Hybrid Access

technischer Netzzugang zu Hybrid Access

Version	1.0
Stand	26.01.2017
Status	final

ERLEBEN, WAS VERBINDET.

IMPRESSUM

Herausgeber		
Deutsche Telekom Technik GmbH		
Version	**Stand**	**Status**
1.0	26.01.2017	final
Fachlicher Ansprechpartner		
Deutsche Telekom Technik GmbH Fixed Mobile Engineering Deutschland Abteilung FMED-32 64307 Darmstadt		

ÄNDERUNGSHISTORIE

Version	Stand	Bearbeiter	Änderungen / Kommentar
1.0	26.01.2017	FMED	freigegeben

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

1 ZIEL DES DOKUMENTS

Das vorliegende Dokument dient der sich aus §5 FTEG herleitenden Verpflichtung der Betreiber öffentlicher Telekommunikationsnetze, hier die Telekom Deutschland GmbH, eine technische Beschreibungen ihrer Netzzugangsschnittstellen bereitzustellen. Sie ist der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen mitzuteilen sowie zu veröffentlichen.

Dieses Dokument wurde durch die Deutsche Telekom Technik GmbH (im Folgenden als Deutsche Telekom (DT) bezeichnet) erstellt und beschreibt die Interaktion zwischen Home Gateway (HG) und dem technischen Netzzugang zum Festnetz und zum Mobilfunk, inklusive dem technischen Netzzugang zu Hybrid Access (im Folgenden „Hybrid“ genannt). „Hybrid“ bietet neben dem Zugang über das Festnetz auch einen kombinierten Zugang über Mobilfunk und Festnetz - diese Art der Anschlüsse werden im folgenden als „Hybrid-Access-Anschluss“ bezeichnet. „Hybrid“ wird von der Deutschen Telekom für ausgewählte Produkte angeboten.

Die Funktionalität „Hybrid“ wird im engen Zusammenspiel zwischen einem speziellen hybridfähigen Router am kundenseitigen Anschluss - dem Home Gateway (HG) – und dem netzseitigen Abschluss, dem „Hybrid Access Aggregation Point“ (HAAP) im Netz der Deutschen Telekom erbracht.

Die vorliegende Beschreibung soll Drittanbieter von Home Gateways in die Lage versetzen, Komponenten (Hard- und Software) zu entwickeln, welche die Nutzung des Netzanschlusses mit der Funktionalität „Hybrid“ ermöglichen. Dazu werden – unter Berücksichtigung der Rechte des Lieferanten HUAWEI – die Nachrichtenflüsse an der Schnittstelle zwischen HG und Netzzugang beschrieben, um eine grundsätzliche Kompatibilität mit der Hybrid-Access-Lösung der Deutschen Telekom sicherzustellen.

2 EINSCHRÄNKUNGEN UND RANDBEDINGUNGEN

Das vorliegende Dokument beschreibt die Interaktion zwischen HG und dem netzseitigen Abschluss, dem HAAP der Deutschen Telekom.

Auswirkungen, die aus den speziellen Eigenschaften des Festnetzes und des Mobilfunknetzes resultieren, können die Hybrid-Funktionalität beeinflussen (z.B. Laufzeitunterschiede zwischen Festnetz und Mobilfunknetz, schwankende Bandbreite durch das "shared Medium" Mobilfunk, etc.) und müssen berücksichtigt werden.

Auf Basis dieser Beschreibung können keine Anforderungen an das Netz der Deutschen Telekom abgeleitet werden. Wenn Drittanbieter Komponenten zur Nutzung des Hybrid-Access-Anschlusses bereitstellen wollen, muss sichergestellt sein, dass die Implementierung der benötigten Funktionalitäten keinen Einfluss auf die bestehende Festnetz- oder Mobilfunk-Infrastruktur hat („no harm to the network") und darüber hinaus keine gesonderten Anforderungen an die Festnetz- oder Mobilfunk-Infrastruktur gestellt werden, um Hybrid über HG von Drittherstellern zu ermöglichen.

Es liegt in der Verantwortung des HG-Herstellers, der als Drittanbieter HG anbietet, bei der Umsetzung dieser Schnittstellenbeschreibung auf eine Kompatibilität zu älteren und zukünftigen Versionen der Beschreibung zu achten: Abwärts- sowie Aufwärtskompatibilität ist sicherzustellen.

Neben dem hybridfähigen Router - dem Home Gateway (HG) - müssen weitere Voraussetzungen zur Nutzung von Hybrid beim Kundenanschluss erfüllt sein:

- Funktionsfähiger DSL-Anschluss inkl. der erforderlichen Zugangsparameter
- Freischaltung zur Nutzung von Hybrid Access auf den Systemen von DT
- vorprovisionierte SIM-Karte, die zur Nutzung von Hybrid Access im Anschlussbereich des DSL-Anschlusses (so genannte Home Zone) freigeschaltet ist
- Die aktuellen ggf. produktspezifischen Zugangsdaten (APN, Nutzername, Passwort) werden mit der Produktbuchung zur Verfügung gestellt werden
- Vollständige Konfiguration des HG zur Nutzung von Hybrid

2.1 Rechtliche Hinweise, Haftungsausschluss und Patentangelegenheiten

- **Die gesamte von der Deutschen Telekom bereitgestellte Lösung beinhaltet gewerbliche Schutzrechte von Huawei Technologies Co., Ltd. (nachfolgend HUAWEI genannt). Aus diesem Grund sind ggf. Lizenzen von HUAWEI bezüglich der Umsetzung der Schnittstellenbeschreibung erforderlich. Eine entsprechende Prüfung und ggf. eine Einholung der benötigten Lizenzen von HUAWEI obliegt dem Drittanbieter.**
- **Die Veröffentlichung der in diesem Dokument aufgeführten Informationen ist - auch auszugsweise – untersagt.**
- **Die Deutsche Telekom übernimmt keinerlei Haftung für etwaige Risiken und Auswirkungen, die sich aus der Umsetzung dieser Schnittstellenbeschreibung ergeben.**
- **Das Dokument verliert mit Veröffentlichung einer aktuelleren Version seine Gültigkeit. Die DT behält sich das Recht vor, im Rahmen von Sicherheitsmaßnahmen kurzfristig und unangekündigt Teile der Schnittstellenbeschreibung zu ändern, bzw. Zugangsinformationen anzupassen.**

2.2 Internationale Standardisierung

Die Deutschen Telekom hat sich zum Ziel gesetzt, die Lösung in internationalen Gremien zu standardisieren. Von daher wurden, zusammen mit HUAWEI, Lösungsbestandteile von Hybrid Access offen gelegt (siehe Kapitel 7, **REFERENZEN**). Informativ können daher aus den genannten Quellen weitere technische Details zur Schnittstellenbeschreibung entnommen werden. Aktuelle Implementierungen werden, nach erfolgreicher Einführung in der Wirkumgebung, in die Standardisierung eingebracht. In den einzelnen Kapiteln wird immer wieder auf diese Standardisierungsarbeiten verwiesen.

