DSCP Marking

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Revision Details	Release
Provided support for DSCP marking of control plane signaling messages	2021.01.0
First introduced.	Pre-2020.02.0

Feature Description

The SMF supports a mechanism for differentiated services code point (DSCP) marking of user plane data packets and control plane signaling messages.

The DSCP Marking feature enables the SMF to perform traffic classification and prioritisation to provide the appropriate quality of service (QoS) treatment. DSCP is the six most significant bit of the DiffServ field.

Implementation of this feature requires the use of certain CLIs commands to configure DSCP parameters for both signaling messages and data packets.

DSCP Marking for User Plane Packets

Feature Description

DSCP Marking supports granular configuration. For Interactive Traffic Class (ITC), the SMF supports per-APN configurable DSCP marking for Uplink and Downlink direction that is based on 5QI and ARP-Priority level. This support allows the users 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 calling via VoLTE.

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

How the DSCP Marking Works for Data Packets

Allocation of different DSCP values for flows with the same 5QI, but different ARP values, works as follows:

- Allows DSCP marking of packets that is based on 5QI+ARP combination.
- 5QI+ARP configuration overrides any pre-entry of DSCP marking of packets that was based on 5QI+ARP combination.
- 5QI-only DSCP entry overrides all existing 5QI+ARP configuration.
- Allows implementation of associated DSCP marking for 5QI+ARP for Uplink and Downlink functionality.

Configuring 5QI-QoS Mapping

Use the following CLI commands to create and map 5QI values to enforceable QoS parameters.

```
configure
   profile qos qos_name
      dscp-map qi5 qi5_value [ arp-priority-level arp_value ] uplink
user-datagram dscp-marking dscp_marking_value
      dscp-map qi5 5qi_value [ arp-priority-level arp_value ] downlink {
encaps-header { copy-inner | dscp-marking dscp_marking_value } | user-datagram
 dscp-marking dscp_marking_value encaps-header { copy-inner | dscp-marking
dscp_marking_value } }
      commit
```

NOTES:

- **dscp-map**: Configures 5QI (referred as qi5 in the code) to DSCP-Marking mapping.

- **qi5** *5qi_value*: Identifier for the authorized QoS parameters. The *5qi_value* must be within the range of 0 through 255.
- **arp-priority-level** *arp_value*: Configures the ARP Priority Level. The *arp_value* must be an integer from 1 through 15.
- **downlink**: Configures the downlink traffic.
- **uplink**: Configures the uplink traffic.
- **user-datagram**: Specifies the DSCP value to be applied to user datagram. Use this keyword to set the DSCP in the inner IP header in uplink or downlink direction.
- **dscp-marking**: Specifies the DSCP value to be applied to packets with this 5QI. The value of **dscp-marking** must be a hexadecimal number from 0x00 through 0x3F.
- **encaps-header**: Configures the DSCP value to be applied to encaps header. Use this keyword to set the DSCP in the outer-ip header in downlink direction.
- **copy-inner**: Copies the DSCP value from inner IP header to the outer IP header.

The following is a sample configuration.

```
profile qos test
 dscp-map qi5 1 downlink encaps-header copy-inner
 dscp-map qi5 1 downlink encaps-header dscp-marking 0x3b
 dscp-map qi5 2 downlink user-datagram dscp-marking 0x3b
 dscp-map qi5 3 downlink user-datagram dscp-marking 0x3b encaps-header copy-inner
 dscp-map qi5 4 downlink user-datagram dscp-marking 0x3b encaps-header dscp-marking 0x3f
 dscp-map qi5 2 uplink user-datagram dscp-marking 0x3b

 dscp-map qi5 1 arp-priority-level 1 downlink encaps-header copy-inner
 dscp-map qi5 2 arp-priority-level 2 downlink encaps-header dscp-marking 0x3b
 dscp-map qi5 4 arp-priority-level 3 downlink user-datagram dscp-marking 0x3b
 dscp-map qi5 2 arp-priority-level 4 downlink user-datagram dscp-marking 0x3b encaps-header
 copy-inner
 dscp-map qi5 4 arp-priority-level 5 downlink user-datagram dscp-marking 0x3b encaps-header
 dscp-marking 0x3f
 dscp-map qi5 4 arp-priority-level 5 uplink user-datagram dscp-marking 0x3b
```

DSCP Marking for Control Plane Signaling

Feature Description

The SMF supports per-interface configurable DSCP marking for control plane signaling messages.

