected in real time using the Access Node Control Protocol (ANCP) [RFC6320].

4.4. Traffic Recombination

For the offloading use case, the recombination function at the receiver provides in-order delivery of subscribers' traffic. The receiver maintains a small reordering buffer and orders the data packets in this buffer via the Sequence Number field [RFC2890] of the GRE header. All packets carried on GRE tunnels that belong to the same bonding connection go into a single reordering buffer.

Operators may configure the maximum allowed size (see MAX_PERFLOW_BUFFER in [RFC2890]) of the buffer for reordering. They may also configure the maximum time (see OUTOFORDER_TIMER in [RFC2890]) that a packet can stay in the buffer for reordering. The OUTOFORDER_TIMER must be configured carefully. Values larger than the difference of the normal Round-Trip Time (RTT) (e.g., 100 ms) of the two connections are not recommended. Implementation and deployment experiences have demonstrated that there is usually a large margin for the value of MAX_PERFLOW_BUFFER. Values larger than the multiplication of the sum of the line rate of the two connections and the value of OUTOFORDER_TIMER should be used.

4.5. Bypass

Service Providers provide some services that should not be delivered over the bonding connection. For example, Service Providers may not expect real-time IPTV to be carried by the LTE GRE tunnel. It is required that IPTV traffic bypass the GRE Tunnel Bonding and use the raw DSL bandwidth. Bypass traffic is not subject to the traffic classification and distribution specified above. The raw connection used for bypass traffic is not controlled by the HAAP. It may or may not go through a device in which the HAAP resides.

The HAAP may announce the service types that need to bypass the bonded GRE tunnels by using the Filter List Package attribute as specified in Section 5.6.2. The HG and the HAAP 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 bypass 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 5.4 are used to carry the timestamp information, and the RTT value can therefore be calculated based on the timestamp.

Besides the end-to-end delay of the GRE tunnels, the HG and the HAAP need to measure the capacity of the tunnels as well. For example, the HG is REQUIRED to measure the downstream bypassing bandwidth and report it to the HAAP in real time (see Section 5.6.1).

4.7. Policy Control Considerations

Operators and users 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 bypass.

Operators and users may offer the service types that need to bypass the bonded GRE tunnels. Service types defined by operators (see Section 5.6.2) will be delivered from the HAAP to the HG through the control plane (see Section 4.1), and the HG will use the raw connection to transmit traffic for these service types. Users may also define bypass service types on the HG. Bypass service types defined by users need not be delivered to the HAAP.

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

Since the GRE tunnels are set up 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 HG and the HAAP should be able to stop the offloading behavior and fall back to a traditional transmission mode, where the LTE GRE tunnel is disused while all traffic is transmitted over the DSL GRE tunnel. Operators are allowed to define this threshold and period.

5. Control Protocol Specification (Control Plane)

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

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 (0xB7EA) is allocated for this purpose, and the standard GRE header as per [RFC2784] with the Key extension specified by [RFC2890] is used. The Checksum Present bit is set to 0. The Key Present bit is set to 1. The Sequence Number Present bit is set to 0. So, the format of the GRE header for control messages of the GRE Tunnel Bonding Protocol 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 0xB7EA        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                               Key                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Key

For security purposes, the Key field is used to carry a random number. The random number is generated by the HAAP, and the HG is informed of it (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 0xB7EA        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                               Key                             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |MsgType|T-Type |                                               |
   +-+-+-+-+-+-+-+-+           Attributes                          +
   ~                                                               ~
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: Format of Control Messages of GRE Tunnel Bonding

MsgType (4 bits)
Message Type. The control message family contains the following six types of control messages (not including "Reserved"):

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

T-Type (4 bits)
Tunnel Type. Set to 0001 if the control message is sent via the primary GRE tunnel (normally the DSL GRE tunnel). Set to 0010 if the control message is sent via the secondary GRE tunnel (normally the LTE GRE tunnel). Values 0000 and values from 0011 through 1111 are reserved for future use and MUST be ignored on receipt.

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

The Attribute Type specifies the type of the attribute.

Attribute Length

Attribute Length indicates the length of the Attribute Value in bytes.

Attribute Value

The Attribute Value includes the value of the attribute.