3 ALLGEMEINE FUNKTIONALITÄT HYBRID ACCESS

Der Zugang zum Netz erfolgt primär über den Festnetz-Anschluss. Bei erhöhter Datenlast (Übertragung großer Datenmengen im Down- und/oder Upload) wird zusätzlich zum Festnetz automatisch das Mobilfunknetz der Telekom in LTE-Technik verwendet, um eine höhere Datenübertragungsrate zu erreichen. Dabei werden die Daten automatisch mit erster Priorität auf Festnetz (DSL) und zweiter Priorität auf Mobilfunk (LTE) verteilt, wie in Abbildung 1 dargestellt.

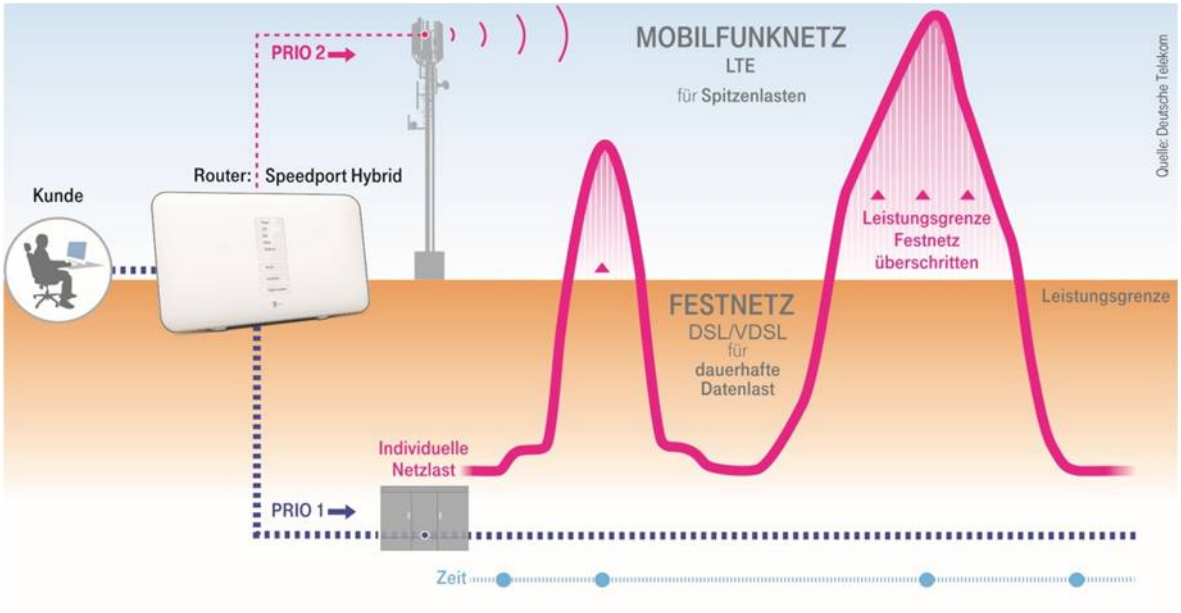

Abbildung 1: Überblick der Funktionsweise von Hybrid Access: Bedarfsorientierte Zuschaltung zusätzlicher Bandbreiten

Die Hybrid-Funktionalität wird ermöglicht, indem einerseits auf Seiten des HG, andererseits auf Seiten des HAAP die Aufteilung und Bündelung beider Datenströme softwaretechnisch implementiert wird – diese Bündelung wird als „Bonding“ bezeichnet.

Grundsätzlich ist die Hybrid-Funktionalität gemäß IETF Draft RFC „Huawei's GRE Tunnel Bonding Protocol“ [3] realisiert. Wie im RFC beschrieben, werden die zu übertragenden Daten zwischen HG und HAAP im Upstream/Downstream in den jeweiligen Endpunkten aufgeteilt und über beide Tunnel gesendet. Das HG bzw. der HAAP verteilt diese Daten automatisch paketbasiert mit erster Priorität auf Festnetz (DSL) und mit zweiter Priorität auf Mobilfunk (LTE).

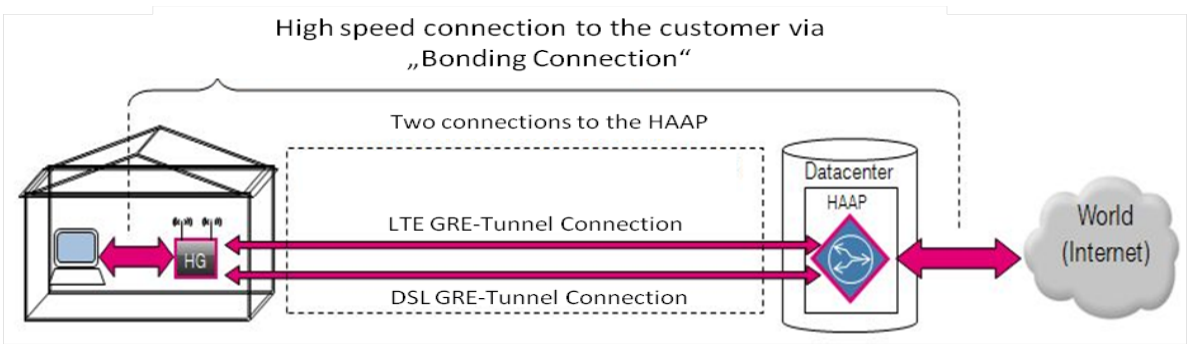

Abbildung 2: Hybrider Kanal als Kombination aus Festnetz und Mobilfunk

Zur Relisierung des Bonding wird eine Hybrid-Access-Kommunikation zwischen HG und HAAP etabliert. Zwei getunnelte Verbindungen - je eine über Festnetz und eine über Mobilfunk - werden miteinander gekoppelt („bonded“) so dass sie eine einzige logische Verbindung ergeben. Die beiden Tunnel bilden zusammen die „Bonding Connection“ (auch „Hybrid-Session“ genannt) (siehe Abbildung 2).

