

Interdomain Routing Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 18, 2015

N. Leymann
C. Heidemann
Deutsche Telekom AG
M. Wesserman
Painless Security
L. Xue
M. Zhang
Huawei
January 14, 2015

GRE Notifications for Hybrid Access
draft-lhwxz-gre-notifications-hybrid-access-01

Abstract

This document specifies a set of GRE (Generic Routing Encapsulation) extensions which enable operators to construct residential networks that are able to access the provider service through more than one hybrid access networks simultaneously in order to satisfy the higher bandwidth requirements.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [[RFC2119](#)].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

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

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 11, 2014.

Internet-Draft

GRE-Notif.

January 14, 2015

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](http://trustee.ietf.org/license-info) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
2.	Terminology	4
3.	GRE Solution Overview	4
4.	IP Address Assignment	7
4.1.	IPv4 Address Assignment	7
4.2.	IPv6 Address Assignment	7
5.	GRE Solution Function	9
5.1.	GRE Tunnels Setup and Management	9
5.2.	Packet-Based Traffic Overflow	12
5.3.	Backward Compatibility	13
5.4.	Bypassing Traffic Statistic	14
5.5.	LTE and DSL Path Difference Consideration	15
6.	GRE Control Message Definition	15
6.1.	GRE Setup Request Message	17
6.2.	GRE Setup Accept Message	17
6.3.	GRE Setup Deny Message	18
6.4.	GRE Hello Message	18
6.5.	GRE Tear Down Message	18
6.6.	GRE Notify Message	19
7.	GRE Control Message Attribute Definitions	20
7.1.	Client Identification Name (CIN)	21
7.2.	Session ID	21
7.3.	Timestamp	22
7.4.	Bypass Traffic Rate	22
7.5.	Filter List Package	23
7.6.	RTT Difference Threshold	24

7.7.	Bypass Bandwidth Check Interval	25
7.8.	Switching to DSL Tunnel	26
7.9.	Overflowing to LTE Tunnel	26
7.10.	Hello Interval	26
7.11.	Hello Retry Times	27

7.12.	Idle Timeout	27
7.13.	Error Code	28
7.14.	DSL Link Failure	28
7.15.	LTE Link Failure	28
7.16.	IPv6 Prefix Assigned to Terminal Host	29
7.17.	Subscribed DSL Upstream BW	30
7.18.	Subscribed DSL Downstream BW	30
7.19.	Delay Difference Threshold Violation	31
7.20.	Delay Difference Threshold Compliance	31
7.21.	Filter list ACK	32
7.22.	End AVP	33
8.	GRE Tunnels State Machine	33
9.	IANA Considerations	34
10.	Security Considerations	34
11.	Acknowledgements	35
12.	Normative References	35
	Authors' Addresses	35

[1.](#) Introduction

In order to provide higher bandwidth for residential subscribers, operators prefer to bond the LTE network with DSL network to transfer the subscriber traffics. Especially, in some certain places (e.g. the old cities downtown), the DSL network is already overloading, even it is extremely difficult to be updated and rebuilt because of construction. To satisfy this requirement, HYbrid Access(HYA) architecture is designed in [\[I-D.lhwxz-hybrid-access-network-architecture\]](#). A solution is required to fill the gaps for operators deploying HYA.

This document proposes a packet-based HYA solution, which achieves bonding the hybrid access networks via extended Generic Routing Encapsulation (GRE)[\[RFC2890\]](#) protocol. This document presents the GRE protocol extensions required for HYA, specifically, those for signalling to setup, bond and management these GRE tunnels, signalling for reorder and reassemble customer traffics.

This remainder of this document is organized as follows. [Section 2](#) lists the key terms used in this document. [Section 3](#) outlines the overview of GRE solutions. In [section 4](#), IP address assignment in HYA is described. [Section 5](#) discusses the GRE solution functions. The definition of GRE control messages needed in HYA are listed in [Section 6](#). The attributions used in GRE solutions are listed in Section 7. In [Section 8](#), GRE Tunnels State Machine [Section 8](#) is discussed.

[2.](#) Terminology

Customer Premise Equipment (CPE): A device that connects multiple hosts to provide connectivity to the service providers network.

DSL GRE Tunnel: The GRE tunnel between CPE DSL WAN and HAAP. The DSL GRE tunnel termination IP addresses are IP address of CPE DSL WAN interface and HAAP address.

HYbrid Access (HYA): HYbrid Access (HYA) is the bundling of two or more access lines over different technologies (e.g. DSL and LTE) to one Internet connection for end customers.

Hybrid Access Aggregation Point (HAAP): The HAAP which acts as a service termination and a service creation implements bonding mechanism and sets up a high speed Internet dual stack IP connection with CPE on top of two or more hybrid access technologies. The packet reorder, reassemble functions in packet-based solutions should be supported on HAAP.

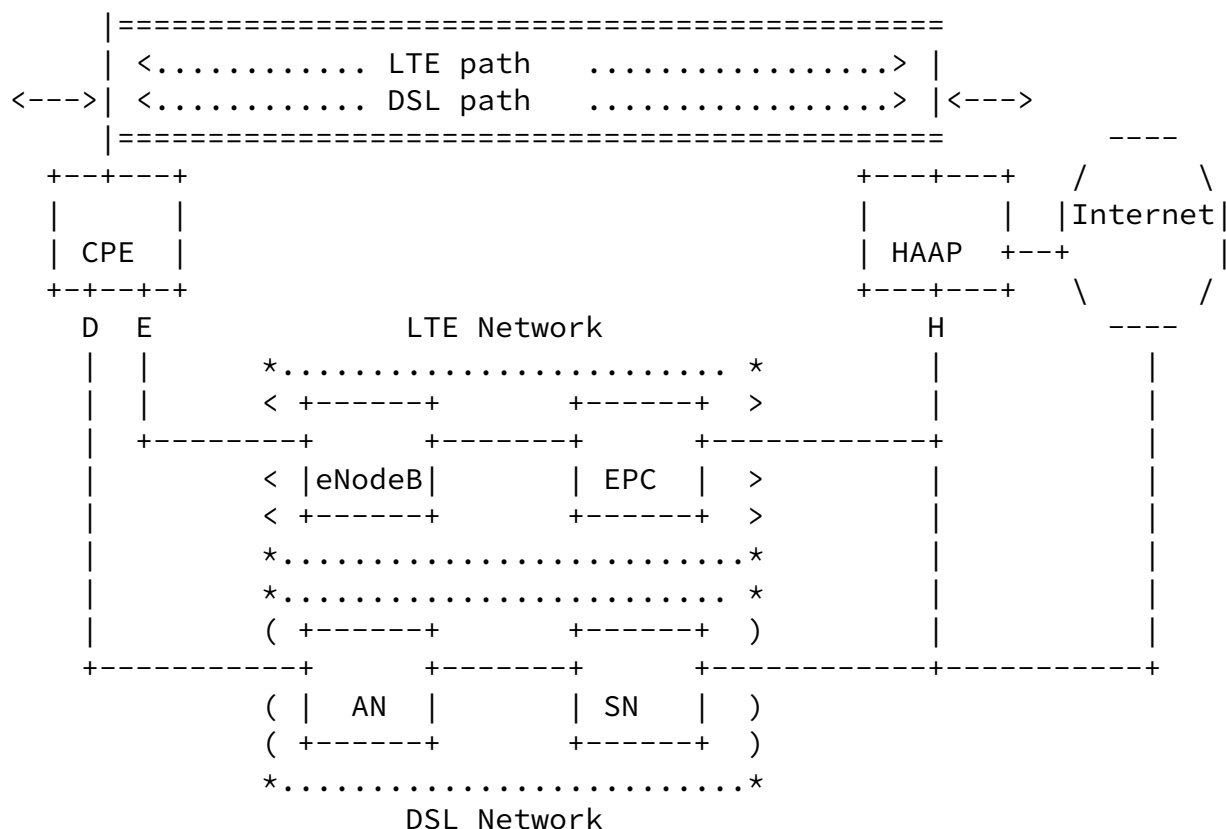
HA Tunnel: HA Tunnel represents LTE GRE tunnel and DSL GRE tunnel defined between CPE and HAAP.

LTE GRE Tunnel: The GRE tunnel between CPE LTE WAN and HAAP. The LTE GRE tunnel termination IP addresses are IP address of CPE LTE WAN interface and HAAP address.

[3.](#) GRE Solution Overview

The GRE solution is proposed as a candidate solution for HYA based on per-packet traffic distribution mechanism. Only a dedicated GRE tunnel is setup over either hybrid access network between CPE and Hybrid Access Aggregation Point (HAAP), DSL GRE tunnel and LTE GRE tunnel. Bonding these GRE tunnels is preformed on CPE and HAAP. In addition, the types of packet distribution rules over hybrid accesses are deployed on both CPE and HAAP according to kinds of criteria (e.g., DSL load, failures, service list, etc).

