3GPP TSG CN Plenary Meeting #16 **NP-020225**
5th - 7th June 2002. Marco Island, USA.

Source: **TSG CN WG 1**

Title: **CRs to Rel-5 on Work Item IMS-CCR towards 24.008**

Agenda item: **8.1**

Document for: **APPROVAL**

Introduction:

This document contains **2** CRs on **Rel-5 on** Work Item **"IMS-CCR"**, that have been agreed by **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #16 for approval.

Spec	CR	Rev	Phase	Subject	Cat	Version Current	Version-New	Meeting-2nd-Level	Doc-2nd-Level
24.008	630		Rel-5	Support for IMS media Multiplexing in Session Management - TFT enhancement	C	5.3.0	5.4.0	N1-24	N1-021289
24.008	634	1	Rel-5	PCO in Session Management procedures	F	5.3.0	5.4.0	N1-24	N1-021475

3GPP TSG-CN1 Meeting #24
Budapest, Hungary, 13. – 17. May 2002

Tdoc N1-021289

CR-Form-v5

CHANGE REQUEST

⌘ **24.008** **CR** **630** ⌘ **rev** **-** ⌘ Current version: **5.3.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE **X** Radio Access Network ☐ Core Network **X**

Title:	⌘	Support for IMS media Multiplexing in Session Management – TFT
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	09.05.02
Category:	⌘	**C**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
REL-4 *(Release 4)*
REL-5 *(Release 5)*

Reason for change:	⌘	Current coding of TFT limits the future enhancements of the Multiplexing control mechanism design by SA2 since it mandates the GGSN to pass only one token to PCF for media authorization. The was agreed by SA2 during SA#24 email approval (see related LS S2-021301) that Multiplexing between session will not be allowed in Rel-5, however for future compatibility reasons the implementation should allow already in Rel-5 carrying multiple sets of binding information. From the LS: *At the same time, the interfaces (and the corresponding information element(s) within) carrying Binding Information shall be designed such a way that they are capable of carrying multiple sets of Binding Informations for forward compatibility reasons.* Currently, 23.207 states that the binding information consists of one authorisation token and several flow IDs. Hence the coding of TFT has to be modified in a way that more than one set of binding information may be carried in TFT.
Summary of change:	⌘	Chapter *10.5.6.12 Traffic Flow Template*, the mandate to ignore all instances of Authorisation Token but the last one, is modified so that all instances shall be considered.
Consequences if not approved:	⌘	In future releases it will not be possible to introduce more than one Authorisation Token per PDP context without causing Interworking problems.

Clauses affected:	⌘	Chapter *10.5.6.12*
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications

Other comments: ⌘	

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

10.5.6.12 Traffic Flow Template

The purpose of the *traffic flow template* information element is to specify the TFT parameters and operations for a PDP context. In addition, this information element may be used to transfer extra parameters to the network (e.g. the Authorization Token; see 3GPP TS 24.229).

The *traffic flow template* is a type 4 information element with a minimum length of 3 octets. The maximum length for the IE is 257 octets.

NOTE 1: The IE length restriction is due to the maximum length that can be encoded in a single length octet.

NOTE 2: A maximum size IPv4 packet filter can be 32 bytes. Therefore, 7 maximum size IPv4 type packet filters, plus the last packet filter which can contain max 30 octets can fit into one TFT, i.e. if needed not all packet filter components can be defined into one message. A maximum size Ipv6 packet filter can be 60 bytes. Therefore, only 4 maximum size IPv6 packet filters can fit into one TFT. However, using "Add packet filters to existing TFT", it's possible to create a TFT including 8 maximum size Ipv4 or IPv6 filters.

The *traffic flow template* information element is coded as shown in figure 10.5.144/3GPP TS 24.008 and table 10.5.162/3GPP TS 24.008.

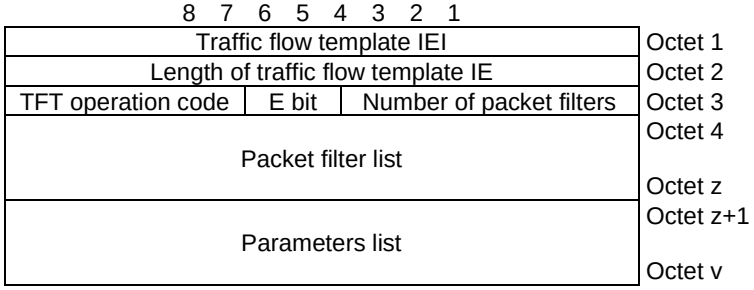

Figure 10.5.144/3GPP TS 24.008: *Traffic flow template* information element

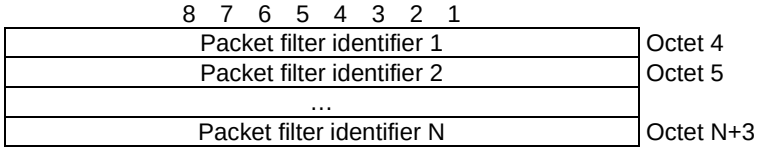

Figure 10.5.144a/3GPP TS 24.008: *Packet filter list* when the TFT operation is "delete packet filters from existing TFT" (z=N+3)