All control messages are sent in network byte order (high-order bytes first). The Protocol Type carried in the GRE header for the control message is 0xB7EA. Based on this number, the receiver will decide to consume the GRE packet locally rather than forward it further.

5.1. GRE Tunnel Setup Request

The HG uses the GRE Tunnel Setup Request message to request that the HAAP establish the GRE tunnels. It is sent out from the HG’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

An operator uses the Client Identification Name (CIN) to identify the HG. The HG sends the CIN to the HAAP 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 contain 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 string value encoded in UTF-8 and set by the operator. It is used as the identification of the HG in the operator’s network.

5.1.2. Session ID

This Session ID is generated by the HAAP when the LTE GRE Tunnel Setup Request message is received. The HAAP announces the Session ID to the HG in the LTE GRE Tunnel Setup Accept message. For those WAN interfaces that need to be bonded together, the HG MUST use the same Session ID. The HG 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 HAAP, the Session ID attribute need not be included. However, if the LTE GRE tunnel fails and the HG 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
An unsigned integer generated by the HAAP. It is used as the identification of bonded GRE tunnels.

5.1.3. DSL Synchronization Rate

The HG uses the DSL Synchronization Rate to notify the HAAP 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
An unsigned integer measured in kbps.

5.2. GRE Tunnel Setup Accept

The HAAP 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 to be included in this message are defined below.

5.2.1. H IPv4 Address

The HAAP uses the H IPv4 Address attribute to inform the HG of the H IPv4 address. The HG uses the H IPv4 address as the destination endpoint IPv4 address of the GRE tunnels (the source endpoint IPv4 addresses of the GRE tunnels are the DSL WAN interface IP address (D) and the LTE WAN interface IP address (E), respectively, as shown in Figure 1). 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 (e.g., an IP address of a Line Card in the HAAP), which is used as the endpoint IP address of GRE tunnels by the HAAP.

5.2.2. H IPv6 Address

The HAAP uses the H IPv6 Address attribute to inform the HG of the H IPv6 address. The HG uses the H IPv6 address as the destination endpoint IPv6 address of the GRE tunnels (the source endpoint IPv6 addresses of the GRE tunnels are the DSL WAN interface IP address (D) and the LTE WAN interface IP address (E), respectively, as shown in Figure 1).

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 2.

Attribute Length
   Set to 16.

H IPv6 Address
   Set to the pre-configured IPv6 address (e.g., an IP address of a Line Card in the HAAP), which is used as the endpoint IP address of GRE tunnels by the HAAP.

5.2.3. Session ID

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

5.2.4. RTT Difference Threshold

The HAAP uses the RTT Difference Threshold attribute to inform the HG of the acceptable threshold of the RTT difference between the DSL link and the LTE link. If the measured RTT difference exceeds this threshold, the HG 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 HAAP uses the Bypass Bandwidth Check Interval attribute to inform the HG of how frequently the bypass bandwidth should be checked. The HG 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 10 through 300.

5.2.6. Active Hello Interval

The HAAP uses the Active Hello Interval attribute to inform the HG of the pre-configured interval for sending out GRE Tunnel Hellos. The HG 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 1 through 100.

5.2.7. Hello Retry Times

The HAAP uses the Hello Retry Times attribute to inform the HG of the retry times for sending GRE Tunnel Hellos. If the HG does not receive any acknowledgement from the HAAP for the number of GRE Tunnel Hello attempts specified in this attribute, the HG 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 that takes values in the range 3 through 10.

5.2.8. Idle Timeout

The HAAP uses the Idle Timeout attribute to inform the HG 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 GRE 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 a granularity of 60. The default value is 86,400 (24 hours). The value 0 indicates that the idle timer never expires.

5.2.9. Bonding Key Value

The HAAP uses the Bonding Key Value attribute to inform the HG of the number that is to be carried as the Key of the GRE header for subsequent control messages. The Bonding Key Value is generated by the HAAP and used for security purposes.

