Integrity Protection at RLC/MAC

1. INTRODUCTION

In order to prevent any possibility to steal bandwidth, control messages sent over the air interface and related to radio resource allocation should be integrity protected. While in UTRAN resource allocation is handled by RRC protocol, it is taken care of by both RRC *and* MAC protocols in GERAN, thus integrity protection should apply -in GERAN- both on RRC and on RLC/MAC control messages with a "RR" flavour. Therefore unless a major redesign of the (RLC)MAC protocol is involved [1], the following RLC/MAC control messages should be integrity protected:

- Packet Resource Request (UL)
- Packet Uplink Assignment (DL)
- Packet Downlink Assignment (DL)
- Packet UL Ack/Nack (fixed allocation possible)
- Packet Timeslot Reconfigure (DL)
- Packet TBF Release (DL)
- Packet Cell Change Order (DL)

Having integrity protection at RLC/MAC level implies additional overhead (authentication code) to the above messages. Due to this, TSG GERAN has foreseen the potential problems below:

- Need for new segmentation mechanisms in case the authentication code makes the message to which it applies span over more than 2 radio blocks (Downlink case) or 1 radio block (Uplink case).
- Different security levels on CCCH and PCCCH for the same system: messages on CCCH cannot be segmented as no segmentation mechanism exists today on CCCH.
- Overhead when integrity protection causes segmentation.

It was highlighted in TSG GERAN#4 that there should not be any cases where integrity protection would not apply, as a security hole in the system is more harmful than some additional overhead. Further the need for additional segmentation would not only be caused by integrity protection but most likely by some new features in GERAN Rel5 like multiple TBFs.

2. INTEGRITY PROTECTION: PRINCIPLE

The principle of integrity protection is depicted below.

The "count" input is yet to be defined in GERAN. It is ffs whether the RTI (Radio Transaction Identifier) field of RLC/MAC Control blocks can be used for this purpose.

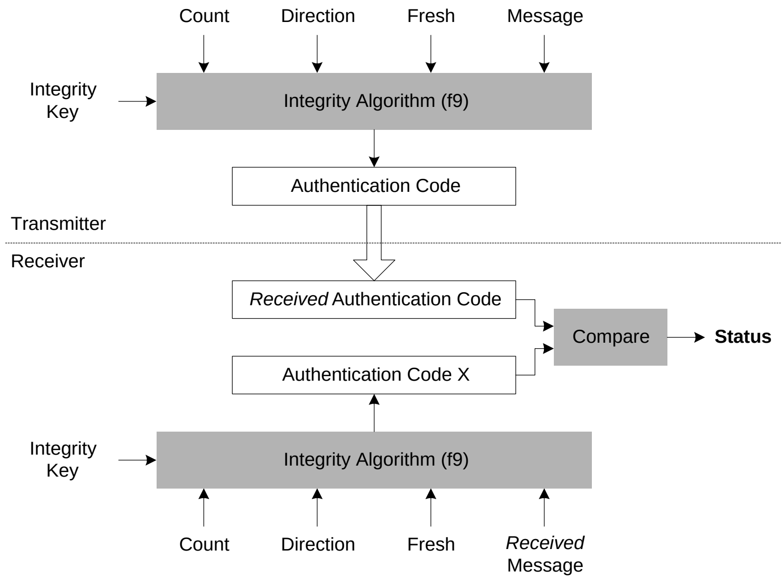


Figure 1. Principle of integrity protection

3. APPLICABILITY OF INTEGRITY PROTECTION AT RLC/MAC LEVEL

Integrity protection may only apply if the MS is assigned:

- a G-RNTI by the network (*MS is in RRC Connected Mode*)
- an integrity protection key, and MS and network are synchronized (input parameters to be used are known and same on both MS and network sides).

Therefore, *integrity protection may not apply at initial TBF establishment* (transition from RRC Idle Mode to RRC Connected Mode). Integrity protection at RLC/MAC level may occur when RLC/MAC procedures are used for assigning resources, the MS being in RRC_GRA_PCH or RRC_Cell_Shared State.

The figures below illustrate the applicability of integrity protection when the two conditions above are fulfilled. PCCCH, CCCH and PACCH cases are depicted for both UL and DL TBF establishment procedures:

<table>
<tr><th>Cases</th><th>RRC State transition</th><th>MAC State transition</th></tr>
<tr><td>a</td><td rowspan="8">RRC_GRA_PCH → RRC Cell Shared</td><td rowspan="8">MAC Idle → MAC Shared</td></tr>
<tr><td>b</td></tr>
<tr><td>c</td></tr>
<tr><td>d</td></tr>
<tr><td>e</td></tr>
<tr><td>f</td></tr>
<tr><td>g</td></tr>
<tr><td>h</td></tr>
<tr><td>i</td><td rowspan="2">RRC Cell Shared ↻</td><td rowspan="2">MAC Shared ↻</td></tr>
<tr><td>j</td></tr>
</table>

As can be seen:

- Integrity protection may apply in DL only when contention resolution is solved on network side i.e. when the network knows exactly the target MS.
- Integrity protection may apply in UL only when contention resolution is solved on MS side i.e. the MS knows it is uniquely identified by the network.