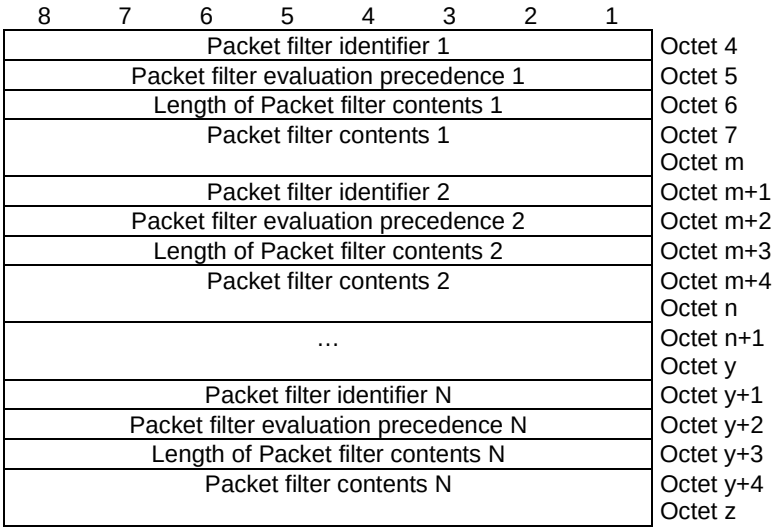

Figure 10.5.144b/3GPP TS 24.008: *Packet filter list* when the TFT operation is "create new TFT", or "add packet filters to existing TFT" or "replace packet filters in existing TFT"

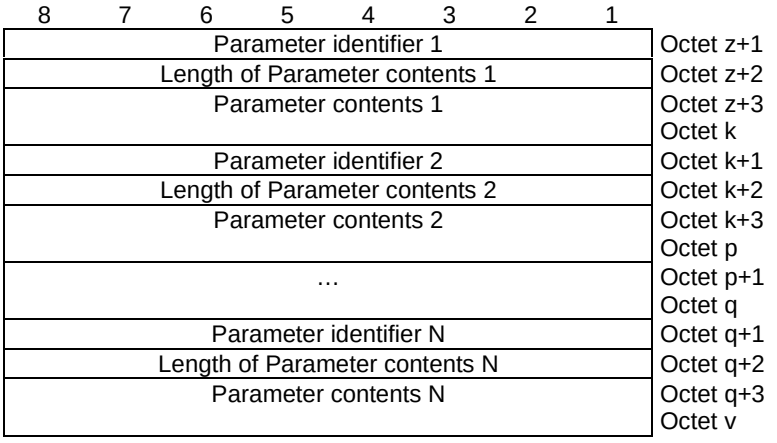

Figure 10.5.144c/3GPP TS 24.008: *Parameters list*

Table 10.5.162/3GPP TS 24.008: *Traffic flow template* information element

TFT operation code (octet 3) Bits 8 7 6 0 0 0 Spare 0 0 1 Create new TFT 0 1 0 Delete existing TFT 0 1 1 Add packet filters to existing TFT 1 0 0 Replace packet filters in existing TFT 1 0 1 Delete packet filters from existing TFT 1 1 0 No TFT operation 1 1 1 Reserved

E bit (bit 5 of octet 3)

The *E bit* indicates if a *parameters list* is included in the TFT IE and it is encoded as follows:
0 *parameters list* is not included
1 *parameters list* is included

Number of packet filters (octet 3)

The *number of packet filters* contains the binary coding for the number of packet filters in the *packet filter list*. The *number of packet filters* field is encoded in bits 4 through 1 of octet 3 where bit 4 is the most significant and bit 1 is the least significant bit. For the "delete existing TFT" operation and for the "no TFT operation", the *number of packet filters* shall be coded as 0. For all other operations, the number of packet filters shall be greater than 0 and less than or equal to 8.

Packet filter list (octets 4 to z)

The *packet filter list* contains a variable number of packet filters. For the "delete existing TFT" operation, the *packet filter list* shall be empty.

