**3GPP TSG-CT WG1 Meeting #136-eC1-223754**

**E-Meeting, 12th – 20th May 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.501** | **CR** | **4380** | **rev** | **-** | **Current version:** | **17.6.1** |  |
|  | | | | | | | | |
| *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:*** | Handling of multiple TAGs in the Ethernet header for signalled and derived QoS rules | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | MediaTek Inc. | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GProtoc17 | | | | |  | ***Date:*** | | | 2022-05-04 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | It is not defined which C-TAG should be evaluated when there are multiple C-TAGs in the Ethernet frame header and the packet filter has an C-tag related packet filter component (i.e., C-TAG VID type and/or C-TAG PCP/DEI type).  Since the outermost C-TAG in the Ethernet frame header is last one to be added and should be the one that the UE or the network is most concerned with. It is proposed that the outermost C-TAG should be evaluated.  There could be multiple C-TAGs or multiple S-TAGs in the DL user data packet as well. It’s not defined how the UE derive reflective QoS for that packet. It’s proposed that the UE should set the the packet filter component based on the outermost C-TAG or S-TAG. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | 1. If there are more than one C-TAG or more than one S-TAG in the Ethernet frame header in the received DL user data packet, the UE should set the packet filter component based on the outermost C-TAG or S-TAG. 2. If there are more than one C-TAG in the Ethernet frame header, the outermost C-TAG is evaluated by the packet filter. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | 1. It is not defined which C-TAG or S-TAG should be used when derived packet filter component for reflective QoS. 2. It is not defined which C-TAG should be evaluated when there are multiple C-TAGs in the Ethernet frame header and the packet filter has an C-TAG related packet filter component (i.e., C-TAG VID type and/or C-TAG PCP/DEI type). | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.2.5.1.4.2, 9.11.4.13 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

**\*\*\*\*\*\*\***

\* \* \* First Change \* \* \* \*

###### 6.2.5.1.4.2 Derivation of packet filter for UL direction from DL user data packet

If the UE needs to derive a packet filter for UL direction from the DL user data packet (see subclause 6.2.5.1.4.3 and 6.2.5.1.4.4), the UE shall proceed as follows:

a) if the received DL user data packet belongs to a PDU session of IPv4 or IPv4v6 PDU session type and is an IPv4 packet and:

1) the protocol field of the received DL user data packet indicates TCP as specified in IETF RFC 793 [33];

2) the protocol field of the received DL user data packet indicates UDP as specified in IETF RFC 768 [32]; or

3) the protocol field of the received DL user data packet indicates ESP as specified in IETF RFC 4303 [38] and an uplink IPSec SA corresponding to a downlink IPSec SA indicated in the security parameters index field of the received DL user data packet exists;

then the packet filter for UL direction contains the following packet filter components:

1) an IPv4 remote address component set to the value of the source address field of the received DL user data packet;

2) an IPv4 local address component set to the value of the destination address field of the received DL user data packet;

3) a protocol identifier/next header type component set to the value of the protocol field of the received DL user data packet;

4) if the protocol field of the received DL user data packet indicates TCP as specified in IETF RFC 793 [33] or UDP as specified in IETF RFC 768 [32]:

i) a single local port type component set to the value of the destination port field of the received DL user data packet; and

ii) a single remote port type component set to the value of the source port field of the received DL user data packet;

5) if the protocol field of the received DL user data packet indicates ESP as specified in IETF RFC 4303 [38]:

i) a security parameter index type component set to the security parameters index of the uplink IPSec SA corresponding to the downlink IPSec SA indicated in the security parameters index field of the received DL user data packet; and

6) if the protocol field of the received DL user data packet indicates UDP and the received DL user data packet contains a UDP-encapsulated ESP header as specified in IETF RFC 3948 [55]:

i) a security parameter index type component set to the security parameters index of the uplink IPSec SA corresponding to the downlink IPSec SA indicated in the security parameters index field of the ESP header field of the UDP-encapsulated ESP header as specified in IETF RFC 3948 [55] of the received DL user data packet;

otherwise it is not possible to derive a packet filter for UL direction from the DL user data packet;

b) if the received DL user data packet belongs to a PDU session of IPv6 or IPv4v6 PDU session type and is an IPv6 packet and:

1) the last next header field of the received DL user data packet indicates TCP as specified in IETF RFC 793 [33];

2) the last next header field of the received DL user data packet indicates UDP as specified in IETF RFC 768 [32]; or

3) the last next header field of the received DL user data packet indicates ESP as specified in IETF RFC 4303 [38] and an uplink IPSec SA corresponding to a downlink IPSec SA indicated in the security parameters index field of the received DL user data packet exists;

then the packet filter for UL direction contains the following packet filter components:

1) an IPv6 remote address/prefix length component set to the value of the source address field of the received DL user data packet;