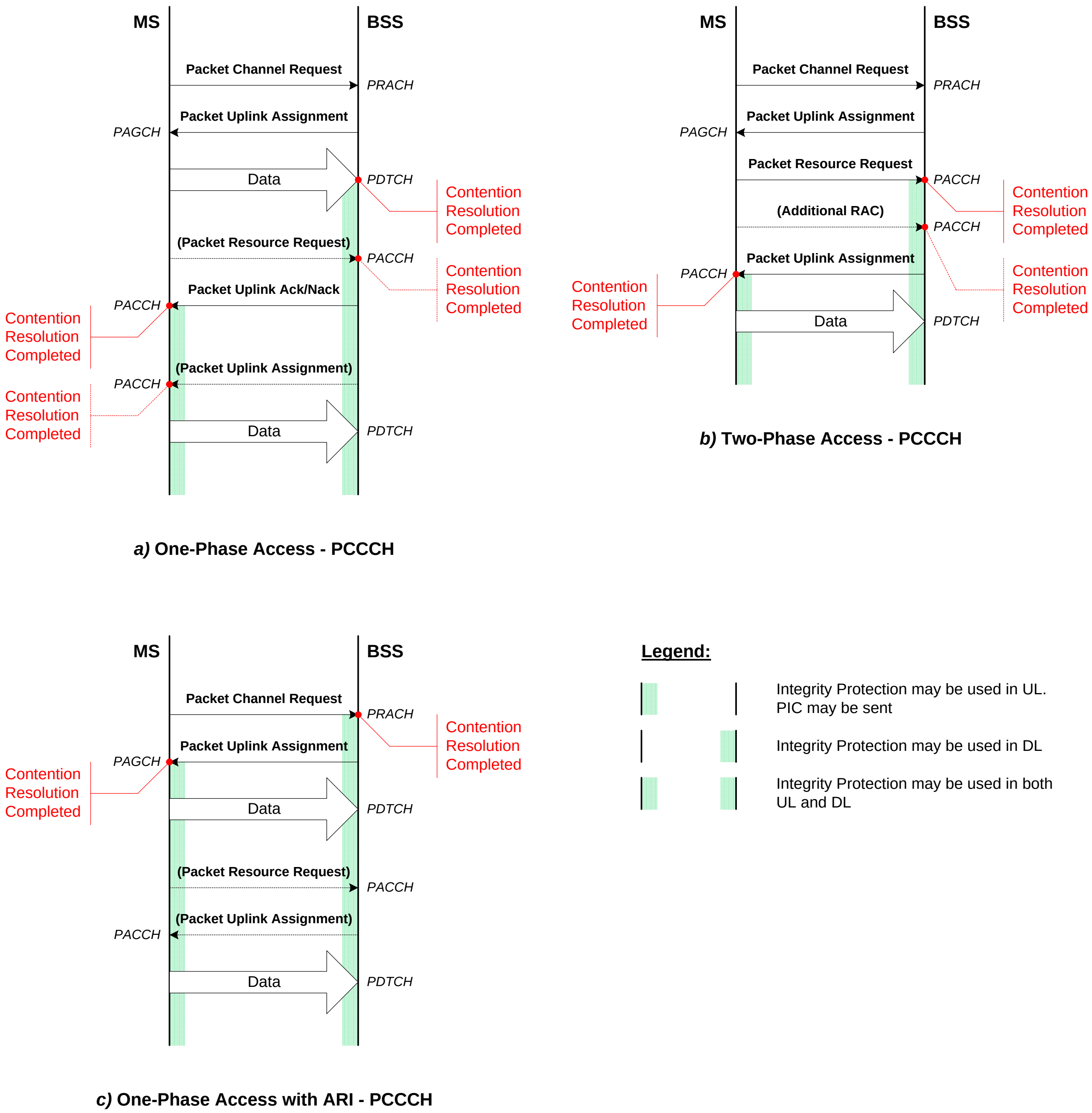
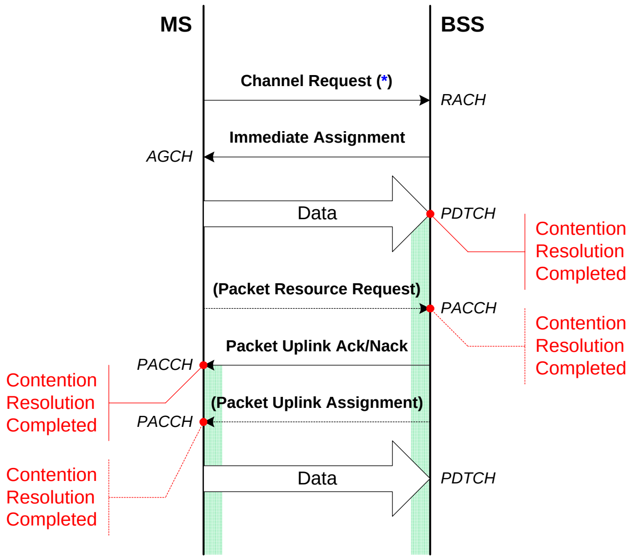
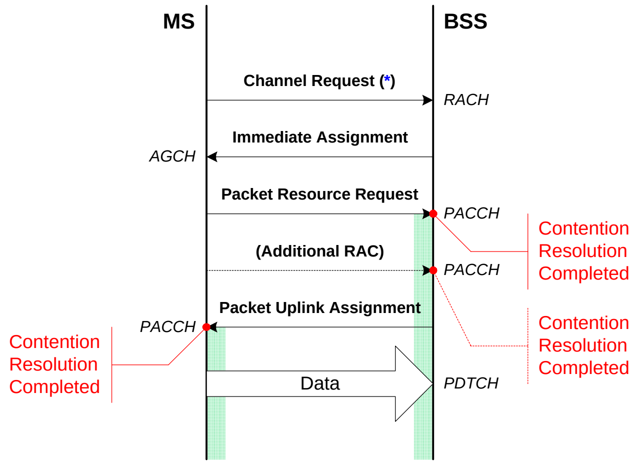


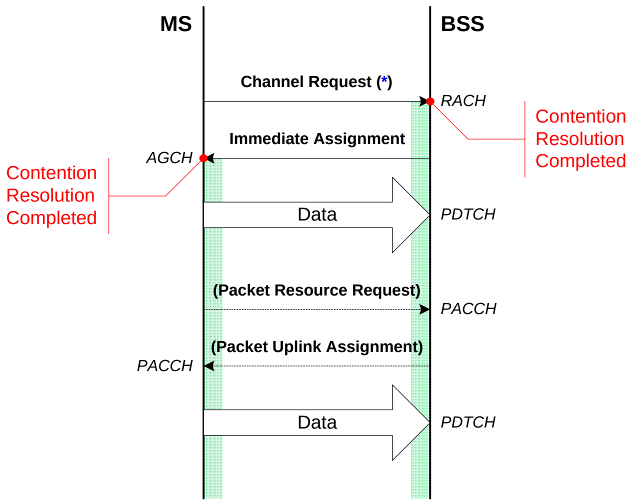
Figure 2. Applicability of integrity protection for UL TBF establishment on PCCCH



***d)* One-Phase Access - CCCH**



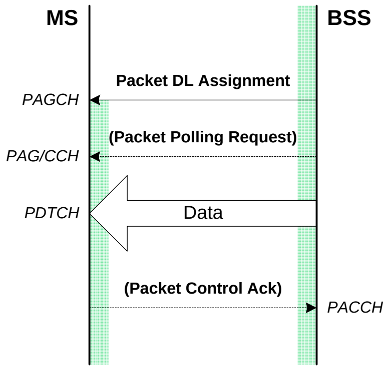
***e)* Two-Phase Access - CCCH**



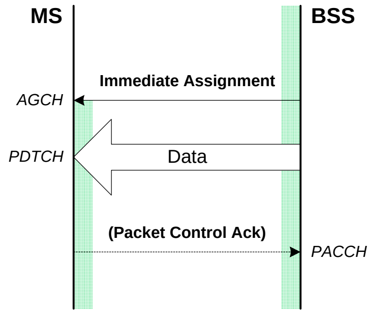
(*) EGPRS Packet Channel Request if supported

***f)* One-Phase Access with ARI - CCCH**

Figure 3. Applicability of integrity protection for UL TBF establishment on CCCH

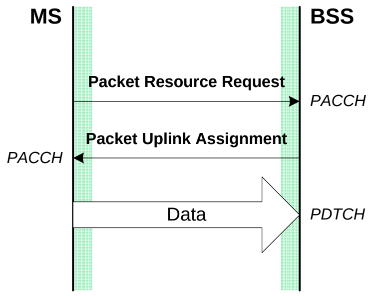


g) **DL TBF Establishment - PCCCH**

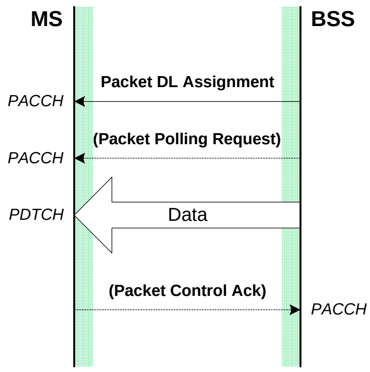


h) **DL TBF Establishment - CCCH**

Figure 4. Applicability of integrity protection for DL TBF establishment on (P)CCCH



i) **UL TBF Establishment - PACCH**



j) **DL TBF Establishment - PACCH**

Figure 5. Applicability of integrity protection for TBF establishment on PACCH

Based on the cases a) to j) the table below summarizes per message when integrity protection is not possible or should apply.

