Verify the 5G SMF DSCP Marking for N3/S5-U/S2-B over PFCP

Contents

Introduction

This document describes Differentiated Services Code Point (DSCP) Marking for N3/S5-U/S2-B over Packet Forwarding Control Protocol (PFCP).

Background Information

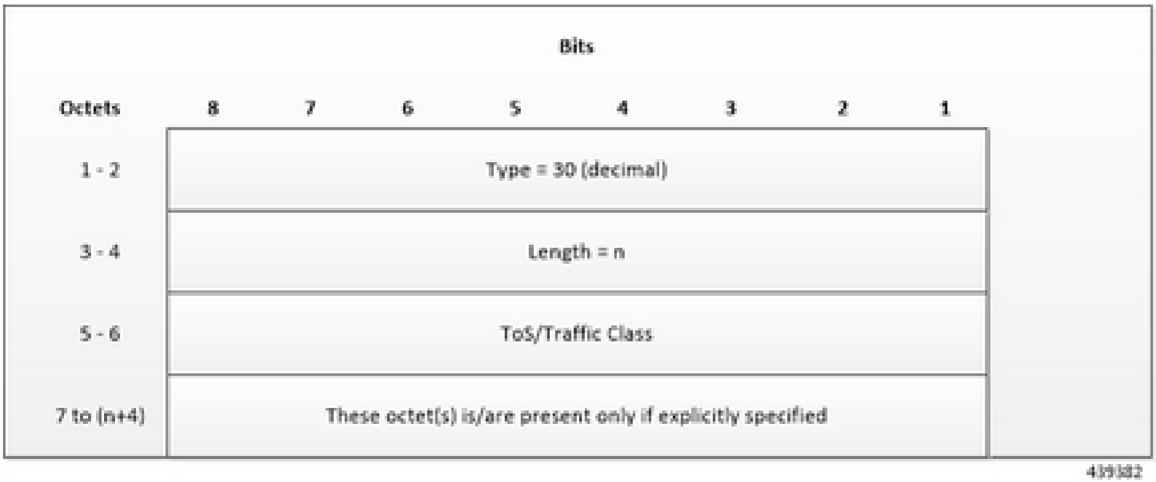
DSCP Marking supports the granular configuration of DSCP. For Interactive Traffic Class (ITC), the Subscriber management Function (SMF) supports per-Access Point Name (APN) configurable DSCP marking for Uplink and Downlink direction that is based on 5QI and Allocation and Retention Policy (ARP)-Priority levels. This allows you to assign different DSCP values for flows with the same 5QI but different ARP priority values. For example, the ability to assign DSCP values that are based on 5QI+ARP can be used to meet compliance on priority and emergency calls via VoLTE.

> **Note**: DSCP Marking is a CLI-controlled feature, which enables to create and map 5QI and ARP values to enforceable QoS parameters.

Transport Level Marking

Transport-level marking is the process of marking traffic at the User Plane Function (UPF) with a DSCP value. The transport-level marking, executed on per-QoS flow, is based on the mapping from the 5QI and optional ARP configuration from the SMF. The SMF controls the transport-level marking and provides the DSCP in the ToS (IPv4) or Traffic Class (IPv6) within the **Transport Level Marking** Information Element (IE) in the Forward AC=ction Rule (FAR), which is associated with the PDR that matches the traffic to be marked. The UPF performs the transport level marking for the detected traffic and sends the marked packet to the peer entity. The SMF can change the transport-level marking by the change of the **Transport Level Marking IE** in the related FAR. The UPF also supports the inner packet marking in which it marks the tunnel packets. As the 3GPP specification does not determine any specific IE, the UPF uses a private IE named **Inner Packet Marking**. In addition, there is also a provision to copy the DSCP of the inner packet to the outer IP header. As the 3GPP specification does not determine any specific IE, the UPF uses a private IE named **Transport Level Marking Options**.

The Transport Level Marking IE type is encoded as shown in this image. It indicates the DSCP value for the downlink transport-level marking.