2) an IPv6 local address/prefix length component set to the value of the destination address field of the received DL user data packet;

3) a protocol identifier/next header type component set to the value of the last next header field of the received DL user data packet;

4) if the last next header field of the received DL user data packet indicates TCP as specified in IETF RFC 793 [33] or UDP as specified in IETF RFC 768 [32]:

i) a single local port type component set to the value of the destination port field of the received DL user data packet; and

ii) a single remote port type component set to the value of the source port field of the received DL user data packet;

5) if the last next header field of the received DL user data packet indicates ESP as specified in IETF RFC 4303 [38]:

i) a security parameter index type component set to the security parameters index of the uplink IPSec SA corresponding to the downlink IPSec SA indicated in the security parameters index field of the received DL user data packet; and

6) if the protocol field of the received DL user data packet indicates UDP, and the received DL user data packet contains a UDP-encapsulated ESP header as specified in IETF RFC 3948 [55]:

i) a security parameter index type component set to the security parameters index of the uplink IPSec SA corresponding to the downlink IPSec SA indicated in the security parameters index field of the ESP header field of the UDP-encapsulated ESP header as specified in IETF RFC 3948 [55] of the received DL user data packet;

otherwise it is not possible to derive a packet filter for UL direction from the DL user data packet;

c) if the received DL user data packet belongs to a PDU session of Ethernet PDU session type, the packet filter for UL direction contains the following packet filter components:

1) a destination MAC address component set to the source MAC address of the received DL user data packet;

2) a source MAC address component set to the destination MAC address of the received DL user data packet;

3) if one or more 802.1Q C-TAG is included in the received DL user data packet, an 802.1Q C-TAG VID component set to the outermost 802.1Q C-TAG VID of the received DL user data packet and an 802.1Q C-TAG PCP/DEI component set to the outermost 802.1Q C-TAG PCP/DEI of the received DL user data packet;

4) if one or more 802.1Q S-TAG is included in the received DL user data packet, an 802.1Q S-TAG VID component set to the outermost 802.1Q S-TAG VID of the received DL user data packet and an 802.1Q S-TAG PCP/DEI component set to the outermost 802.1Q S-TAG PCP/DEI of the received DL user data packet;

5) If the Ethertype field of the received DL user data packet is set to a value of 1536 or above, an Ethertype component set to the Ethertype of the received DL user data packet;

6) if the Ethertype field of the Ethernet frame header indicates that the data carried in the Ethernet frame is IPv4 data, the UE shall also add to the packet filter for UL direction the IP-specific components based on the contents of the IP header of the received DL user data packet as described in bullet a) above; and

7) if the Ethertype field of the Ethernet frame header indicates that the data carried in the Ethernet frame is IPv6 data, the UE shall also add to the packet filter for UL direction the IP-specific components based on the contents of the IP header of the received DL user data packet as described in bullet b) above; and

d) if the received DL user data packet belongs to a PDU session of PDU session type other than Ethernet, IPv4, IPv6 and IPv4v6, it is not possible to derive a packet filter for UL direction from the DL user data packet.

\* \* \* Next Change \* \* \* \*

<Proposed change in revision marks>

#### 9.11.4.13 QoS rules

The purpose of the QoS rulesinformation element is to indicate a set of QoS rules to be used by the UE, where each QoS rule is a set of parameters as described in subclause 6.2.5.1.1.2:

a) for classification and marking of uplink user traffic; and

b) for identification of a QoS flow which the network is to use for a particular downlink user traffic.

NOTE: The UE needs to be aware of a QoS flow which the network is to use for a particular downlink user traffic e.g. to determine whether a resource is available for downlink media of a media stream of an SDP media description provided by the UE in an IMS session.

The QoS rules may contain a set of packet filters consisting of zero or more packet filters for UL direction, zero or more packet filters for DL direction, zero or more packet filters for both UL and DL directions or any combinations of these. The set of packet filters determine the traffic mapping to QoS flows.

The QoS rules information element is a type 6 information element with a minimum length of 7 octets. The maximum length for the information element is 65538 octets.

The QoS rulesinformation element is coded as shown in figure 9.11.4.13.1, figure 9.11.4.13.2, figure 9.11.4.13.3, figure 9.11.4.13.4 and table 9.11.4.13.1.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | QoS rules IEI | | | | | | | | octet 1 |
|  | Length of QoS rules IE | | | | | | | | octet 2 |
|  | octet 3 |
|  | QoS rule 1 | | | | | | | | octet 4  octet u |
|  | QoS rule 2 | | | | | | | | octet u+1  octet v |
|  | … | | | | | | | | octet v+1  octet w |
|  | QoS rule n | | | | | | | | octet w+1  octet x |