Cases		Packet Resource Request	Packet Uplink Assignment	(Packet) Immediate Assignment	Packet Downlink Assignment
PCCCH	*a)* 1PA	Not possible	Not possible before contention resolution is solved	-	-
	b) 2PA	Not possible	1st phase: Not possible 2nd phase: Should apply	-	-
	c) 1PA – ARI	Should apply after contention resolution - see case *i)* MS RAC already known(1) (ARI assigned): No segmentation problem.	Should apply	-	-
CCCH	*d)* 1PA	Not possible	-	Not possible	-
	e) 2PA	Not possible	2nd phase: Should apply	1st phase: Not possible	-
	f) 1PA – ARI	Should apply after contention resolution - see case *i)* MS RAC already known (ARI assigned): No segmentation problem.	-	Should apply (PUA/EGPRS PUA construction) (2)	-
g) DL TBF PCCCH		-	-	-	Should apply
h) DL TBF CCCH		-	-	Should apply (PDA construction) (2)	-
i) UL TBF PACCH		Should apply MS RAC already known (ARI assigned): No segmentation problem.	Should apply	-	-
j) DL TBF PACCH		-	-	-	Should apply

(1) The indication of the MS RAC should be made at initial TBF establishment.
(2) Two-message assignment procedure is possible. See 44.018.

Note: 1PA: One Phase Access
2PA: Two Phase Access
PRR: Packet Resource Request
P[U/D]A: Packet Uplink/Downlink Assignment
IA: Immediate Assignment
MS RAC: Mobile Station Radio Access Capabilities

Table 1. Applicability of Integrity Protection per message at TBF establishment

4. LENGTH OF RLC/MAC CONTROL MESSAGES WITH MAC-I

This section summarizes based on the analysis made in §3 the outcome from the calculations given in [2] and in appendix A.

- Packet Resource Request: 32-bit MAC-I may be introduced w/o any segmentation.
- Packet Uplink Assignment: 32-bit MAC-I may be introduced w/o any new segmentation.
- Packet Downlink Assignment: 32-bit MAC-I may be introduced w/o any new segmentation.
- Packet Uplink Ack/Nack: 32-bit MAC-I may be introduced w/o any new segmentation. Possible restriction on the fixed allocation bitmap.
- Packet TBF Release: 32-bit MAC-I may be introduced w/o any segmentation.

- Packet Timeslot Reconfigure: 32-bit MAC-I may be introduced w/o any new segmentation.
- Packet Cell Change Order: open.

- Immediate Assignment (EGPRS Packet Uplink Assignment/Packet Uplink Assignment/Packet Downlink Assignment construction): Variable size MAC-I with a minimum size may be introduced w/o any new segmentation in the IA Rest Octets IE.

No problem is induced by the introduction of a 32-bit MAC-I at RLC/MAC level, on the messages with an "RR flavour". The status of Packet Cell Change Order is open, however it is believed that a variable size MAC-I with a minimum guaranteed size can be introduced without any need for a new segmentation mechanism.

5. CONCLUSIONS

This document highlights that no major redesign of the RLC/MAC protocols is needed for supporting integrity protection of RR flavoured RLC/MAC control messages, as the existing segmentation mechanism is enough. Therefore, MAC-I must be introduced in all RLC/MAC control messages dealing with resource allocation. Depending on the frequency of the cases where integrity protection causes segmentation, a minimum size MAC-I could be considered. However if the overhead due to this segmentation is acceptable, a 32-bit MAC-I should be introduced in all cases. The status of Packet Cell Change Order is open, however it is believed that a variable size MAC-I with a minimum guaranteed size can be introduced. The same would apply to Immediate Assignment for TBF establishment.

Though addressing the extreme cases for the different messages (maximum size), this paper does not address the cases where the authentication code for integrity protection causes segmentation from one to two radio blocks.

6. REFERENCES

[1] 3GPP TSG GERAN#4, Tdoc GP-010570, " Reply to LS on integrity protection for GERAN ", TSG SA3, 2-6 April, 2001, Biarritz, France

[2] 3GPP TSG GERAN#4, Tdoc GP-010981, " Length of RLC/MAC control messages", Alcatel, 2-6 April, 2001, Biarritz, France

A. APPENDIX 1: LENGTH OF RLC/MAC CONTROL MESSAGES

A.1 Packet Resource Request

The table below shows the size of the Packet Resource Request when sent on PACCH (case *i)*) assuming MS RAC are not resent.

<table>
<tr><td>< Packet Resource Request message content > ::=</td><td>Message Size:</td></tr>
<tr><td>{ 0 | 1 < ACCESS_TYPE : bit (2) > }</td><td>1 no response to PRACH access</td></tr>
<tr><td>{ 0 < Global TFI : < Global TFI IE > ></td><td>1+6 G-RNTI not needed</td></tr>
<tr><td>| 1 < TLLI : < TLLI IE > > }</td><td>-</td></tr>
<tr><td>{ 0 | 1 < MS Radio Access Capability : < MS Radio Access Capability IE > > }</td><td>1 not included</td></tr>
<tr><td>< Channel Request Description : < Channel Request Description IE > ></td><td>24</td></tr>
<tr><td>{ 0 | 1 < CHANGE_MARK : bit (2) > }</td><td>1+2 valid change mark</td></tr>
<tr><td>< C_VALUE : bit (6) ></td><td>6</td></tr>
<tr><td>{ 0 | 1 < SIGN_VAR : bit (6) >}</td><td>1 not present (EGPRS mode)</td></tr>
<tr><td>{ 0 | 1 < I_LEVEL_TN0 : bit (4) > }</td><td>1 |</td></tr>
<tr><td>{ 0 | 1 < I_LEVEL_TN1 : bit (4) > }</td><td>1 |</td></tr>
<tr><td>{ 0 | 1 < I_LEVEL_TN2 : bit (4) > }</td><td>1 |</td></tr>
<tr><td>{ 0 | 1 < I_LEVEL_TN3 : bit (4) > }</td><td>1 |> not present (EGPRS mode)</td></tr>
<tr><td>{ 0 | 1 < I_LEVEL_TN4 : bit (4) > }</td><td>1 |</td></tr>
<tr><td>{ 0 | 1 < I_LEVEL_TN5 : bit (4) > }</td><td>1 |</td></tr>
<tr><td>{ 0 | 1 < I_LEVEL_TN6 : bit (4) > }</td><td>1 |</td></tr>
<tr><td>{ 0 | 1 < I_LEVEL_TN7 : bit (4) > }</td><td>1 |</td></tr>
<tr><td>{ null | 0 bit** = <no string> -- Receiver backward compatible with earlier version</td><td></td></tr>
<tr><td>| 1 -- Additional contents for Release 1999</td><td>1</td></tr>
<tr><td>{ 0 | 1 < EGPRS BEP Link Quality Measurements : < EGPRS BEP Link Quality Measurements IE >> }</td><td>1 incl only if no segmentation implied</td></tr>
<tr><td>{ 0 | 1 < EGPRS Timeslot Link Quality Measurements : < EGPRS Timeslot Link Quality Measurements IE >>}</td><td>1 incl only if no segmentation implied</td></tr>
<tr><td>{ 0 | 1 < PFI: bit(7) > }</td><td>1 Not used in Rel5</td></tr>
<tr><td>< ADDITIONAL MS RAC INFORMATION AVAILABLE : bit (1) ></td><td>1</td></tr>
<tr><td>< RETRANSMISSION OF PRR : bit (1) ></td><td>1</td></tr>
<tr><td>< padding bits > };</td><td></td></tr>
<tr><td></td><td>Total:
57 bits</td></tr>
</table>

Similarly, the message size for a Pre-Rel99 TBF mode (no segmentation mechanism possible in UL) would be: 51 bits (no I_LEVEL measurements sent), and for a Rel99 GPRS TBF mode (PFI included): 64 bits.