The method used to generate this number is left up to implementations. The pseudorandom number generator defined in ANSI X9.31, Appendix A.2.4 [ANSI-X9.31-1998] is RECOMMENDED. Note that random number generation "collisions" are allowed in the GRE Tunnel Bonding Protocol.

```
   +-+-+-+-+-+-+-+-+
   |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 random number generated by the HAAP.

5.2.10. Configured DSL Upstream Bandwidth

The HAAP obtains the upstream bandwidth of the DSL link from the management system and uses the Configured DSL Upstream Bandwidth attribute to inform the HG. The HG uses the received upstream bandwidth as the CIR [RFC2697] for the DSL link. 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 HAAP obtains the downstream bandwidth of the DSL link from the management system and uses the Configured DSL Downstream Bandwidth attribute to inform the HG. The HG 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 HAAP uses the RTT Difference Threshold Violation attribute to inform the HG of the number of times in a row that the RTT Difference Threshold (see Section 5.2.4) may be violated before the HG MUST stop using the LTE GRE tunnel. If the RTT Difference Threshold is continuously violated for more than the indicated number of measurements, the HG 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 that takes values in the range 1 through 25. A typical value is 3.

5.2.13. RTT Difference Threshold Compliance

The HAAP uses the RTT Difference Threshold Compliance attribute to inform the HG of the number of times in a row that 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 measurements, the HG 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 Difference Threshold Compliance, set to 25.

Attribute Length
Set to 4.

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

5.2.14. Idle Hello Interval

The HAAP uses the Idle Hello Interval attribute to inform the HG of the pre-configured interval for sending out GRE Tunnel Hellos when the subscriber is detected to be idle. The HG 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 bonded tunnels have seen no traffic for a period 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 in the range 100 through 86,400 (24 hours) with a granularity of 100. The default value is 1800 (30 minutes).

5.2.15. No Traffic Monitored Interval

The HAAP uses the No Traffic Monitored Interval attribute to inform the HG of the pre-configured interval for switching the GRE Tunnel Hello mode. If traffic is detected on the bonded GRE tunnels before this interval expires, the HG 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

The HAAP MUST send the GRE Tunnel Setup Deny message to the HG if the GRE Tunnel Setup Request from this HG is denied. The HG MUST terminate the GRE tunnel setup process as soon as it receives the GRE Tunnel Setup Deny message.

5.3.1. Error Code

The HAAP uses the Error Code attribute to inform the HG of the error code. The error code depicts 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 codes is as follows:

1: The HAAP was not reachable over LTE during the GRE Tunnel Setup Request.

2: The HAAP was not reachable via DSL during the GRE Tunnel Setup Request.

3: The LTE GRE tunnel to the HAAP failed.

4: The DSL GRE tunnel to the HAAP failed.

5: The given DSL User ID is not allowed to use the GRE Tunnel Bonding service.

6: The given User Alias / User ID (Globally Unique Identifier (GUID)) is not allowed to use the GRE Tunnel Bonding service.

7: The LTE and DSL User IDs do not match.

8: The HAAP denied the GRE Tunnel Setup Request because a bonding session with the same User ID already exists.

9: The HAAP denied the GRE Tunnel Setup Request because the user’s CIN is not permitted.

10: The HAAP terminated a GRE Tunnel Bonding session for maintenance reasons.

11: There was a communication error between the HAAP and the management system during the LTE GRE Tunnel Setup Request.

12: There was a communication error between the HAAP and the management system during the DSL GRE Tunnel Setup Request.

5.4. GRE Tunnel Hello

After the DSL/LTE GRE tunnel is established, the HG begins to periodically send out GRE Tunnel Hello messages via the tunnel; the HAAP acknowledges the HG’s messages by returning GRE Tunnel Hello messages to the HG. This continues until the tunnel is terminated.

5.4.1. Timestamp

The HAAP uses the Timestamp attribute to inform the HG of the timestamp value that is used for RTT calculation. Both the LTE GRE Tunnel Hello message and the 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 time since the system restarted. The high-order 4 bytes indicate an unsigned integer in units of 1 second; the low-order 4 bytes indicate an unsigned integer in units of 1 millisecond.

5.4.2. IPv6 Prefix Assigned by HAAP

The HAAP uses the IPv6 Prefix Assigned by HAAP attribute to inform the HG of the assigned IPv6 prefix. This IPv6 prefix is to be captured via lawful intercept. Both the LTE GRE Tunnel Hello message and the DSL GRE Tunnel Hello message MUST include the IPv6 Prefix Assigned by HAAP attribute.

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

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

Attribute Length
Set to 17.

IPv6 Prefix Assigned by HAAP
The highest-order 16 bytes encode an IPv6 address. The lowest-order 1 byte encodes the prefix length. These two values are put together to represent an IPv6 prefix.

5.5. GRE Tunnel Tear Down

The HAAP can terminate a DSL/LTE GRE tunnel by sending the GRE Tunnel Tear Down message to the HG via the tunnel. The Error Code attribute as defined in Section 5.3.1 MUST be included in this message. After receiving the GRE Tunnel Tear Down message, the HG removes the IP address of H, which is the destination IP addresses of the DSL and LTE GRE tunnels.

5.6. GRE Tunnel Notify

The HG and the HAAP use the GRE Tunnel Notify message, which is transmitted through either the DSL GRE tunnel or the LTE GRE tunnel, to notify each other about their status regarding the DSL/LTE GRE tunnels, the information for the bonded 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. However, 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 -- the Filter List Package ACK attribute -- is used as the acknowledgement (see Section 5.6.12).

Attributes that need to be 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 be transmitted over the raw DSL WAN interface rather than the bonded GRE tunnels. The HG 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 HG uses the Bypass Traffic Rate attribute to inform the HAAP 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 HAAP calculates the available downstream bandwidth for the DSL GRE tunnel as the Configured DSL Downstream Bandwidth minus the bypass bandwidth provided by the HG. The available DSL bandwidth will be used as the CIR of the coloring system [RFC2697].