Figure 9.11.4.13.1: QoS rules information element

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | 6 | 5 | | 4 | | 3 | 2 | 1 |  |
|  | QoS rule identifier | | | | | | | | | | octet 4 |
|  | Length of QoS rule | | | | | | | | | | octet 5 |
|  | octet 6 |
|  | Rule operation code | | | | DQR bit | | Number of packet filters | | | | octet 7 |
|  | Packet filter list | | | | | | | | | | octet 8\*  octet m\* |
|  | QoS rule precedence | | | | | | | | | | octet m+1\* |
|  | 0  Spare | Segregation | QoS flow identifier (QFI) | | | | | | | | octet m+2\* |

Figure 9.11.4.13.2: QoS rule (u=m+2)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | 0 | 0 | 0 | 0 | Packet filter identifier 1 | | | | octet 8 |
| Spare | | | |
|  | 0 | 0 | 0 | 0 | Packet filter identifier 2 | | | | octet 9 |
| Spare | | | |
|  | … | | | | | | | |  |
|  | 0 | 0 | 0 | 0 | Packet filter identifier N | | | | octet N+7 |
| Spare | | | |

Figure 9.11.4.13.3: Packet filter list when the rule operation is "modify existing QoS rule and delete packet filters" (z=N+7)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | 0 | 0 | Packet filter direction 1 | | Packet filter identifier 1 | | | | octet 8 |
| Spare | |
|  | Length of packet filter contents 1 | | | | | | | | octet 9 |
|  | Packet filter contents 1 | | | | | | | | octet 10  octet m |
|  | 0 | 0 | Packet filter direction 2 | | Packet filter identifier 2 | | | | octet m+1 |
| Spare | |
|  | Length of packet filter contents 2 | | | | | | | | octet m+2 |
|  | Packet filter contents 2 | | | | | | | | octet m+3  octet n |
|  | … | | | | | | | | octet n+1  octet y |
|  | 0 | 0 | Packet filter direction N | | Packet filter identifier N | | | | octet y+1 |
| Spare | |
|  | Length of packet filter contents N | | | | | | | | octet y+2 |
|  | Packet filter contents N | | | | | | | | octet y+3  octet z |

Figure 9.11.4.13.4: Packet filter list when the rule operation is "create new QoS rule", or "modify existing QoS rule and add packet filters" or "modify existing QoS rule and replace all packet filters"