Therefore no segmentation problem is foreseen with Packet Resource Request message, a 32 bit MAC-I can be introduced (113 bits are free: 184 - 8 [MAC header] – 6 [Message Type] -57).

Link quality measurements could also be included.

A.2 Packet Timeslot Reconfigure

The table below shows the maximum size of the Packet Timeslot Reconfigure message.

<table>
<tr><td>< Packet Timeslot Reconfigure message content > ::=</td><td>Message Size:</td></tr>
<tr><td>< PAGE_MODE : bit (2) ></td><td>2</td></tr>
<tr><td>{0 < GLOBAL_TFI : < Global TFI IE > ></td><td>1 + 6</td></tr>
<tr><td></td><td></td></tr>
<tr><td>{ 0 -- Message escape</td><td>1</td></tr>
<tr><td>{< CHANNEL_CODING_COMMAND : bit (2) ></td><td>2</td></tr>
<tr><td>< Global Packet Timing Advance : < Global Packet Timing Advance IE > ></td><td>23</td></tr>
<tr><td>< DOWNLINK_RLC_MODE : bit (1) ></td><td>1</td></tr>
<tr><td>< CONTROL_ACK : bit (1) ></td><td>1</td></tr>
<tr><td>{ 0 | 1 < DOWNLINK_TFI_ASSIGNMENT : bit (5) > }</td><td>1</td></tr>
<tr><td>{ 0 | 1 < UPLINK_TFI_ASSIGNMENT : bit (5) > }</td><td>1+5 Uplink TBF</td></tr>
<tr><td>< DOWNLINK_TIMESLOT_ALLOCATION : bit (8) ></td><td>8</td></tr>
<tr><td>{ 0 | 1 < Frequency Parameters : < Frequency Parameters IE > > }</td><td>1+40 Direct Encoding 2 used</td></tr>
<tr><td>{ 0 < Dynamic Allocation : < Dynamic Allocation struct > ></td><td>1+104 Maximum Size</td></tr>
<tr><td>| 1 < Fixed allocation : < Fixed Allocation struct > >}</td><td>-</td></tr>
<tr><td>{ null | 0 bit** = < no string > -- Receiver backward compatible</td><td>1</td></tr>
<tr><td>| 1 -- Additions for R99</td><td></td></tr>
<tr><td>{ 0 | 1 <Packet Extended Timing Advance : bit (2)> }</td><td>1 + 2</td></tr>
<tr><td>< padding bits > }</td><td></td></tr>
<tr><td>! < Non-distribution part error : bit (*) = < no string > > }</td><td></td></tr>
<tr><td>| 1-- Message escape bit used to define EGPRS message contents</td><td>1</td></tr>
<tr><td>{ 00 { { 0 | 1 < COMPACT reduced MA : < COMPACT reduced MA IE >> }</td><td>2 + 1 COMPACT not used</td></tr>
<tr><td>< EGPRS Channel Coding Command : < EGPRS Modulation and Coding IE >></td><td>4</td></tr>
<tr><td><Resegment : < Resegment IE >></td><td>1</td></tr>
<tr><td>{ 0 | 1 < DOWNLINK EGPRS Window Size : < EGPRS Window Size IE >}</td><td>1</td></tr>
<tr><td>{ 0 | 1 < UPLINK EGPRS Window Size : < EGPRS Window Size IE >}</td><td>1+ 5</td></tr>
<tr><td>< LINK_QUALITY_MEASUREMENT_MODE : bit (2) ></td><td>2</td></tr>
<tr><td>< Global Packet Timing Advance : < Global Packet Timing Advance IE > ></td><td>23</td></tr>
<tr><td>{ 0 | 1 <Packet Extended Timing Advance : bit (2)> }</td><td>2</td></tr>
<tr><td>< DOWNLINK_RLC_MODE : bit (1) ></td><td>1</td></tr>
<tr><td>< CONTROL_ACK : bit (1) ></td><td>1</td></tr>
<tr><td>{ 0 | 1 < DOWNLINK_TFI_ASSIGNMENT : bit (5) > }</td><td>1</td></tr>
<tr><td>{ 0 | 1 < UPLINK_TFI_ASSIGNMENT : bit (5) > }</td><td>1+ 5</td></tr>
<tr><td>< DOWNLINK_TIMESLOT_ALLOCATION : bit (8) ></td><td>8</td></tr>
<tr><td>{ 0 | 1 < Frequency Parameters : < Frequency Parameters IE > > }</td><td>1+40 Direct Encoding 2 used</td></tr>
<tr><td>{ 0 < Dynamic Allocation : < Dynamic Allocation struct > ></td><td>1+104 Maximum Size</td></tr>
<tr><td>| 1 < Fixed allocation : < Fixed Allocation struct > >}</td><td>-</td></tr>
<tr><td>< padding bits ></td><td>Total:</td></tr>
<tr><td>! < Non-distribution part error : bit (*) = < no string > > }</td><td>GPRS Pre-Rel99: 198</td></tr>
<tr><td>! < Message escape : { 01| 10 | 11} bit (*) = <no string> > }} –Extended for future changes</td><td>GPRS Rel99: 201
EGPRS: 215</td></tr>
<tr><td>! < Address information part error : bit (*) = < no string > > }</td><td></td></tr>
<tr><td>! < Distribution part error : bit (*) = < no string > > ;</td><td></td></tr>
</table>

Note: Direct Encoding 1 not used for description of the Frequency Parameters

With the maximum configuration used, the message needs to be segmented (RLC/MAC Control block header: 24 bits for each block of the segmentation). 320 bits aof payload are available for a segmentation into two blocks which implies that:

– GPRS Pre-Rel99: 116 bits are free (320-6 [message type]-198)
– GPRS Rel99: 113 bits are free (320-6-201)
– EGPRS: 99 bits are free (320-6-215).

I.e. a 32-bit MAC-I can be introduced without any need for a further segmentation mechanism.

A.3 Packet TBF Release

The table below shows the maximum size of the Packet TBF Release message.

< Packet TBF Release message content > ::=	**Message Size:**
< **PAGE_MODE** : bit (2) >	2
{0 < **GLOBAL_TFI** : Global TFI IE >	1 + **5**
{< **UPLINK_RELEASE** : bit (1) >	1
< **DOWNLINK_RELEASE** : bit (1) >	1
< **TBF_RELEASE_CAUSE** : bit (4) = { 0000 | 0010 } >	4
< padding bits >	Total:
! < Non-distribution part error : bit (*) = < no string > > }	**14 bits**
! < Address information part error : bit (*) = < no string > > }	
! < Distribution part error : bit (*) = < no string > > ;	

A 32-bit MAC-I may be introduced without any need for segmentation.

A.4 Packet Uplink Ack/Nack

A fixed allocation mobile station may also be assigned uplink resources with Packet Uplink Ack/Nack.