```
+-+-+-+-+-+-+-+-+
|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 HAAP uses the Filter List Package attribute to inform the HG of the service types that need to bypass the bonded GRE tunnels. The full list of all Filter Items may be given by a series of Filter List Package attributes with each specifying a partial list. At the HG, a full list of Filter Items is maintained. Also, the HG 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 raw DSL rather than the bonded GRE tunnels. Both the LTE GRE Tunnel Notify message and the DSL 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 TLV                  (variable) ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+...+-+
```

Attribute Type
Filter List Package, set to 8.

Attribute Length
The total length of the Filter List TLV. The maximum allowed length is 969 bytes.

Filter List TLV

The Filter List TLV occurs one time in a Filter List Package attribute. It 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             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Filter Item (1)                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         ......                                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Filter Item (n)                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

where each Filter Item is of the following format:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Type                  |          Length               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Enable                |     Description Length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                 Description Value                             ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                        Value                                  ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Commit_Count

An unsigned integer that identifies the version of the Filter Item list. The version is shared by all Filter List Packages and increases monotonically by one for each new Filter Item list. The HG MUST refresh its Filter Item list when a new Commit_Count is received.

Packet_Sum

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

Packet_ID

The fragmentation index for this Filter List Package attribute. Each fragment is numbered starting at 1 and increasing by one up to Packet_Sum.

Type

The Type of the Filter Item. Currently, the following types are supported:

Filter Item	Type
FQDN [RFC7031]	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

Other values are reserved for future use and MUST be ignored on receipt.

Length

The length of the Filter Item in bytes. Type and Length are excluded.

Enable

An integer that indicates whether or not the Filter Item is enabled. A value of 1 means "enabled", and a value of 0 means "disabled". Other possible values are reserved and MUST be ignored on receipt.

Description Length

The length of the Description Value in bytes.

Description Value

A variable-length string value encoded in UTF-8 that describes the Filter List TLV (e.g., "FQDN").

Value

A variable-length string encoded in UTF-8 that specifies the value of the Filter Item (e.g., "www.yahoo.com"). As an example, Type = 1 and Value = "www.yahoo.com" mean that packets whose FQDN field equals "www.yahoo.com" match the Filter Item. "Source MAC" (source Media Access Control address) values are specified using hexadecimal numbers. Port numbers are decimals as assigned by IANA in [Port-NO]. For the "Protocol" type, the value could be either a decimal or a keyword specified by IANA in [Pro-NO]. The formats for IP addresses and IP address ranges are defined in [RFC4632] and [RFC4291] for IPv4 and IPv6, respectively. A Filter Item of Type 5, 8, 13, or 14 is a combination of two parameters; values for the two parameters are separated by a colon (":").

5.6.3. Switching to DSL Tunnel