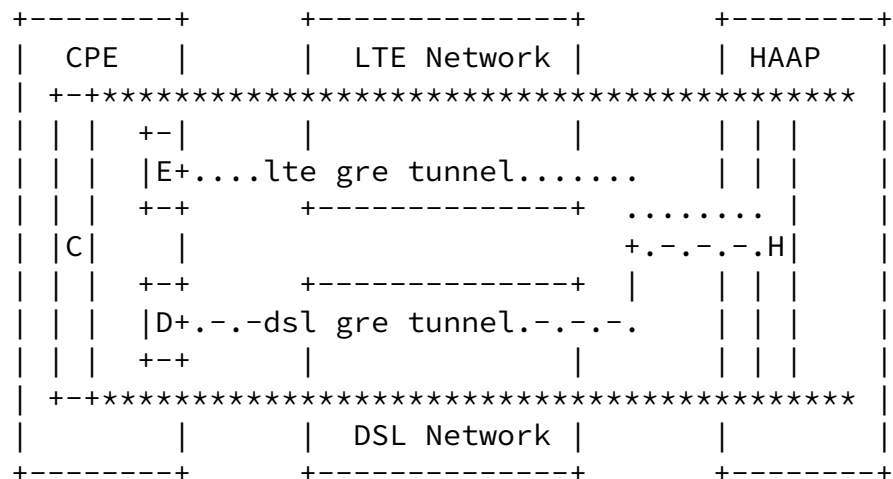
To achieve these performances, the possible communications between CPE and HAAP are needed to achieve GRE tunnel setup, bonding and management, while to deploy and control the consistent traffic distribution for efficiency use of network resources. In addition, packet reorder, reassemble and fragmentation issues should be settled based on this communication [I-D.lhwxz-hybrid-access-network-architecture].



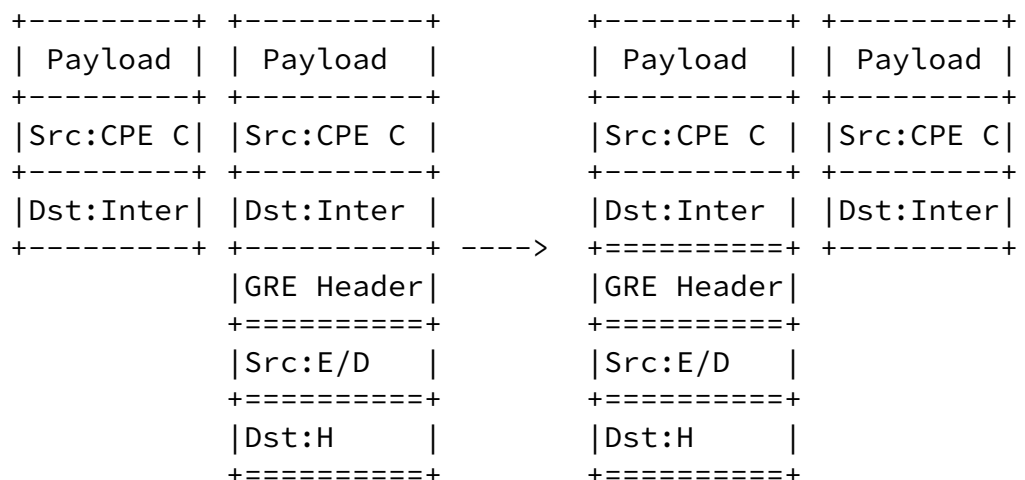
AN	Access Node
SN	Service Node
EPC	Evolved Packet Core

Figure 1: Hybrid Access Network Architecture

Once LTE and DSL GRE tunnels establishment and bonding procedure are completed, customer traffics can be distributed into LTE and/or DSL GRE tunnel based on traffic distribution rules on CPE and HAAP. The traffic encapsulation is shown in Figure 2.



-----> Upstream Traffic



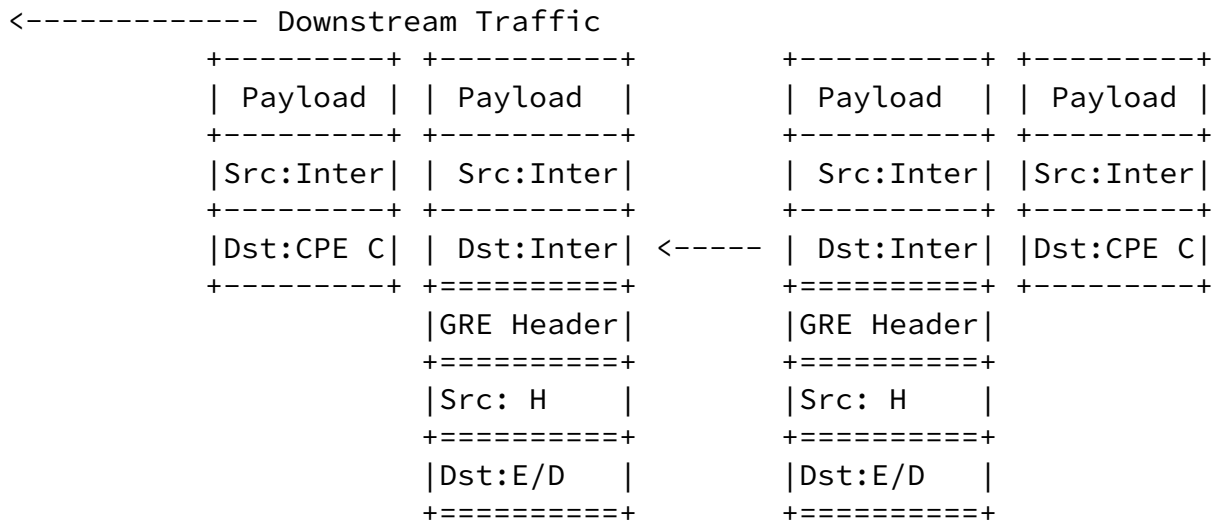


Figure 2: GRE Solution Overview

As shown in Figure 2 , particularly, the traffic going to upstream is encapsulated by GRE on CPE and decapsulated on HAAP. On the other side, HAAP encapsulates the downstream traffic by GRE which will be decapsulated on CPE. In order to clarify the details, the traffic forward actions is described following taking the upstream traffic as an example. A Internet service is initiated at CPE, whose source address is Src:CPE C, which is the public address of CPE assigned by HAAP, the destination address is dst: Inter, the specific Internet server address (e.g. google, youtube,etc). Receiving the upstream traffic, CPE encapsulates the packets of the upstream traffic by GRE tunnel, either LTE GRE tunnel header (Src: E and Dst: H) or DSL GRE tunnel header (Src:D and Dst:H) in order to balance the traffic between LTE and DSL network when DSL network is almost fully

occupied. When the GRE packets the HAAP, they will be decapsulated and then be forwarded as general IP packets.

[4. IP Address Assignment](#)

[4.1. IPv4 Address Assignment](#)

The IPv4 address assignment in Figure 2 are shown as follows:

- o E: CPE LTE WAN Interface IPv4 address (LTE GRE tunnel termination on CPE side)

In LTE network, during Packet Data Protocol (PDP) establishment[TS23.401], the PDN Gateway in LTE network will allocate IPv4 address to CPE LTE WAN interface , referred as E . This IPv4 address is used as LTE GRE tunnel termination's IPv4 address on CPE side.

- o D: CPE DSL WAN Interface IPv4 address (DSL GRE tunnel termination on CPE side)

In DSL network, during PPPoE exchanges [[RFC2561](#)], it is the DSL gateway (e.g. Broadband Network Gateway (BNG)) responsibility to allocate the IPv4 address to CPE DSL WAN interface. This IPv4 address is referred as D, which is used as DSL GRE tunnel termination's IPv4 address on CPE side.

- o C: CPE Public IPv4 address for route advertisement__

This address is assigned by HAAP acting as DHCPv4 server. CPE advertises this IPv4 address during Interior Gateway Protocol (IGP) exchanges for following service transmit. This is the IPv4 address used for the Internet communication.

- o H: HAAP IPv4 address (LTE/DSL GRE tunnel termination on HAAP side)

This address can be pre-configured statically on HAAP.

[4.2.](#) IPv6 Address Assignment

The IPv6 addresses in Figure 2 are shown as follows:

- o E: CPE LTE WAN Interface IPv6 prefix (LTE GRE tunnel termination on CPE side)

In LTE network the CPE LTE WAN interface gets assigned a specific IPv6 prefix (e.g. /64 prefix) by establishing PDP context with PGW, referred as D in Figure 2.

- o D: CPE DSL WAN Interface IPv6 prefix (DSL GRE tunnel termination

on CPE side)

For IPv6 communication, the CPE DSL WAN interface is assigned a specific IPv6 prefix (e.g. /64 prefix) by BNG during PPPoE procedure.

- o C: CPE IPv6 prefix

This IPv6 prefix is assigned by HAAP. This address is stored both on CPE and HAAP. In this case, HAAP will act as DHCPv6 service.

- o H: HAAP IPv6 prefix (LTE/DSL GRE tunnel termination on HAAP side)

This address can be pre-configured statically on HAAP.

There may be two routing for terminal host traffic via the same CPE DSL WAN interface, one route is for bypass traffic without arriving HAAP in [Section 5.3](#), the other route is for HYA traffic with arriving HAAP. So there must be two IPv6 address advertisement for one host in Internet. To achieve this purpose, the IPv6 prefix translation is deployed.

There are two scenarios:

1 DSL GRE Tunnel UP and LTE GRE Tunnel UP

Terminal Host will get a IPv6 prefix D-LAN from D prefix via SLAAC [[RFC4862](#)]. This prefix is used for DSL bypass traffic route advertisement.