<table>
<tr><td>< Packet Uplink Ack/Nack message content > ::=</td><td>**Message Size:**</td></tr>
<tr><td>< **PAGE MODE** : bit (2) ></td><td>2</td></tr>
<tr><td>{00 < **UPLINK_TFI** : bit (5) ></td><td>2 + **5**</td></tr>
<tr><td>{ 0 -- *Message escape*</td><td>1</td></tr>
<tr><td>{ < **CHANNEL_CODING_COMMAND** : bit (2) ></td><td>2</td></tr>
<tr><td>< **Ack/Nack Description** : < Ack/Nack Description IE > ></td><td>72 no trunc.</td></tr>
<tr><td>{ 0 | 1 < **CONTENTION_RESOLUTION_TLLI** : bit (32) > }</td><td>1+**32**</td></tr>
<tr><td>{ 0 | 1 < **Packet Timing Advance** : < Packet Timing Advance IE > > }</td><td>1+**15**</td></tr>
<tr><td>{ 0 | 1 < **Power Control Parameters** : < Power Control Parameters IE > > }</td><td>1+**52** 8TS</td></tr>
<tr><td>{ 0 | 1 < **Extension Bits** : Extension Bits IE > } -- *sub-clause 12.26*</td><td>1</td></tr>
<tr><td>{ 0 | 1 < **Fixed Allocation Parameters** : < Fixed Allocation struct > > }</td><td>1+**166**</td></tr>
<tr><td>{ null | 0 bit** = < no string > -- *Receiver backward compatible with earlier version*</td><td></td></tr>
<tr><td>| 1 -- *Additions for R99*</td><td>1</td></tr>
<tr><td>{ 0 | 1 <**Packet Extended Timing Advance** : bit (2)>}</td><td>1+**2**</td></tr>
<tr><td><**TBF_EST** : bit (1)></td><td>1</td></tr>
<tr><td>< padding bits > }</td><td></td></tr>
<tr><td>! < Non-distribution part error : bit (*) = < no string > > }</td><td></td></tr>
<tr><td>| 1 -- *Message escape bit used to define EGPRS message contents*</td><td>1</td></tr>
<tr><td>{ 00 { < **EGPRS Channel Coding Command** : < EGPRS Modulation and Coding IE >></td><td>2+**4**</td></tr>
<tr><td><**Resegment** : < Resegment IE >></td><td>1</td></tr>
<tr><td><**PRE_EMPTIVE_TRANSMISSION** : bit (1) ></td><td>1</td></tr>
<tr><td>**< PRR RETRANSMISSION REQUEST** : bit (1) ></td><td>1</td></tr>
<tr><td>< **ARAC RETRANSMISSION REQUEST** : bit (1) ></td><td>1</td></tr>
<tr><td>{ 0 | 1 < **CONTENTION_RESOLUTION_TLLI** : bit (32) > }</td><td>1+**32**</td></tr>
<tr><td><**TBF_EST** : bit (1)></td><td>1</td></tr>
<tr><td>{ 0 | 1 < **Packet Timing Advance** : < Packet Timing Advance IE > > }</td><td>1+**32**</td></tr>
<tr><td>{ 0 | 1 <**Packet Extended Timing Advance** : bit (2)> }}</td><td>1+**2**</td></tr>
<tr><td>{ 0 | 1 < **Power Control Parameters** : < Power Control Parameters IE > > }</td><td>1+**52** 8TS</td></tr>
<tr><td>{ 0 | 1 < **Extension Bits** : Extension Bits IE > } -- *sub-clause 12.26*</td><td>1</td></tr>
<tr><td>{ < **EGPRS Ack/Nack Description** : < EGPRS Ack/Nack Description IE > ></td><td>15+n Or 23+n Trunc. if needed</td></tr>
<tr><td>{ 0 | 1 < **Fixed Allocation Parameters** : < Fixed Allocation struct > > } } //</td><td>1+**166**</td></tr>
<tr><td>< padding bits ></td><td></td></tr>
<tr><td>! < Non-distribution part error : bit (*) = < no string > > }
! < Message escape : {01| 10 | 11} bit (*) = <no string> > } } – *Extended for future changes*
! < Address information part error : bit (*) = < no string > > }</td><td>Note: n=bitmap size (uncompressed or compressed). n=64 was used in the calculation.</td></tr>
<tr><td>! < Distribution part error : bit (*) = < no string > > ;</td><td>Total:
GPRS Pre-Rel: 354 (188)
GPRS Rel99: 359 (193)
EGPRS: 398 (232)
In parenthesis is the size w/o the fixed allocation parameters.</td></tr>
</table>

<table>
<tr><td>< Fixed Allocation struct > ::=</td><td></td></tr>
<tr><td>< **FINAL_ALLOCATION** : bit (1) ></td><td>1</td></tr>
<tr><td>{ 0 *-- Repeat Allocation*</td><td></td></tr>
<tr><td>< **TS_OVERRIDE** : bit (8) ></td><td></td></tr>
<tr><td>| 1 *-- Allocation with Allocation bitmap*</td><td>1</td></tr>
<tr><td>< **TBF Starting Time** : < Starting Frame Number Description IE > ></td><td>17 absolute frame nr encoding</td></tr>
<tr><td>{ 0 | 1 <**TIMESLOT_ALLOCATION** : bit (8) > }</td><td>1+**8**</td></tr>
<tr><td>{ 0 { 0 *-- with length of Allocation Bitmap*</td><td>1+1</td></tr>
<tr><td>< **BLOCKS_OR_BLOCK_PERIODS** : bit (1) ></td><td>1</td></tr>
<tr><td>< **ALLOCATION_BITMAP_LENGTH** : bit (7) ></td><td>7</td></tr>
<tr><td>< **ALLOCATION_BITMAP** : bit (val(ALLOCATION_BITMAP_LENGTH)) ></td><td>128</td></tr>
<tr><td>| 1 *-- without length of Allocation Bitmap (fills remainder of the message)*</td><td></td></tr>
<tr><td>< **ALLOCATION_BITMAP** : bit ** > }</td><td>**166**</td></tr>
<tr><td>! < Message escape : 1 bit (*) = <no string> >;}</td><td></td></tr>
</table>

As can be seen, the message with its maximum size cannot even be sent neither in GPRS nor in EGPRS when allocating fixed allocation resources with a full allocation bitmap of 128bits. In order to avoid introducing a new segmentation mechanism, a smaller allocation bitmap could be used. This would also allow the introduction of a 32-bit MAC-I without any need for further segmentation mechanism.

With the configuration used, GPRS Pre-Rel99 offers 126 free bits to accommodate the fixed allocation parameters and a 32-bit MAC-I, GPRS Rel99 offers 121 free bits, and EGPRS 82 free bits. Introducing the MAC-I, 55 bits (GPRS Pre-Rel99), 50bits (GPRS Rel99), 50 bits (EGPRS) are free for the fixed allocation bitmap. Also, considering an allocation over less than 8 timeslots makes bits free for the bitmap. The impact of reducing the amount of bits for the fixed allocation bitmap is seen as negligible.

Note: it should be noted that for the GPRS case, the acknowledgement bitmap is included (64 bits). In EGPRS, the acknowledgement bitmap may be truncated. In the calculation above it was set to 64 bits although a shorter size is possible.

A 32-bit MAC-I may be introduced without any need for segmentation, upon a few restrictions (limited fixed allocation).

A.5 Packet Cell Change Order

<table>
<tr><td>< Packet Cell Change Order message content > ::=
< **PAGE_MODE** : bit (2) >
{ { 0 < **Global TFI** : < Global TFI IE > >
| 10 < **TLLI** : bit (32) > }
{ 0
{ < **IMMEDIATE_REL** : bit >
< **GSM target cell:** < GSM target cell struct >>
! < Non-distribution part error : bit (*) = < no string > > }
| 1
{ 00 -- *Message escape*
{ < **IMMEDIATE_REL** : bit >
< **3G-target cell:** < 3G-target cell struct >>
! < Non-distribution part error : bit (*) = < no string > > }
! < Message escape : { 01 | 10 | 11} bit (*) = <no string> > } }
! < Address information part error : bit (*) = < no string > > }
! < Distribution part error : bit (*) = < no string > > ;</td><td>**Message Size:**
2

2+**32**
1
1
?