For the "delete packet filters from existing TFT" operation, the *packet filter list* shall contain a variable number of packet filter identifiers. This number shall be derived from the coding of the *number of packet filters* field in octet 3.

For the "create new TFT", "add packet filters to existing TFT" and "replace packet filters in existing TFT" operations, the *packet filter list* shall contain a variable number of packet filters. This number shall be derived from the coding of the *number of packet filters* field in octet 3.

Each packet filter is of variable length and consists of

- a packet filter identifier (1 octet);
- a packet filter evaluation precedence (1 octet);
- the length of the packet filter contents (1 octet); and
- the packet filter contents itself (v octets).

The *packet filter identifier* field is used to identify each packet filter in a TFT. Since the maximum number of packet filters in a TFT is 8, only the least significant 3 bits are used. Bits 8 through 4 are spare bits.

The *packet filter evaluation precedence* field is used to specify the precedence for the packet filter among all packet filters in all TFTs associated with this PDP address. Higher the value of the *packet filter evaluation precedence* field, lower the precedence of that packet filter is. The first bit in transmission order is the most significant bit.

The *length of the packet filter contents* field contains the binary coded representation of the length of the *packet filter contents* field of a packet filter. The first bit in transmission order is the most significant bit.

Parameters list (octets z+1 to v)

The *parameters list* contains a variable number of parameters that might need to be transferred in addition to the packet filters. If the *parameters list* is included, the *E bit* is set to 1; otherwise, the *E bit* is set to 0.

Each parameter included in the *parameters list* is of variable length and consists of:

- a parameter identifier (1 octet);
- the length of the parameter contents (1 octet); and
- the parameter contents itself (v octets).

The *parameter identifier* field is used to identify each parameter included in the *parameters list* and it contains the hexadecimal coding of the parameter identifier. Bit 8 of the *parameter identifier* field contains the most significant bit and bit 1

contains the least significant bit. In this version of the protocol, the following parameter identifiers are specified:

- 01H (Authorization Token);
- 02H (Flow Identifier).

If the *parameters list* contains a parameter identifier that is not supported by the receiving entity the corresponding parameter shall be discarded.

The *length of parameter contents* field contains the binary coded representation of the length of the *parameter contents* field. The first bit in transmission order is the most significant bit.

When the *parameter identifier* indicates Authorization Token, the *parameter contents* field contains an authorization token, as specified in 3GPP TS 24.229. This authorization token is represented as a string of digits encoded in hexadecimal form. The least significant digit is encoded in bits 4321 of the first octet, the second least significant digit is encoded in bits 8765 of the first octet, the third least significant digit is encoded in bits 4321 of the second octet, etc. When the total number of digits is even, bits 8765 of the last octet are marked as unused with the value "1111".

The *parameters list* shall be coded in a way that an Authorization Token (i.e. a parameter with identifier 01H) is always followed by one or more Flow Identifiers (i.e. one or more parameters with identifier 02H).

If the *parameters list* contains two or more consecutive Authorization Tokens without any Flow Identifiers in between, the receiver shall treat this as a semantical TFT error.

~~If the *parameters list* contains more than one instance of the Authorization Token, then all instances except the last instance shall be ignored.~~

When the *parameter identifier* indicates Flow Identifier, the *parameter contents* field contains the binary representation of a flow identifier, as specified in 3GPP TS 24.229. Bit 1 of the first octet is least significant bit, and bit 8 of the last octet is the most significant bit.

~~If the *parameters list* contains more than one instance of the Flow Identifier, then all instances shall be considered.~~

Table 10.5.162/3GPP TS 24.008 (continued): *Traffic flow template* information element

The *packet filter contents* field is of variable size and contains a variable number (at least one) of *packet filter components*. Each *packet filter component* shall be encoded as a sequence of a one octet *packet filter component type identifier* and a fixed length *packet filter component value* field. The *packet filter component type identifier* shall be transmitted first.

In each packet filter, there shall not be more than one occurrence of each packet filter component type. Among the "IPv4 source address type" and "IPv6 source address type" packet filter components, only one shall be present in one packet filter. Among the "single destination port type" and "destination port range type" packet filter components, only one shall be present in one packet filter. Among the "single source port type" and "source port range type" packet filter components, only one shall be present in one packet filter.

Packet filter component type identifier

Bits	
8 7 6 5 4 3 2 1	
0 0 0 1 0 0 0 0	IPv4 source address type
0 0 1 0 0 0 0 0	IPv6 source address type
0 0 1 1 0 0 0 0	Protocol identifier/Next header type
0 1 0 0 0 0 0 0	Single destination port type
0 1 0 0 0 0 0 1	Destination port range type
0 1 0 1 0 0 0 0	Single source port type
0 1 0 1 0 0 0 1	Source port range type
0 1 1 0 0 0 0 0	Security parameter index type
0 1 1 1 0 0 0 0	Type of service/Traffic class type
1 0 0 0 0 0 0 0	Flow label type

All other values are reserved.