Note The current implementation of DSCP marking supports only per RPC and Endpoint. Also, the customers should be aware of the DSCP code value range and its denoted priority.

How the DSCP Marking Works for Control Signaling

The SMF marks the ingress and egress packets after the QoS classification. The protocol endpoints provide the DSCP values at the time of registering the Endpoint and RPC host.

The SMF uses the **dscp** command in the endpoint and interface configuration to define the DSCP values.

The following table lists the commonly used DSCP values as described in RFC 2475.

Table 1: Commonly Used DSCP Values

DSCP Value	Decimal Value	Meaning	Drop Probability	Equivalent IP Precedence Value
101 110	46	High Priority Expedited Forwarding (EF)	N/A	101 - Critical
000 000	0	Best Effort	N/A	000 - Routine
001 010	10	AF11	Low	001 - Priority
001 100	12	AF12	Medium	001 - Priority
001 110	14	AF13	High	001 - Priority
010 010	18	AF21	Low	010 - Immediate
010 100	20	AF22	Medium	010 - Immediate
010 110	22	AF23	High	010 - Immediate
011 010	26	AF31	Low	011 - Flash
011 100	28	AF32	Medium	011 - Flash
011 110	30	AF33	High	011 - Flash
100 010	34	AF41	Low	100 - Flash Override
100 100	36	AF42	Medium	100 - Flash Override
100 110	38	AF43	High	100 - Flash Override
001 000	8	CS1		1
010 000	16	CS2		2
011 000	24	CS3		3
100 000	32	CS4		4
101 000	40	CS5		5
110 000	48	CS6		6
111 000	56	CS7		7

DSCP Value	Decimal Value	Meaning	Drop Probability	Equivalent IP Precedence Value
000 000	0	Default		
101 110	46	EF		

Limitations

The DSCP Marking is per interface basis and not per peer or session.

Configuring DSCP Marking for Control Plane Signaling

The following sections provide the configurations required for the DSCP marking of signaling messages.

Configuring DSCP Marking per Endpoint

Use the following sample configuration to configure the DSCP values at the endpoint level.

```
config
      endpoint { gtp | li | protocol | radius | sbi }
         dscp dscp_value
         commit
```

NOTES:

- The DSCP Marking configuration is applicable only to the following endpoints:
  - protocol
  - sbi
  - gtp
  - radius
  - li
- **dscp** *dscp_value*: Specify the DSCP value for the control plane signaling messages. *dscp_value* must be a hexadecimal number from 0x00 through 0x3F or a decimal value ranging from 0 through 63.
- The DSCP Marking feature supports dynamic change of the configuration.

Confuring DSCP Marking per Interface

Use the following sample configuration to configure the DSCP values at the interface level.

```
configure
      endpoint { gtp | li | protocol | radius | sbi }
         interface { coa-nas | gtpu | n4 | n7 | n10 | n11 | n16 | n40 |
nrf | radius-client | s2b | s5 | s8 | upf-rcm-conn | upf-rcm-reg }
```

```
dscp dscp_value
commit
```

NOTES:

- The DSCP marking configuration is applicable to all the interfaces defined within the configured endpoints.
- **dscp** *dscp_value*: Configures the DSCP value for the control plane signaling messages. *dscp_value* must be a hexadecimal number from 0x00 through 0x3F or a decimal value ranging from 0 through 63.
- The DSCP Marking feature supports dynamic change of the configuration.
- The Service-based Interface (SBI) configuration applies to all the interfaces. If a specific interface configuration is present, it overrides the DSCP values.
- For the interfaces to work properly, it is mandatory to configure vip-ip, vip-port, and loopbackPort at each interface level.