1
2
1
57

Total:
3G Target Cell: 97 bits
GSM Target Cell:</td></tr>
<tr><td>< GSM target cell struct > ::=
< **ARFCN** : bit (10) >
< **BSIC** : bit (6) >
< **NC Measurement Parameters** : < NC Measurement Parameters struct > >
{ null | 0 bit ** = < no string > -- *Receiver compatible with earlier release*
| 1 -- *Additions in release 98 :*
{ 0 | 1 < **LSA Parameters** : < LSA Parameters IE >> }
{ null | 0 bit ** = < no string > -- *Receiver compatible with earlier release*
| 1 -- *Additions in release 99 :*
< **ENH Measurement parameters** : < ENH Measurement parameters struct >>
{ null | 0 bit ** = < no string > -- *Receiver compatible with earlier release*
| 1 -- *Additions in release R4 :*
< **CCN_ACTIVE** : bit (1) >
{ 0 | 1 < **CONTAINER_ID** : bit (2) > }

< padding bits > } } } ;</td><td>
10
6
?>298

1
?</td></tr>
<tr><td>< 3G-target cell struct > ::=
{ 0 | 1 < **FDD-ARFCN** : bit (14) >
-- 3G UMTS FDD
< **Diversity** : bit >
{ 0 | 1 < **Bandwidth_FDD** : bit (3) > }
< **SCRAMBLING_CODE** : bit (9) > }
{ 0 | 1 < **TDD-ARFCN** : bit (14) >
-- 3G UMTS TDD
< **Diversity** : bit >
{ 0 | 1 < **Bandwidth_TDD** : bit (3) > }
< **Cell Parameter** : bit (7) >
< **Sync Case** : bit > }
< padding bits > ;</td><td>
1+**14**

1
1+**3**
9
1+**14**

1
1+**3**
7
1

57</td></tr>
<tr><td>< NC Measurement Parameters struct > ::=
< **NETWORK_CONTROL_ORDER** : bit (2) >
{ 0 | 1 < **NC_NON_DRX_PERIOD** : bit (3) >
< **NC_REPORTING_PERIOD_I** : bit (3) >
< **NC_REPORTING_PERIOD_T** : bit (3) > }
{ 0 | 1 < **NC_FREQUENCY_LIST** : NC Frequency list struct > } ;</td><td>
2
1+**3**
3
3
1+**?>285**</td></tr>
<tr><td>< NC Frequency list struct > ::=
{ 0 | 1 < **NR_OF_REMOVED_FREQ** : bit (5) >
{ < **REMOVED_FREQ_INDEX** : bit (6) > } * (1 + val(NR_OF_REMOVED_FREQ)) }
{ 1 < **List of added Frequency** : < Add Frequency list struct > >} ** 0;</td><td>
1+**5**
6**32**

1+**?>86**
>285</td></tr>
</table>

<table>
<tr><td>< Add Frequency list struct > ::=
< START_FREQUENCY : bit (10) >
< BSIC : bit (6) >
{ 0 | 1 < Cell selection params : < Cell Selection struct > > }
< NR_OF_FREQUENCIES : bit (5) >
< FREQ_DIFF_LENGTH : bit (3) >
{ < FREQUENCY_DIFF : bit (val(FREQ_DIFF_LENGTH)) >
< BSIC : bit (6) >
{ 0 | 1 < Cell selection params :
< Cell Selection struct > > } } * (val(NR_OF_FREQUENCIES));</td><td>
10
6
1+47
5
3
8
6
1+?

>86</td></tr>
<tr><td>< Cell Selection struct > ::=
< CELL_BAR_ACCESS_2 : bit (1) >
< EXC_ACC : bit >
< SAME_RA_AS_SERVING_CELL : bit (1) >
{ 0 | 1 < GPRS_RXLEV_ACCESS_MIN : bit (6) >
< GPRS_MS_TXPWR_MAX_CCH : bit (5) > }
{ 0 | < GPRS_TEMPORARY_OFFSET : bit (3) >
< GPRS_PENALTY_TIME : bit (5) > }
{ 0 | 1 < GPRS_RESELECT_OFFSET : bit (5) > }
{ 0 | 1 < HCS params : < HCS struct > > }
{ 0 | 1 < SI13_PBCCH_LOCATION : < SI13_PBCCH_LOCATION struct > > } ;</td><td>
1
1
1
1+6
5
1+3
5
1+5
1+8
1+7
47</td></tr>
<tr><td>< SI13_PBCCH_LOCATION struct > ::=
{ 0 < SI13_LOCATION : bit (1) >
| 1 < PBCCH_LOCATION : bit (2) >
< PSI1_REPEAT_PERIOD : bit (4) > } ;</td><td>

1+2
4
7</td></tr>
<tr><td>< HCS struct > ::=
< PRIORITY_CLASS : bit (3) >
< HCS_THR : bit (5) > ;</td><td>
3
5
8</td></tr>
<tr><td>< ENH Measurement parameters struct > :: =
{ 0 < BA_IND : bit > < 3G_BA_IND : bit > | 1 < PSI3_CHANGE_MARK : bit(2) > }
< PMO_IND : bit >
< REPORT_TYPE : bit >
< REPORTING_RATE : bit >
< UNKNOWN_BSIC_REPORTING : bit >
{ 0 | 1 < 3G Neighbour Cell Description : < 3G Neighbour Cell Description struct >> }
{ 0 | 1 < GPRS REP PRIORITY Description : < GPRS REP PRIORITY Description struct >> }
{ 0 | 1 < GPRS MEASUREMENT Parameters Description : < GPRS MEASUREMENT PARAMETERS Description struct >> }
{ 0 | 1 < GPRS 3G MEASUREMENT Parameters Description : < GPRS 3G MEASUREMENT PARAMETERS Description struct >> } ;</td><td>
1+2
1
1
1
1
1+?
1+?>8
1+29
1+26
>75</td></tr>
<tr><td>< 3G Neighbour Cell Description struct > ::=
{ 0 | 1 < Index_Start_3G : bit (7) > }
{ 0 | 1 < Absolute_Index_Start_EMR : bit (7) > }
{ 0 | 1 < UMTS FDD Description : < UMTS FDD Description struct >> }
{ 0 | 1 < UMTS TDD Description : < UMTS TDD Description struct >> }
{ 0 | 1 < REMOVED_3GCELL_Description : < REMOVED_3GCELL_Description struct >> } ;</td><td>
?</td></tr>
<tr><td>< REMOVED_3GCELL_Description struct > ::=
< N1 : bit (2) >
{ < N2 : bit (5) >
{ < REMOVED_3GCELL_INDEX : bit (7) >
< 3G_CELL_DIFF_LENGTH : bit (3) >
< 3GCELL_DIFF : bit (val(3G_CELL_DIFF_LENGTH)) >
} * (1+val(N2))
} * (1+val(N1)) ;</td><td>
2
5
7
3
8

