**3GPP TSG-CT WG1 Meeting #130-eC1-213563**

**Electronic meeting, 20-28 May 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.008** | **CR** | **3267** | **rev** | **1** | **Current version:** | **17.2.0** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Correction on the number of the maximum size packet filters in TFT | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | NTT DOCOMO | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SAES17, TEI17 | | | | |  | ***Date:*** | | | 2021-05-21 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change 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](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) ... Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Currently, TS 24.008 specifies the maximum number of supported packet filters of the UE as:  *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 IE, i.e. if needed not all packet filter components can be defined into one message.*  However, this text is wrong due to following reasons.   1. in Rel-11, IPv4/6 local address type packet filters are specified. Therefore, the above statement (from pre-Rel-11) is no longer valid. 2. Calculated max values are based on wrong assumption that both ”port” or “Security parameter index” can be included at the same time. However, as specified in TS 23.060 (see below), it should be only one of them.   *TS 23.060 subclause 15.3.2.0*  *Some of the above-listed attributes may coexist in a packet filter while others mutually exclude each other. In table 12 below, the possible combinations are shown. Only those attributes marked with an "X" may be specified for a single packet filter. All marked attributes may be specified, but at least one shall be specified.*  Table 12: Valid Packet Filter Attribute Combinations   |  |  |  |  | | --- | --- | --- | --- | |  | Valid combination types | | | | Packet filter attribute | I | II | III | | Remote Address and Subnet Mask | X | X | X | | Protocol Number (IPv4) / Next Header (IPv6) | X | X |  | | Local Address and Mask | X | X | X | | Local Port Range | X |  |  | | Remote Port Range | X |  |  | | IPSec SPI |  | X |  | | TOS (IPv4) / Traffic Class (IPv6) and Mask | X | X | X | | Flow Label (IPv6) |  |  | X |   Based on this, as calculated in the below table, the correct number should be 36 for IPv4.   |  |  | | --- | --- | | Type of packet filter (for IPv4) | Length (bytes) | | Packet filter identifier | 1 | | Packet filter evaluation precedence | 1 | | Length of packet filter contents | 1 | | IPv4 remote address | 9 | | IPv4 local address | 9 | | Protocol identifier | 2 | | Remote port range | 5 | | Local port range | 5 | | Type of service | 3 | | Sum | 36 |   *Note that “length” above contains the lentgh of the packet filter component type identifiert.*  Thus, considering that we can use 254 bytes for above information, we can conclude that we can include 7 maximum size IPv4 packet filters (since 36 \* 7 + 2 = 254) but, as the remaining field is 2 octet, we cannot include another packet filter (since the length of packet filter > 2)  Similarly, as calculated below,the correct number should be 54 for IPv6. (Note that if the UE/NW does not support IPv6 local address type packet filter, then the maximum size will be 51 bytes.)   |  |  | | --- | --- | | Type of packet filter (for IPv6) | Length (bytes) | | Packet filter identifier | 1 | | Packet filter evaluation precedence | 1 | | Length of packet filter contents | 1 | | IPv6 remote address/prefix length | 18 | | IPv6 local address/prefix length | 18 | | Protocol identifier | 2 | | Remote port range | 5 | | Local port range | 5 | | Type of service | 3 | | Sum | 54 |   *Note that “length” above contains the lentgh of the packet filter component type identifiert.*  Thus, similar as above, we can conclude that we can include 4 maximum size IPv6 packet filters (since 54 \* 4 + 38 = 254) and tha last packet filter can only contain max 38 octets. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Correct the maximum number of supported packet filters | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The NW operators may try to send too many packet filters | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 10.5.6.12 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

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 [95]). The TFT may contain packet filters for the downlink direction, the uplink direction or packet filters that are applicable to both directions. The packet filters determine the traffic mapping to PDP contexts. The downlink packet filters shall be used by the network and the uplink packet filters shall be used by the MS. A packet filter that is applicable to both directions shall be used by the network as a downlink packet filter and by the MS as an uplink packet filter.

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 36 bytes. Therefore, 7 maximum size IPv4 type packet filters can fit into one TFT IE, i.e. if needed not all packet filter components can be defined into one message. A maximum size IPv6 packet filter can be 54 bytes. Therefore, only 4 maximum size IPv6 packet filters, plus the last packet filter which can contain max 38 octets can fit into one TFT IE. However, using "Add packet filters to existing TFT", it's possible to create a TFT data structure including 16 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.