For "IPv4 source address type", the *packet filter component value* field shall be encoded as a sequence of a four octet *IPv4 address* field and a four octet *IPv4 address mask* field. The *IPv4 address* field shall be transmitted first.

For "IPv6 source address type", the *packet filter component value* field shall be encoded as a sequence of a sixteen octet *IPv6 address* field and a sixteen octet *IPv6 address mask* field. The *IPv6 address* field shall be transmitted first.

For "Protocol identifier/Next header type", the *packet filter component value* field shall be encoded as one octet which specifies the IPv4 protocol identifier or IPv6 next header.

For "Single destination port type" and "Single source port type", the *packet filter component value* field shall be encoded as two octet which specifies a port number.

For "Destination port range type" and "Source port range type", the *packet filter component value* field shall be encoded as a sequence of a two octet *port range low limit* field and a two octet *port range high limit* field. The *port range low limit* field shall be transmitted first.

For "Security parameter index", the *packet filter component value* field shall be encoded as four octet which specifies the IPSec security parameter index.

For "Type of service/Traffic class type", the *packet filter component value* field shall be encoded as a sequence of a one octet *Type-of-Service/Traffic Class* field and a one octet *Type-of-Service/Traffic Class mask* field. The *Type-of-Service/Traffic Class* field shall be transmitted first.

For "Flow label type", the *packet filter component value* field shall be encoded as three octet which specifies the IPv6 flow label. The bits 8 through 5 of the first octet shall be spare whereas the remaining 20 bits shall contain the IPv6 flow label.

3GPP TSG-CN1 Meeting #24
Budapest, Hungary, 13. – 17. May 2002

Tdoc N1-021475

CR-Form-v5

CHANGE REQUEST

⌘ **24.008** **CR** **634** ⌘ **rev** **1** ⌘ Current version: **5.3.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE **X** Radio Access Network ☐ Core Network **X**

Title:	⌘	PCO in Session Management procedures
Source:	⌘	Nokia, Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	16.05.02
Category:	⌘	**B**
Release:	⌘	REL-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
REL-4 *(Release 4)*
REL-5 *(Release 5)*

Reason for change:	⌘	During SA#22 meeting it was agreed the convenience of adding PCO IE to other PDP context procedures than the currently existing ones, see LS in N1-021362. The reason for this is to avoid backward compatibility problems in future releases. This was discussed during the joint meeting with CN1 and the starting point was adding PCO to the PDP context modification procedure and the possible use case was to prepare 24.008 for signalling flags for future application level signalling. Same reasoning should be used for rejected messages since there might be a need for GGSN to indicate to UE why the PDP context procedure failed. Examples of this could be: To carry Go related error codes to the UE. For example, when media authorization fails in PCF because the token is incorrect the context has to be rejected. When P-CSCF discovery is performed and the PDP context activation is rejected for some other reason, we could still provide the P-CSCF address to the UE and this way avoid extra signalling. Currently PCO is included in Activate PDP context reject message, the insertion of this IE has to be clarified. It is said that it should be inserted only in case when SM cause is “activation rejected by GGSN” however this cause code does not exist in 29.060 and the mapping is not specified in any other specification.
Summary of change:	⌘	o Addition of PCO IE to: Secondary PDP context reject, PDP context modification request/response/reject messages. o Removal of the restriction in Activate PDP context reject message for the addition of PCO.
Consequences if not approved:	⌘	In Rel-6 CN1 will face the same backwards compatibility problems as with TFT and PCO, a non optimal solution will have to be adopted again. In addition there will be no way in Rel-5 to indicate to the UE that the PDP context failed due to

	PCF rejection.

Clauses affected:	⌘	9.5.3, 9.5.6, 9.5.10, 9.5.12, 9.5.13		
Other specs Affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	
Other comments:	⌘			

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

********** FIRST MODIFICATION **********

9.5.3 Activate PDP context reject

This message is sent by the network to the MS to reject activation of a PDP context.
See table 9.5.3/3GPP TS 24.008.

Message type: ACTIVATE PDP CONTEXT REJECT

Significance: global

Direction: network to MS

Table 9.5.3/3GPP TS 24.008: ACTIVATE PDP CONTEXT REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Transaction identifier	Transaction identifier 10.3.2	M	V	1/2– 3/2
	Activate PDP context reject message identity	Message type 10.4	M	V	1
	SM cause	SM Cause 10.5.6.6	M	V	1
27	Protocol configuration options	Protocol configuration options 10.5.6.3	O	TLV	3 - 253

9.5.3.1 Protocol configuration options

This IE may be included in the message if the network wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the MS.