?</td></tr>
</table>

< UMTS FDD Description struct > ::= { 0 | 1 < **Bandwidth_FDD** : bit (3) > } { 1 { < **Repeated UMTS FDD Neighbour Cells** : < Repeated UMTS FDD Neighbour Cells struct >> } ** 0 } ;	 1+**3** ?
< Repeated UMTS FDD Neighbour Cells struct > ::= { 0 < **FDD-ARFCN** : bit (14) > | 1 < **FDD-ARFCN-INDEX** : bit (3) > } < **FDD_Indic0 :** bit > < **NR_OF_FDD_CELLS** : bit (5) > < **FDD_CELL_INFORMATION Field** : bit(p(NR_OF_FDD_CELLS)) > ; -- p(x) defined in table 60.1/3GPP TS 04.60	 1+**14** 1 5 ? **>21**
< UMTS TDD Description struct > ::= { 0 | 1 < **Bandwidth_TDD** : bit (3) > } { 1 { < **Repeated UMTS TDD Neighbour Cells** : < Repeated UMTS TDD Neighbour Cells struct >> } ** 0 } ;	 1+**3** ?
< Repeated UMTS TDD Neighbour Cells struct > ::= { 0 < **TDD-ARFCN** : bit (14) > | 1 < **TDD-ARFCN-INDEX** : bit (3) > } < **TDD_Indic0 :** bit > < **NR_OF_TDD_CELLS** : bit (5) > < **TDD_CELL_INFORMATION Field** : bit(q(NR_OF_TDD_CELLS)) > ; -- q(x) defined in table 60.2/3GPP TS 04.60.	 1+**14** 1 5 ? **>21**
< GPRS REP PRIORITY Description struct > ::= < **Number_Cells** : bit(7) > { < **REP_PRIORITY** : bit > } * (val(Number_Cells)) ;	 7 ? **>8**
< GPRS MEASUREMENT PARAMETERS Description struct > ::= { 0 | 1 < **MULTIBAND_REPORTING** : bit (2) > } { 0 | 1 < **SERVING_BAND_REPORTING** : bit (2) > } < **SCALE_ORD** : bit(2) > { 0 | 1 < **900_REPORTING_OFFSET** : bit (3) > < **900_REPORTING_THRESHOLD** : bit (3) > } { 0 | 1 < **1800_REPORTING_OFFSET** : bit (3) > < **1800_REPORTING_THRESHOLD** : bit (3) > } { 0 | 1 < **450_REPORTING_OFFSET** : bit (3) > < **450_REPORTING_THRESHOLD** : bit (3) > } { 0 | 1 < **1900_REPORTING_OFFSET** : bit (3) > < **1900_REPORTING_THRESHOLD** : bit (3) > } { 0 | 1 < **850_REPORTING_OFFSET** : bit (3) > < **850_REPORTING_THRESHOLD** : bit (3) > } ;	 1+**2** 1+**2** 2 1+**3** 3 1+**3** 3 1+**3** 3 **29**
< GPRS 3G MEASUREMENT PARAMETERS Description struct > ::= < **Qsearch_P :** bit (4) > < **3G_SEARCH_PRIO** : bit > { 0 | 1 < **FDD_REP_QUANT** : bit > -- FDD Parameters < **FDD_MULTIRAT_REPORTING** : bit (2) > } { 0 | 1 < **FDD_REPORTING_OFFSET** : bit (3) > < **FDD_REPORTING_THRESHOLD** : bit (3) > } { 0 | 1 < **TDD_MULTIRAT_REPORTING** : bit (2) > } -- TDD Parameters { 0 | 1 < **TDD_REPORTING_OFFSET** : bit (3) > < **TDD_REPORTING_THRESHOLD** : bit (3) > } ;	 4 1 1+**1** 2 1+**3** 3 1+**2** 1+**3** 3 **26**

Packet Cell Change order seems problematic already today.