Das zugrundeliegende Referenzmodel ist in Abbildung 3.1 des Draft RFC „Huawei’s GRE Tunnel Bonding Protocol“ [3] dargestellt.

3.1 Control Plane

Wie im Draft RFC „Huawei’s GRE Tunnel Bonding Protocol“ [3] beschrieben, wird die Control-Plane zur Tunnel-Steuerung zwischen HG und HAAP per GRE realisiert. Die GRE-Steuerungspakete sind anhand eines eigenen GRE-Protokoll-Typs gekennzeichnet (siehe Kapitel 5.2 „GRE-Steuerungspakete für Hybrid Access“). Mit Hilfe dieser GRE-Steuerungspakete werden verschiedene Nachrichtentypen abgebildet und die einzelnen Parameter mittels unterschiedlicher Attribute übertragen.

3.2 Data Plane

Wie im Draft RFC „Huawei’s GRE Tunnel Bonding Protocol“ [3] beschrieben, werden die Datenpakete zwischen HG und HAAP per GRE enkapsuliert übertragen. Der eine GRE-Tunnel-Endpunkt liegt auf der DSL-WAN-Schnittstelle und bildet den Endpunkt des DSL-GRE-Tunnel. Der andere GRE-Tunnel-Endpunkt liegt auf der LTE-WAN- Schnittstelle und bildet den Endpunkt des LTE-GRE-Tunnel. DSL-GRE-Tunnel und LTE-GRE-Tunnel werden miteinander gekoppelt („gebondet“). Die GRE-Datenpakete, mit denen der IP-Verkehr des Kunden zwischen HG und HAAP enkapsuliert werden, sind anhand eines eigenen GRE-Protokoll-Typs gekennzeichnet (siehe Abschnitt 5.1“GRE-Datenpakete für Hybrid Access“).

Innerhalb der Hybrid-Session erhält der Kunde eine IPv4 Adresse und einen IPv6-Prefix (Dual Stack) für den Transport seines IP-Verkehres vom HG über den HAAP zum Internet.

3.3 Verkehrsaufteilung und -zusammenführung

Verkehrsaufteilung und Verkehrszusammenführung sind im Draft RFC „Huawei’s GRE Tunnel Bonding Protocol“ [3] beschrieben.

Die Verkehrsaufteilung des IP-Verkehrs des Kunden erfolgt auf Basis des „Coloring Mechanism“ nach IETF RFC 2698 [12]. Die sog. „grünen“ Pakete werden über den DSL-GRE-Tunnel übertragen, die „gelben“ Pakete über den LTE-GRE-Tunnel. Die „Commited Information Rate“ (CIR) entspricht der verfügbaren DSL-Bandbreite abzüglich der Bypass-Bandbreite auf DSL. Die verfügbare DSL-Bandbreite am Anschluss wird dem HG über GRE-Control-Pakete vom HAAP mitgeteilt. Mit erster Priorität muss immer der DSL-GRE-Tunnel verwendet werden. Erst wenn die Bandbreite des DSL-GRE-Tunnels nicht ausreicht, darf ein „Overflow“ in den LTE-GRE-Tunnel erfolgen. Die Zusammenführung der Pakete aus den beiden GRE-Tunneln geschieht auf Basis der Sequenznummer innerhalb von Re-Ordering-Buffern im HG und HAAP.

3.4 Bypassing

“Bypassing“ ist im Draft RFC „Huawei’s GRE Tunnel Bonding Protocol“ [3] beschrieben.

Alle IP-Pakete eines Kunden, die nicht in der Hybrid-Session zwischen HG und HAAP getunnelt werden, werden auf die DSL-WAN- Schnittstelle geroutet und direkt auf DSL vom HG über BRAS/BNG gesendet. Dieser Verkehr ist aus Sicht von Hybrid Access sogenannter „Bypass“-Verkehr. Gemäß Draft RFC „Huawei’s GRE Tunnel Bonding Protocol“ [3] muss der Bypass-Verkehr die DSL-Bandbreite vollständig ausnutzen können. Bypass-Verkehr ist ausschließlich über DSL zu übertragen und daher nicht bei der Verkehrsaufteilung gemäß Kapitel 3.3 zu berücksichtigen. Die verfügbare Bandbreite für den DSL-GRE-Tunnel ist gleich der verfügbaren DSL-Bandbreite abzüglich der Bypass-Bandbreite. Damit der HAAP die Kapazität des DSL-GRE-Tunnels berechnen kann, muss das HG die Downstream Bypass-Bandbreite messen und in Echtzeit an den HAAP melden (AVP #6 „Bypass Traffic Rate“).

Über GRE-Control-Nachrichten sendet der HAAP eine Liste mit Verkehrstypen, die im HG als Bypass-Verkehre direkt auf die DSL-WAN-Schnittstelle geroutet werden müssen und nicht in der Hybrid-Session übertragen werden dürfen. Diese Verkehrstypen werden mittels sog. Filter-List-Pakete und Filter-List-TLV übermittelt und müssen vom HG zwingend angewendet werden.

Im Netz von DT werden alle IP-Pakete einer Hybrid-Session ausschließlich als „Best-Effort"-Verkehre behandelt. Deshalb müssen alle Verkehre, die eine qualitativ hochwertigere Behandlung im Netz erfordern, außerhalb der Hybrid-Session im Bypass-Verkehr geführt werden.

