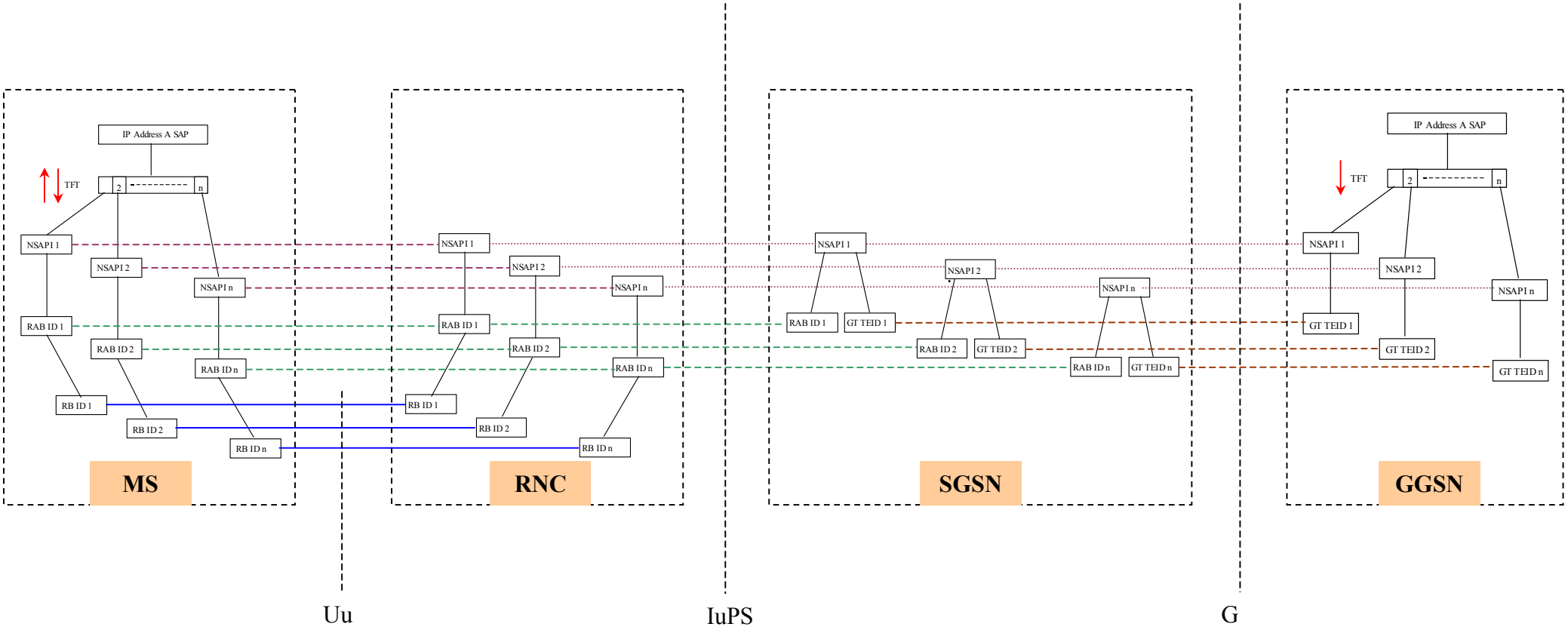

The MS is responsible for creating or modifying PDP contexts and their QoS (see details of TFT from TS24.008). Each NSAPI has an associated UMTS QoS. The MS should define TFTs in such a way that downlink PDP PDUs are routed to a PDP context that best matches the QoS requested by the receiver of this PDU (e.g., an application supporting QoS).

For each uplink PDP PDU, the MS should choose the PDP context that best matches the QoS requested by the sender of this PDP PDU (e.g., an application supporting QoS). Packet classification and routeing within the MS is an MS-local matter.

For downlink PSUs, when multiple PDP contexts exist for the same PDP address of an MS, the GGSN routes each to different GTP tunnels based on the TFTs assigned to the PDP contexts. Upon reception of a PDP PDU, the GGSN evaluates for a match, first the packet filter amongst all TFTs that has the smallest evaluation precedence index and, in case no match is found, proceeds with the evaluation of packet filters in increasing order of their evaluation precedence index. This procedure shall be executed until a match is found, in which case the N-PDU is tunnelled to the SGSN via the PDP context that is associated with the TFT of the matching packet filter. If no match is found, the N-PDU shall be sent via the PDP context that does not have a TFT assigned to it; if all PDP contexts have a TFT assigned, the GGSN shall silently discard the PDP PDU.

The GGSN shall not match uplink N-PDUs against TFTs. For uplink PDUs, the GGSN doesn't route using TFT – all PDUs are routed to the same next hop IP router. If supported RSVP or Diffserv QoS can be setup for individual IP streams from each UMTS bearer.

From TS24.008

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 (Source address of external server)
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 (TCP/UDP etc)
0 1 0 0 0 0 0 0 Single destination port type (destination port number at UE)
0 1 0 0 0 0 0 1 Destination port range type
0 1 0 1 0 0 0 0 Single source port type (destination port number at external server)
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 (ToS byte in IP header)
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.

Example from TS23.060

15.3.3 Example Usage of Packet Filters

Based on the type of traffic or the external-network QoS capabilities, different types of packet filters can be used to classify a given PDP PDU in order to determine the right PDP context. Some examples are given below.

15.3.3.1 IPv4 Multi-field Classification

In the case of multi-field classification, the packet filter consists of a number of packet header fields. For example, to classify TCP/IPv4 packets originating from 172.168.8.0/24 destined to port 5 003 at the TE, the following packet filter can be used:

- Packet Filter Identifier = 1;
- IPv4 Source Address = {172.168.8.0 [255.255.255.0]};
- Protocol Number for TCP = 6; and
- Destination Port = 5 003.

15.3.3.2 IPv4 TOS-based Classification

In the case of TOS-based classification, the packet filter consists of only the TOS octet coding. For example to classify IPv4 packets marked with TOS coding 001010xx, the following packet filter can be used:

- Packet Filter Identifier = 3;
- Type of Service / Traffic Class = 00101000 and Mask = 11111100.

NOTE: The TOS-based classification can always be augmented with the source address attribute if it is known that different source domains use different TOS octet codings for the same traffic class.

15.3.3.3 IPv4 Multi-field Classification for IPSec Traffic

In the case of multi-field classification of IPSec traffic, the packet filter contains the SPI instead of the port numbers that are not available due to encryption. If IPSec (ESP) was used with an SPI of 0x0F80F000, then the following packet filter can be used:

- Packet Filter Identifier = 4;
- Protocol Number for ESP = 50; and
- SPI = 0x0F80F000.