IPv6 translation happens on HAAP. On HAAP, the terminal host IPv6 prefix D-LAN will be mapped to C, which is CPE IPv6 prefix assigned by HAAP. The C is used for HYA traffic route advertisement.

2 DSL GRE Tunnel Down and LTE GRE Tunnel UP

Terminal Host will get a IPv6 prefix C-LAN from C prefix via SLAAC [[RFC4862](#)]. This prefix is used for DSL bypass traffic route advertisement.

IPv6 translation happens on HAAP. On HAAP, the terminal host IPv6 prefix C-LAN will be mapped to C, which is CPE IPv6 prefix assigned by HAAP. The C is used for HYA traffic route advertisement.

[5.](#) GRE Solution Function

[5.1.](#) GRE Tunnels Setup and Management

In this document, the LTE and DSL GRE tunnels described in Figure 2 are established by GRE control messages exchanges between CPE and HAAP. The general procedures for the tunnels establishment are illustrated in the following diagram Figure 3.

The annotated ladder diagram shows CPE on the left, HAAP on the right. LTE and DSL network support customer traffic transmission as shown in the middle.

Internet-Draft

GRE-Notif.

January 14, 2015

```

=====
CPE          LTE/DSL          HAAP
=====

```

```

[....CPE obtains LTE WAN IF address during PDP from PGW....]
[...CPE obtains DSL WAN IF address during PPPoE from BNG...]
[..... CPE obtains HAAP address H via DNS      ....]

```

```

[..... begin tunnel establishment and bond.....]

```

```

(..... begin lte gre tunnel establishment.....)

```

```

---- GRE Setup Request Message over LTE ----->
** Authentication and Authorization Passed **
<- (1) GRE Setup Accept Message over LTE-----
      (carrying session ID)
** Authentication and Authorization Failed **
<-(2) GRE Setup Deny Message over LTE -----
if (1)
(..... lte gre tunnel establishment finishes ..... )
if (2)
(----- end -----)

```

```

---- Request CPE IP Address(C) (DHCP over LTE GRE) ----->
<--IP Address (C) Assigned to CPE(DHCP over LTE GRE)-----

```

```

(..... begin dsl gre tunnel establishment ..... )

```

```

----- GRE Setup Request Message over DSL ----->
(same session ID acquired during LTE establishment )
** Authentication and Authorization Passed **
<----(3) GRE Setup Accept Message over DSL ----
** Authentication and Authorization Failed **
<----(4) GRE Setup Deny Message over DSL -----
If (3)
(..... dsl gre tunnel establishment finishes.....)
(.....finish tunnel establishment and bond ..... )
if (4)
(----- end -----)

```

Figure 3: GRE Tunnel Establishment Procedure

The procedure of tunnel establishment is achieved by GRE control message exchanging. Meanwhile, the LTE and DSL GRE tunnels are bonded via the same "session ID" exchanged during the tunnel establishment procedure.

The details procedures are shown as follows:

Leymann, et al.

Expires July 18, 2015

[Page 10]

Internet-Draft

GRE-Notif.

January 14, 2015

1. CPE already gets DSL WAN interface IP address through PPPoE from BRAS and LTE WAN interface IP address through PDP from PGW.
2. CPE request DNS resolution for HAAP domain name via DSL WAN or LTE WAN interface, DNS server will return a corresponding HAAP IP address which can be pre-configured by operators.
3. Then CPE tries to setup the tunnels and bundling them. CPE will setup LTE GRE tunnel before DSL GRE tunnel. CPE sends GRE Tunnel Setup Request message to HAAP via LTE WAN interface.
4. The HAAP receives the message and then initiates the Authentication and Authorization procedure in order to check whether CPE is trusted for PGW. It is similar like UE authentication in [\[TS23.401\]](#).
5. After authentication and authorization succeed, HAAP then replies GRE Tunnel Setup Accept message to CPE via LTE. Specially, Session ID generated randomly by HAAP will be carried in this message, which is used for bonding LTE GRE tunnel and DSL GRE tunnel for one subscriber later. If authentication and authorization failed, HAAP must send the GRE Setup Deny message to CPE over LTE, the tunnel establishment procedure must be tore down.
6. After LTE GRE tunnel setup is success, CPE begins to obtain C address defined in [Section 4](#) from HAAP through DHCP over LTE GRE tunnel. At the same time, CPE begins to setup DSL GRE tunnel.
7. CPE sends GRE Setup Request message with HAAP address as the destination IP of GRE via DSL WAN interface, carrying the same session ID received from HAAP in Step 5.

8. The HAAP receives the message and then initiates the Authentication and Authorization procedure in order to check whether CPE is trusted for BRAS and validate the HYA service rights for CPE.
9. After authentication and authorization succeed, HAAP sends GRE Setup Accept message to CPE via DSL. CPE then bundle the two GRE tunnels based on same Session ID.
10. CPE sends GRE Notify message via DSL WAN immediately after the DSL GRE tunnel setup successfully in order to inform the DSL bypass bandwidth to HAAP. More details is shown in [Section 6](#).

For management and control motivations, GRE tunnel management process message exchanges between CPE and HAAP are needed, shown in the following figureFigure 4.

```

=====          ::::::::::          =====
      CPE          LTE/DSL          HAAP
=====          ::::::::::          =====

(..... lte/dsl tunnel failure detection and keepalive...)
  ----- GRE Hello Message over LTE ----->
<----- GRE Hello Message over LTE -----
  ----- GRE Hello Message over DSL ----->
<----- GRE Hello Message over DSL -----

(.....lte/dsl tunnel information inform.....)
  ----- GRE Notify Message over LTE-----> <-----
    GRE Notify Message over LTE ----- GRE
    Notify Message over DSL-----> <----- GRE Notify
    Message over DSL -----

( ..... lte/dsl tunnel teardown ..... )
<----- GRE Tear Down Message over LTE -----
<----- GRE Tear Down Message over DSL -----

```

Figure 4: GRE Tunnel Management Procedure

GRE Hello messages exchange between CPE and HAAP for LTE/DSL tunnel failure detection and keep-alive. GRE Notify message is used to inform status/information (e.g., dsl network status, service list for HYA, etc) between CPE and HAAP. A notify acknowledgement (ACK) via GRE Notify message and retransmission mechanism can be used to provide certain level reliable transport capability. For maintenance reasons, GRE Tear Down message can be used by HAAP to terminate the bond LTE GRE tunnel and DSL GRE tunnel for some reasons because of network failures. The detailed control messages are proposed in [Section 6.1](#).

[5.2](#). Packet-Based Traffic Overflow

In this document, traffic distribution between the established and bond LTE and DSL GRE tunnel is packet-based overflow. The packet-based traffic overflow mechanism includes two requirements, cheapest path used first (e.g., DSL GRE tunnel Figure 2) and traffics overflowed when cheapest path is almost fully occupied. To satisfy these requirements, Two Rate Three Color Marker (trTCM) [[RFC2698](#)] can be used.

Two token buckets based on DSL and LTE resource are used to meter if the packets is overflowed or not. The details rate configuration is based on the operators' requirement, which is out of the scope. Clearly, the packet can be marked with yellow if the packet is overflowed, otherwise the packet is marked with green based on [[RFC2698](#)]. Then the colored based policy routing is executed on CPE and HAAP. The packet will be routed into the corresponding tunnel based on the marked color. For example, yellow color packet will be routed to LTE GRE tunnel; green color packet will be routed into DSL GRE tunnel. The GRE IP headed is used to encapsulate the traffic on CPE and HAAP as shown in . (Figure 2).

On the received side, the packets encapsulated in GRE will come from DSL GRE tunnel and/or LTE GRE tunnel. Due to different transporting delivery caused by LTE and DSL paths, the packets in the same flow may reach out of the order. Consequentially the packets will be sent to a buffer for reordering based on the sequence information in GRE header, details in [Section 6](#). After reordering, the GRE header will

be removed and the packet will be sent to the ordinary IP packet processing.

5.3. Backward Compatibility

The solution should satisfy the backward compatibility requirements. While deploying HYA architecture, the existing services must not be influenced. For example, IPTV traffic must be remained into the DSL path only for performance reasons, instead of LTE tunnel. In addition some control messages (e.g. for TR069/ACS, DNS etc.) might not be reachable through the HAAP as well due to control and management entities deployment scenario in the network. These kinds of services can be defined and managed by operators during HYA deployment.

In this document, the mechanism must be defined for deploying and maintaining the list of these kinds of traffic. The negotiation between HG and HAAP Figure 5 is described for this purpose.

During network arrangement, operators may configure this service list. HAAP provision the information to CPE via LTE/DSL GRE tunnel. And the list must be updateable during the established tunnel. At each time when CPE try to establish the tunnel, the list is pushed by HAAP. CPE will flash the the list if it have a previous one. If the list is taken some errors during list flashing, CPE should keep the previous one and reply the error code to HAAP via GRE Notify message. The errors include download unsuccessfully, incorrect format, wrong syntax etc defined in [Section 6](#).