NOTE 3: The 3GPP TS 24.301 [120] reuses the *traffic flow template* information element for the purpose of the traffic flow aggregate description, where the use of individual TFT parameters, e.g. the packet filter identifier in the parameter list, can differ from this specification.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | 8 | 7 | 6 | 5 | | 4 | | 3 | 2 | 1 | |  | |
|  | | Traffic flow template IEI | | | | | | | | | | | Octet 1 | |
|  | | Length of traffic flow template IE | | | | | | | | | | | Octet 2 | |
|  | | TFT operation code | | | | E bit | | Number of packet filters | | | | | Octet 3 | |
|  | | Packet filter list | | | | | | | | | | | Octet 4  Octet z | |
|  | | Parameters list | | | | | | | | | | | Octet z+1  Octet v | |

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

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | 0 | 0 | 0 | 0 | Packet filter identifier 1 | | | | Octet 4 |
| Spare | | | |
|  | 0 | 0 | 0 | 0 | Packet filter identifier 2 | | | | Octet 5 |
| Spare | | | |
|  | … | | | | | | | |  |
|  | 0 | 0 | 0 | 0 | Packet filter identifier N | | | | Octet N+3 |
| Spare | | | |

**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)**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | 0 | 0 | Packet filter direction 1 | | Packet filter identifier 1 | | | | Octet 4 |
| Spare | |
|  | Packet filter evaluation precedence 1 | | | | | | | | Octet 5 |
|  | Length of Packet filter contents 1 | | | | | | | | Octet 6 |
|  | Packet filter contents 1 | | | | | | | | Octet 7  Octet m |
|  | 0 | 0 | Packet filter direction 2 | | Packet filter identifier 2 | | | | Octet m+1 |
| Spare | |
|  | Packet filter evaluation precedence 2 | | | | | | | | Octet m+2 |
|  | Length of Packet filter contents 2 | | | | | | | | Octet m+3 |
|  | Packet filter contents 2 | | | | | | | | Octet m+4  Octet n |
|  | … | | | | | | | | Octet n+1  Octet y |
|  | 0 | 0 | Packet filter direction N | | Packet filter identifier N | | | | Octet y+1 |
| Spare | |
|  | Packet filter evaluation precedence N | | | | | | | | Octet y+2 |
|  | Length of Packet filter contents N | | | | | | | | Octet y+3 |
|  | Packet filter contents N | | | | | | | | Octet y+4  Octet z |

**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"**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | Parameter identifier 1 | | | | | | | | Octet z+1 |
|  | Length of Parameter contents 1 | | | | | | | | Octet z+2 |
|  | Parameter contents 1 | | | | | | | | Octet z+3  Octet k |
|  | Parameter identifier 2 | | | | | | | | Octet k+1 |
|  | Length of Parameter contents 2 | | | | | | | | Octet k+2 |
|  | Parameter contents 2 | | | | | | | | Octet k+3  Octet p |
|  | … | | | | | | | | Octet p+1  Octet q |
|  | Parameter identifier N | | | | | | | | Octet q+1 |
|  | Length of Parameter contents N | | | | | | | | Octet q+2 |
|  | Parameter contents N | | | | | | | | Octet q+3  Octet v |