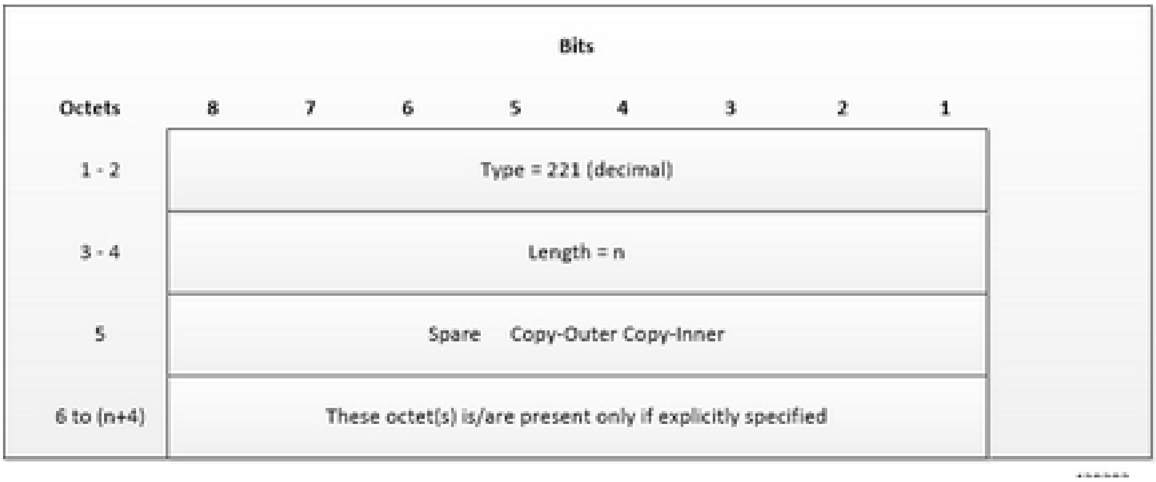
	Bits
Octets	8 7 6 5 4 3 2 1
1 - 2	Type = 30 (decimal)
3 - 4	Length = n
5 - 6	ToS/Traffic Class
7 to (n+4)	These octet(s) is/are present only if explicitly specified

439382

At this point, you encode the Type-of-Service (ToS) or the Traffic Class takes place in the form of two octets as an OctetString. The first octet contains the DSCP value in the IPv4 Type-of-Service or the IPv6 Traffic-Class field and the second octet contains the ToS or Traffic Class mask field, which is set to 0xFC.

Transport Level Marking Options IE

The **Transport Level Marking Options** IE type is encoded as shown in this image. The DSCP for downlink transport-level marking is copied from the inner packet.

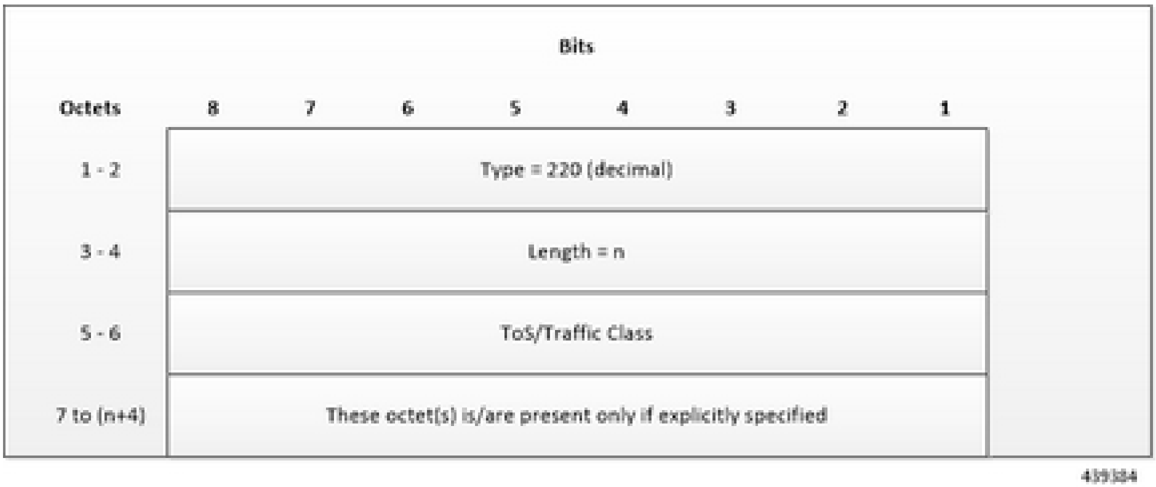


	Bits
Octets	8 7 6 5 4 3 2 1
1 - 2	Type = 221 (decimal)
3 - 4	Length = n
5	Spare Copy-Outer Copy-Inner
6 to (n+4)	These octet(s) is/are present only if explicitly specified