Die Nutzung des Mobilfunks ist ausschließlich zum Aufbau der Konnektivität zum HAAP über LTE und zur Übertragung von GRE-Paketen zum HAAP vorgesehen. Ein Bypass in LTE wird nicht unterstützt.

4 ANFORDERUNGEN AN DAS HOME GATEWAY

Netzwerkseitig verbindet sich das HG sowohl über das Festnetz (DSL) als auch über das mobile Netz (LTE). Hier gelten die einschlägigen Schnittstellenbeschreibungen für DSL-Anschlüsse und LTE im Netz der Deutschen Telekom, welche als bekannt vorausgesetzt und deshalb nicht erneut dargestellt werden.

Folgende Mindestanforderungen sind zu erfüllen:

- DSL:
  Für ADSL und VDSL gilt hierbei 1TR112 [2], wobei SDSL und GPON nicht unterstützt werden. VDSL2 Profile 35b ("Super Vectoring"), das in der nächsten Version der 1TR112 enthalten sein wird, wird derzeit nicht durch Hybrid Access unterstützt.
- LTE:
  Für LTE gilt die „Schnittstellenbeschreibung für das Mobilfunknetz der Telekom Deutschland GmbH" [1]. Es ist ausschließlich eine Nutzung über LTE zum HAAP vorgesehen. Eine Nutzung von GPRS und UMTS wird nicht unterstützt.
  - Der Hybrid-Access-Verkehr, der im LTE übertragen wird, muss mit einem betreiberspezifischen QCI-Wert gemäß 3GPP gekennzeichnet werden. Hierbei ist der QCI = 159 (Best Effort) zwingend vom HG zu verwenden.
- DNS:
  Für den Tunnelaufbau sind die DNS-Server der Deutschen Telekom zu verwenden, die im Rahmen der Einwahl verhandelt werden. Folgende DNS Priorität ist dabei anzuwenden:
  - 1. DSL IPv6 (primary/secondary)
  - 2. DSL IPv4 (primary/secondary)
  - 3. LTE IPv6 (primary/secondary)
- Routerspezifische Parameter:
  Im HG sind alle notwendigen netzspezifischen Parameter zu hinterlegen:
  - APN und LTE-Zugangsdaten: werden bei Vertragsabschluss zur Verfügung gestellt
  - FQDN der HAAP Service-Adresse: „haap.t-online.de"
  - Client Identification Name (CIN):
    muss für die jeweilige Hersteller/HW/SW-Kombination eineindeutig sein und ist mit DT abzustimmen.
- Hybrid Access spezifische Funktionalitäten:
  Es sind alle Anforderungen dieser Beschreibung des technischen Netzzugangs zu unterstützen.

5 GRE-PAKETE FÜR DIE KOMMUNIKATION ZWISCHEN HG UND HAAP

Zum Tunnelaufbau, zur Enkapsulierung und für die Kommunikation zwischen HAAP und HG wurde das GRE-Protokoll ausgewählt. Der verwendete GRE-Header basiert auf IETF RFC 1701 („Generic Routing Encapsulation“, [7]) und IETF RFC 2784 („Generic Routing Encapsulation (GRE)“, [8]) sowie IETF RFC 2890 („Key and Sequence Number Extensions to GRE“, [9]). Der generische GRE-Header ist in IETF Draft RFC „Huawei’s GRE Tunnel Bonding Protocol“ [3] grundsätzlich definiert und wird wie folgt verwendet.

Bits 0 - 3				4 - 12	13 - 15	16 - 31
C		K	S	Reserved	Version	Protocol Type
Checksum (optional – nicht bei Hybrid verwendet)						Offset (optional – nicht bei Hybrid verwendet)
Key (optional)						
Sequence Number (optional)						
Routing (optional – nicht bei Hybrid verwendet)						

Abbildung 3: Definition des generischen GRE-Header

Nach IETF Draft RFC „Huawei’s GRE Tunnel Bonding Protocol“ [3] sind folgende Arten von GRE-Paket-Typen für Hybrid Access definiert:

- GRE-Datenpakete, mit denen der IP-Verkehr des Kunden zwischen HG und HAAP enkapsuliert wird
- GRE-Steuerungspakete, mit denen die Tunnel-Steuerung zwischen HG und HAAP erfolgt

5.1 GRE-Datenpakete für Hybrid Access

GRE-Datenpakete dienen der Enkapsulierung des IP-Verkehr des Kunden und enthalten ausschließlich IP-Pakete. Ihr Format folgt grundsätzlich den Festlegungen gemäß IETF Draft RFC „Huawei’s GRE Tunnel Bonding Protocol“ [3].

GRE Data Packet Format																															
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
C		K	S	Reserved0									Ver			Protocol Type (0x0800 bzw. 0x86DD)															
Key (Bonding Key Value)																															
Sequence Number																															

Abbildung 4: GRE-Header für Datenpakete für IP-Pakete

Die einzelnen Felder werden folgendermaßen verwendet:

- “C“: “Checksum Present” = “0”
- “ ”: = “0”
- “K“: „Key Present“ = “1”
- “S”: “Sequence Number Present” = “1”
- “Reserved”: =”0”
- “Ver”: “Version” = “0“
- “Protocol Type”:
  = “0x0800” für IPv4 Verkehr innerhalb des Tunnel bzw.
  = “0x86DD” für IPv6 Verkehr innerhalb des Tunnel
- “Key“: „Bonding Key Value“: Zufallszahl, die für die gesamte Hybrid-Session (Bonding Connection) gilt
- “Sequence-Number”: Sequenznummer

5.2 GRE-Steuerungspakete für Hybrid Access

Die Tunnel-Steuerung zwischen HG und HAAP erfolgt mit Hilfe der GRE-Steuerungspakete. GRE-Steuerungspakete sind grundsätzlich über eine Kombination von Message Type/Attribute Type/Data Value (AVP) definiert. Format und Inhalt folgen grundsätzlich den Festlegungen in IETF Draft RFC „Huawei's GRE Tunnel Bonding Protocol" [3].