A.6 Packet Immediate Assignment

<table>
<tr><td><IA Rest Octets> ::=</td><td>Message Size:</td></tr>
<tr><td>{ LL</td><td>2</td></tr>
<tr><td>| LH</td><td></td></tr>
<tr><td>{ 00 < EGPRS Packet Uplink Assignment ></td><td>2+131</td></tr>
<tr><td>| 01 -- reserved for future use</td><td></td></tr>
<tr><td>| 1 -- reserved for future use (however the value 7C for the first octet shall not be used)</td><td></td></tr>
<tr><td>}</td><td></td></tr>
<tr><td>| HL</td><td></td></tr>
<tr><td>< Length of frequency parameters : bit string (6) ></td><td></td></tr>
<tr><td>< Frequency Parameters, before time ></td><td></td></tr>
<tr><td>| HH</td><td></td></tr>
<tr><td>{ 00 < Packet Uplink Assignment ></td><td>2+94</td></tr>
<tr><td>| 01 < Packet Downlink Assignment ></td><td>2+93</td></tr>
<tr><td>| 1 < Second Part Packet Assignment > }</td><td>1+7</td></tr>
<tr><td>}</td><td></td></tr>
<tr><td><spare padding>;</td><td></td></tr>
<tr><td></td><td>135 EGPRS PUA
98 PUA
97 PDA</td></tr>
<tr><td>< EGPRS Packet Uplink Assignment > : :=</td><td></td></tr>
<tr><td>< Extended RA : bit (5) ></td><td>5</td></tr>
<tr><td>{ 0 | 1 < Access Technologies Request : Access Technologies Request struct > }</td><td>1+25</td></tr>
<tr><td>{ 1</td><td>1</td></tr>
<tr><td>< TFI_ASSIGNMENT : bit (5) ></td><td>5</td></tr>
<tr><td>< POLLING : bit ></td><td>1</td></tr>
<tr><td>{ 0 -- Dynamic Allocation</td><td>1</td></tr>
<tr><td>< USF: bit (3) ></td><td>3</td></tr>
<tr><td>< USF_GRANULARITY : bit ></td><td>1</td></tr>
<tr><td>{ 0 | 1 < P0 : bit (4) ></td><td>1+4</td></tr>
<tr><td>< PR_MODE : bit (1) >}</td><td>1 11</td></tr>
<tr><td>| 1 -- Fixed Allocation</td><td>1</td></tr>
<tr><td>< ALLOCATION_BITMAP_LENGTH : bit (5) ></td><td>5</td></tr>
<tr><td>< ALLOCATION_BITMAP : bit (val(ALLOCATION_BITMAP_LENGTH)) ></td><td>32 max</td></tr>
<tr><td>{ 0 | 1 < P0 : bit (4) ></td><td>1+4</td></tr>
<tr><td>< BTS_PWR_CTRL_MODE : bit (1) ></td><td>1</td></tr>
<tr><td>< PR_MODE : bit (1) >}</td><td>1 45</td></tr>
<tr><td>}</td><td></td></tr>
<tr><td>< EGPRS CHANNEL_CODING_COMMAND : < EGPRS Modulation and Coding IE>></td><td>4</td></tr>
<tr><td>< TLLI_BLOCK_CHANNEL_CODING : bit (1) ></td><td>1</td></tr>
<tr><td>{ 0 | 1 < BEP_PERIOD2 : bit (4) >}</td><td>1+4</td></tr>
<tr><td>< Resegment : < Resegment IE>></td><td>1</td></tr>
<tr><td>< EGPRS Window Size : < EGPRS Window Size IE>></td><td>5</td></tr>
<tr><td>{ 0 | 1 < ALPHA : bit (4) >}</td><td>1+4</td></tr>
<tr><td>< GAMMA : bit (5) ></td><td>5</td></tr>
<tr><td>{ 0 | 1 < TIMING_ADVANCE_INDEX : bit (4) > }</td><td>1+4</td></tr>
<tr><td>{ 0 | 1 < TBF_STARTING_TIME : bit (16) > }</td><td>1+16 99 fixed allocation</td></tr>
<tr><td>| 0 -- Multi Block Allocation</td><td>1</td></tr>
<tr><td>{ 0 | 1 < ALPHA : bit (4) >}</td><td>1+4</td></tr>
<tr><td>< GAMMA : bit (5) ></td><td>5</td></tr>
<tr><td>< TBF_STARTING_TIME : bit (16) ></td><td>16</td></tr>
<tr><td>< NUMBER OF RADIO BLOCKS ALLOCATED : bit (2) ></td><td>2</td></tr>
<tr><td>{ 0 | 1 < P0 : bit (4) ></td><td>1+4</td></tr>
<tr><td>< BTS_PWR_CTRL_MODE : bit (1) ></td><td>1</td></tr>
<tr><td>< PR_MODE : bit (1) >}</td><td>1 35</td></tr>
<tr><td>} ;</td><td></td></tr>
<tr><td></td><td>131 fixed allocation
97 dynamic allocation
68 multiblock allocation</td></tr>
</table>

```
<Access Technologies Request struct> ::= -- recursive structure allows any combination of Access
technologies
    <Access Technology Type : bit (4)>
    { 0 | 1 <Access Technologies Request struct> };
                                                                                          25
                                                                         450/480/900/1800/UMTS
< Packet Uplink Assignment > ::=

    { 1                                                                  1
        < TFI_ASSIGNMENT : bit (5) >                                     5
        < POLLING : bit >                                                1
        { 0                                   -- Dynamic Allocation      1
            < USF: bit (3) >                                             3
            < USF_GRANULARITY : bit >                                    1
            { 0 | 1 < P0 : bit (4) >                                     1+4
            < PR_MODE : bit (1) >}                                       1          11
        | 1                                   -- Fixed Allocation        1
            < ALLOCATION_BITMAP_LENGTH : bit (5) >                       5
            < ALLOCATION_BITMAP : bit (val(ALLOCATION_BITMAP_LENGTH)) >  32 max
            { 0 | 1 < P0 : bit (4) >                                     1+4
                < BTS_PWR_CTRL_MODE : bit (1) >                            1
                < PR_MODE : bit (1) >}                                     1        45
        }
            < CHANNEL_CODING_COMMAND : bit (2) >                         2
            < TLLI_BLOCK_CHANNEL_CODING : bit >                          1
        { 0 | 1 < ALPHA : bit (4) >}                                     1+4
        < GAMMA : bit (5) >                                              5
        { 0 | 1 < TIMING_ADVANCE_INDEX : bit (4) > }                     1+4
        { 0 | 1 < TBF_STARTING_TIME : bit (16) > }                       1+16   86 fixed allocation
    | 0                                       -- Single Block Allocation 1
        { 0 | 1 < ALPHA : bit (4) >}                                     1+4
        < GAMMA : bit (5) >                                              5
        0 1                                   -- See Note 1              2
        < TBF_STARTING_TIME : bit (16) >                                 16
        { L | H < P0 : bit (4) >                                         1+4
                < BTS_PWR_CTRL_MODE : bit (1) >                            1
                < PR_MODE : bit (1) >}                                     1
    }                                                                               35
    { L | H                                   -- Additions for R99       1
    { 0 | 1 < Extended RA : bit (5) > }} ;                               1+5

                                                                   94 Fixed allocation
                                                                      and R99 additions
                                                                 60 Dynamic allocation
                                                                      and R99 additions
< Packet Downlink Assignment > ::=
    < TLLI : bit (32) >                                              32 (TLLI not used)
    { 0 | 1                                                          1
        < TFI_ASSIGNMENT : bit (5) >                                 5
        < RLC_MODE : bit >                                           1
        {0 | 1 < ALPHA : bit (4) >}                                  1+4
        < GAMMA : bit (5) >                                          5
        < POLLING : bit >                                            1
        < TA_VALID : bit (1) >}                                      1
        { 0 | 1 < TIMING_ADVANCE_INDEX : bit (4) > }                 1+4
        { 0 | 1 < TBF_STARTING_TIME : bit (16) > }                   1+16
        { 0 | 1 < P0 : bit (4) >                                     1+4
            < BTS_PWR_CRTL_MODE : bit (1) >                            1
            < PR_MODE : bit (1) >}                                     1
{ L | H -- indicates EGPRS TBF mode, see 04.60                       1
        < EGPRS Window Size : < EGPRS Window Size IE>>               5
        < LINK_QUALITY_MEASUREMENT_MODE : bit (2)>  ;                2
        { 0 | 1 < BEP_PERIOD2 : bit (4) > } };                       1+4
                                                                                93
```

< Frequency Parameters, before time > ::= { null *-- Length of frequency parameters = 0* | 0 0 < MAIO : bit (6) > < Mobile Allocation : octet (val (Length of frequency parameters) – 1) }; < Second Part Packet Assignment > ::= { L | H *- - Additions for R99* { 0 | 1 < Extended RA : bit (5) > }} ;	 1 1+**5** **7**

The table below shows the size of the Immediate Assignment message considering the previous calculation:

IEI	Information element	Type / Reference	Presence	Format	length	Size (bits)
	L2 Pseudo Length	L2 Pseudo Length 10.5.2.19	M	V	1	8
	RR management Protocol Discriminator	Protocol Discriminator 10.2	M	V	1/2	4
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2	4
	Immediate Assignment Message Type	Message Type 10.4	M	V	1	8
	Page Mode	Page Mode 10.5.2.26	M	V	1/2	4
	Dedicated mode or TBF	Dedicated mode or TBF 10.5.2.25b	M	V	1/2	4
	Channel Description	Channel Description 10.5.2.5	C	V	3	0 Only the packet channel description is included
	Packet Channel Description	Packet Channel Description 10.5.2.25a	C	V	3	24
	Request Reference	Request Reference 10.5.2.30	M	V	3	24
	Timing Advance	Timing Advance 10.5.2.40	M	V	1	8
	Mobile Allocation	Mobile Allocation 10.5.2.21	M	LV	1-9	72 (not included in the 2nd message of a two message assignment)
7C	Starting Time	Starting Time 10.5.2.38	O	TV	3	0 no change of frequency
						160
	IA Rest Octets	IA Rest Octets 10.5.2.16	M	V	0-11	See above.
Total Size: The figures below assume the use of a two-message assignment procedure: EGPRS PUA fixed allocation: 383 EGPRS PUA dynamic allocation: 349 PUA fixed allocation: 346 PUA dynamic allocation: 312 PDA: 345						

In case of TBF establishment via CCCH, a two-message assignment procedure is possible in case the amount of fields/IE is too big to fit into one single Immediate Assignment message. A two-message assignment offers 368 bits of payload, while a single message provides 184 bits. Therefore, the maximum configuration considering EGPRS PUA does not fit in this payload if a fixed allocation is made with a full bitmap of 32 bits. A smaller bitmap would allow the inclusion of a MAC-I shorter than 32 bits. A MAC-I shorter than 32 bits is also the only possibility (except for PUA dynamic allocation) for the other assignment cases. Therefore a **variable size MAC-I with a minimum size** could be included in the EGPRS PUA/PUA/PDA constructions. The impact would mainly be a possible reduced flexibility in the EGPRS PUA fixed allocation (shorter bitmap than 32 bits).