The Copy-Inner and Copy-Outer flags are present in bit-0 and bit-1 of octet 5. Copy-Outer flag is not used for downlink packets because there is no outer header present in packets received from ISP. If a Copy-Inner flag is present, then the UPF uses the DSCP value from the inner packet to mark the transport-level IP header.

Inner Packet Marking IE

The **Inner Packet Marking** IE type is encoded as shown in this image. It indicates the DSCP value for the downlink **Inner Packet Marking**.



	Bits							
Octets	8	7	6	5	4	3	2	1
1 - 2	Type = 220 (decimal)							
3 - 4	Length = n							
5 - 6	ToS/Traffic Class							
7 to (n+4)	These octet(s) is/are present only if explicitly specified							

439384

Now, encode the ToS or Traffic Class in the form of two octets as an OctetString. The first octet contains the DSCP value in the IPv4 ToS or the IPv6 Traffic Class field and the second octet contains the ToS or Traffic Class mask field, which is set to 0xFC.

> **Note**: The original Ethernet Consist Network (ECN) bits in the IP header of User Plane packets do not change after the transport-level marking or **Inner Packet Marking** is applied. If **Transport Level Marking IE**, **Inner Packet Marking IE**, or both the IEs are associated with uplink FAR, then the next rule applies for uplink packet marking: If **Transport Level Marking** or **Inner Packet Marking IE** is present, its DSCP value is used. If both **Transport Level Marking** and **Inner Packet Marking IE** are present, then the value from **Transport Level Marking IE** is used for uplink packet marking.

Now let's look at the SMF configuration. You can see that in the dnn profile for **dnnprof-alpha** that the qos-profile is set to **5qi-to-dscp-mapping-table**.

```
profile dnn dnnprof-alpha dns primary ipv4 10.177.0.34 dns primary ipv6 fd00:976a::9 dns
secondary ipv4 10.177.0.210 dns secondary ipv6 fd00:976a::10 network-element-profiles chf nfprf-
chf1 network-element-profiles amf nfprf-amf1 network-element-profiles pcf nfprf-pcf1 network-
element-profiles udm nfprf-udm1 dnn alpha network-function-list [ chf pcf upf ] dnn rmgr mvno-
pool-ipv6 timeout up-idle 3600 cp-idle 7320 charging-profile chgprof-1 wps-profile dynamic-wps
ssc-mode 1 allowed [ 2 ] session type IPV4V6 allowed [ IPV4 IPV6 ] upf apn alpha qos-profile
5qi-to-dscp-mapping-table always-on false userplane-inactivity-timer 3600 only-nr-capable-ue
true exit
```

The 5qi-to-dscp-mapping-table can be seen in the profile qos configuration.

```
profile qos 5qi-to-dscp-mapping-table dscp-map qi5 6 uplink user-datagram dscp-marking 0x0c
dscp-map qi5 6 downlink encsp-header dscp-marking 0x0c dscp-map qi5 7 uplink user-datagram dscp-
marking 0x0e dscp-map qi5 7 downlink encsp-header dscp-marking 0x0e dscp-map qi5 8 uplink user-
datagram dscp-marking 0x0e dscp-map qi5 8 downlink encsp-header dscp-marking 0x0e dscp-map qi5 9
uplink user-datagram dscp-marking 0x0a dscp-map qi5 9 downlink encsp-header dscp-marking 0x0a
exit
```

The Cisco UPF provides different enforcement mechanisms based on policy received from the SMF. The UPF is the boundary between the Access and IP domains and is the ideal location to implement policy-based enforcement. The pcc-rules provided by the PCF and the pre-defined rules on the SMF are uploaded over the N4 interface and installed on the UPF on a per-Data

Networking Name (DNN) basis. This allows for dynamic policy changes that enable differentiated charging and QoS enforcement.