<table>
<tr><th colspan="32">GRE Control Message Format</th></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td>C</td><td></td><td>K</td><td>S</td><td colspan="12">Reserved0</td><td colspan="4">Ver</td><td colspan="16">Protocol Type (0x0101)</td></tr>
<tr><td colspan="32">Key (Bonding Key Value)</td></tr>
<tr><td colspan="8">MsgType</td><td>T</td><td colspan="4">Res</td><td colspan="12">Attribute Type</td><td colspan="16">Attribute Length</td></tr>
<tr><td colspan="32">Attribute Value</td></tr>
</table>

Abbildung 5: Definition des GRE-Headers zur Steuerung

Die einzelnen Felder werden folgendermaßen verwendet:

- "C": "Checksum Present" = "0"
- " ": = "0"
- "K": „Key Present" = "1"
- "S": "Sequence Number Present" = "0"
- "Reserved0": "Reserved" = "0"
- "Ver": "Version" = "0"
- "Protocol Type": = "0x0101"
- "Key": „Bonding Key Value": Zufallszahl, die für die gesamte Hybrid-Session (Bonding Connection) gilt.
- „MsgType": Message Type
  „1" = GRE Tunnel Setup Request
  „2" = GRE Tunnel Setup Accept
  „3" = GRE Tunnel Setup Deny
  „4" = GRE Tunnel Hello
  „5" = GRE Tunnel Tear Down
  „6" = GRE Tunnel Notify
  „10" = GRE Link Detection
  alle anderen Werte: reserved
- „T": Tunnel Type
  = „0" = LTE Control Message ist für den LTE-GRE-Tunnel bestimmt
  =„1" = Control Message ist für den DSL-GRE-Tunnel bestimmt
- „Res" = „0", alle anderen Werte sind reserviert
- Attribut: alle Attribute, die innerhalb einer Control-Nachricht übertragen werden sollen.
  Jedes Attribut besteht aus:
  - Attribute Type (1 Byte)
  - Attribute Length (2 Byte)
  - Attribute Value (variable)

Anmerkung: Die Codierung der Felder „Tunnel Type" und „Res" ist wie oben beschrieben vorzunehmen. Diese weicht von der Beschreibung in IETF Draft RFC „Huawei's GRE Tunnel Bonding Protocol" [3] ab.

5.2.1 GRE Tunnel Setup Request

„GRE Tunnel Setup Request“ ist im IETF Draft RFC „Huawei’s GRE Tunnel Bonding Protocol“ [3] beschrieben. Diese Nachricht wird vom HG verwendet, um die beiden LTE- und DSL-GRE-Tunnel zum HAAP aufzubauen. Die verwendeten Attribute sind ebenfalls in [3] definiert:

- Client Identification Name (CIN), die CIN muss für die jeweilige Hersteller/HW/SW-Kombination eindeutig sein und ist mit DT abzustimmen
- Session ID
- DSL Synchronization Rate downstream (Layer 2, unkorrigiert)
- Und weitere DT-spezifische Attribute, die verpflichtend unterstützt werden müssen:
    - DSL Synchronization Rate upstream (Layer 2, unkorrigiert)
      Attribute Type: 59
      Attribute Length: 4 Byte
      Attribute Value: unsigned integer (kbps)
    - DSL protocol / Link Type
      Attribute Type: 53
      Attribute Length: 4 Byte
      Attribute Value:
      -> 0: undefiniert
      -> 1: ADSL/ADSL2/ADSL2+ Annex B
      -> 2: ADSL2+ Annex J
      -> 3: VDSL2
      -> 4: VDSL Vectoring
    - BRAS name:
      Attribute Type: 54
      Attribute Length: 32 byte
      Attribute Value: BRAS-Name (aus PPP)
    - End AVP:
      Attribute Type: 255
      Attribute Length: 0 byte

5.2.2 GRE Tunnel Setup Accept

„GRE Tunnel Setup Accept“ ist im IETF Draft RFC „Huawei’s GRE Tunnel Bonding Protocol“ [3] beschrieben. Mit dieser Nachricht teilt der HAAP dem HG mit, dass der Tunnel-Aufbau erlaubt ist und übermittelt dem HG die zu verwendenden Parameter. Die verwendeten Attribute sind ebenfalls im Draft RFC „Huawei’s GRE Tunnel Bonding Protocol“ definiert:

- H IPv6 Address
- Session ID
- RTT Difference Threshold
- Bypass Bandwidth Check Interval
- Active Hello Interval
- Hello Retry Times
- Idle Timeout
- Bonding Key Value
- Configured DSL Upstream Bandwidth (Layer 3)
- Configured DSL Downstream Bandwidth (Layer 3)
- RTT Difference Threshold Violation
- RTT Difference Threshold Compliance
- Idle Hello Interval
- No Traffic Monitored Interval

- Weitere DT-spezifische Attribute, die verpflichtend unterstützt werden müssen:
  - Maximum downstream reordering buffer time
    Attribute Type: 56
    Attribute Length: 4 Byte
    Attribute Value: unsigned Integer in Millisekunden (ms)
  - Committed Upstream Burst Time
    Attribute Type: 57
    Attribute Length: 4 Byte
    Attribute Value: unsigned Integer in Millisekunden (ms)
  - End AVP

Das Attribut #1 "H IPv4 Address" wird im Netz von DT nicht verwendet, da die GRE-Tunnel ausschließlich mittels IPv6 etabliert werden.

5.2.3 GRE Tunnel Setup Deny

„GRE Tunnel Deny" ist im IETF Draft RFC „Huawei's GRE Tunnel Bonding Protocol" [3] beschrieben. Diese Nachricht wird vom HAAP gesendet, wenn die „GRE Setup Request"-Nachricht abgelehnt wird. Das HG muss dann sofort den Tunnel-Aufbau-Prozess beenden. Das verwendete Error-Attribute ist ebenfalls in [3] definiert. Die Error-Codes sind DT-spezifisch und werden als Hex-Wert in den 4 Byte des AVP dargestellt.