~~The protocol configuration options IE may only be inserted by the network (see TS29.060) if the SM Cause indicates "activation rejected by GGSN".~~

********** NEXT MODIFICATION **********

9.5.6 Activate Secondary PDP Context Reject

This message is sent by the network to the UE to reject activation of an additional PDP context associated with the same PDP address and APN as an already active PDP context. See Table 9.5.6/3GPP TS 24.008.

Message type: ACTIVATE SECONDARY PDP CONTEXT REJECT

Significance: global

Direction: network to MS

Table 9.5.6/3GPP TS 24.008: ACTIVATE SECONDARY PDP CONTEXT REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	½
	Transaction identifier	Transaction identifier 10.3.2	M	V	1/2– 3/2
	Activate secondary PDP context reject message identity	Message type 10.4	M	V	1
	SM cause	SM Cause 10.5.6.6	M	V	1
27	Protocol configuration options	Protocol configuration options 10.5.6.3	O	TLV	3 – 253

9.5.6.1 Protocol configuration options

This IE may be included in the message if the network wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the MS.

********** NEXT MODIFICATION **********

9.5.10 Modify PDP context request (MS to network direction)

This message is sent by the MS to the network to request modification of an active PDP context. See table 9.5.10/3GPP TS 24.008.

Message type: MODIFY PDP CONTEXT REQUEST (MS TO NETWORK DIRECTION)

Significance: global

Direction: MS to network

Table 9.5.10/3GPP TS 24.008: MODIFY PDP CONTEXT REQUEST (MS to network direction) message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	~~1/2~~½
	Transaction identifier	Transaction identifier 10.3.2	M	V	½– 3/2
	Modify PDP context request message identity	Message type 10.4	M	V	1
32	Requested LLC SAPI	LLC service access point identifier 10.5.6.9	O	TV	2
30	Requested new QoS	Quality of service 10.5.6.5	O	TLV	14
31	New TFT	Traffic Flow Template 10.5.6.12	O	TLV	3-257
27	Protocol configuration options	Protocol configuration options 10.5.6.3	O	TLV	3-253

9.5.10.4 Protocol configuration options

This IE may be included in the message if the MS wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

********** NEXT MODIFICATION **********

9.5.12 Modify PDP context accept (Network to MS direction)

This message is sent by the network to the MS to acknowledge the modification of an active PDP context. See table 9.5.12/3GPP TS 24.008.

Message type: MODIFY PDP CONTEXT ACCEPT (NETWORK TO MS DIRECTION)

Significance: global

Direction: Network to MS

Table 9.5.12/3GPP TS 24.008: MODIFY PDP CONTEXT ACCEPT (NETWORK to MS direction) message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	½
	Transaction identifier	Transaction identifier 10.3.2	M	V	½– 3/2
	Modify PDP context accept message identity	Message type 10.4	M	V	1
30	Negotiated QoS	Quality of service 10.5.6.5	O	TLV	14
32	Negotiated LLC SAPI	LLC service access point identifier 10.5.6.9	O	TV	2
8	New radio priority	Radio priority 10.5.7.2	O	TV	1
34	Packet Flow Identifier	Packet Flow Identifier 10.5.6.11	O	TLV	3
27	Protocol configuration options	Protocol configuration options 10.5.6.3	O	TLV	3 – 253

9.5.12.5 Protocol configuration options

This IE may be included in the message if the network wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the MS.

********** NEXT MODIFICATION **********

9.5.13 Modify PDP Context Reject

This message is sent by the network to the UE to reject the requested modification of the TFT. The network should not send a MODIFY PDP CONTEXT REJECT message only if the requested QoS is not available. If a TFT modification was requested and the requested new TFT is not available then MODIFY PDP CONTEXT REJECT shall be sent. See Table 9.5.13/3GPP TS 24.008.

Message type: MODIFY PDP CONTEXT REJECT

Significance: global

Direction: network to MS

Table 9.5.13/3GPP TS 24.008: MODIFY PDP CONTEXT REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	½
	Transaction identifier	Transaction identifier 10.3.2	M	V	1/2– 3/2
	Modify PDP Context Reject	Message type 10.4	M	V	1
	SM cause	SM Cause 10.5.6.6	M	V	1
27	Protocol configuration options	Protocol configuration options 10.5.6.3	O	TLV	3 – 253

9.5.13.1 Protocol configuration options

This IE may be included in the message if the network wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the MS.