If the RTT difference is continuously detected to be in violation of the RTT Difference Threshold (see Section 5.2.4) more than the number of times specified in the RTT Difference Threshold Violation attribute (see Section 5.2.12), the HG uses the Switching to DSL Tunnel attribute to inform the HAAP to use the DSL GRE tunnel only. When the HAAP receives this attribute, it MUST begin to transmit downstream traffic to this HG 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 be in violation of the RTT Difference Threshold (see Section 5.2.4) more than the number of times specified in the RTT Difference Threshold Compliance attribute (see Section 5.2.13), the HG uses the Overflowing to LTE Tunnel attribute to inform the HAAP that the 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 HG detects that the DSL WAN interface status is "down", it MUST tear down the DSL GRE tunnel. It informs the HAAP about the failure by using the DSL Link Failure attribute. The HAAP MUST tear down the DSL GRE tunnel upon receipt of the DSL Link Failure attribute. 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 HG detects that the LTE WAN interface status is "down", it MUST tear down the LTE GRE tunnel. It informs the HAAP about the failure by using the LTE Link Failure attribute. The HAAP MUST tear down the LTE GRE tunnel upon receipt of the LTE Link Failure attribute. 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 HG changes the IPv6 prefix assigned to the host, it uses the IPv6 Prefix Assigned to Host attribute to inform the HAAP. 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 bytes encode an IPv6 address. The lowest-order 1 byte encodes the prefix length. These two values are put together to represent an IPv6 prefix.

5.6.8. Diagnostic Start: Bonding Tunnel

The HG uses the Diagnostic Start: Bonding Tunnel attribute to inform the HAAP 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 HG uses the Diagnostic Start: DSL Tunnel attribute to inform the HAAP 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 HG uses the Diagnostic Start: LTE Tunnel attribute to inform the HAAP to switch to diagnostic mode to test the performance of the LTE GRE 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 28.

Attribute Length
   Set to 0.

5.6.11. Diagnostic End

The HG uses the Diagnostic End attribute to inform the HAAP 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 HG uses the Filter List Package ACK attribute to acknowledge the Filter List Package sent by the HAAP. 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 bytes are the Commit_Count as defined in Section 5.6.2. The lowest-order 1 byte encodes the following error codes:

0: The Filter List Package is acknowledged.

1: The Filter List Package is not acknowledged. The HG is a new subscriber and has not ever received a Filter List Package. In this case, the HAAP SHOULD tear down the bonding tunnels and force the HG to re-establish the GRE tunnels.

2: The Filter List Package is not acknowledged. The HG has already gotten a valid Filter List Package. The filter list on the HG will continue to be used, while the HAAP need not do anything.

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 HG sends the HAAP a GRE Tunnel Notify message containing the Switching to Active Hello State attribute.

The HAAP will switch to Active Hello State and send the HG a GRE Tunnel Notify message carrying the Switching to Active Hello State attribute as the ACK.

When the HG 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 HG 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 HG sends the HAAP a GRE Tunnel Notify message containing the Switching to Idle Hello State attribute.

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

When the HG receives the ACK, it will (1) switch to Idle Hello State, (2) stop RTT detection and clear RTT state, and (3) 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 HAAP uses the Tunnel Verification attribute to inform the HG 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 a much longer time to detect this tunnel.

When the HAAP receives an LTE GRE Tunnel Setup Request and finds that the requested tunnel conflicts with an existing tunnel, the HAAP initiates tunnel verification. The HAAP 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 HG MUST respond to the HAAP 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 HG, the HAAP determines that the existing tunnel is still functioning. An LTE GRE Tunnel Deny message (with Error Code = 8) will be sent to the HG. The HG SHOULD terminate the GRE Tunnel Setup Request process immediately.

If the HAAP does not receive a tunnel verification ACK message after three attempts (one initial attempt and two 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 HG and the HAAP. Users' IP (inner) packets are encapsulated in GRE packets that are in turn carried in IP (outer) packets. The general structure of data packets of the GRE Tunnel Bonding Protocol is shown below.