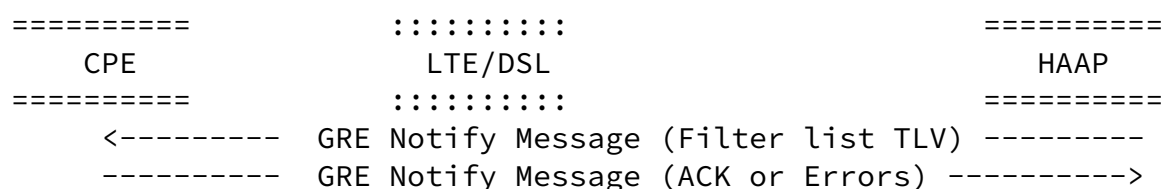


Figure 5: GRE Tunnel Service List Management

As shown Figure 5, only one GRE tunnel (LTE/GRE) will be used for one time transmission of GRE Notify message carrying the service list, and each notification will be replied by a notification ACK. If

several times of transmission failure for notification, the tunnel for sending notification will be switched to the other one.

HG will validate the received filter list packet, if no error found, CPE will reply GRE Notify message as ACK to HAAP. So HAAP directly stops to send the following filter list packet, that means this time of filter list notification is completed successfully. If any error found, CPE will reply GRE Notify message as errors feedback, HAAP will try to send it again or stop it. The details are described in [Section 6](#).

In case of large size of the service list, multiple GRE Notify messages to CPE are needed to carry multiple fragments of the list. Each of these GRE Notify message needs a notification ACK.

[5.4](#). Bypassing Traffic Statistic

Bypassing Traffic means that the traffic MUST bypass the HYA GRE tunnel but directly over DSL WAN interface as mentioned filter list in [Section 5.3](#), and this happens on the CPE. The traffic bypass behavior is accomplished by implementing a routing table on CPE. Distinctly, part of DSL bandwidth is already occupied by these types of bypass traffic with higher priority. As a result, only the DSL bandwidth left can be used for HYA DSL GRE tunnel.

The solution must consider how to meter the bypassing traffic statistic on DSL bandwidth and adjust the free resource left in DSL for HYA. The DSL bandwidth for HYA must be adjusted dynamically when bypass traffics are presenting. CPE can check the bypass traffic rate periodically, and notify the parameters to the HAAP. HAAP can adjust the token buckets for packet overflow action later on defined in [Section 5.2](#).

[5.5](#). LTE and DSL Path Difference Consideration

In HYA, LTE and DSL tunnel may have different characters, such as rates, delay and MTU which cause the throughput and traffic

fragmentation issues. These differences should be considered during the GRE solution design.

The rate, Round Trip Time (RTT) /delay of a DSL link is relatively fixed, but the RTT/delay character of an LTE link vary over time. When the DSL and LTE link are combined in HYA, the CPE has a larger combined bandwidth (DSL_BW + LTE_BW), but the RTT/delay of the bonded tunnels may become bigger for customer traffics. The maximum RTT/delay of customer HYA traffic is equal to bigger one of the LTE and DSL links. Usually, the buffering size for packet reorder is related to the RTT/delay difference between both LTE and DSL link. If the RTT/delay difference is too big, the buffer size will be too huge to be achieved on CPE/HAAP. In this case, the bandwidth efficiency of the HYA will disappeared comparing the bigger RTT/delay and huge buffer requirement.

The MTU difference may impact the packet fragmentation and reorder. The minimum MTU on DSL path is PPPoE MTU, which is 1492. The minimum MTU on LTE path is UGW MTU, which is 1436. In HYA, the maxium tunnel MTU is LTE MTU minus GRE overhead. Static calculation for GRE tunnel MTU sized based on DSL path MTU and LTE path MTU is configured. MSS adjustment for TCP on CPE based on the calculation in order to avoid IP fragmentation on both GRE outer IP layer and inner IP layer.

6. GRE Control Message Definition

In this section, GRE encapsulation control messages are defined for negotiation between CPE and HAAP for the LTE and DSL tunnel establishment, bond, management, etc, which are not standardized yet. The GRE control messages format are according to [\[RFC2890\]](#). The GRE header as described in Figure 6 indicates a control protocol with the Protocol Type section set to 0x0101 in this document.

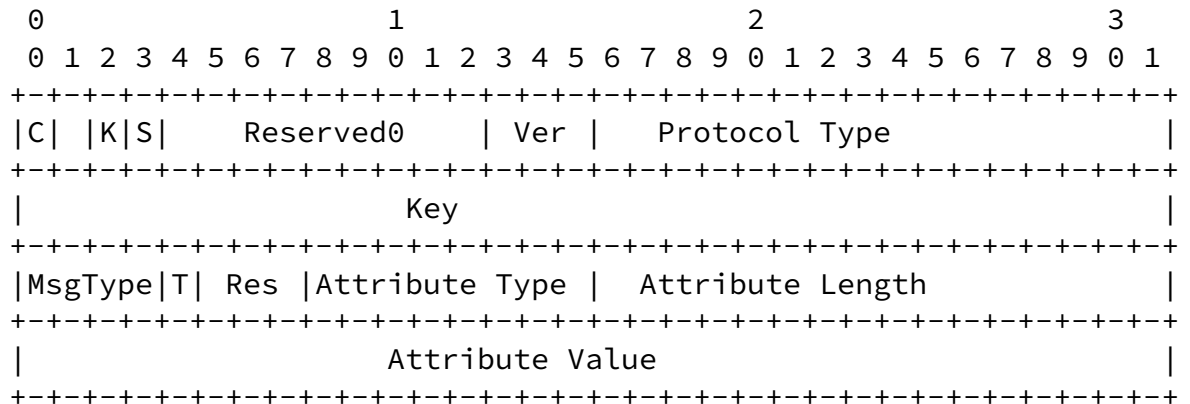


Figure 6: GRE Header Format

Protocol Type (2 octets)

The Protocol Type field identifies the GRE protocol for HYA network. The value 0x0101 is proposed.

Message Type (MesType) (4 bits)

The Message Type field identifies GRE protocol control messages for HYA network. Right now, there are 6 valid types of GRE control message mentioned , shown as belowFigure 7:

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

Figure 7: GRE Control Messages

Tunnel Type (T) (1 bit)

If the Tunnel Type bit is set to 1, then it indicates that this control message is used for the DSL GRE tunnel. Otherwise it indicates that this control message is used for the LTE GRE tunnel.

Attribute Type (1 octet)

Attribute Type indicates the type of the appended attributes included

in the GRE header. The types of attributes are defined in [Section 7](#).

Internet-Draft

GRE-Notif.

January 14, 2015

Attribute Length (2 octets)

Attribute Length field indicates the length of the attribute by byte.

Attribute Value (variable)

Attribute Value field includes the value of the attribute.

[6.1](#). GRE Setup Request Message

GRE Setup Request message is sent by CPE to HAAP via LTE and DSL WAN in order to set up LTE and DSL GRE tunnel.

The following attributions MUST be included in the GRE Setup Request Message.

- o Client Identification Name (CIN) Figure 10. Only the GRE Tunnel Setup Request Message through LTE WAN must contain the CIN.
- o Session ID Figure 11. CPE must encapsulate the Session ID attribute in GRE Setup Request message via DSL WAN. This Session ID is generated by HAAP during LTE tunnel establishment Figure 3. The value in Session ID attribute must be same via both DSL and LTE WAN. In addition, when LTE GRE tunnel recovery from failure while DSL GRE tunnel exists, the re-established LTE tunnel request needs to carry the Session ID Attribute.
- o End AVP, see [Section 7](#).

[6.2](#). GRE Setup Accept Message

HAAP sends GRE Setup Accept Message to CPE if HAAP accepts associated GRE Setup Request from CPE. The routing path of a pair of GRE Setup Request message and GRE Setup Accept message must be the same, either LTE or DSL.

The following attributions MUST be included in the GRE Setup Accept Message via LTE WAN.

- o Session ID Figure 11, HAAP generates a session ID for a CPE and

sends the Session ID attribute to CPE LTE WAN via GRE Setup Accept Message.

- o RTT Difference Threshold AttributeFigure 16, see [Section 7.6](#).
- o Bypass Bandwidth Check IntervalFigure 17, see [Section 7.7](#).
- o Hello IntervalFigure 18, see [Section 7.10](#).

Leymann, et al.

Expires July 18, 2015

[Page 17]

Internet-Draft

GRE-Notif.

January 14, 2015

- o Hello Retry TimesFigure 19, see [Section 7.11](#).
- o Idle TimeoutFigure 20, see [Section 7.12](#).
- o Delay Difference Threshold Violation, see [Section 7.19](#)
- o Delay Difference Threshold Compliance, see [Section 7.20](#)
- o End AVP, see [Section 7.22](#)

The following attributions MUST be included in the GRE Setup Accept Message via DSL WAN.

- o Subscribed DSL Upstream BWFigure 23, see [Section 7.17](#).
- o Subscribed DSL Downstream BWFigure 24, see [Section 7.18](#).
- o End AVP, see [Section 7.22](#)

[6.3](#). GRE Setup Deny Message

HAAP will send GRE Setup Deny Message to CPE through LTE and/or DSL path if HAAP denies the GRE Setup Request for LTE and/or DSL GRE tunnel from CPE.

The following attributions MUST be included in the GRE Setup Deny Message.

- o Error CodeFigure 21, see [Section 7.13](#).
- o End AVP, see [Section 7.22](#).

[6.4](#). GRE Hello Message

The GRE Hello Message is used for CPE and HAAP on both LTE GRE tunnel and DSL GRE tunnel for failure detection and keepalive of the tunnel.