**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 Ignore this IE 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  The TFT operation code "No TFT operation" shall be used if a *parameters list* is included but no *packet filter list* is included in the *traffic flow template* information element.  The TFT operation code "Ignore this IE" shall be used by the MS if the Traffic flow aggregate information element has presence requirement "M" in a message, but the information element does not serve any useful purpose in the specific procedure for which the message is sent (see 3GPP TS 24.301 [120], subclauses 6.5.3.2 and 6.5.4.2). If the TFT operation code indicates "Ignore this IE", the MS shall also set the E bit and the number of packet filters to zero.  If the TFT operation code is set to "Ignore this IE" and the the E bit and the number of packet filters to zero, then the network shall ignore the contents of the traffic flow template information element.  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 15.  Packet filter list (octets 4 to z)  The *packet filter list* contains a variable number of packet filters. For the "delete existing TFT" operation and the "no 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 and direction (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. The least significant 4 bits are used.  The *packet filter direction* is used to indicate, in bits 5 and 6, for what traffic direction the filter applies:  00 - pre Rel-7 TFT filter 01 - downlink only 10 - uplink only 11 - bidirectional  Bits 8 through 7 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.  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 remote address type" and "IPv6 remote address type" packet filter components, only one shall be present in one packet filter. Among the "single local port type" and "local port range type" packet filter components, only one shall be present in one packet filter. Among the "single remote port type" and "remote port range type" packet filter components, only one shall be present in one packet filter.  The term *local* refers to the MS and the term *remote* refers to an external network entity.  Packet filter component type identifier Bits 8 7 6 5 4 3 2 1  0 0 0 1 0 0 0 0 IPv4 remote address type 0 0 0 1 0 0 0 1 IPv4 local address type  0 0 1 0 0 0 0 0 IPv6 remote address type 0 0 1 0 0 0 0 1 IPv6 remote address/prefix length type 0 0 1 0 0 0 1 1 IPv6 local address/prefix length type 0 0 1 1 0 0 0 0 Protocol identifier/Next header type 0 1 0 0 0 0 0 0 Single local port type 0 1 0 0 0 0 0 1 Local port range type 0 1 0 1 0 0 0 0 Single remote port type  0 1 0 1 0 0 0 1 Remote 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 1 0 0 0 0 0 0 1 Destination MAC address type 1 0 0 0 0 0 1 0 Source MAC address type 1 0 0 0 0 0 1 1 802.1Q C-TAG VID type 1 0 0 0 0 1 0 0 802.1Q S-TAG VID type 1 0 0 0 0 1 0 1 802.1Q C-TAG PCP/DEI type 1 0 0 0 0 1 1 0 802.1Q S-TAG PCP/DEI type 1 0 0 0 0 1 1 1 Ethertype type  All other values are reserved.  The description and valid combinations of packet filter component type identifiers in a packet filter are defined in 3GPP TS 23.060 [74] subclause 15.3.2.  For "IPv4 remote 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 "IPv4 local address type", the *packet filter component value* field shall be encoded as defined for "IPv4 remote address type". Both the MS and network indication for support of the Local address in TFTs are required to use this packet filter component.  For "IPv6 remote 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 "IPv6 remote address/prefix length type", the packet filter component value field shall be encoded as a sequence of a sixteen octet IPv6 address field and one octet prefix length field. The IPv6 address field shall be transmitted first. This parameter shall be used, instead of IPv6 remote address type, when both the MS and network indication for support of the Local address in TFT are present.  For "IPv6 local address/prefix length type", the packet filter component value field shall be encoded as defined for "IPv6 remote address /prefix length".  Both the MS and network indication for support of the Local address in TFTs are required to use this packet filter component.  NOTE 1: Local IP address and mask can be used when IPv6 prefix delegation is used (see 3GPP TS 23.060 [74] subclause  9.2.1.2).  NOTE 2: After inter-system change from N1 mode to S1 mode, the MS operating in single-registration mode in a network supporting N26 interface shall deem that Local address in TFT is supported by the network on the PDN connection corresponding to the PDU session (see subclause 6.1.4.1 of 3GPP TS 24.501 [167]).  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 local port type" and "Single remote port type", the *packet filter component value* field shall be encoded as two octet which specifies a port number.  For "Local port range type" and "Remote 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.  Parameters list (octets z+1 to v)  For "destination MAC address type" and "source MAC address type", the *packet filter component value* field shall be encoded as 6 octets which specify a MAC address.  For "802.1Q C-TAG VID type", the *packet filter component value* field shall be encoded as two octets which specify the VID of the customer-VLAN tag (C-TAG). The bits 8 through 5 of the first octet shall be spare whereas the remaining 12 bits shall contain the VID.  For "802.1Q S-TAG VID type", the *packet filter component value* field shall be encoded as two octets which specify the VID of the service-VLAN tag (S-TAG). The bits 8 through 5 of the first octet shall be spare whereas the remaining 12 bits shall contain the VID.  For "802.1Q C-TAG PCP/DEI type", the *packet filter component value* field shall be encoded as one octet which specifies the 802.1Q C-TAG PCP and DEI. The bits 8 through 5 of the octet shall be spare, the bits 4 through 2 contain the PCP and bit 1 contains the DEI.  For "802.1Q S-TAG PCP/DEI type", the *packet filter component value* field shall be encoded as one octet which specifies the 802.1Q S-TAG PCP. The bits 8 through 5 of the octet shall be spare, the bits 4 through 2 contain the PCP and bit 1 contains the DEI.  For "ethertype type", the *packet filter component value* field shall be encoded as two octets which specify an ethertype.  The *parameters list* contains a variable number of parameters that may be transferred. 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); and - 03H (Packet Filter 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 29.207 [100]. The first octet is the most significant octet of the authorization token and the last octet is the least significant octet of the authorization token.  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.  When the *parameter identifier* indicates Flow Identifier, the *parameter contents* field contains the binary representation of a flow identifier. The Flow Identifier consists of four octets. Octets 1 and 2 contains the Media Component number as specified in 3GPP TS 29.207 [100]. Bit 1 of octet 2 is the least significant bit, and bit 8 of octet 1 is the most significant bit. Octets 3 and 4 contains the IP flow number as specified in 3GPP TS 29.207 [100]. Bit 1 of octet 4 is the least significant bit, and bit 8 of octet 3 is the most significant bit.  When the *parameter identifier* indicates Packet Filter Identifier, the parameter contents field contains the binary representation of one or more packet filter identifiers. Each packet filter identifier is encoded in one octet, in the 4 least significant bits. This parameter is used by the MS and the network to identify one or more packet filters in a TFT when modifying the QoS of a PDP context without modifying the packet filter itself. |