

DSCP Marking

- Feature Summary and Revision History, on page 1
- Feature Description, on page 1
- DSCP Marking for Data Packets, on page 2
- DSCP Marking for Control Plane Signaling, on page 4

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 prioritization to provide the appropriate quality of service (QoS) treatment. DSCP is a significant bit in the DiffServ field.

This feature uses CLI commands to configure DSCP parameters for both signaling messages and data packets. For configuration details, see the Configuring 5QI-QoS Mapping, on page 2 and Configuring DSCP Marking for Control Plane Signaling, on page 6 sections in this chapter.



Note This feature is also applicable on 4G calls with legacy interfaces.

DSCP Marking for Data 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.

The SMF sends the configured DSCP value to the UPF. Then, the UPF applies the DSCP marking on the uplink and downlink packets based on the 5QI and ARP.

How the DSCP Marking Works for Data Packets

This section describes how the DSCP marking can be performed for the 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 based on 5QI and ARP combination.
- 5QI and ARP configuration overrides any pre-entry of DSCP marking of packets that was based on 5QI and ARP combination.
- 5QI-only DSCP entry overrides all the existing 5QI and ARP configuration.
- Allows implementation of associated DSCP marking for 5QI and ARP for uplink and downlink traffic.

Configuring 5QI-QoS Mapping

Use the following sample configuration to create and map 5QI values to enforceable QoS parameters.

```
config
   profile qos qos_profile_name
      dscp-map qi5 qos_id
      arp-priority-level arp_value uplink user-datagram dscp-marking
```

```
dscp_marking_value
      arp-priority-level arp_value downlink { encsp-header { copy-inner |
dscp-marking dscp_marking_value } | user-datagram dscp-marking dscp_marking_value
 } }
      commit
```

NOTES:

- **dscp-map qi5** *qos_id*: Specify the ID for the authorized QoS parameters. *qos_id* must be an integer in the range of 1-255.



Note If the DSCP configuration is unavailable at the QoS flow level but available at the QoS profile level, then DSCP configuration is used from the QoS profile level.

- **arp-priority-level** *arp_value* **uplink user-datagram dscp-marking** *dscp_marking_value*: Configure the ARP priority level and then set the DSCP value in the inner IP header in uplink direction. This DSCP value is applied to the packets with the configured 5QI value.

  arp_value must be an integer in the range of 1-255.

  dscp_marking_value must be a hexadecimal number from 0x00 through 0x3F.

- **arp-priority-level** *arp_value* **downlink { encsp-header { copy-inner | dscp-marking** *dscp_marking_value* **} | user-datagram dscp-marking** *dscp_marking_value* **} }**: Configure the ARP priority level and then set the DSCP value to be applied to encapsulation header or user datagram.

  If **encsp-header** is configured, set the DSCP in the outer-ip header in downlink direction or copy the DSCP value from inner IP header to the outer IP header.

  If **user-datagram** is configured, set the DSCP in the inner IP header in downlink direction.

  arp_value must be an integer in the range of 1-255.

  dscp_marking_value must be a hexadecimal number from 0x00 through 0x3F.

The following is an example 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
```

Verifying DSCP Configuration for UP Packets

This section describes how to verify the DSCP Marking feature configuration for the UP packets.

Use the **show running-config profile qos** command to verify the DSCP configuration for UP packets.

The following is an example output of the **show running-config profile qos** command.

```
smf# show running-config profile qos
profile qos abc
 ambr ul "250 Kbps"
 ambr dl "500 Kbps"
 qi5      7
 arp priority-level 14
 arp preempt-cap NOT_PREEMPT
 arp preempt-vuln PREEMPTABLE
 priority 120
 max data-burst 2000
exit
profile qos qos_1
 dscp-map qi5 1 arp-priority-level 5 uplink user-datagram dscp-marking 0x1e
 dscp-map qi5 1 arp-priority-level 5 downlink user-datagram dscp-marking 0x22 encsp-header
 copy-inner
 dscp-map qi5 2 arp-priority-level 6 uplink user-datagram dscp-marking 0x3e
 dscp-map qi5 2 arp-priority-level 6 downlink user-datagram dscp-marking 0x23 encsp-header
 copy-inner
 dscp-map qi5 3 arp-priority-level 12 uplink user-datagram dscp-marking 0x2f
 dscp-map qi5 3 arp-priority-level 12 downlink user-datagram dscp-marking 0x14 encsp-header
 copy-inner
 dscp-map qi5 6 downlink encsp-header copy-inner
 dscp-map qi5 7 downlink encsp-header dscp-marking 0x01
exit
```

DSCP Marking for Control Plane Signaling

Feature Description

The SMF supports marking of DSCP values to control packets as per the configuration at the interface.

Note The current implementation of DSCP marking supports only per interface and protocol 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 interface.

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)	—	101 - Critical
000 000	0	Best Effort	—	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
000 000	0	Default		
101 110	46	EF		

Limitations

The DSCP Marking feature has the following limitation:

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

Configuring DSCP Marking for Control Plane Signaling

This section describes how to configure the DSCP Marking feature for CP signaling messages.

Configuring the DSCP Marking feature involves the following steps:

- Configuring DSCP Marking per Endpoint, on page 6
- Configuring DSCP Marking per Interface, on page 6

Configuring DSCP Marking per Endpoint

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

```
config
   instance instance-id gr_instance_id
      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.

Configuring DSCP Marking per Interface

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

```
config
   instance instance-id gr_instance_id
      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.

Verifying DSCP Configuration for CP Signaling Messages

This section describes how to verify the DSCP Marking feature configuration for the CP signaling messages.

Use the **show running-config instance instance-id** *gr_instance_id* **endpoint** command to verify the DSCP configuration for control packets.

The following is an example output of the **show running-config instance instance-id 1 endpoint** command.

```
smf# show running-config instance instance-id 1 endpoint
instance instance-id 1
 endpoint sbi
  replicas 2
  nodes 1
  dscp 24
  vip-ip 209.165.200.230
  interface nrf
   loopbackPort 9050
   vip-ip 209.165.200.236 vip-port 8090
   dscp 24
  exit
 exit
exit
```

OAM Support for DSCP Marking

Monitoring Support

The SMF uses the **monitor protocol** and **monitor subscriber** commands to view the configured DSCP value.