The following attributes MUST be included in the GRE Hello Message.

- o TimestampFigure 12, see [Section 7.3](#).
- o End AVP, see [Section 7.22](#).

[6.5](#). GRE Tear Down Message

GRE Tear down message is used to maintain the state and can only be send from HAAP to CPE to terminate the established LTE and/or DSL tunnels.

The following attributes MUST be included in the GRE Tear Down Message.

- o Error CodeFigure 21, see [Section 7.13](#).
- o End AVP, see [Section 7.22](#).

[6.6](#). GRE Notify Message

GRE notify message is used to inform status/information changing and the filter list information between CPE and HAAP.

The following attributes MUST be included in the GRE Notify Message via both LTE and DSL WAN.

- o End AVP, see [Section 7.22](#).

The following attributes MAY be included in the GRE Notify Message via LTE WAN .

- o Filter list packageFigure 14, see [Section 7.5](#).
- o DSL link failure, see [Section 7.14](#).
- o IPv6 prefix assigned to terminal hostFigure 22, see [Section 7.16](#).

- o Filter list ACKFigure 14, see [Section 7.21](#).

The following attributes MAY be included in the GER Notify Message via DSL WAN.

- o Bypass traffic rateFigure 13, see [Section 7.4](#).
- o Filter list packageFigure 14, see [Section 7.5](#).
- o Switching to DSL tunnel, see [Section 7.8](#).
- o Overflowing to LTE tunnel, see [Section 7.9](#).
- o LTE link failure, see [Section 7.15](#).
- o IPv6 prefix assigned to terminal hostFigure 22, see [Section 7.16](#).
- o Filter list ACKFigure 14, see [Section 7.21](#).

[7](#). GRE Control Message Attribute Definitions

All the attributions are identified by the Type, Length, Value field, shown as below Figure 8. The 8-bits Type field identifies the type of the attribution.

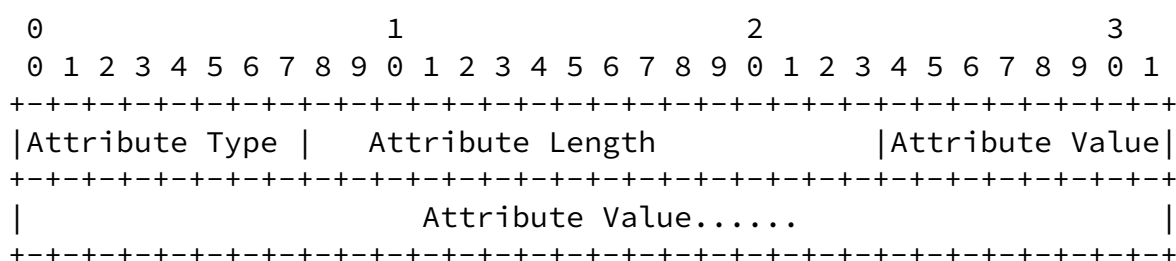


Figure 8: GRE Control Message Attribute Definitions

The following GRE control message attributes for HYA are defined in this documentFigure 9 .

Control Message Family =====	Type =====
CIN	3
Session ID	4
Timestamp	5
Bypass Traffic Rate	6
Filter List Package	8
RTT Difference Threshold	9
Bypass Bandwidth Check Interval	10
Switching to DSL Tunnel	11
Overflowing to LTE Tunnel	12
Hello Interval	14
Hello Retry Times	15
Idle Timeout	16
Error Code	17
DSL Link Failure	18
LTE Link Failure	19
IPv6 Prefix Assigned to Terminal Host	21
Subscribed DSL Upstream BW	22
Subscribed DSL Downstream BW	23
Delay Difference Threshold Violation	24
Delay Difference Threshold Compliance	25
Filter list ACK	30
End AVP	255
Reserved	

Figure 9: GRE Control Message Attributes

[7.1.](#) Client Identification Name (CIN)

CIN is used to identified the RG in operator network. CIN is sent to HAAP by CPE for authentication and authorization purpose. It is similar like UE authentication in [\[TS23.401\]](#).Any CPE must transmit a CIN during the tunnel request procedure for authentication. CIN must be unique for each CPE in operator's network.

The attribute contains the following value Figure 10:

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			

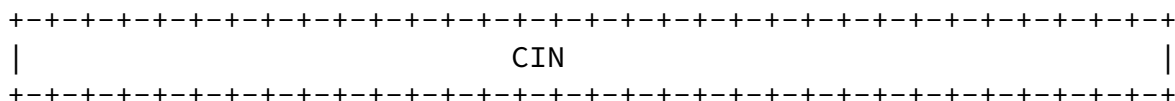


Figure 10: CIN Attribute

Type:3 for CIN Attribute

Length: 40 Bytes

CIN: String defined by operators

7.2. Session ID

Session ID attribute is used to bind the DSL tunnel and LTE tunnel together for individual CPE. Session ID 32bit value is generated by HAAP, and unique within a HAAP. It is used to identify a certain subscriber CPE.

HAAP sends this attribute to requesting CPE LTE WAN via GRE Setup Accept message, then CPE encapsulates this attribute in GRE Setup Request through DSL WAN. With this information, CPE and HAAP can bind these two tunnels together. When LTE recovery from failure with DSL tunnel exists, the re-established LTE tunnel request needs to carry the Session ID.

The attribute contains the following value Figure 11:

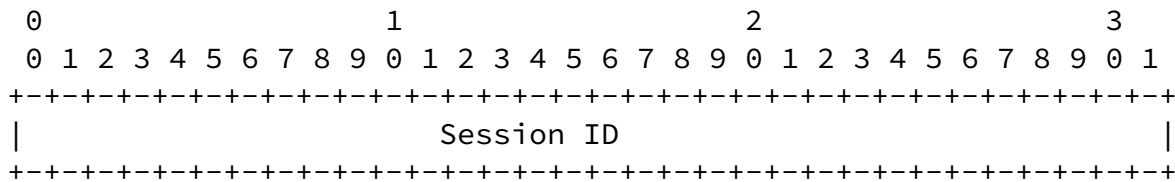


Figure 11: Session ID Attribute

Type:4 for Session ID Attribute

Length: 4 Bytes

Session ID: String value generated by HAAP to identify a certain CPE.

7.3. Timestamp

The Timestamp attribute is used for Round-Trip Time (RTT) calculation.

The attribute contains the following value Figure 12.

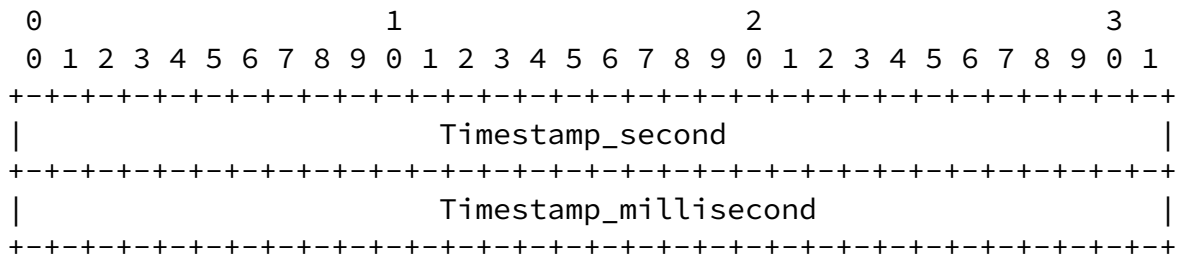


Figure 12: Timestamp Attribute

Type:5 for Timestamp Attribute

Length: 8 Bytes

Session ID: The higher order 4 bytes is seconds, the low-order 4 bytes is millisecond

7.4. Bypass Traffic Rate

The Bypass Traffic Rate attribute is used by HG to notify HAAP of the bypass traffic rate on CPE, such as IPTV, DNS, etc, see [Section 5.4](#) for details. HAAP will calculate the available DSL bandwidth for HYA DSL GRE tunnel based on this information.

The attribute contains the following valuesFigure 13.

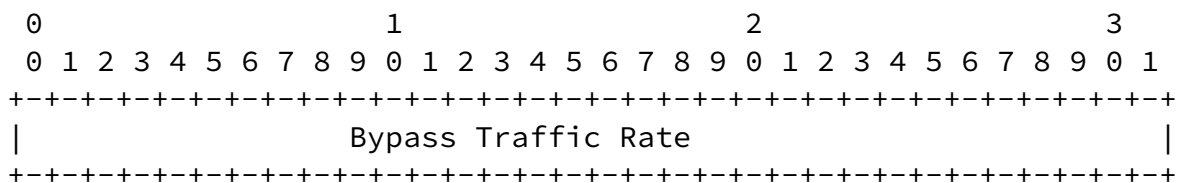


Figure 13: Bypass Traffic Rate Attribute

Type:6 for BypassTraffic Rate Attribute

Length: 4 Bytes

Bypass Traffic Rate: A 4-bytes length integer to identify the resource already occupied in DSL by kinds of bypass traffic referred as [Section 5.4](#) .The CPE will check the bypass traffic rate periodically, if the bypass traffic rate difference is greater than specified percentage of the DSL bandwidth, and then notify the bypass traffic rate to the HAAP. HAAP can adjust the token buckets for packet overflow action later on [Section 5.4](#).