Table 9.11.4.13.1: QoS rules information element

|  |
| --- |
| QoS rule identifier (octet 4)  The QoS rule identifier field is used to identify the QoS rule.  Bits  8 7 6 5 4 3 2 1  0 0 0 0 0 0 0 0 no QoS rule identifier assigned  0 0 0 0 0 0 0 1 QRI 1  to  1 1 1 1 1 1 1 1 QRI 255  The network shall not set the QRI value to 0.  QoS rule precedence (octet m+1)  The QoS rule precedence field is used to specify the precedence of the QoS rule among all QoS rules (both the signalled QoS rules as described in subclause 6.2.5.1.1.2 and the derived QoS rules as described in subclause 6.2.5.1.1.3) associated with the PDU session of the QoS flow. This field includes the binary coded value of the QoS rule precedence in the range from 0 to 255 (decimal). The higher the value of the QoS rule precedence field, the lower the precedence of that QoS rule is. For the "delete existing QoS rule" operation, the QoS rule precedence value field shall not be included. For the "create new QoS rule" operation, the QoS rule precedence value field shall be included.  The value 80 (decimal) is reserved.  Segregation bit (bit 7 of octet m+2) (see NOTE 1)  In the UE to network direction the segregation bit indicates whether the UE is requesting the network to bind service data flows described by the QoS rule to a dedicated QoS Flow and it is encoded as follows. In the network to UE direction this bit is spare.  Bit  7  0 Segregation not requested  1 Segregation requested  QoS flow identifier (QFI) (bits 6 to 1 of octet m+2) (see NOTE 1)  The QoS flow identifier (QFI) field contains the QoS flow identifier.  Bits  6 5 4 3 2 1  0 0 0 0 0 0 no QoS flow identifier assigned  0 0 0 0 0 1 QFI 1  to  1 1 1 1 1 1 QFI 63  The network shall not set the QFI value to 0.  For the "delete existing QoS rule" operation, the QoS flow identifier value field shall not be included. For the "create new QoS rule" operation, the QoS flow identifier value field shall be included.  DQR bit (bit 5 of octet 7)  The DQR bit indicates whether the QoS rule is the default QoS rule and it is encoded as follows:  Bit  5  0 the QoS rule is not the default QoS rule.  1 the QoS rule is the default QoS rule.  Rule operation code (bits 8 to 6 of octet 7) Bits 8 7 6  0 0 0 Reserved 0 0 1 Create new QoS rule  0 1 0 Delete existing QoS rule  0 1 1 Modify existing QoS rule and add packet filters  1 0 0 Modify existing QoS rule and replace all packet filters  1 0 1 Modify existing QoS rule and delete packet filters  1 1 0 Modify existing QoS rule without modifying packet filters  1 1 1 Reserved  Number of packet filters (bits 4 to 1 of octet 7)  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 7 where bit 4 is the most significant and bit 1 is the least significant bit. For the "delete existing QoS rule" operation and for the "modify existing QoS rule without modifying packet filters" operation, the number of packet filters shall be coded as 0. For the "create new QoS rule" operation and the "modify existing QoS rule and replace all packet filters" operation, the number of packet filters shall be greater than or equal to 0 and less than or equal to 15. 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 8 to m)  The packet filter list contains a variable number of packet filters.  For the "delete existing QoS rule" operation, the length of QoS rule field is set to one.  For the "delete existing QoS rule" operation and the "modify existing QoS rule without modifying packet filters" operation, the packet filter list shall be empty.  For the "modify existing QoS rule and delete packet filters" 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 7.  For the "create new QoS rule" operation and for the "modify existing QoS rule and replace all packet filters" operation, the packet filter list shall contain 0 or a variable number of packet filters. This number shall be derived from the coding of the number of packet filters field in octet 7.  For the "modify existing QoS rule and add packet filters" operation, 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 7.  Each packet filter is of variable length and consists of  a packet filter direction (2 bits);  - a packet filter identifier (4 bits);  - the length of the packet filter contents (1 octet); and - the packet filter contents itself (variable amount of octets).  The packet filter direction field is used to indicate for what traffic direction the filter applies.  Bits  6 5  0 0 reserved  0 1 downlink only (see NOTE 2)  1 0 uplink only  1 1 bidirectional  The packet filter identifier field is used to identify each packet filter in a QoS rule. The least significant 4 bits are used. When the UE requests to "create new QoS rule", "modify existing QoS rule and replace all packet filters" or "modify existing QoS rule and add packet filters", the packet filter identifier values shall be set to 0.  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/prefix length type" packet filter components, only one shall be present in one packet filter. Among the "IPv4 local address type" and "IPv6 local address/prefix length 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. If the "match-all type" packet filter component is present in the packet filter, no other packet filter component shall be present in the packet filter and the length of the packet filter contents field shall be set to one. If the "Ethertype type" packet filter component is present in the packet filter and the "Ethertype type" packet filter component value is neither "0x0800" (for IPv4) nor "0x86DD" (for IPv6), no IP packet filter component shall be present in the packet filter.  The term "IP packet filter component" refers to "IPv4 remote address type", "IPv4 local address type", "IPv6 remote address/prefix length type", "IPv6 local address/prefix length type", "Protocol identifier/Next header type", "Single local port type", "Local port range type", "Single remote port type", "Remote port range type", "Security parameter index type", "Type of service/Traffic class type" and "Flow label type".  The term local refers to the UE 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 0 0 0 0 1 Match-all type (see NOTE 2) 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 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 1 0 0 0 1 0 0 0 Destination MAC address range type 1 0 0 0 1 0 0 1 Source MAC address range 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 23.501 [8].  For "match-all type", the packet filter component shall not include the packet filter component value field.  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".  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.  For "IPv6 local address/prefix length type", the packet filter component value field shall be encoded as defined for "IPv6 remote address /prefix length".  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 octets which specify 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 octets which specify 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 octets which specify 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.  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. When the packet filter direction field indicates "bidirectional", the destination MAC address is the remote MAC address and the source MAC address is the local 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. If there are more than one C-TAG in the Ethernet frame header, the outermost C-TAG is evaluated.  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. If there are more than one S-TAG in the Ethernet frame header, the outermost S-TAG is evaluated.  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. If there are more than one C-TAG in the Ethernet frame header, the outermost C-TAG is evaluated.  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. If there are more than one S-TAG in the Ethernet frame header, the outermost S-TAG is evaluated.  For "ethertype type", the packet filter component value field shall be encoded as two octets which specify an ethertype.    For "destination MAC address range type", the packet filter component value field shall be encoded as a sequence of a 6 octet destination MAC address range low limit field and a 6 octet destination MAC address range high limit field. The destination MAC address range low limit field shall be transmitted first. When the packet filter direction field indicates "bidirectional", the destination MAC address range is the remote MAC address range.  For "source MAC address range type", the packet filter component value field shall be encoded as a sequence of a 6 octet source MAC address range low limit field and a 6 octet source MAC address range high limit field. The source MAC address range low limit field shall be transmitted first. When the packet filter direction field indicates "bidirectional", the source MAC address is the local MAC address range. |
| NOTE 1: Octet m+2 shall not be included without octet m+1.  NOTE 2: The "Match-all type" packet filter component type identifier shall not be used with packet filter direction "downlink only". |

\* \* \* End of Changes \* \* \* \*