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

6.1. The GRE Header

The GRE header was first standardized in [RFC2784]. [RFC2890] added the optional Key and Sequence Number fields.

The Checksum and the Reserved1 fields are not used in the GRE Tunnel Bonding; therefore, the C bit is set to 0.

The Key bit is set to 1 so that the Key field is present. The Key field is used as a 32-bit random number. It is generated by the HAAP per bonding connection, and the HG is notified (see Section 5.2.9).

The S bit is set to 1, and the Sequence Number field is present and used for in-order delivery as per [RFC2890].

The Protocol Type field in the GRE header MUST be set to 0x0800 for IPv4 or 0x86DD for IPv6. So, the GRE header used by data packets of the GRE Tunnel Bonding Protocol 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0| |1|1| Reserved0       | Ver |  Protocol Type 0x0800/86DD    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              Key                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sequence Number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 3: GRE Header for Data Packets of GRE Tunnel Bonding

6.2. Automatic Setup of GRE Tunnels

The HG gets the DSL WAN interface IP address (D) from the Broadband Remote Access Server (BRAS) via the Point-to-Point Protocol over Ethernet (PPPoE) and gets the LTE WAN interface IP address (E) through the Packet Data Protocol (PDP) from the Packet Data Network Gateway (PGW). The domain name of a HAAP group may be configured or obtained via the DSL/LTE WAN interface based on gateway configuration protocols such as [TR-069], where the HAAP group comprises one or multiple HAAPs. The Domain Name System (DNS) resolution of the HAAP group’s domain name is requested via the DSL/LTE WAN interface. The DNS server will reply with an anycast HAAP IP address (G), which MAY be pre-configured by the operator.

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

The HG sends the GRE Tunnel Setup Request message to the HAAP via the LTE WAN interface. The outer source IP address for this message is the LTE WAN interface IP address (E), while the outer destination IP address is the anycast HAAP IP address (G). The HAAP with the highest priority (e.g., the one that the HG has the least-cost path to reach) in the HAAP group, which receives the GRE Tunnel Setup

Request message, will initiate the procedure for authentication and authorization, as specified in [TS23.401], to check whether the HG is trusted by the PGW.

If the authentication and authorization succeed, the HAAP sets the LTE WAN interface IP address (E), which is obtained from the GRE Tunnel Setup Request message (i.e., its outer source IP address), as the destination endpoint IP address of the GRE tunnel and replies to the HG’s LTE WAN interface with the GRE Tunnel Setup Accept message in which an IP address (H) of the HAAP (e.g., an IP address of a Line Card in the HAAP) and a Session ID randomly generated by the HAAP are carried as attributes. The outer source IP address for this message is the IP address (H) or the anycast HAAP IP address (G), while the outer destination IP address is the LTE WAN interface IP address (E). Otherwise, the HAAP MUST send to the HG’s LTE WAN interface the GRE Tunnel Setup Deny message, and the HG MUST terminate the tunnel setup process once it receives the GRE Tunnel Setup Deny message.

After the LTE GRE tunnel is successfully set up, the HG will obtain the C address (see Figure 1) over the tunnel from the HAAP through the Dynamic Host Configuration Protocol (DHCP). After that, the HG starts to set up the DSL GRE tunnel. It sends a GRE Tunnel Setup Request message via the DSL WAN interface, carrying the aforementioned Session ID received from the HAAP. The outer source IP address for this message is the DSL WAN interface IP address (D), while the outer destination IP address is the IP address (H) of the HAAP. The HAAP, which receives the GRE Tunnel Setup Request message, will initiate the procedure for authentication and authorization in order to check whether the HG is trusted by the BRAS.