7.5. Filter List Package

The Filter List Package is the collection of the services list which MUST not be routed through HYA, but directly over the specific interface mentioned in [Section 5.3](#). The filter service list is configured on CPE by HAAP. This attribute is the collection of filter list TLVs, each TLV carries one kinds of filter service list.

The attribute contains the following valuesFigure 14:

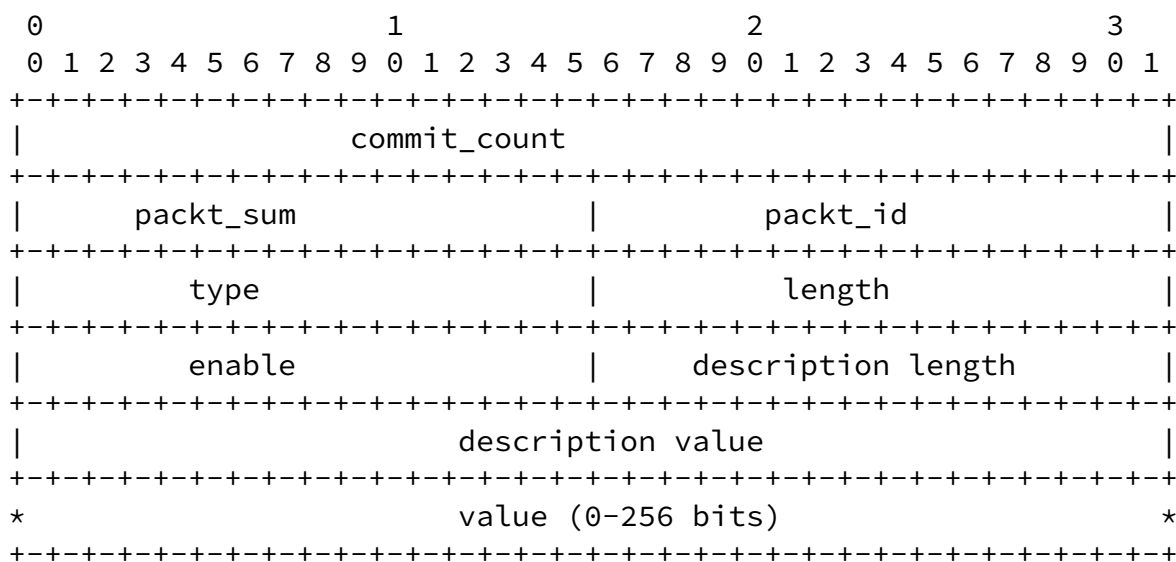


Figure 14: Filter List Package Attribute

Type: 8 for Filter List Package Attribute

Length: <= 969 Bytes

Commit_count: It is used to identify the Filter list version. If the Filter list recieved from HAAP changed, the commit_count will be updated. CPE will refresh the previous filter list.

Internet-Draft

GRE-Notif.

January 14, 2015

Packet_sum: If the filter list packet is larger than the MTU and should be divided into multiple fragments, the Packet_sum indicate the fragments numbers of the filter list packet.

Packet_ID: The index of the multiple fragments.

Type: Several filter list type can be defined, which is described as followingFigure 15.

Length: The length of the specific type of filter list.

Enable: Indicate this type of filter list is enabled. Only can be 1(Enabled) or 0 (Unenabled), other values are reserved.

Description Length: The length of this type of filter list description, the unit is byte.

Description Value:The value of this type of the filter list

Value: Value of the specific type of filter list.

Filter List	Type
=====	=====
Fully Qualified Domain Name	1
DSCP	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	

Figure 15: Filter List Type

[7.6.](#) RTT Difference Threshold

The difference RTT/delay between DSL and LTE should impact the HYA network efficiency, mentioned in [Section 5.5](#). So the acceptable RTT difference threshold in HYA must be defined. This value is signed to CPE by HAAP. When the RTT difference exceeds the configured RTT

difference threshold, CPE may changing the traffic distribution into DSL only rather than LTE GRE tunnel.

The attribute contains the following valuesFigure 16

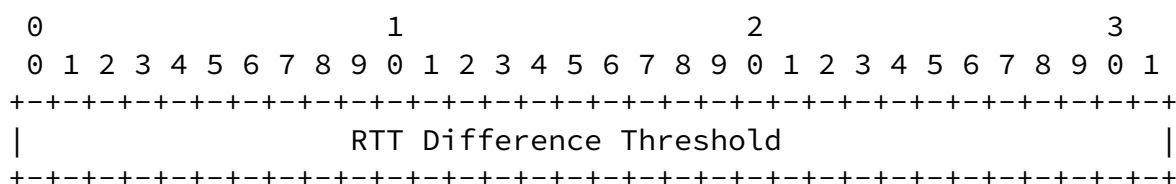


Figure 16: RTT Difference Threshold

Type: 9 for RTT Difference Threshold Attribute

Length: 4 Bytes

RTT Difference Threshold: The unit of this integer value is ms (milliseconds). This value is configurable, the value range can be from 0~1200ms, changing step is 1ms.

[7.7](#). Bypass Bandwidth Check Interval

The Bypass Bandwidth Check Interval is assigned to CPE by HAAP. Based on requirement in [Section 5.4](#), CPE will check the bypass bandwidth on DSL path after this interval.

The attribute contains the following valueFigure 17:

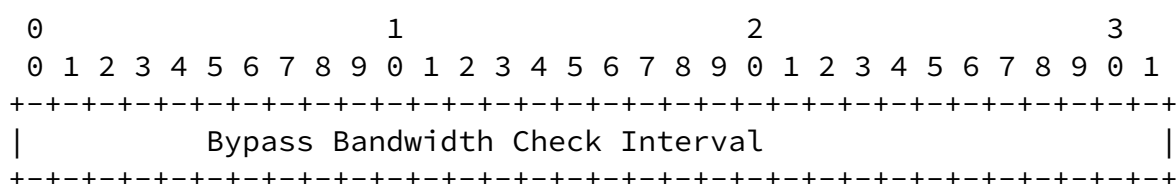


Figure 17: Bypass Bandwidth Check Interval Attribute

Type: 10 for Bypass Bandwidth Check Interval Attribute

Length: 4 Bytes

Bypass Bandwidth Check Interval: Integer as seconds. This value is configurable, the range is from 10-300s, changing step is 1s.

[7.8.](#) Switching to DSL Tunnel

The Switching to DSL Tunnel is used by CPE to notify HAAP to switch the traffic to DSL only. When the RTT difference between DSL and LTE tunnel exceeds the RTT difference thresholdFigure 16 3 times (default value), the CPE will send a Notify message with "Switching to DSL tunnel" attribute to HAAP. Then the traffic will be sent through the DSL tunnel only no matter HAAP or CPE.

There is no value in this attribute.

Type: 11 for Switching to DSL Tunnel

Length: 0

[7.9.](#) Overflowing to LTE Tunnel

The Overflowing to LTE Tunnel is used by CPE to notify HAAP to overflow the traffic to LTE tunnel. When the RTT difference between DSL and LTE tunnel is lower than the RTT difference thresholdFigure 16 3 times (default value), the CPE will send a a Notify message with "Overflowing to LTE tunnel" attribute to HAAP. Then the traffic can overflow to the LTE tunnel.

There is no value in this attribute.

Type: 12 for Overflowing to LTE Tunnel

Length: 0

[7.10.](#) Hello Interval

The Hello Interval is configured to CPE by HAAP. The GRE Hello message between CPE and HAAP will be negotiated in each hello interval period.

The attribute contains the following valueFigure 18:

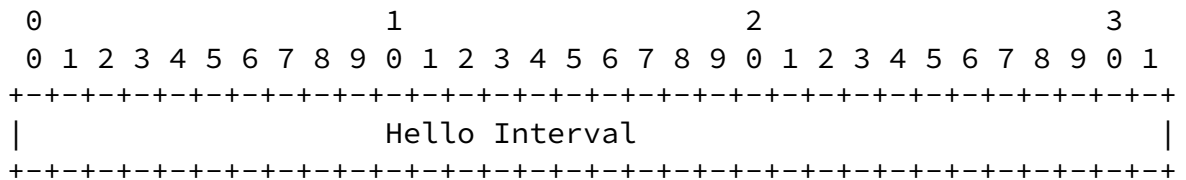


Figure 18: Hello Interval Attribute

Type: 14 for Hello Interval Attribute

Length: 4 Bytes

Hello Interval: Integer. The unit of this value is second. This value should be configurable, with range 1~100s, changing step is 1s.

[7.11.](#) Hello Retry Times

The Hello Retry Times is configured to CPE by HAAP. The GRE Hello message between CPE and HAAP will be retried several times defined in this attribute.

The attribute contains the following valueFigure 19.

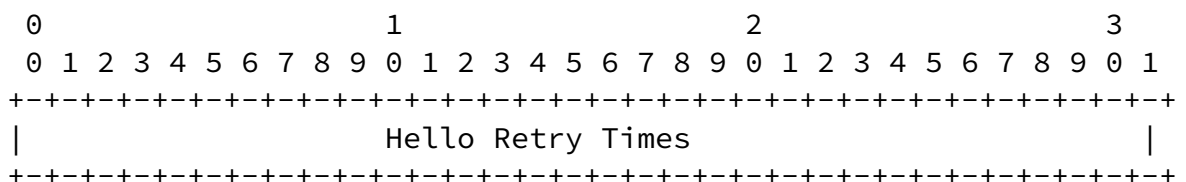


Figure 19: Hello Retry Times Attribute

Type: 15 for Hello Retry Times Attribute

Length: 4 Bytes

Hello Retry Times: Integer. It is the times about the GRE Hello Message retry. This value is configurable, the value range is from 3~10, changing step is 1.