- Error Code:
  - 401: DSL GRE tunnel to the HAAP failed
  - 402: LTE GRE tunnel to the HAAP failed
  - 403: Mismatch of LTE and DSL User IDs
  - 404: Session with the same User ID already exists.
  - 405: Client uses a not permitted CIN
  - 406: Communication error during the DSL Tunnel setup
  - 407: Communication error during the LTE Tunnel setup
  - 501: Maintenance reasons
- End AVP

5.2.4 GRE Tunnel Hello

„GRE Tunnel Hello" ist im IETF Draft RFC „Huawei's GRE Tunnel Bonding Protocol" [3] beschrieben. Diese Nachricht wird vom HG in regelmäßigen Abständen über die Tunnel gesendet. Der HAAP quittiert jede „Hello"-Nachricht. Die verwendeten Attribute sind ebenfalls in [3] definiert:

- Timestamp
- IPv6 Prefix Assigned by HAAP
- End AVP

5.2.5 GRE Tunnel Tear Down

„GRE Tunnel Tear Down" ist im IETF Draft RFC „Huawei's GRE Tunnel Bonding Protocol" [3] beschrieben. Diese Nachricht wird vom HAAP an das HG gesendet, um die Tunnel zu beenden. Das verwendete Error-Attribute und ist ebenfalls in [3] definiert:

- Error Code: siehe Abschnitt 5.2.3 und zusätzlich
  - 502: HAAP terminates LTE Tunnel for Update of Parameters
  - 503: HAAP terminates DSL Tunnel for Update of Parameters
- End AVP

Je nach verwendetem Error Code werden entweder der DSL-Tunnel, der LTE-Tunnel oder die Hybrid-Session terminiert.

5.2.6 GRE Tunnel Notify

„GRE Tunnel Notify“ ist im IETF Draft RFC „Huawei’s GRE Tunnel Bonding Protocol“ [3] beschrieben. Diese Nachricht wird vom HAAP und/oder vom HG verwendet, um Statusinformationen und Filterlisten auszutauschen. Der HAAP bzw. das HG quittiert jede „Notify“-Nachricht. Die verwendeten Attribute sind ebenfalls in [3] definiert:

- Bypass Traffic Rate
- Filter List Package
    - Filter List TLVs <-> Type
        - FQDN [RFC1594] <-> 1
        - DSCP [RFC2724] <-> 2
        - Destination Port <-> 3
        - Destination IP <-> 4
        - Destination IP&Port <-> 5
        - Source Port <-> 6
        - Source IP <-> 7
        - Source IP&Port <-> 8
        - Source Mac <-> 9
        - Protocol <-> 10
        - Combination <-> 15 (DT spezifisch)
        - Reserved <->
- Switching to DSL Tunnel
- Overflowing to LTE Tunnel
- DSL Link Failure
- LTE Link Failure
- IPv6 Prefix Assigned to Host
- Filter List Package ACK
- Switching to Active Hello State
- Switching to Idle Hello State
- Tunnel Verification
- End AVP

Die Diagnostic-Attribute #26 - #29 werden im Netz von DT nicht verwendet.

Im Netz von DT können weitere Attribute in einer „Notify“-Nachricht enthalten sein, die gemäß IETF Draft RFC „Huawei’s GRE Tunnel Bonding Protocol“ [3] in der „Tunnel-Setup-Accept“-Nachricht definiert sind. Hierdurch wird es möglich, auch während einer bestehenden Hybrid-Session Parameter zu ändern. Folgende Attribute müssen auch in der „GRE Tunnel Notify“-Nachricht verpflichtend unterstützt werden:

- RTT Difference Threshold
- Bypass Bandwidth Check Interval
- Active Hello Interval
- Hello Retry Times
- Idle Timeout
- RTT Difference Threshold Violation
- RTT Difference Threshold Compliance
- Idle Hello Interval
- No Traffic Monitored Interval
- Maximum downstream reordering buffer time
- Committed Upstream Burst Time

6 STEUERUNG DER KOMMUNIKATION ZWISCHEN HG UND HAAP

6.1 Tunnelaufbau

Die GRE-Tunnel müssen selbstständig durch das HG aufgebaut werden. Dabei ist der Ablauf nach IETF Draft RFC „Huawei's GRE Tunnel Bonding Protocol", Abschnitt 6.2 „Automatic Setup of GRE Tunnels "[3], zu beachten.

Nachdem das HG erfolgreich die Erstinbetriebnahme abgeschlossen hat, kann die Hybrid-Session aufgebaut werden. Sobald eine LTE-Verbindung verfügbar ist, beginnt der GRE-Tunnelaufbau für LTE und anschließend der GRE-Tunnelaufbau für DSL.