If the authentication and authorization succeed, the HAAP sets the DSL WAN interface IP address (D), which is obtained from the GRE Tunnel Setup Request message (i.e., its outer source IP address), as the destination endpoint IP address of the GRE tunnel and replies to the HG’s DSL WAN interface with the GRE Tunnel Setup Accept message. The outer source IP address for this message is the IP address (H) of the HAAP, while the outer destination IP address is the DSL WAN interface IP address (D). 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 HAAP MUST send to the HG’s DSL WAN interface the GRE Tunnel Setup Deny message. Meanwhile, it MUST send to the HG’s LTE WAN interface the GRE Tunnel Tear Down message. The HG MUST terminate the tunnel setup 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 from the target HG.

As a security feature, the Key field of the GRE header of the control messages and the data packets is generated as a 32-bit cleartext password, except for the first GRE Setup Request message per bonding connection sent from the HG to the HAAP, whose Key field is filled with all zeros. The HAAP and the HG validate the Key value and the outer source IP address, and they discard any packets with invalid combinations.

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

8. IANA Considerations

IANA need not assign anything for the GRE Tunnel Bonding Protocol. The GRE Protocol Type, the Ethertype for the GRE Channel, is set to 0xB7EA, which is under the control of the IEEE Registration Authority. However, IANA has updated the "IEEE 802 Numbers" IANA web page [802Type], which is of primarily historic interest.

9. References

9.1. Normative References

[Port-NO] IANA, "Service Name and Transport Protocol Port Number Registry", <http://www.iana.org/assignments/service-names-port-numbers>.

[Pro-NO] IANA, "Assigned Internet Protocol Numbers", <http://www.iana.org/assignments/protocol-numbers>.

[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>.

[RFC2697] Heinanen, J. and R. Guerin, "A Single Rate Three Color Marker", RFC 2697, DOI 10.17487/RFC2697, September 1999, <http://www.rfc-editor.org/info/rfc2697>.

[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>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <http://www.rfc-editor.org/info/rfc4291>.

[RFC4632] Fuller, V. and T. Li, "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan", BCP 122, RFC 4632, DOI 10.17487/RFC4632, August 2006, <http://www.rfc-editor.org/info/rfc4632>.

[TR-069] Broadband Forum, "CPE WAN Management Protocol", Issue: 1 Amendment 5, November 2013, <https://www.broadband-forum.org/technical/download/TR-069_Amendment-5.pdf>.

[TS23.401] 3GPP TS23.401, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", v11.7.0, September 2013.

9.2. Informative References

[802Type] IANA, "IEEE 802 Numbers", <http://www.iana.org/assignments/ieee-802-numbers>.

[ANSI-X9.31-1998] ANSI Standard X9.31-1998, "Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)", 1998.

[RFC2724] Handelman, S., Stibler, S., Brownlee, N., and G. Ruth, "RTFM: New Attributes for Traffic Flow Measurement", RFC 2724, DOI 10.17487/RFC2724, October 1999, <http://www.rfc-editor.org/info/rfc2724>.

[RFC6320] Wadhwa, S., Moisand, J., Haag, T., Voigt, N., and T. Taylor, Ed., "Protocol for Access Node Control Mechanism in Broadband Networks", RFC 6320, DOI 10.17487/RFC6320, October 2011, <http://www.rfc-editor.org/info/rfc6320>.

[RFC6733] Fajardo, V., Ed., Arkko, J., Loughney, J., and G. Zorn, Ed., "Diameter Base Protocol", RFC 6733, DOI 10.17487/RFC6733, October 2012, <http://www.rfc-editor.org/info/rfc6733>.

[RFC7031] Mrugalski, T. and K. Kinnear, "DHCPv6 Failover Requirements", RFC 7031, DOI 10.17487/RFC7031, September 2013, <http://www.rfc-editor.org/info/rfc7031>.

[RFC7676] Pignataro, C., Bonica, R., and S. Krishnan, "IPv6 Support for Generic Routing Encapsulation (GRE)", RFC 7676, DOI 10.17487/RFC7676, October 2015, <http://www.rfc-editor.org/info/rfc7676>.

Contributors

Li Xue
Individual
Email: xueli_jas@163.com

Zhongwen Jiang
Huawei Technologies
Email: jiangzhongwen@huawei.com

Authors' 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: +49-6151-5812721
Email: heidemannc@telekom.de

Mingui Zhang
Huawei Technologies
No. 156 Beiqing Rd.
Haidian District
Beijing 100095
China
Email: zhangmingui@huawei.com

Behcet Sarikaya
Huawei USA
5340 Legacy Dr. Building 3
Plano, TX 75024
United States of America
Email: sarikaya@ieee.org

Margaret Cullen
Painless Security
14 Summer St. Suite 202
Malden, MA 02148
United States of America
Email: margaret@painless-security.com