[7.12.](#) Idle Timeout

The Idle Timeout is configured on CPE by HAAP. If GRE tunnels are already established via DSL and LTE, idle timeoutFigure 28 will occur. All tunnels must be terminated if LTE/DSL tunnel isn't restored within a period time (e.g., idle timeout).

The attribute contains the following valueFigure 20.

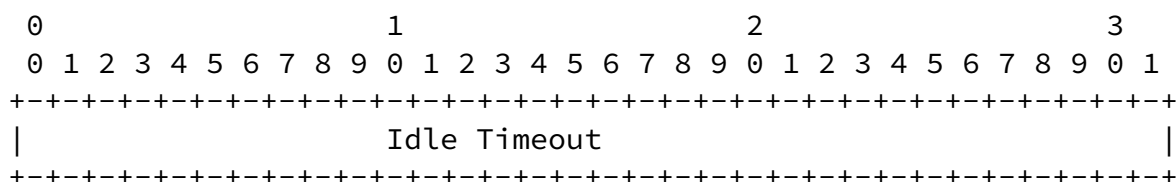


Figure 20: Idle Timeout Attribute

Type: 16 for Idle Timeout Attribute

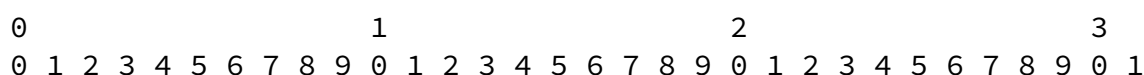
Length: 4 Bytes

Idle Timeout: Integer. The unit of this value is seconds. The value is configurable, with range from 0~172800s, step is 60s.

[7.13.](#) Error Code

The Error Code is used when the erros happens in HYA network.

The attribute contains the following valueFigure 21.



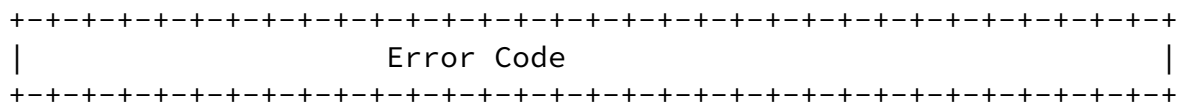


Figure 21: Error Code Attribute

Type: 17 for Error Code Attribute

Length: 4 Bytes

Idle Timeout: Integer. Error cases have to be handled.

[7.14.](#) DSL Link Failure

The DSL Link Failure will be used by CPE to inform HAAP of CPE DSL link failure through LTE WAN. Usually, the failure can be detected by HAAP via GRE Hello message. However, it is possible that the local failures happen on CPE. In this case, direct notification to HAAP is a efficiency way than GRE hello mechanism (Failure Detection time is $\text{retry times} \times \text{hello interval}$)

There is no value in this attribute.

Type: 18 for DSL Link Failure

Length: 0

[7.15.](#) LTE Link Failure

The LTE Link Failure will be used by CPE to inform HAAP of CPE LTE link failure through DSL WAN. Usually, the failure can be detected by HAAP via GRE Hello message. However, it is possible that the local failures happen on CPE. In this case, direct notification to

HAAP is a efficiency way than GRE hello mechanism (Failure Detection time is $\text{retry times} \times \text{hello interval}$)

There is no value in this attribute.

Type: 19 for LTE Link Failure

Length: 0

[7.16.](#) IPv6 Prefix Assigned to Terminal Host

The IPv6 Prefix assigned to terminal host on CPE will be notified to HAAP. Then HAAP can setup the IPv6 prefix translation mapping between CPE HA IPv6 prefix and the terminal host IPv6 prefix. When the downstream traffic arriving, HAAP can advertise the CPE HA IPv6 prefix for HYA refereed to [Section 4.2](#).

When both DSL link and LTE link are working, CPE will assign BRAS IPv6 prefix to terminal host. When DSL line failure and lead to PPPoE terminated, CPE will assign HAAP IPv6 prefix to terminal host. When DSL line recovers from failure and obtains a new IPv6 prefix from BRAS, CPE will assign BRAS IPv6 prefix to terminal host again. When HG change the IPv6 prefix assigned to terminal host, need to send notify to HAAP.

The attribute contains the following valueFigure 22:

```

      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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
\               IPv6 Prefix Assigned to Terminal Host               \
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Network Mask   |
+---+---+---+---+---+---+

```

Figure 22: IPv6 Prefix Assigned to Terminal Host Attribute

Type: 21 for IPv6 Prefix Assigned to Terminal Host Attribute

Length: 17 Bytes

Value: The first 16 bytes are the IPv6 prefix, the last byte indicates the network mask.

7.17. Subscribed DSL Upstream BW

The Subscribed DSL Upstream BW is used by HAAP to notify CPE the available DSL upstream Bandwidth. The subscribed DSL Upstream BW can be obtained by HAAP during authentication and authorization process. CPE/HAAP will use this value to set the token bucket on DSL for traffic overflow referred to [Section 5.4](#).

The attribute contains the following valueFigure 23

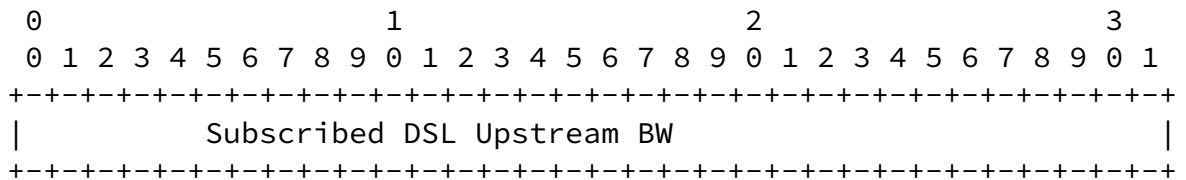


Figure 23: Subscribed DSL Upstream BW

Type: 22 for Subscribed DSL Upstream BW

Length: 4 Bytes

Subscribed DSL Upstream BW: The conventional DSL upstream BW is provided by operator for CPE.The unit of this value is kbps.

7.18. Subscribed DSL Downstream BW

The Subscribed DSL Downstream BW is used by HAAP to notify CPE the available DSL downstream Bandwidth. The subscribed DSL Downstream BW can be obtained by HAAP during authentication and authorization process. CPE/HAAP will use this value to set the token bucket on DSL for traffic overflow referred to [Section 5.4](#).

The attribute contains the following valueFigure 24:

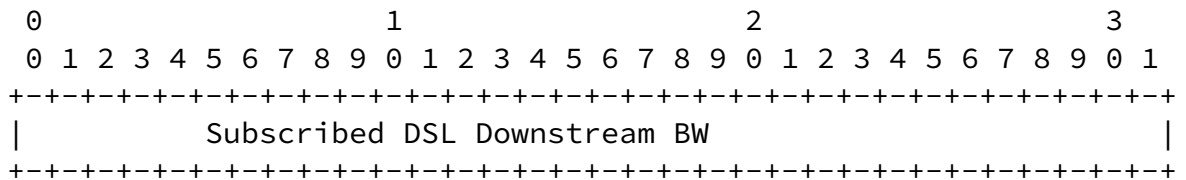


Figure 24: Subscribed DSL Downstream BW

Type: 23 for Subscribed DSL Downstream BW

Length: 4 Bytes

Internet-Draft

GRE-Notif.

January 14, 2015

Subscribed DSL Downstream BW: The conventional DSL downstream BW is provided by operator for CPE. The unit of this value is kbps.

[7.19.](#) Delay Difference Threshold Violation

The Delay Different Threshold Violation is used to carry the times when the RTT/delay difference exceeds the threshold defined in Figure 16. This times will impact the decision to switch the traffic to DSL GRE tunnel only. When the RTT/delay difference exceeds the threshold above the times defined in this attribute, all the traffic will be switched to DSL tunnel, rather than LTE tunnel. This is the configuration to CPE by HAAP.

The attribute contains the following valueFigure 25.

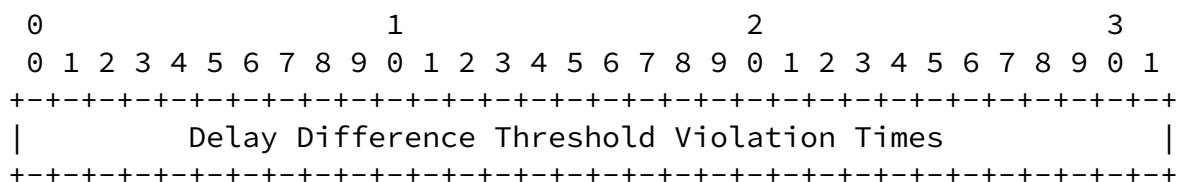


Figure 25: Delay Difference Threshold Violation

Type: 24 for Delay Difference Threshold Violation Attribute

Length: 4 Bytes

Delay Difference Threshold Violation Times: The times when the RTT/delay difference exceeds the threshold defined in Figure 16. This value can be configured by operators.