1. Während der Einwahl in das Mobilfunknetz bzw. in das Festnetz erhält das HG jeweils eine IPv6 Adresse für die LTE-WAN-Schnittstelle (per PDP) bzw. für die DSL-WAN- Schnittstelle (per PPPoE). Das HG erhält die Service-Adresse des HAAP durch einen DNS-Request für die Domain „haap.t-online.de".
2. Das HG startet automatisch den Aufbau der beiden Tunnel, dabei verwendet das HG die beiden IPv6 WAN-Adressen als Source-IP-Adressen für den GRE-Tunnelaufbau. Die Ziel-IP-Adresse ist die Service-Adresse des HAAP. Es ist zwingend notwendig, erst den LTE-GRE-Tunnel und danach den DSL-GRE-Tunnel aufzubauen. Das HG sendet eine „GRE Setup Request"-Nachricht an die Service-Adresse des HAAP über die LTE-WAN-Schnittstelle. Die „GRE Setup Request"-Nachricht muss das AVP #3 (CIN) enthalten. Das Feld „Bonding Key Value" muss für dieses erste „LTE GRE Setup request" auf „0" gesetzt sein. Der HAAP veranlasst die Authentifizierung und Autorisierung des HG für den LTE-Anteil.
3. Nach erfolgreicher Autorisierung des Kunden schickt der HAAP eine „GRE Setup Accept"-Nachricht über LTE zum HG zurück. Als Parameter werden darin u.a. AVP #2 (IPv6 address), AVP #4 (Session ID) sowie AVP #20 (Bonding Key Value) übergeben. Ab diesem Zeitpunkt verwendet das HG diese „IPv6 address" als HAAP-Tunnel-Transit-IP-Adresse für alle folgenden GRE-Steuerungs- und GRE-Datenpakete. Der „Bonding Key Value" muss in allen folgenden GRE-Steuerungsnachrichten und GRE-Datenpaketen übernommen werden.
   Falls die Autorisierung nicht erfolgreich ist, schickt der HAAP eine passende Fehlernachricht an das HG („GRE Tunnel Setup Deny"-Nachricht über LTE). In diesem Fall wird der DSL-GRE-Tunnel nicht aufgebaut und der gesamte IP-Verkehr des Kunden wird direkt über DSL übertragen. Wenn das HG nicht innerhalb von 5 Sekunden eine positive Antwort erhält, muss das HG bis zu neunmal erneut versuchen, die Verbindung aufzubauen (inkrementelle Verzögerung 1, 2, 4, 8, 16, 34, 64, 128, 256 Sekunden). Nach dem zehnten erfolglosen Verbindungsversuch darf das HG erst wieder nach 600 Sekunden einen Setup-Request senden.
4. Nach dem erfolgreichen Aufbau des LTE-GRE-Tunnel sendet das HG über die DSL-Schnittstelle eine „GRE Setup Request"-Nachricht incl. CIN, Session ID, Bonding Key, DSL Synchronization Rate downstream und DSL Synchronization Rate upstream an die HAAP-Tunnel-Transit-IP-Adresse. Der HAAP veranlasst die Authentifizierung und Autorisierung des HG für den DSL-Anteil.
5. Nach der erfolgreichen Autorisierung des HG antwortet der HAAP mit einem „GRE Setup Accept". Diese Meldung enthält die für den DSL-GRE- Tunnel notwendigen Steuerungsparameter, u.a. die verfügbaren Bandbreiten für DSL (upstream/downstream) (AVP #22, AVP #23).
   Falls die Autorisierung auf DSL nicht erfolgreich ist, sendet der HAAP eine „GRE Setup Deny"-Nachricht an das HG. Das HG muss daraufhin den DSL-GRE-Tunnelaufbau beenden. Daneben sendet der HAAP eine „GRE Tear Down"-Nachricht über LTE an das HG. Daraufhin muss das HG den LTE-Tunnel abbauen.

6.2 Tunnel ist erfolgreich aufgebaut

Nachdem die Tunnel aufgebaut sind, erfolgt die weitere Kommunikation zwischen HG und HAAP per „GRE-Notify"-Nachrichten, „GRE Hello"-Nachrichten und per DHCP/DHCPv6.

6.2.1 IP-Adresszuweisung und -bindung

Die IP-Adresszuweisung und die Adressbindung erfolgt per DHCP/DHCPv6 (siehe [10] und [11]). Sobald ein GRE-Tunnel zwischen HG und HAAP aufgebaut ist, kann das HG per DHCP/DHCPv6 öffentlich routbare IP Adressen vom HAAP beziehen. Das DHCP-Protokoll wird innerhalb von speziellen GRE-Datenpaketen übertragen („S" = „0").

Die vom HAAP zugeteilte öffentliche IPv4 Adresse muss vom HG zur Network Address Translation (NAT) verwendet werden für allen IP-Verkehr des Kunden, der über die Hybrid-Session übertragen wird.

Das HG signalisiert den bei der DSL-Einwahl vom Access Server zugewiesenen IPv6 Präfix an den HAAP per „GRE Notify"-Nachricht mit AVP #21. Endgeräte, die lokal an das HG angeschlossen werden, erhalten bei Bedarf eine IPv6 Adresse aus diesem Bereich. Der vom HAAP zugewiesene IPv6 Präfix darf nur verwendet werden, wenn DSL nicht verfügbar ist. Der DSL- Präfix muss dann im LAN als invalid gekennzeichnet werden.

Ist die Zuweisung der IPv4 bzw. IPv6 Adresse nicht erfolgreich, wiederholt das HG die DHCP Discover bzw. DHCPv6 Solicit Messages fünfmal nach einem festgelegten Zeitschema: 1 – 2 – 4 – 8 – 16 Sekunden. Wenn nach fünfmaliger Wiederholung der Adressanforderung die Adresszuordnung immer noch nicht erfolgreich aufgebaut werden konnte, muss auf dem HG die Session terminiert werden und anschließend wieder neu gestartet werden mit einer „GRE Setup Request"-Nachricht über die LTE-WAN-Schnittstelle.

6.2.2 Bypass-Bandbreite

Nach erfolgreichem Aufbau des DSL-GRE-Tunnels muss das HG sofort über den DSL-GRE-Tunnel eine „GRE Notify"-Nachricht zum HAAP mit der aktuellen" Bypass Traffic Rate" (AVP #6) an den HAAP senden. Nach IETF Draft RFC „Huawei's GRE Tunnel Bonding Protocol" [3] muss das HG die Bypass-Bandbreite in regelmäßigen Abständen an den HAAP melden.

6.2.3 Tunnel-Maintenance

Es werden verschiedene Tunnel-Maintance-Funktionen umgesetzt: Monitoring des Tunnel Status, Keep Alive sowie Steuerung des Active/Idle Hello. Gemäß IETF Draft RFC „Huawei's GRE Tunnel Bonding Protocol" [3] werden diese Funktionen mittels „GRE Hello"- und „GRE Notify"-Nachrichten realisiert.

Sobald die Tunnel aufgebaut sind, beginnt das HG sofort auf jedem Tunnel „GRE Hello"-Nachrichten in regelmäßigen Abständen zu senden und die vom HAAP quittierten „Hello"-Nachrichten zu empfangen. Die „GRE Hello"-Nachrichten ermöglichen, den Tunnel zu überwachen.

Mittels „GRE Notify"-Nachrichten werden Informationen über den Status zwischen HG und HAAP ausgetauscht.

Die Steuerung des Idle/Active Hello –Zustandes im LTE-Tunnel erfolgt mittels „GRE Notify"-Nachrichten (AVP #33, #34).

6.2.4 Änderung von Parametern innerhalb einer bestehenden Session

Während des Tunnelaufbaus übermittelt der HAAP innerhalb der „GRE Setup Accept"-Nachricht verschiedene Parameter an das HG. Auch während einer bestehenden Hybrid-Session kann der HAAP einige dieser Parameter ändern. Die Änderung kann erfolgen, ohne dass die Tunnel abgebaut werden müssen. Zur Änderung der Parameter werden folgende AVP innerhalb von „GRE Notify"-Nachrichten verwendet: AVP #9, #10, #14, #15, #16, #24, #25, #31, #32, #56 und #57.