[7.20.](#) Delay Difference Threshold Compliance

The Delay Different Threshold Compliance is used to carry the times when the RTT/delay difference stays below the threshold defined in Figure 16. This times will impact the decision to switch the traffic to DSL GRE tunnel only. When the RTT/delay difference stays below the threshold above the times defined in this attribute, all the traffic can be transmitted over HYA, with both LTE and DSL tunnel. This is the configuration to CPE by HAAP.

The attribute contains the following valueFigure 26.

Internet-Draft

GRE-Notif.

January 14, 2015

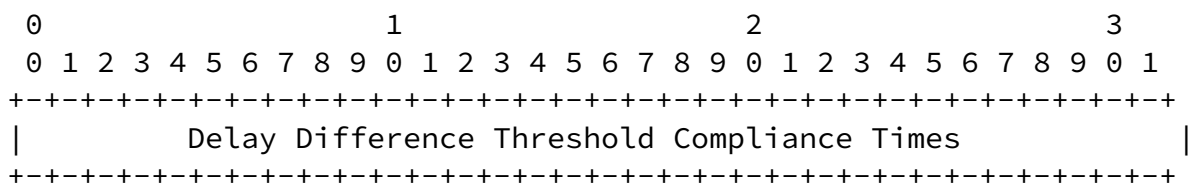


Figure 26: Delay Difference Threshold Compliance

Type: 25 for Delay Difference Threshold Compliance Attribute

Length: 4 Bytes

Delay Difference Threshold Compliance Times: The times when the RTT/delay difference stays below the threshold defined in Figure 16. This value can be configured by operators.

[7.21.](#) Filter list ACK

The Filter List ACK attribute is defined for acknowledgement of filter list notify and filter list error notification. This attribute is used as a reply for Figure 14.

The attribute contains the following value Figure 27.

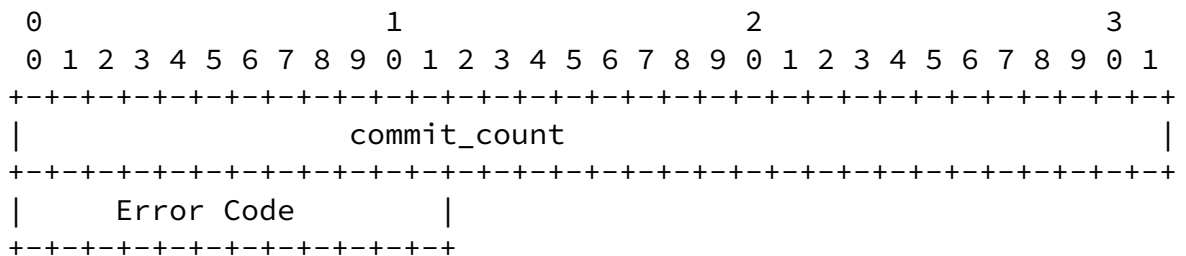


Figure 27: Filter List ACK Attribute

Type: 30 for Filter List ACK Attribute

Length: 5 Bytes

Commit_count: The first 4 bytes is committed count, to differentiate filter list packages in case of change of the filter list package.

Error Code: Code 0 is ACK; code 1 is NACK and indicates this is new dial-in subscriber, which means HAAP should teardown this user to let this user to redial; code 2 is NACK and indicates this is a existing subscriber, HAAP should sent the filter list package to this subscriber again.

[7.22.](#) End AVP

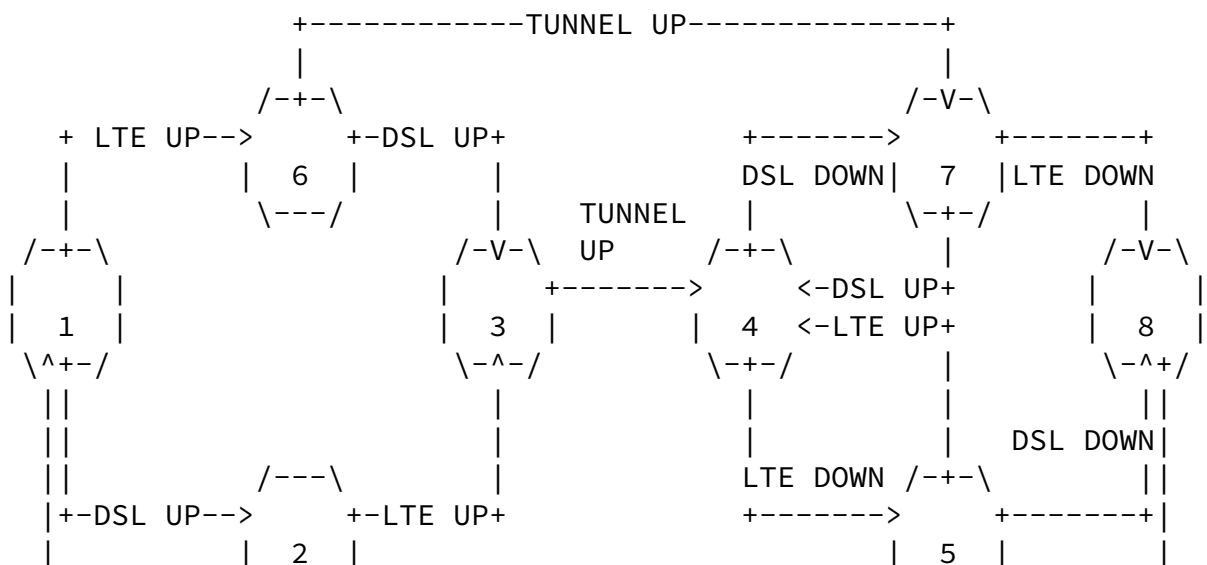
The End AVP is used to indicate that this is the last attribute contained in the GRE control messages. There is no value in End AVP.

Type: 255 for End AVP

Length: 0

[8.](#) GRE Tunnels State Machine

The following state diagram (Figure 28) represents the life cycle of HYA bonding tunnel.



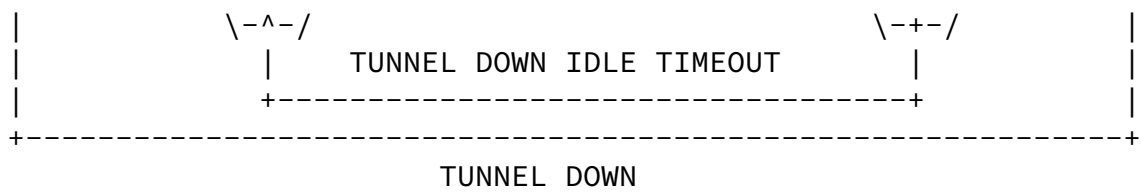


Figure 28: GRE State Machine

The various states are described as below:

State No. =====	DSL Tunnel =====	LTE Tunnel =====	Bonding Tunnel =====
1	Down	Down	Down
2	Up	Down	Down
3	Up	Up	Down
4	Up	Up	Up
5	Up	Down	Up
6	Down	Up	Down
7	Down	Up	Up
8	Down	Down	Up

Tunnel / GRE States

9. IANA Considerations

IANA is requested to allocate one code TBD for the dynamic GRE protocol.

10. Security Considerations

In the whole processing of HA, security of control messages MUST be

guaranteed. The CPE discovers the HAAP by resolving the HAAP address over DNS. This protects the CPE against connections to foreign HAAP, if the DNS service and the domain name in the CPE isn't corrupted.

The CPE should be prevented against receiving GRE notifications without a valid session. In the whole processing of end to end HAAP session establishing and GRE notification signaling, the source IP address for session establishment from CPE MUST be strictly verified, including IP address authentication and identification at the HAAP side. Any authentication mechanism with credential or checking the IP address is feasible.

GRE notification key poisoning Every new session at the HAAP generates a magic number, which is encapsulated in the key field of the GRE header and will be carried in the signalling messages and data traffic for verification by comparing the Magic Number in the message and the Magic Number in the local session table. Traffic without a valid Magic Number and outer IP address will be discarded on the HAAP. Magic number is used for both control message and data message security.

For data traffic security, it is also proposed to use IP address validation to protect against IP Spoofing attacks.

[11.](#) Acknowledgements

Many thanks to Dennis Kusidlo.

[12.](#) Normative References

[I-D.lhwxz-hybrid-access-network-architecture]

Leymann, N., Heidemann, C., Wasserman, M., and D. Zhang, "Hybrid Access Network Architecture", [draft-lhwxz-hybrid-access-network-architecture-00](#) (work in progress), June 2014.

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

- [RFC2561] White, K. and R. Moore, "Base Definitions of Managed Objects for TN3270E Using SMIV2", [RFC 2561](#), April 1999.
- [RFC2697] Heinanen, J. and R. Guerin, "A Single Rate Three Color Marker", [RFC 2697](#), September 1999.
- [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.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", [RFC 4862](#), September 2007.
- [TS23.401] "3GPP TS23.401, General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", September 2013.

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: +4961515812721
Email: heidemannc@telekom.de

Margaret Wesserman
Painless Security

Email: mrw@painless-security.com

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

Email: xueli@huawei.com

Mingui Zhang
Huawei
NO.156 Beiqing Rd. Z-park, Shi-Chuang-Ke-Ji-Shi-Fan-Yuan
Beijing, HaiDian District 100095
China

Email: zhangmingui@huawei.com