Die Änderung kann erfolgen, ohne die vollständige Hybrid-Session zu terminieren. Dazu wird nur derjenige GRE-Tunnel abgebaut, dessen Parameter geändert werden soll. Der HAAP sendet eine „GRE Tear Down"-Nachricht mit Error Code 502 bzw. 503.

6.3 Tunnelabbau

Nach IETF Draft RFC „Huawei's GRE Tunnel Bonding Protocol" [3] erfolgt Tunnel-Maintenance über den Austausch von „GRE Hello"-Nachrichten bzw. deren Quittierung. Wenn das HG auf Basis der „GRE Hello"-Nachrichten eine Verbindungsunterbrechung erkennt, sendet das HG eine „GRE Notify"-Nachricht mit einem DSL bzw. LTE Link Failure AVP (AVP #18, #19) an den HAAP. Daraufhin terminiert der HAAP lokal den signalisierten Tunnel.

Der HAAP kann auch aus anderen Gründen (z.B. Wartungsarbeiten) die Hybrid-Session oder einzelne GRE-Tunnel durch eine „GRE Tear Down"-Nachricht beenden. Je nach Ursache werden entweder der DSL-Tunnel, der LTE-Tunnel oder die Hybrid-Session terminiert und anschließend vom HG wieder neu aufgebaut.

7 REFERENZEN

[1] Telekom Deutschland GmbH: „Schnittstellenbeschreibung für das Mobilfunknetz der Telekom Deutschland GmbH“, Bonn 19.07.2011, https://www.telekom.de/hilfe/downloads/schnittstellenbeschreibung_telekom_deutschland_gmbh_07_2011.pdf

[2] Deutsche Telekom Technik GmbH „1TR112, Technical Specification of the U-Interfaces of xDSL Systems in the network of Deutsche Telekom. Version 12.3“, Stand 03 / 2015, https://www.telekom.de/hilfe/downloads/1tr112.zip

[3] Internet Engineering Task Force: IETF Draft RFC “Huawei's GRE Tunnel Bonding Protocol”, Version 5 vom 21. 12.2016, https://datatracker.ietf.org/doc/draft-zhang-gre-tunnel-bonding/

[4] Internet Engineering Task Force: IETF Draft RFC “Hybrid Access Network Architecture”, Version 2 vom 13.01. 2015, https://datatracker.ietf.org/doc/draft-lhwxz-hybrid-access-network-architecture/

[5] Internet Engineering Task Force: IETF Draft RFC “Flow Control for Bonding Tunnels”, Version 0 vom 21.03.2016, https://datatracker.ietf.org/doc/draft-zhang-banana-tcp-in-bonding-tunnels/

[6] Internet Engineering Task Force: IETF Draft “Problem Statement: Bandwidth Aggregation for Internet Access”, Version 3 vom 31.10.2016, https://datatracker.ietf.org/doc/draft-zhang-banana-problem-statement/

[7] Internet Engineering Task Force: IETF RFC 1701: "Generic Routing Encapsulation", Oktober 1994, https://datatracker.ietf.org/doc/rfc1701/

[8] Internet Engineering Task Force: IETF RFC 2784: "Generic Routing Encapsulation (GRE)", März 2000, https://datatracker.ietf.org/doc/rfc2784/

[9] Internet Engineering Task Force: IETF RFC 2890: “Key and Sequence Number Extensions to GRE”, Update zu [8], September 2000, https://datatracker.ietf.org/doc/rfc2890/

[10] Internet Engineering Task Force: IETF RFC 2131: “Dynamic Host Configuration Protocol (DHCP)”, März 1997, https://datatracker.ietf.org/doc/rfc2131/

[11] Internet Engineering Task Force: IETF RFC 3315: “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, Juli 2003, https://datatracker.ietf.org/doc/rfc3315/

[12] Internet Engineering Task Force: IETF RFC 2698: “A Two Rate Three Color Marker”, September 1999, https://datatracker.ietf.org/doc/rfc2698/

[13] Broadband Forum: TR-348: “Hybrid Access Broadband Network Architecture”, Issue 1, Juli 2016, insb. Abschnitt 5.4.1 (L3 Overlay Tunneling), S. 25, https://www.broadband-forum.org/technical/download/TR-348.pdf

8 ABKÜRZUNGEN

Abkürzung	Erklärung
3GPP	3rd Generation Partnership Project
ACK	Acknowledge
ADSL	Asymmetric Digital Subscriber Line
APN	Access Point Name
AVP	Attribute Value Pair (dt. „Attribut-Wert-Paar“)
BNG	Broadband Network Gateway
BRAS	Broadband Remote Access Server
CIN	Client Identification Name bzw. Client Identification Number
CIR	Commited Information Rate
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSCP	6-Bit Codepoint (DSCP) im Differentiated Services Field (DS Field)
DSL	Digital Subscriber Line
DT	Deutsche Telekom
FTEG	Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen
FQDN	Fully Qualified Domain Name
GPON	Gigabit Passive Optical Network
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
HA	Hybrid Access
HAAP	Hybrid Access Aggregation Point
HG	Home Gateway
HUAWEI	Huawei Technologies Co., Ltd.
HW	Hardware
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
LAN	Local Area Network
LTE	Long Term Evolution: Standard for wireless communication of high-speed data for mobile phones and data terminals
NAT	Network Access Translation
PDP	Packet Data Protocol
PPPoE	Point to point protocol over Ethernet
QCI	QoS Class Identifier, a mechanism to ensure proper Quality of Service for bearer traffic in LTE networks
QoS	Quality Of Service
RFC	Request For Comments
RTT	Round Trip Time
SDSL	Symmetric Digital Subscriber Line
SIM	Subscriber Identity Module
SW	Software
TLV	Type Length Value

TR	Technical Report
UMTS	Universal Mobile Telecommunications System
VDSL	Very High Bitrate Digital Subscriber Line
WAN	Wide Area Network